

Title:	Document Version:
D3.1 WiseGRID architecture, data models, standards and data protection (V1)	1.0

Project Number:	Project Acronym:	Project Title:
H2020-731205	WiseGRID	Wide scale demonstration of Integrated Solutions for European SmartGrid

Contractual Delivery Date:	Actual Delivery Date:	Deliverable Type*-Security*:
M12 (Oct 2017)	M12 (Oct 2017)	R-PU

\*Type: P: Prototype; R: Report; D: Demonstrator; O: Other.

\*\*Security Class: PU: Public; PP: Restricted to other programme participants (including the Commission); RE: Restricted to a group defined by the consortium (including the Commission); CO: Confidential, only for members of the consortium (including the Commission).

Responsible:	Organisation:	Contributing WP:
Ioannis Vlachos	ICCS	WP3

#### Authors (organisation):

Antonis Papanikolaou (HYP), Sanduleac Mihai (CRE), Macarie Mihai (CRE), Mladin Mihai (CRE), Lacatus Paul (CRE), Chimirel Catalin Lucian (CRE), Irene Aguado Cortezon (ITE), Julio Cesar Diaz Cabrera (ITE), Ana María Arias (ETRA), Diego García-Casarrubios (ETRA), Álvaro Nofuentes (ETRA), Alberto Zambrano (ETRA), Giuseppa Caruso (ENG), Luca Bevilacqua (ENG), Massimo Magaldi (ENG), Benjamin Craft (VS), Alexandre Lapedra (BYES), Xavier Benavides (AMP), Jorge Sanjuán (AMP), Andreas Davros (ICCS), Ioannis Vlachos (ICCS)

#### Abstract:

This deliverable presents and in-depth analysis of the architecture of the various tools to be developed within the WiseGRID project, as well as the various use cases. Issues related to data models and standards and also to data privacy are presented in full detail in this deliverable.

#### Keywords:

SGAM framework, WiseGRID tools, data privacy, data protection, Use Case, data models, standards

## Revision History

Revision	Date	Description	Author (Organisation)
V0.1	01.06.2017	New document	Ioannis Vlachos (ICCS)
V0.2	20.09.2017	Peer review document preparation	Ioannis Vlachos (ICCS)
V0.3	01.10.2017	First review	Ana María Arias, Alberto Zambrano, Álvaro Nofuentes (ETRA)
V0.4	10.10.2017	Second review	Catalin Chimirel (CRE)
V1.0	30.10.2017	Final document	Ioannis Vlachos, Andreas Davros (ICCS)

# INDEX

## 1 Contents

<b>EXECUTIVE SUMMARY .....</b>	<b>32</b>
<b>1 INTRODUCTION .....</b>	<b>44</b>
1.1 Purpose of the Document.....	44
1.2 Scope of the Document .....	44
1.3 Structure of the Document .....	44
<b>2 WISEGRID ARCHITECTURE SPECIFICATION .....</b>	<b>46</b>
2.1 The Smart Grid Reference Architecture .....	46
2.2 The Smart Grid Architecture Model Framework .....	48
2.3 Model-Driven Architecture Specification using the SGAM Toolbox .....	51
2.4 The Smart Grid Architecture Concepts in WiseGRID .....	55
2.5 Relation of WiseGRID Modelling Concepts with other Projects .....	56
<b>3 SGAM GOALS AND OBJECTIVES .....</b>	<b>59</b>
3.1 SGAM Business Layer Overview .....	59
3.2 SGAM Business Actor Analysis.....	61
3.3 WiseGRID Actors .....	63
<b>4 GENERAL WISEGRID ARCHITECTURE SPECIFICATION .....</b>	<b>67</b>
4.1 WiseGRID Architecture Principles .....	67
4.2 WiseGRID SGAM Function Layer .....	69
4.3 WiseGRID SGAM Component Layer .....	70
4.4 WiseGRID SGAM Communication Layer .....	71
4.5 WiseGRID SGAM Information Layer .....	75
4.5.1 Integration technology .....	75
4.5.2 Data Models.....	76
4.5.3 Interfaces .....	76
4.6 SGAM Framework in the Context of WiseGRID.....	80
<b>5 WG INTEROPERABLE PLATFORM (IOP) .....</b>	<b>81</b>
5.1 WG Interoperable Platform SGAM Component Layer .....	82

5.2	WG Interoperable Platform SGAM Communication Layer.....	85
5.3	WG Interoperable Platform SGAM Information Layer.....	86
5.4	WG Interoperable Platform Privacy and Data Protection.....	87
<b>6</b>	<b>WG COCKPIT SGAM ARCHITECTURE SPECIFICATION.....</b>	<b>88</b>
6.1	WG Cockpit SGAM Component Layer.....	89
6.2	WG Cockpit SGAM Communication Layer .....	93
6.3	WG Cockpit SGAM Information Layer .....	95
6.4	WG Cockpit Privacy and Data Protection.....	100
<b>7</b>	<b>WISECOOP ARCHITECTURE SPECIFICATION .....</b>	<b>102</b>
7.1	WiseCOOP SGAM Component Layer .....	103
7.2	WiseCOOP SGAM Communication Layer .....	106
7.3	WiseCOOP SGAM Information Layer .....	107
7.4	WiseCOOP Privacy and Data Protection .....	109
<b>8</b>	<b>WG STaaS ARCHITECTURE SPECIFICATION.....</b>	<b>110</b>
8.1	WG STaaS SGAM Component Layer .....	110
8.2	WG STaaS SGAM Communication Layer .....	112
8.3	WG STaaS SGAM Information Layer .....	112
8.4	WG STaaS Privacy and Data Protection .....	115
<b>9</b>	<b>WISEEVP ARCHITECTURE SPECIFICATION .....</b>	<b>116</b>
9.1	WiseEVP SGAM Component Layer .....	117
9.2	WiseEVP SGAM Communication Layer .....	122
9.3	WiseEVP SGAM Information Layer .....	123
9.4	WiseEVP Privacy and Data Protection .....	125
<b>10</b>	<b>WG FASTV2G ARCHITECTURE SPECIFICATION .....</b>	<b>127</b>
10.1	WG FastV2G SGAM Component Layer.....	128
10.2	WG FastV2G SGAM Communication Layer .....	130
10.3	WG FastV2G SGAM Information Layer .....	131
10.4	WG FastV2G Privacy and Data Protection .....	132
<b>11</b>	<b>WISEHOME ARCHITECTURE SPECIFICATION .....</b>	<b>134</b>
11.1	WiseHOME SGAM Component Layer .....	135
11.2	WiseHOME SGAM Communication Layer .....	137
11.3	WiseHOME SGAM Information Layer .....	138



11.4 WiseHOME Privacy and Data Protection .....	141
<b>12 WISECORP ARCHITECTURE SPECIFICATION .....</b>	<b>142</b>
12.1 WiseCORP SGAM Component Layer.....	143
12.2 WiseCORP SGAM Communication Layer .....	147
12.3 WiseCORP SGAM Information Layer .....	148
12.4 WiseCORP Privacy and Data Protection.....	150
<b>13 WG RESCO ARCHITECTURE SPECIFICATION .....</b>	<b>151</b>
13.1 WG RESCO SGAM Component Layer .....	152
13.2 WG RESCO SGAM Communication Layer .....	154
13.3 WG RESCO SGAM Information Layer.....	155
13.4 WG RESCO Privacy and Data Protection .....	156
<b>14 PRIVACY AND DATA PROTECTION IN WISEGRID .....</b>	<b>158</b>
14.1 General considerations.....	158
14.1.1 THE SCOPE OF THE DATA PROTECTION IMPACT ASSESSMENT (DPIA).....	159
14.1.2 LEGAL BASIS FOR DPIA .....	160
14.1.3 THE POLICY OF PRIVACY AND DATA PROTECTION.....	161
14.2 IDENTIFICATION OF SENSITIVE DATA SOURCES FOR DSOS .....	168
14.3 IDENTIFICATION OF SENSITIVE DATA SOURCES FOR NON-DSOS.....	168
14.4 SURVEY OF PRIVACY AND DATA PROTECTION RISKS.....	168
14.4.1 PRE-ASSESSMENT AND CRITERIA DETERMINING THE NEED TO CONDUCT THE DPIA	170
14.4.2 INITIATION .....	175
14.4.3 THE RESOURCES .....	177
14.4.4 IDENTIFICATION, CHARACTERIZATION AND DESCRIPTION OF SMART GRID SYSTEMS / APPLICATIONS PROCESSING PERSONAL DATA.....	178
14.4.5 IDENTIFICATION OF RELEVANT RISKS AND EVENTS;.....	182
14.4.6 DATA PROTECTION RISK ASSESSMENT; .....	189
14.4.7 IDENTIFICATION AND RECOMMENDATION OF CONTROLS AND RESIDUAL RISKS;.....	217
14.4.8 DOCUMENTATION AND DRAFTING OF THE DPIA REPORT, REVIEWING AND MAINTENANCE .....	243
14.5 COLLECTION AND REVIEW OF NATIONAL REGULATIONS AND LEGISLATION (SURVEY) ...	244
14.5.1 SPECIFIC PRIVACY REQUIREMENTS IN BELGIUM .....	244
14.5.2 SPECIFIC PRIVACY REQUIREMENTS IN GREECE .....	245
14.5.3 SPECIFIC PRIVACY REQUIREMENTS IN ITALY .....	246
14.5.4 SPECIFIC PRIVACY REQUIREMENTS IN SPAIN .....	247

<b>15 STANDARDS AND INTEROPERABLE DATA MODELS.....</b>	<b>250</b>
15.1 GENERAL CONSIDERATIONS .....	250
15.2 WISEGRID PRODUCTS AND INTERFACES.....	250
15.2.1 WISEGRID SIMPLIFIED ARCHITECTURE .....	250
15.2.2 WISEGRID EXTERNAL ACTORS DESCRIPTION .....	251
15.2.3 WISEGRID PRODUCTS DESCRIPTION .....	252
15.2.4 WISEGRID INTERFACES.....	262
15.3 STANDARDS AND DATA MODELS STATE OF THE ART .....	269
15.3.1 AVAILABLE STANDARDS FOR WISEGRID .....	269
15.3.2 AVAILABLE DATA MODELS FOR WISEGRID .....	272
15.3.3 AVAILABLE NEW DATA MODELS BASED ON ONTOLOGIES FOR WISEGRID .....	274
<b>16 CONCLUSIONS AND NEXT STEPS .....</b>	<b>276</b>
<b>17 REFERENCES AND ACRONYMS .....</b>	<b>279</b>
17.1 References.....	279
17.2 Acronyms.....	284
<b>18 APPENDIX A - ARCHITECTURE HL-UC 1: DISTRIBUTED RES INTEGRATION IN THE GRID.....</b>	<b>287</b>
18.1 HL-UC 1_PUC_1: Network Monitoring.....	288
18.1.1 Primary Use Case description .....	288
18.1.2 Secondary Use Case description.....	288
18.1.3 SGAM Function Layer.....	290
18.1.4 SGAM Component Layer.....	292
18.1.5 SGAM Communication Layer .....	294
18.1.6 SGAM Information Layer .....	296
18.1.7 Activity diagram .....	298
18.1.8 Sequence diagram .....	299
18.2 HL-UC 1_PUC_2: Control strategies for reducing RES curtailment.....	300
18.2.1 Primary Use Case description .....	300
18.2.2 Secondary Use Case interactions.....	300
18.2.3 SGAM Function Layer.....	301
18.2.4 SGAM Component Layer.....	303
18.2.5 SGAM Communication Layer .....	304
18.2.6 SGAM Information Layer .....	305
18.2.7 activity diagram .....	307
18.2.8 Sequence diagram .....	308

<b>18.3 HL-UC 1_PUC_3: Voltage support and congestion management.....</b>	<b>309</b>
18.3.1 Primary Use Case description .....	309
18.3.2 Secondary Use Case interactions.....	309
18.3.3 SGAM Function Layer.....	311
18.3.4 SGAM Component Layer.....	311
18.3.5 SGAM Communication Layer .....	313
18.3.6 SGAM Information Layer .....	315
18.3.7 Activity diagram .....	319
18.3.8 Sequence diagram .....	320
<b>18.4 HL-UC 1_PUC_4: Grid planning analysis.....</b>	<b>321</b>
18.4.1 Primary Use Case description .....	321
18.4.2 Secondary Use Case interactions.....	321
18.4.3 SGAM Function Layer.....	322
18.4.4 SGAM Component Layer.....	323
18.4.5 SGAM Communication Layer .....	324
18.4.6 SGAM Information Layer .....	326
18.4.7 Activity diagram .....	328
18.4.8 Sequence diagram .....	329
<b>18.5 HL-UC 1_PUC_5: Promote RES via RESCO companies .....</b>	<b>330</b>
18.5.1 Primary Use Case description .....	330
18.5.2 Secondary Use Case interactions.....	331
18.5.3 SGAM Function Layer.....	335
18.5.4 SGAM Component Layer.....	336
18.5.5 SGAM Communication Layer .....	338
18.5.6 SGAM Information Layer .....	339
18.5.7 ctivity diagram .....	341
18.5.8 Sequence diagram .....	342
<b>19 APPENDIX B - ARCHITECTURE HL-UC 2: DECENTRALIZED GRID CONTROL AUTOMATION .....</b>	<b>343</b>
<b>19.1 HL-UC 2_PUC_1: Distribution network real-time monitoring.....</b>	<b>344</b>
19.1.1 Primary Use Case description .....	344
19.1.2 Secondary Use Case interactions.....	344
19.1.3 SGAM Function Layer.....	346
19.1.4 SGAM Component Layer.....	349
19.1.5 SGAM Communication Layer .....	352
19.1.6 SGAM Information Layer .....	354
19.1.7 Activity diagram .....	356

19.1.8 Sequence diagram .....	357
<b>19.2 HL-UC 2_PUC_2: Real-time distribution system awareness .....</b>	<b>358</b>
19.2.1 Primary Use Case description .....	358
19.2.2 Secondary Use Case interactions.....	359
19.2.3 SGAM Function Layer.....	360
19.2.4 SGAM Component Layer.....	362
19.2.5 SGAM Communication Layer .....	364
19.2.6 SGAM Information Layer .....	366
19.2.7 Activity diagram .....	368
19.2.8 Sequence diagram .....	369
<b>19.3 HL-UC 2_PUC_3: Grid control .....</b>	<b>370</b>
19.3.1 Primary Use Case description .....	370
19.3.2 Secondary Use Case interactions.....	371
19.3.3 SGAM Function Layer.....	372
19.3.4 SGAM Component Layer.....	375
19.3.5 SGAM Communication Layer .....	377
19.3.6 SGAM Information Layer .....	379
19.3.7 Activity diagram .....	381
19.3.8 Sequence diagram .....	382
<b>20 APPENDIX C - ARCHITECTURE HL-UC 3: E-MOBILITY INTEGRATION IN THE GRID WITH V2G .....</b>	<b>383</b>
<b>20.1 HL-UC 3_PUC_1: EVSE and EV fleet monitoring.....</b>	<b>384</b>
20.1.1 Primary Use Case description .....	384
20.1.2 Secondary Use Case interactions.....	384
20.1.3 SGAM Function Layer.....	385
20.1.4 SGAM Component Layer.....	386
20.1.5 SGAM Communication Layer .....	387
20.1.6 SGAM Information Layer .....	389
20.1.7 Activity diagram .....	391
20.1.8 Sequence diagram .....	392
<b>20.2 HL-UC 3_PUC_2: Interaction of the user with EVSE .....</b>	<b>392</b>
20.2.1 PRIMARY USE CASE DESCRIPTION .....	392
20.2.2 SECONDARY USE CASE INTERACTIONS .....	394
20.2.3 SGAM FUNCTION LAYER .....	395
20.2.4 SGAM COMPONENT LAYER.....	396
20.2.5 SGAM COMMUNICATION LAYER .....	398
20.2.6 SGAM INFORMATION LAYER .....	399

20.2.7	400
20.2.8 ACTIVITY DIAGRAM.....	401
20.2.9 SEQUENCE DIAGRAM.....	402
<b>20.3 HL-UC 3_PUC_3: EV charging management .....</b>	<b>403</b>
20.3.1 PRIMARY USE CASE DESCRIPTION .....	403
20.3.2 SECONDARY USE CASE INTERACTIONS .....	404
20.3.3 SGAM FUNCTION LAYER .....	406
20.3.4 SGAM COMPONENT LAYER.....	407
20.3.5 SGAM COMMUNICATION LAYER .....	408
20.3.6 SGAM INFORMATION LAYER .....	409
20.3.7 ACTIVITY DIAGRAM.....	411
20.3.8 SEQUENCE DIAGRAM.....	412
<b>20.4 HL-UC 3_PUC_4: Interaction with the energy infrastructure .....</b>	<b>413</b>
20.4.1 PRIMARY USE CASE DESCRIPTION .....	413
20.4.2 SECONDARY USE CASE INTERACTIONS .....	414
20.4.3 SGAM FUNCTION LAYER .....	416
20.4.4 SGAM COMPONENT LAYER.....	417
20.4.5 SGAM COMMUNICATION LAYER .....	419
20.4.6 SGAM INFORMATION LAYER .....	421
20.4.7 SEQUENCE DIAGRAM.....	423
<b>21 APPENDIX D - ARCHITECTURE HL-UC 4: BATTERY STORAGE INTEGRATION AT SUBSTATION AND PROSUMER LEVEL .....</b>	<b>424</b>
<b>21.1 HL-UC 4_PUC_1: Batteries management at prosumer level.....</b>	<b>425</b>
21.1.1 Primary Use Case description .....	425
21.1.2 Secondary Use Case interactions.....	426
21.1.3 SGAM Function Layer.....	427
21.1.4 SGAM Component Layer.....	428
21.1.5 SGAM Communication Layer .....	430
21.1.6 SGAM Information Layer .....	432
21.1.7 Activity diagram .....	434
21.1.8 Sequence diagram .....	435
<b>21.2 HL-CU 4_PUC_2: Batteries management at aggregator level.....</b>	<b>436</b>
21.2.1 PRIMARY USE CASE DESCRIPTION .....	436
21.2.2 SECONDARY USE CASE INTERACTIONS .....	436
21.2.3 SGAM FUNCTION LAYER .....	439
21.2.4 SGAM COMPONENT LAYER.....	441
21.2.5 SGAM COMMUNICATION LAYER .....	442

21.2.6 SGAM INFORMATION LAYER .....	443
21.2.7 ACTIVITY DIAGRAM.....	445
21.2.8 SEQUENCE DIAGRAM.....	446
<b>21.3 HL-UC 4_PUC_3: Ancillary services .....</b>	<b>447</b>
21.3.1 PRIMARY USE CASE DESCRIPTION .....	447
21.3.2 SECONDARY USE CASE INTERACTIONS .....	448
21.3.3 SGAM FUNCTION LAYER .....	449
21.3.4 SGAM COMPONENT LAYER.....	450
21.3.5 SGAM COMMUNICATION LAYER .....	451
21.3.6 SGAM INFORMATION LAYER .....	453
21.3.7 ACTIVITY DIAGRAM.....	455
21.3.8 SEQUENCE DIAGRAM.....	456
<b>21.4 HL-UC 4_PUC_4: Combination of battery storage systems .....</b>	<b>457</b>
21.4.1 Primary Use Case description .....	457
21.4.2 Secondary Use Case interactions.....	457
21.4.3 SGAM Function Layer.....	459
21.4.4 SGAM Component Layer.....	459
21.4.5 SGAM Communication Layer .....	461
21.4.6 SGAM Information Layer .....	462
21.4.7 Activity diagram .....	464
21.4.8 Sequence diagram .....	465
<b>22 APPENDIX E - ARCHITECTURE HL-UC 5: COGENERATION INTEGRATION IN PUBLIC BUILDINGS/HOUSING .....</b>	<b>466</b>
<b>22.1 HL-UC 5_PUC_1: Thermal monitoring.....</b>	<b>467</b>
1.1.1 Primary Use Case description .....	467
22.1.1 Secondary Use Case interactions.....	467
22.1.2 SGAM Function Layer.....	468
22.1.3 SGAM Component Layer.....	470
22.1.4 SGAM Communication Layer .....	471
22.1.5 SGAM Information Layer .....	472
22.1.6 Activity diagram .....	474
22.1.7 Sequence diagram .....	475
<b>22.2 HL-UC 5_PUC_2: Cogeneration and HVAC management .....</b>	<b>476</b>
22.2.1 Primary Use Case description .....	476
22.2.2 Secondary Use Case Interactions.....	476
22.2.3 SGAM Function Layer.....	478
22.2.4 SGAM Component Layer.....	478

22.2.5 SGAM Communication Layer .....	480
22.2.6 SGAM Information Layer .....	482
22.2.7 Activity diagram .....	487
22.2.1 Sequence diagram .....	488
<b>22.3 HL-UC 5_PUC 3: Comfort-based demand flexibility models .....</b>	<b>490</b>
22.3.1 Primary Use Case description .....	490
22.3.2 Secondary Use Case Interactions.....	491
22.3.3 SGAM Function Layer.....	492
22.3.4 SGAM Component Layer.....	493
22.3.5 SGAM Communication Layer .....	494
22.3.6 SGAM Information Layer .....	496
22.3.7 Activity diagram .....	499
22.3.8 Sequence diagram .....	500
<b>22.4 HL-UC 5_PUC_4: Cogeneration and HVAC optimisation .....</b>	<b>501</b>
22.4.1 Primary Use Case description .....	501
22.4.2 Secondary Use Case Interactions.....	502
22.4.3 SGAM Function Layer.....	503
22.4.4 SGAM Component Layer.....	504
22.4.5 SGAM Communication Layer .....	506
22.4.6 SGAM Information Layer .....	508
22.4.7 Activity diagram .....	513
22.4.8 Sequence diagram .....	514
<b>23 APPENDIX F - ARCHITECTURE HL-UC 6: VPP TECHNICAL AND ECONOMIC FEASIBILITY .....</b>	<b>515</b>
<b>23.1 HL-UC 6_PUC_1: VPP Monitoring and Management .....</b>	<b>516</b>
23.1.1 Primary Use Case description .....	516
23.1.2 Secondary Use Case interactions.....	516
23.1.3 SGAM Function Layer.....	520
23.1.4 SGAM Component Layer.....	522
23.1.5 SGAM COMMUNICATION Layer .....	523
23.1.6 SGAM Information Layer .....	525
23.1.7 Activity diagram .....	526
23.1.8 Sequence diagram .....	527
<b>23.2 HL-UC 6_PUC_2: VPP Market Participation.....</b>	<b>528</b>
23.2.1 Primary Use Case description .....	528
23.2.2 Secondary Use Case interactions.....	528
23.2.3 SGAM Function Layer.....	530

23.2.4 SGAM Component Layer.....	531
23.2.5 SGAM Communication Layer .....	532
23.2.6 SGAM Information Layer .....	532
23.2.7 Activity diagram .....	534
23.2.8 Sequence diagram .....	535
<b>23.3 HL-UC 6_PUC_3: VPP Real Time Control .....</b>	<b>536</b>
23.3.1 PRIMARY USE CASE DESCRIPTION .....	536
23.3.2 SECONDARY USE CASE INTERACTIONS .....	536
23.3.3 SGAM FUNCTION LAYER .....	538
23.3.4 SGAM COMPONENT LAYER.....	539
23.3.5 SGAM COMMUNICATION LAYER .....	540
23.3.6 SGAM INFORMATION LAYER .....	541
23.3.7 ACTIVITY DIAGRAM.....	543
23.3.8 SEQUENCE DIAGRAM.....	544
<b>23.4 HL-UC 6_PUC_4: VPP users relationship management .....</b>	<b>545</b>
23.4.1 PRIMARY USE CASE DESCRIPTION .....	545
23.4.2 SECONDARY USE CASE INTERACTIONS .....	545
23.4.3 SGAM FUNCTION LAYER .....	547
23.4.4 SGAM COMPONENT LAYER.....	548
23.4.5 SGAM COMMUNICATION LAYER .....	549
23.4.6 SGAM INFORMATION LAYER .....	550
23.4.7 ACTIVITY DIAGRAM.....	551
23.4.8 SEQUENCE DIAGRAM.....	552
<b>24 APPENDIX G - ARCHITECTURE HL-UC 7: CITIZENS EMPOWERMENT IN ENERGY MARKET AND REDUCTION OF ENERGY POVERTY .....</b>	<b>553</b>
<b>24.1 HL-UC 7_PUC_1: Dynamic management of demand side assets in tertiary sector .....</b>	<b>554</b>
24.1.1 Primary Use Case description .....	554
24.1.2 Secondary Use Case interactions.....	555
24.1.3 SGAM Function Layer.....	556
24.1.4 SGAM Component Layer.....	558
24.1.5 SGAM Communication Layer .....	560
24.1.6 SGAM Information Layer .....	562
24.1.7 Activity diagram .....	565
24.1.8 Sequence diagram .....	566
<b>24.2 HL-UC 7_PUC_2: dynamic aggregation of demand side assets and active participation into energy market.....</b>	<b>567</b>
24.2.1 Primary Use Case description .....	567



24.2.2 Secondary Use Case interactions.....	567
24.2.3 SGAM Function Layer.....	569
24.2.4 SGAM Component Layer.....	570
24.2.5 SGAM Communication Layer .....	573
24.2.6 SGAM Information Layer .....	575
24.2.7 Activity diagram .....	577
24.2.8 Sequence diagram .....	578
<b>24.3 HL-UC 7_PUC_3: Customers Engagement for Active Market Participation .....</b>	<b>579</b>
24.3.1 Primary Use Case description .....	579
24.3.2 Secondary Use Case interactions.....	580
24.3.3 SGAM Function Layer.....	582
24.3.4 SGAM Component Layer.....	584
24.3.5 SGAM Communication Layer .....	586
24.3.6 SGAM Information Layer .....	588
24.3.7 Activity diagram .....	591
24.3.8 Sequence diagram .....	592
<b>25 APPENDIX H - PRIVACY &amp; DATA PROTECTION LIST OF POSSIBLE CONTROLS .....</b>	<b>593</b>
25.1 Possible Controls.....	594
<b>26 APPENDIX I - ARCHITECTURE DEFINITIONS.....</b>	<b>598</b>
26.1 List Of Definitions.....	599
<b>27 APPENDIX J - STANDARDS AND INTEROPERABLE DATA MODELS STANDARDS .....</b>	<b>601</b>
27.1 List of Standards .....	602
<b>28 APPENDIX K - ARCHITECTURE COMMUNICATION INTERFACES .....</b>	<b>617</b>
28.1 Obtained input during Kythnos workshop.....	618
28.2 WG STaaS/VPP.....	618
28.3 WISECORP .....	619
28.4 WISECOOP .....	620
28.5 WG FastV2G.....	620
28.6 WISEEVP .....	621
28.7 WISEHOME .....	622
28.8 WG RESCO .....	622
28.9 WG COCKPIT .....	623

<b>29 APPENDIX L - PRIVACY AND DATA PROTECTION QUESTIONS RELATED TO THE WISEGRID COMPONENTS .....</b>	<b>624</b>
<b>29.1 Questionnaire References .....</b>	<b>639</b>
<b>29.2 Extras .....</b>	<b>640</b>
 <b>30 APPENDIX M - PRIVACY &amp; DATA PROTECTION - DATA SOURCES FOR DSO .....</b>	<b>642</b>
 <b>31 APPENDIX N - PRIVACY &amp; DATA PROTECTION - DATA SOURCES FOR NON-DSO.....</b>	<b>644</b>



## LIST OF FIGURES

Figure 1 - EU extension of the NIST Model.....	47
Figure 2 - European Conceptual Model for the Smart Grid (1) .....	48
Figure 3 - Interoperability Categories and Cross Cutting Issues (1).....	49
Figure 4 - Interoperability Categories and layers (1) .....	49
Figure 5 - The SGAM Framework (1).....	50
Figure 6 - The SGAM Toolbox Architecture .....	52
Figure 7 - The SGAM Metamodel (2) .....	53
Figure 8 - SGAM Development Process (2).....	54
Figure 9 - TOGAF ADM Model (1) .....	57
Figure 10 - Archimate representation of the architectural viewpoints and Mapping of GWAC dimensions onto Archimate (1) .....	58
Figure 11 - Business Layer «Control reactive power of DER unit» (1) .....	59
Figure 12 - Relation Meta-Model to SGAM (1) .....	60
Figure 13 - Alignment process between market model developments and ICT architecture (1) .....	61
Figure 14 - Flexibility Concept (result of WGSP) (1).....	68
Figure 15 - Meta-model for the European conceptual model for Smart Grids (1).....	68
Figure 16 - Evolution of centralized/decentralized power systems deployments (1).....	69
Figure 17 - Functional Architecture meta-model (1) .....	69
Figure 18 - SGAM Function Layer (example) (2) .....	70
Figure 19 : Actor Mapping Model (example) (1) .....	71
Figure 20 - SGAM Component Layer (example) (2) .....	71
Figure 21 - Mapping of communication networks on SGAM Communication Layer (1).....	74
Figure 22 - Applicability statement of the communication technologies to the smart grid sub-networks (1).....	74
Figure 23 - SGAM Communication Layer (Example) (2) .....	75
Figure 24 - Concept of logical interfaces in the context of domains and zones (1) .....	77
Figure 25 - Business Context View (example) (2) .....	78
Figure 26 - Standard and Information Object Mapping (example) (2) .....	79
Figure 27 - Canonical Data Model View (example) (2) .....	79
Figure 28: WiseGRID UCs and tools analysis and design process.....	80
Figure 29 - WG IOP structure.....	81
Figure 30 - SGAM Component Layer of WG IOP.....	83
Figure 31 - SGAM Communication Layer of WG IOP .....	85
Figure 32 - SGAM Information Layer of WG IOP .....	86
Figure 33 - WiseGRID Cockpit .....	88
Figure 34 - WG Cockpit SGAM Component Layer.....	90

Figure 35 - WG Cockpit SGAM Communication Layer .....	94
Figure 36 - WG Cockpit SGAM Information Layer .....	96
Figure 37 - Offline Processes diagram .....	97
Figure 38 - Information retrieval diagram .....	98
Figure 39 - Problem detection diagram .....	99
Figure 40 - WiseCOOP .....	102
Figure 41 - WiseCOOP SGAM Component layer .....	104
Figure 42 - WiseCOOP SGAM Communication layer .....	106
Figure 43 - WiseCOOP SGAM Information layer .....	107
Figure 44 - Important elements and exchanged data items .....	108
Figure 45 - WG StaaS Component Layer .....	111
Figure 46 - WG StaaS Communication Layer .....	112
Figure 47 - WG StaaS Information Layer .....	113
Figure 48 - Items and related data models .....	113
Figure 49 - Important elements and exchanged data items .....	114
Figure 50 - WiseEVP .....	116
Figure 51 - WiseEVP SGAM Component layer .....	119
Figure 52 - WiseEVP SGAM Communication layer .....	122
Figure 53 - WiseEVP SGAM Information layer .....	123
Figure 54 - Important elements and exchanged data items .....	124
Figure 55 - WiseFASTV2G .....	127
Figure 56 - SGAM Component Layer of WG FastV2G .....	129
Figure 57 - SGAM Communication Layer of WG FastV2G .....	130
Figure 58 - SGAM Information Layer of WG FastV2G .....	131
Figure 59 - Information flow for the WG FastV2G tool .....	132
Figure 60 - SGAM Component Layer of WiseHOME .....	136
Figure 61 - SGAM Communication Layer of WiseHOME .....	138
Figure 62 - SGAM Information Layer of WiseHOME .....	139
Figure 63 - Information flow diagram for WiseHOME .....	140
Figure 64 - WiseCORP .....	142
Figure 65 - SGAM Component Layer for WiseCORP .....	144
Figure 66 - SGAM Communication Layer of WiseCORP .....	147
Figure 67 - SGAM Information Layer for WiseCORP .....	148
Figure 68 - Information flows for WiseCORP .....	149
Figure 69 - WG RESCO .....	151
Figure 70 - SGAM Component Layer for WG RESCO .....	153
Figure 71 - SGAM Communication Layer of WG RESCO .....	154

Figure 72 - SGAM Information Layer of WG RESCO .....	155
Figure 73 - WG RESCO component process diagram .....	156
Figure 74 - DPIA iterative cycle .....	170
Figure 75 - Architecture for DPIA.....	178
Figure 76 – HL-UCs mapping to project objectives and WiseGRID tools.....	179
Figure 77 – Threats/Events identification process .....	194
Figure 78 - Risk map for WG IOP .....	197
Figure 79 - Risk map for WG Cockpit .....	200
Figure 80 - Risk map for WiseCOOP.....	202
Figure 81 - Risk map for WG STaaS.....	204
Figure 82 - Risk map for WiseEVP.....	206
Figure 83 - Risk map for WG FastV2G.....	209
Figure 84 - Risk map for WiseCORP .....	211
Figure 85 - Risk map for WiseHOME.....	214
Figure 86 - Risk map for WG RESCO .....	216
Figure 87 – Risk level identification diagram.....	217
Figure 88 - Risk map for WG IOP with implemented/planned controls.....	222
Figure 89 - Risk map for WG Cockpit with implemented/planned controls.....	224
Figure 90 - Risk map for WG COOP with implemented/planned controls .....	226
Figure 91 - Risk map for WG STaaS with implemented/planned controls .....	228
Figure 92 - Risk map for WiseEVP with implemented/planned controls .....	230
Figure 93 - Risk map for WG FastV2G with implemented/planned controls .....	233
Figure 94 - Risk map for WiseCORP with implemented/planned controls.....	235
Figure 95 - Risk map for WiseHOME with implemented/planned controls .....	238
Figure 96 - Risk map for WG RESCO with implemented/planned controls .....	241
Figure 97 – WiseGRID simplified architecture schema.....	250
Figure 98 - Smart Grids Standards Map (75). .....	253
Figure 99 - Standards map for WG IOP.....	254
Figure 100 - Standards map for WG Cockpit. ....	255
Figure 101 – Standards map for WiseCORP.....	256
Figure 102 - Standards map for WiseCOOP.....	257
Figure 103 - Standards map for WiseHOME.....	258
Figure 104 - Standards map for WiseEVP. ....	259
Figure 105 - Standards map for WG FastV2G.....	260
Figure 106 - Standards map for WG STaaS/VPP. ....	261
Figure 107 - Standards map for WG RESCO.....	262
Figure 108 - Communication interfaces of WG IOP.....	263

Figure 109 - Communication interfaces of WG Cockpit. ....	263
Figure 110 - Communication interfaces of WiseCORP. ....	264
Figure 111 - Communication interfaces of WiseCOOP. ....	265
Figure 112 - Communication interfaces of WiseHOME. ....	266
Figure 113 - Communication interfaces of WiseEVP. ....	266
Figure 114 - Communication interfaces of WG STaaS/VPP. ....	267
Figure 115 - Communication interfaces of WG STaaS/VPP. ....	268
Figure 116 - Communication interfaces of WG RESCO. ....	268
Figure 117 - Relationship among applied standards in Smart Grids. ....	273
Figure 118 - OpenADR communication architecture schema (76). ....	275
Figure 119 - SUCs Interactions Diagram ....	288
Figure 120 - SGAM Function Layer ....	290
Figure 121 - SGAM Component Layer ....	292
Figure 122 - SGAM Communication Layer ....	294
Figure 123 - SGAM Information Layer ....	296
Figure 124 - Primary Use Case Activity Diagram. ....	298
Figure 125 - Primary Use Case Sequence Diagram. ....	299
Figure 126 - SUCs Interactions Diagram ....	300
Figure 127 - SGAM Function Layer ....	301
Figure 128 - SGAM Component Layer ....	303
Figure 129 - SGAM Communication Layer. ....	304
Figure 130 - SGAM Information Layer ....	305
Figure 131 - Primary Use Case Activity Diagram. ....	307
Figure 132 - Primary Use Case Sequence Diagram. ....	308
Figure 133 - SUCs Interactions Diagram ....	309
Figure 134 - SGAM Function Layer ....	311
Figure 135 - SGAM Component Layer ....	312
Figure 136 - SGAM Communication Layer. ....	313
Figure 137 - SGAM Information Layer ....	315
Figure 138 - Canonical Data Model diagram ....	316
Figure 139 - Standard and information object mapping diagram ....	317
Figure 140 - Primary Use Case Activity Diagram. ....	319
Figure 141 - Primary Use Case Sequence Diagram. ....	320
Figure 142 - SUCs Interactions Diagram ....	321
Figure 143 - SGAM Function Layer ....	322
Figure 144 - SGAM Component Layer ....	323
Figure 145 - SGAM Communication Layer. ....	324

Figure 146 - SGAM Information Layer .....	326
Figure 147 - Primary Use Case Activity Diagram.....	328
Figure 148 - Primary Use Case Sequence Diagram .....	329
Figure 149 - SUCs Interactions Diagram .....	331
Figure 150 - SGAM Function Layer .....	335
Figure 151 - SGAM Component Layer .....	336
Figure 152 - SGAM Communication Layer .....	338
Figure 153 - SGAM Information Layer .....	339
Figure 154 - Primary Use Case Activity Diagram.....	341
Figure 155 - Primary Use Case Sequence Diagram .....	342
Figure 156 - SUCs Interactions Diagram .....	345
Figure 157 - SGAM Function Layer .....	347
Figure 158 - SGAM Component Layer .....	350
Figure 159 - SGAM Communication Layer .....	352
Figure 160 - SGAM Information Layer .....	354
Figure 161 - Primary Use Case Activity Diagram.....	356
Figure 162 - Primary Use Case Sequence Diagram.....	357
Figure 163 - SUCs Interactions Diagram .....	359
Figure 164 - SGAM Function Layer .....	360
Figure 165 - SGAM Component Layer .....	362
Figure 166 - SGAM Communication Layer.....	364
Figure 167 - SGAM Information Layer .....	366
Figure 168 - Primary Use Case Activity Diagram.....	368
Figure 169 - Primary Use Case Sequence Diagram.....	369
Figure 170 - SUCs Interactions Diagram .....	371
Figure 171 - SGAM Function Layer .....	373
Figure 172 - SGAM Component Layer .....	375
Figure 173 - SGAM Communication Layer.....	377
Figure 174 - SGAM Information Layer .....	379
Figure 175 - Primary Use Case Activity Diagram.....	381
Figure 176 - Primary Use Case Sequence Diagram.....	382
Figure 177 - SUCs Interactions Diagram .....	384
Figure 178 - SGAM Function Layer .....	385
Figure 179 - SGAM Component Layer .....	386
Figure 180 - SGAM Communication Layer.....	388
Figure 181 - SGAM Information Layer .....	389
Figure 182 - Primary Use Case Activity Diagram.....	391



Figure 183 - Primary Use Case Sequence Diagram .....	392
Figure 184 - SUCs Interactions Diagram .....	394
Figure 185 - SGAM Function Layer .....	395
Figure 186 - SGAM Component Layer .....	396
Figure 187 - SGAM Communication Layer .....	398
Figure 188 - SGAM Information Layer .....	399
Figure 189 - Primary Use Case Activity Diagram.....	401
Figure 190 - Primary Use Case Sequence Diagram .....	402
Figure 191 - SUCs Interactions Diagram .....	404
Figure 192 - SGAM Function Layer .....	406
Figure 193 - SGAM Component Layer .....	407
Figure 194 - SGAM Communication Layer.....	408
Figure 195 - SGAM Information Layer .....	409
Figure 196 - Primary Use Case Activity Diagram.....	411
Figure 197 - Primary Use Case Sequence Diagram.....	412
Figure 198 - SUCs Interactions Diagram .....	414
Figure 199 - SGAM Function Layer .....	416
Figure 200 - SGAM Component Layer .....	417
Figure 201 - SGAM Communication Layer .....	419
Figure 202 - SGAM Information Layer .....	421
Figure 204 - Primary Use Case Sequence Diagram.....	423
Figure 205 - SUCs Interactions Diagram .....	426
Figure 206 - SGAM Function Layer .....	427
Figure 207 - SGAM Component Layer .....	428
Figure 208 - SGAM Communication Layer.....	430
Figure 209 - SGAM Information Layer .....	432
Figure 210 - Primary Use Case Activity Diagram.....	434
Figure 211 - Primary Use Case Sequence Diagram.....	435
Figure 212 - SUCs Interactions Diagram .....	437
Figure 213 - SGAM Function Layer .....	439
Figure 214 - SGAM Component Layer .....	441
Figure 215 - SGAM Communication Layer.....	442
Figure 216 - SGAM Information Layer .....	443
Figure 217 - Primary Use Case Activity Diagram.....	445
Figure 218 - Primary Use Case Sequence Diagram .....	446
Figure 219 - SUCs Interactions Diagram .....	448
Figure 220 - SGAM Function Layer .....	449



Figure 221 - SGAM Component Layer .....	450
Figure 222 - SGAM Communication Layer .....	451
Figure 223 - SGAM Information Layer .....	453
Figure 224 - Primary Use Case Activity Diagram.....	455
Figure 225 - Primary Use Case Sequence Diagram .....	456
Figure 226 - SUCs Interactions Diagram .....	468
Figure 227 - SGAM Function Layer .....	469
Figure 228 - SGAM Component Layer .....	470
Figure 229 - SGAM Communication Layer .....	471
Figure 230 - SGAM Information Layer .....	472
Figure 231 - Standard and Information Object Mapping diagram .....	473
Figure 232 - Primary Use Case Activity Diagram.....	474
Figure 233: Basic path sequence diagram for HL-UC 5 PUC 1 .....	475
Figure 234: Exception path sequence diagram for HL-UC 5 PUC 1 .....	475
Figure 235 - SUCs Interactions Diagram .....	476
Figure 236 - SGAM Function Layer .....	478
Figure 237 - SGAM Component Layer .....	479
Figure 238 - SGAM Communication Layer .....	480
Figure 239 - SGAM Information Layer .....	482
Figure 240 - Canonical Data Model diagram .....	483
Figure 241 - Standard and Information Object Mapping diagram .....	485
Figure 242 - Primary Use Case Activity Diagram.....	487
Figure 243: Basic path sequence diagram for HL-UC 5 PUC 2 .....	488
Figure 244 - Forecasting error exception path sequence diagram for HL-UC 5 PUC 2.....	489
Figure 245 - Dangerous setpoint exception path sequence diagram for HL-UC 5 PUC 2.....	489
Figure 246 - SUCs Interactions Diagram .....	491
Figure 247 - SGAM Function Layer .....	492
Figure 248 - SGAM Component Layer .....	494
Figure 249 - SGAM Communication Layer .....	494
Figure 250 - SGAM Information Layer .....	496
Figure 251 - Canonical Data Model diagram .....	497
Figure 252 - Standard and Information Object Mapping diagram .....	498
Figure 253 - Primary Use Case Activity Diagram.....	499
Figure 254 - Basic path sequence diagram for HL-UC 5 PUC 3 .....	500
Figure 255 - SUCs Interactions Diagram .....	502
Figure 256 - SGAM Function Layer .....	503
Figure 257 - SGAM Component Layer .....	505

Figure 258 - SGAM Communication Layer .....	506
Figure 259 - SGAM Information Layer .....	508
Figure 260 - Canonical Data Model diagram .....	509
Figure 261 - Standard and Information Object Mapping diagram .....	511
Figure 262 - Primary Use Case Activity Diagram.....	513
Figure 263 - Basic path sequence diagram for HL-UC 5 PUC 4 .....	514
Figure 264 - SUCs Interactions Diagram .....	516
Figure 265 - SGAM Function Layer .....	520
Figure 266 - SGAM Component Layer .....	522
Figure 267 - SGAM Communication Layer.....	523
Figure 268 - SGAM Information Layer .....	525
Figure 269 - Primary Use Case Activity Diagram.....	526
Figure 270 - Primary Use Case Activity Diagram.....	527
Figure 271 - SUCs Interactions Diagram .....	528
Figure 272 - SGAM Function Layer .....	530
Figure 273 - SGAM Component Layer .....	531
Figure 274 - SGAM Communication Layer.....	532
Figure 275 - SGAM Information Layer .....	533
Figure 276 - Primary Use Case Activity Diagram.....	534
Figure 277 - Primary Use Case Sequence Diagram.....	535
Figure 278 - SUCs Interactions Diagram .....	536
Figure 279 - SGAM Function Layer .....	538
Figure 280 - SGAM Component Layer .....	539
Figure 281 - SGAM Communication Layer.....	540
Figure 282 - SGAM Information Layer .....	541
Figure 283 - Primary Use Case Activity Diagram.....	543
Figure 284 - Primary Use Case Sequence Diagram.....	544
Figure 285 - SUCs Interactions Diagram .....	545
Figure 286 - SGAM Function Layer .....	547
Figure 287 - SGAM Component Layer .....	548
Figure 288 - SGAM Communication Layer.....	549
Figure 289 - SGAM Information Layer .....	550
Figure 290 - Primary Use Case Activity Diagram.....	551
Figure 291 - Primary Use Case Sequence Diagram.....	552
Figure 292 - SUCs Interactions Diagram .....	555
Figure 293 - SGAM Function Layer .....	556
Figure 294 - SGAM Component Layer .....	558

Figure 295 - SGAM Communication Layer .....	560
Figure 296 - SGAM Information Layer .....	562
Figure 297 - Primary Use Case Activity Diagram.....	565
Figure 298 - Primary Use Case Sequence Diagram .....	566
Figure 299 - SUCs Interactions Diagram .....	567
Figure 300 - SGAM Function Layer .....	569
Figure 301 - SGAM Component Layer .....	571
Figure 302 - SGAM Communication Layer .....	573
Figure 303 - SGAM Information Layer .....	575
Figure 304 - Primary Use Case Activity Diagram.....	577
Figure 305 - Primary Use Case Sequence Diagram .....	578
Figure 306 - SUCs Interactions Diagram .....	580
Figure 307 - SGAM Function Layer .....	582
Figure 308 - SGAM Component Layer .....	584
Figure 309 - SGAM Communication Layer .....	586
Figure 310 - SGAM Information Layer .....	588
Figure 311 - Primary Use Case Activity Diagram.....	591
Figure 312 - Primary Use Case Sequence Diagram .....	592

## LIST OF TABLES

Table 1 - WiseGRID Actors .....	63
Table 2 - Mapping of sub-network technologies .....	72
Table 3 - Modules of message brokering component of WG IOP .....	84
Table 4 - Data item - model matching .....	86
Table 5 - Threat and feared events identification for WG IOP .....	87
Table 6 - Modules composing the WG Cockpit.....	90
Table 7 - Data item Description .....	97
Table 8 - Data item description .....	98
Table 9 - Data item description .....	99
Table 10 - Items and related data models .....	100
Table 11 - Threat and feared events identification for WiseGRID Cockpit.....	100
Table 12 - WiseCOOP modules .....	104
Table 13 - Data item description .....	108
Table 14 - Items and related data models .....	109
Table 15 - Threat and feared events identification for WiseCOOP .....	109
Table 16 - WG StaaS Components .....	111
Table 17 - Threat and feared events identification for WiseGRID STaaS .....	115
Table 18 - WiseEVP modules .....	120
Table 19 - Data item description .....	124
Table 20 - Items and related data models .....	125
Table 21 - Threat and feared events identification for WiseEVP.....	125
Table 22 - WG FastV2G modules .....	129
Table 23 - Data item description .....	132
Table 24 - Items and related data models .....	132
Table 25 - Threat and feared events identification for WiseGRID FastV2G .....	133
Table 26 - Data item description .....	140
Table 27 - Items and related data models .....	141
Table 28 - Threat and feared events identification for WG HOME .....	141
Table 29 - WiseCORP modules.....	145
Table 30 - Data item description .....	149
Table 31 - Items and related data models .....	150
Table 32 - Threat and feared events identification for WiseCORP .....	150
Table 33 - WG RESCO modules .....	153
Table 34 - Items and related data models .....	156
Table 35 - Threat and feared events identification for WG RESCO .....	156
Table 36 – WISEGRID Tools and Pilot sites .....	159

Table 37 – Data Sources for DSOs.....	168
Table 38 – Data Sources for non-DSOs .....	168
Table 39 – DPIA team.....	175
Table 40 – DPIA resources .....	176
Table 41 – Correlation between WG tools and HLUCs .....	178
Table 42 - Generic threats that may jeopardize confidentiality .....	183
Table 43 - Generic threats that may jeopardize integrity.....	184
Table 44 - Generic threats that may jeopardize availability.....	187
Table 45 - Generic threats that may jeopardize personal data .....	188
Table 46 – Description of privacy targets .....	190
Table 47 – Determination of Severity/Impact level.....	192
Table 48 – Determination of Likelihood level.....	193
Table 49 – Risk evaluation for WiseGRID IOP .....	195
Table 50 – Risk evaluation for WG Cockpit.....	198
Table 51 – Risk evaluation for WiseCOOP .....	201
Table 52 – Risk evaluation for WG STaaS .....	203
Table 53 – Risk evaluation for WiseEVP.....	205
Table 54 – Risk evaluation for WG V2G .....	207
Table 55– Risk evaluation for WiseCORP .....	210
Table 56 – Risk evaluation for WiseHOME .....	212
Table 57 – Risk evaluation for WG RESCO .....	215
Table 58 – Risk treatment and residual risk for WG IOP .....	220
Table 59 – Risk treatment and residual risk for WG Cockpit .....	223
Table 60 – Risk treatment and residual risk for WiseCOOP.....	225
Table 61 – Risk treatment and residual risk for WG STaaS.....	227
Table 62 – Risk treatment and residual risk for WiseEVP.....	229
Table 63 – Risk treatment and residual risk for WG FastV2G.....	231
Table 64 – Risk treatment and residual risk for WiseCORP .....	234
Table 65 – Risk treatment and residual risk for WiseHOME .....	236
Table 66 – Risk treatment and residual risk for WG RESCO .....	239
Table 67 – Smart Grid fields associated to WG IOP.....	269
Table 68 -Smart Grid fields associated to WG Cockpit. ....	269
Table 69 -Smart Grid fields associated to Wise CORP. ....	270
Table 70 -Smart Grid fields associated to Wise COOP.....	270
Table 71 -Smart Grid fields associated to Wise HOME.....	270
Table 72–Smart Grid fields associated to Wise EVP. ....	270
Table 73–Smart Grid fields associated to WG FastV2G.....	270

Table 74 - Smart Grid fields associated to WG STaaS/VPP.....	272
Table 75 - Smart Grid fields associated to WG RESCO. ....	272
Table 76 - List of Acronyms.....	284
Table 77 - Table of list of participating SUCs .....	289
Table 78 - List of Actors Involved.....	291
Table 79 - List of Components Participating in the Primary Use Case.....	293
Table 80 - List of Communication Technologies Involved .....	294
Table 81 - List of Data Models .....	296
Table 82 - List of Data Standards .....	297
Table 83 - List of Information Objects .....	297
Table 84 - Table of list of participating SUCs .....	300
Table 85 - List of Actors Involved.....	302
Table 86 - List of Components Participating in the Primary Use Case.....	303
Table 87 - List of Communication Technologies Involved .....	304
Table 88 - List of Data Models .....	306
Table 89 - List of Data Standards .....	306
Table 90 - List of Information Objects .....	306
Table 91 - Table of list of participating SUCs .....	310
Table 92 - List of Actors Involved.....	311
Table 93 - List of Components Participating in the Primary Use Case.....	312
Table 94 - List of Communication Technologies Involved .....	313
Table 95 - List of Data Models .....	316
Table 96 - List of Information Objects .....	318
Table 97 - Table of list of participating SUCs .....	322
Table 98 - List of Actors Involved.....	322
Table 99 - List of Components Participating in the Primary Use Case.....	323
Table 100 - List of Communication Technologies Involved .....	324
Table 101 - List of Data Models .....	327
Table 102 - List of Data Standards .....	327
Table 103 - List of Information Objects .....	327
Table 104 - Table of list of participating SUCs .....	331
Table 105 - List of Actors Involved.....	335
Table 106 - List of Components Participating in the Primary Use Case.....	336
Table 107 - List of Communication Technologies Involved .....	338
Table 108 - List of Data Models .....	340
Table 109 - List of Data Standards .....	340
Table 110 - Table of list of participating SUCs .....	345

Table 111 - List of Actors Involved.....	347
Table 112 - List of Components Participating in the Primary Use Case.....	351
Table 113 - List of Communication Technologies Involved .....	353
Table 114 - List of Data Models .....	355
Table 115 - List of Data Standards .....	355
Table 116 - List of Information Objects .....	355
Table 117 - Table of list of participating SUCs .....	359
Table 118 - List of Actors Involved.....	360
Table 119 - List of Components Participating in the Primary Use Case.....	363
Table 120 - List of Communication Technologies Involved .....	365
Table 121 - List of Data Models .....	367
Table 122 - List of Data Standards .....	367
Table 123 - List of Information Objects .....	367
Table 124 - Table of list of participating SUCs .....	372
Table 125 - List of Actors Involved.....	374
Table 126 - List of Components Participating in the Primary Use Case.....	376
Table 127 - List of Communication Technologies Involved .....	378
Table 128 - List of Data Models .....	380
Table 129 - List of Data Standards .....	380
Table 130 - List of Information Objects .....	380
Table 131 - Table of list of participating SUCs .....	384
Table 132 - List of Actors Involved.....	385
Table 133 - List of Components Participating in the Primary Use Case.....	386
Table 134 - List of Communication Technologies Involved .....	388
Table 135 - List of Data Models .....	389
Table 136 - List of Data Standards .....	390
Table 137 - List of Information Objects .....	390
Table 138 - Table of list of participating SUCs .....	394
Table 139: Participating actors .....	395
Table 140 - List of Components Participating in the Primary Use Case.....	397
Table 141 - List of Communication Technologies involved .....	398
Table 142 - List of Data Models .....	400
Table 143 - List of Data Standards .....	400
Table 144 - List of Information Objects .....	400
Table 145 - Table of list of participating SUCs .....	405
Table 146 - List of Actors Involved.....	406
Table 147 - List of Components Participating in the Primary Use Case.....	407



Table 148 - List of Communication Technologies Involved .....	408
Table 149 - List of Data Models .....	409
Table 150 - List of Data Standards .....	410
Table 151 - List of Information Objects .....	410
Table 152 - Table of list of participating SUCs .....	415
Table 153 - List of Actors Involved.....	417
Table 154 - List of Components Participating in the Primary Use Case.....	418
Table 155 - List of Communication Technologies Involved .....	420
Table 156 - List of Data Models .....	422
Table 157 - List of Data Standards .....	422
Table 158 - List of Information Objects .....	422
Table 159 - Table of list of participating SUCs .....	426
Table 160 - List of Actors Involved.....	427
Table 161 - List of Components Participating in the Primary Use Case.....	428
Table 162 - List of Communication Technologies Involved .....	431
Table 163 - List of Data Models .....	433
Table 164 - List of Data Standards .....	433
Table 165 - List of Information Objects .....	433
Table 166 - Table of list of participating SUCs .....	438
Table 167 - List of Actors Involved.....	440
Table 168 - List of Components Participating in the Primary Use Case.....	441
Table 169 - List of Communication Technologies Involved .....	442
Table 170 - List of Data Models .....	443
Table 171 - List of Data Standards .....	443
Table 172 - List of Information Objects .....	444
Table 173 - Table of list of participating SUCs .....	448
Table 174 - List of Actors Involved.....	449
Table 175 - List of Components Participating in the Primary Use Case.....	450
Table 176 - List of Communication Technologies Involved .....	452
Table 177 - List of Data Models .....	453
Table 178 - List of Data Standards .....	454
Table 179: List of Information Objects .....	454
Table 180 - Table of list of participating SUCs .....	468
Table 181 - List of Actors Involved.....	469
Table 182 - List of Components Participating in the Primary Use Case.....	470
Table 183 - List of Communication Technologies Involved .....	471
Table 184 - List of Data Models .....	472



Table 185 - List of Data Standards .....	474
Table 186: List of Information Objects .....	474
Table 187 - Table of list of participating SUCs .....	476
Table 188 - List of Actors Involved.....	478
Table 189 - List of Components Participating in the Primary Use Case.....	479
Table 190 - List of Communication Technologies Involved .....	481
Table 191 - List of Data Models .....	483
Table 192 - List of Data Standards .....	485
Table 193: List of Information Objects .....	486
Table 194 - Table of list of participating SUCs .....	492
Table 195 - List of Actors Involved.....	493
Table 196 - List of Components Participating in the Primary Use Case.....	494
Table 197 - List of Communication Technologies Involved .....	495
Table 198 - List of Data Models .....	497
Table 199 - List of Data Standards .....	499
Table 200 - List of Information Objects .....	499
Table 201 - Table of list of participating SUCs .....	503
Table 202 - List of Actors Involved.....	504
Table 203 - List of Components Participating in the Primary Use Case.....	505
Table 204 - List of Communication Technologies Involved .....	507
Table 205 - List of Data Models .....	510
Table 206 - List of Data Standards .....	512
Table 207: List of Information Objects .....	512
Table 208 - Table of list of participating SUCs .....	517
Table 209 - List of Actors Involved.....	521
Table 210 - List of Components Participating in the Primary Use Case.....	522
Table 211 - List of Communication Technologies Involved .....	524
Table 212 - List of Data Models .....	525
Table 213 - List of Data Standards .....	526
Table 214 - Table of list of participating SUCs .....	529
Table 215 - List of Actors Involved.....	530
Table 216 - List of Components Participating in the Primary Use Case.....	531
Table 217 - List of Communication Technologies Involved .....	532
Table 218 - List of Data Models .....	533
Table 219 - List of Data Standards .....	534
Table 220 - Table of list of participating SUCs .....	537
Table 221 - List of Actors Involved.....	538

Table 222 - List of Components Participating in the Primary Use Case.....	539
Table 223 - List of Communication Technologies Involved .....	540
Table 224 - List of Data Models .....	541
Table 225 - List of Data Standards .....	542
Table 226 - List of Information Objects .....	542
Table 227 - Table of list of participating SUCs .....	546
Table 228 - List of Actors Involved.....	547
Table 229 - List of Components Participating in the Primary Use Case.....	548
Table 230 - List of Communication Technologies Involved .....	549
Table 231 - List of Data Models .....	550
Table 232 - List of Data Standards .....	551
Table 233 - List of Information Objects .....	551
Table 234 - Table of list of participating SUCs .....	555
Table 235 - List of Actors Involved.....	557
Table 236 - List of Components Participating in the Primary Use Case.....	559
Table 237 - List of Communication Technologies Involved .....	561
Table 238 - List of Data Models .....	563
Table 239 - List of Data Standards .....	563
Table 240 - List of Information Objects .....	564
Table 241 - Table of list of participating SUCs .....	568
Table 242 - List of Actors Involved.....	569
Table 243 - List of Components Participating in the Primary Use Case.....	572
Table 244 - List of Communication Technologies Involved .....	574
Table 245 - List of Data Models .....	576
Table 246 - List of Data Standards .....	576
Table 247 - List of Information Objects .....	576
Table 248 - Table of list of participating SUCs .....	581
Table 249 - List of Actors Involved.....	582
Table 250 - List of Components Participating in the Primary Use Case.....	585
Table 251 - List of Communication Technologies Involved .....	586
Table 252 - List of Data Models .....	589
Table 253 - List of Data Standards .....	589
Table 254: List of Information Objects .....	590
Table 255 - List of available standards for WiseGRID (75).....	616
Table 256 - Interfaces with WiseGRID products of WG STaaS/VPP.....	618
Table 257 - Interfaces with actors and other resources of WG STaaS/VPP. ....	618
Table 258 - Interfaces with WiseGRID products of WiseCORP.....	619

Table 259 - Interfaces with actors and other resources of WiseCORP.....	619
Table 260 - Interfaces with WiseGRID products of WiseCOOP. ....	620
Table 261 - Interfaces with WiseGRID products of WG FastV2G. ....	620
Table 262 - Interfaces with actors and other resource for WG FastV2G. ....	620
Table 263 - Interfaces with WiseGRID products of WiseEVP. ....	621
Table 264 - Interfaces with actors and other resources of WiseEVP. ....	621
Table 265 - Interfaces with WiseGRID products of WiseHOME. Source: ITE. ....	622
Table 266 - Interfaces with actors and other resources of WiseHOME. ....	622
Table 267 - Interfaces with WiseGRID products of WG RESCO. ....	622
Table 268 - Interfaces with actors and other resources of WG RESCO. ....	622
Table 269 - Interfaces with WiseGRID products of WG Cockpit.....	623
Table 270 - Interfaces with actors and other resources of WG Cockpit.....	623
Table 271 - PRIVACY & DATA PROTECTION - DATA SOURCES FOR DSO.....	643
Table 272 - PRIVACY & DATA PROTECTION - DATA SOURCES FOR NON-DSO.....	645

## EXECUTIVE SUMMARY

WiseGRID aims at integrating a multitude of assets of the Smart Grid ecosystem in an efficient and effective way. However, this challenging task requires a systematic approach in order to realize the vision of the project itself and also to combine efficiently the diverse energy components that consist the products of the WiseGRID project.

To bring this challenging task into a successful completion, the SGAM framework and underlying methodology have been applied to analyze and design the architecture of the WiseGRID services, tools, and use cases. More specifically the following design and analysis process has been followed.

1. Definition of the various WiseGRID-related use cases
2. Modelling of the use cases using the SGAM methodology and framework
3. Identification of proper WiseGRID applications to tackle the respective use cases
4. Modelling of the WiseGRID tools and services using the SGAM methodology and framework after the detailed analysis of the related use cases.

An overview of the WiseGRID applications/tools to address the requirements of the respective use case is presented briefly below. A detailed analysis of the architecture of the tools is provided in the respective chapters.

### *WiseGRID Tools*

#### **WG INTEROPERABLE PLATFORM (IOP)**

The WG IOP in the aims to provide a scalable, secure and open ICT platform, with interoperable interfaces, for real-time monitoring and decentralized control to support effective operation of the energy network.

The objective of the platform is to manage and process the heterogeneous and massive data stream coming from the distributed energy infrastructure deployed. This platform should enable new services and reduce ICT costs for prosumers and smaller players, whilst it will facilitate cross-network and cross-entity interoperability. It will enable the cooperation and synergies among the different actors targeted by the different WiseGRID technological solutions.

#### **WG COCKPIT**

WiseGRID Cockpit is the WiseGRID technological solution targeting DSOs and microgrid operators, allowing them to control, manage and monitor their own grid, improving flexibility, stability and security of their net-work. Taking into account the goals of the project, the features to be implemented within WiseGRID cockpit consider a scenario of increasing share of distributed renewable resources and services provided by communities of prosumers (aggregated in the form of VPPs or cooperatives in order to achieve higher participation and environmental, social and economic benefits). The main purpose of the WiseGRID Cockpit is to enable DSOs to manage the fundamental changes that distribution grids are facing nowadays.

#### **WISECOOP**

WiseCOOP is the WiseGRID technological solution targeting aggregators of consumers and prosumers - particularly focused on domestic and small businesses -, supporting them in their

roles of energy retailers, local communities and cooperatives – which may have different objectives.

The main goal of the solution is helping consumers and prosumers to work together in order to achieve better energy deals while relieving them from administrative procedures and cumbersome research.

### **WG STAAS**

WiseGRID STaaS/VPP is a platform developed in WiseGRID context to manage a communication and information flow of many systems to get an improvement on the behavior of the whole system.

The main goal of this platform is to establish a communication way to exchange information about every single system for becoming these individual energy storage system as more complex system with better efficiency and capacity.

### **WISEVP**

WiseEVP is the WiseGRID technological solution for Vehicle-sharing companies or electric vehicle fleet managers and Electric vehicle infrastructure (EVSE) operators. In order to optimize the activities related with smart charging and discharging of the EVs including V2G (vehicle to grid, energy injection in the distribution network) and V2H (vehicle to home, energy injection in the household electric installation). The management of the EVSEs charging and discharging processes will meet number of objectives, subordinated to the EV user preferences: desired state of charge (SOC) at the time of unplugging the EV.

### **WG FASTV2G**

WG FastV2G is the WiseGRID technological solution to use EVs as dynamic distributed storage devices. Under smart grid environment, where two-way instantaneous communication is available, the energy flow from EVs to the grid is feasible. Energy stored in the batteries of available vehicles runs back to the grid when needed (fast V2G supply) to support ease up domestic peak load. The main goal of this solution is make possible the energy transfer from the vehicle to the grid (V2G) as proactive method of balancing utility supply and demand.

### **WISEHOME**

WiseHOME is the WiseGRID IT solution that aims to raise the awareness of residential energy users regarding their energy consumption, and more importantly to provide them with detailed analytics that lead to actionable triggers so that they start realizing the benefits of modifying their demand profile. Its ultimate aim is to serve as the user interface that will transform conventional, passive energy consumers in households into active participants of the energy system through modulation of their demand according to the needs of the network and energy supply. A key factor towards achieving these objectives is the adequate retrieval and analysis of energy usage data, and visualization of meaningful information extracted from it.

### **WISECORP**

WiseCORP is the WiseGRID technological solution targeting businesses, industries, ESCOs and public facility consumers and prosumers, with the objective of providing them the necessary mechanisms to become smarter energy players. By means of energy usage monitoring and analysis, proper information can be given to facility managers helping them to reduce energy costs and environmental impact. A key factor towards achieving these objectives is a proper retrieval and analysis of energy usage data, and visualization of meaningful information extracted from it.

### **WG RESCO**

The WiseGRID RESCO will be a tool conceived for RESCOs – Renewable Energy Service Companies and ESCOs that want to provide RES services to end-users (households or businesses) that do not own nor wish to maintain the necessary equipment. According to that, the WG RESCO tool will support RESCOs in managing the relationship with their customers and the provision of energy to the consumers from renewable energy sources, usually PV, wind power or micro hydro. Since the generation equipment will be owned, serviced and operated by the RESCO itself, the WG RESCO will have a central feature in supporting the maintenance management of those assets.

As already mentioned, prior concluding to the WiseGRID tools to be developed during the project and tested subsequently in the various pilot sites, the definition of the various use case has been carried out. This use cases were defined in deliverable D2.1 and cover a wide variety of challenging case to be tested during the WiseGRID project.

In order to have a systematic, consistent, and homogenous description of the analysis and the design of the Use Cases (UCs) the Smart Grid Architecture Model (SGAM) and the underlying methodology and framework was applied. In the SGAM framework each particular UC can be modelled and analyzed from different aspects. The most important factor while modelling a UC is the coherency of the whole process, as well as the production of an analytic and detailed object, where the role of each stakeholder is clearly defined. In the SGAM framework the interoperability to be modeled is aggregated into five different levels, the SGAM layers. Each layer refers to a different aspect of every UC, starting from the Business layer (referring to the business usage of the smart grid information exchanged, the involved market partners, business objectives, constraints, etc.), moving step by step to the Component layer (physical layer, including all entities of smart grid, such as the system equipment, the network infrastructure and the protection devices). Between these two, lie the Function, the Information and the Communication layer. These layers refer to the functions implemented (functionality of UC), the information object and data models exchanged between functions or actors (devices, applications, persons, organizations) and the protocols/mechanisms used for the exchange of information, respectively.

In succession, the interoperability layers need to be merged with another concept, the smart grid plane, to compose the 3D SGAM framework. In the smart grid plane, an important distinguish is made between the electrical processes (domains) and the information management viewpoints (zones) involved in every UC. The five SGAM domains contain the Bulk Generation domain (massive generation of electricity), the Transmission domain (infrastructure and organization for the transportation of energy), the Distribution domain, the Distributed Electrical Resources domain (DER connected to the public distribution grid ranging from 3 kW~10.000 kW) and the Customer Premises domain (prosumers of electricity).

Moving on to the six SGAM zones, these are distinguished as follows. The Process zone (refers to the transformation of energy and the equipment involved) is followed by the Field zone (protection,



control and monitor equipment) which, in turn, is succeeded by the Station zone (areal aggregation of previous level). Next comes the Operation zone (control operation systems such as DMS/EMS), followed by the Enterprise zone (commercial aspect/e.g. logistics, staff training, etc.) and finally the Market zone (commercialization of the produced energy).

Using the SGAM methodology the following Primary Use Cases (PUCs) were considered, that are also grouped in respective High Level Use Cases (HL-UCs).

### ***WiseGRID Primary Use Cases (PUCs)***

#### ***HL-UC 1\_PUC\_1: NETWORK MONITORING***

This PUC addresses the observability of the electricity distribution network in presence of RES. It has four main components. The first one deals with measurements acquisition (Voltage [U], Active Power [P], Reactive Power [Q] from nodes, P, Q from RES production connected to the nodes and P, Q from network sections or specific lines). The second one deals with the forecast of RES production, consumption and of total power flow in critical sections, based on the data already collected. The third component is looking to provide the DSO with the necessary mechanisms in order to calculate Key Performance Indicators (KPIs) to assess the correct operation of the grid. The fourth component is dealing with the big amount of data –field measurements, mainly– obtained from the Advance Metering Infrastructure (AMI) deployed in the grid during the scope of the project.

#### ***HL-UC 1\_PUC\_2: CONTROL STRATEGIES FOR REDUCING RES CURTAILMENT***

This PUC focuses on optimizing the general strategy of reducing or avoiding RES curtailment by using the relevant inputs from secondary use-cases, which have different technics in order to achieve the afore-mentioned goal. For this, all HL-UC 1\_SUC\_2.1 to HL-UC 1\_SUC\_2.4, are used as candidates for the optimization. The main purpose is to find various solutions for solving the grid congestions by various means: stimulate local consumption, storage, use of V2G or other means, thus making a stable energy ecosystem which does not stress the grid and the system stability.

#### ***HL-UC 1\_PUC\_3: VOLTAGE SUPPORT AND CONGESTION MANAGEMENT***

In this PUC global and local methods are demonstrated, aiming to keep the voltage level in accepted boundaries. Network losses are reduced and possible network congestions should be signaled. These important activities must be performed diligently, through centralized and decentralized voltage control solutions.

#### ***HL-UC 1\_PUC\_4: GRID PLANNING ANALYSIS***

The objective of this PUC is to provide to DSOs tools for the grid planning activities. Indicative examples of possible topics that need to be addressed are: where is storage needed and what type of storage is needed? Where should public EVSEs be more convenient installed?

#### ***HL-UC 1\_PUC\_5: Promote RES via RESCO companies***

According to the description already provided in the D2.1, the objective of this PUC is to support the operations of RESCO companies, namely to create an inventory of their assets, and monitor and control all parameters related to their assets. Measuring the economic impact for RESCO companies and their customers, RESCO companies will enable the provision of energy from RES to its consumers, where the serviced household/business does not own (operate and maintain) the RES generation equipment. Customers of RESCO will be able to self-consume energy produced by RES units, while RESCO will be able to bring on market the energy surplus. These companies will encourage the adoption of distributed generation through RES.

#### ***HL-UC 2\_PUC\_1: DISTRIBUTION NETWORK REAL-TIME MONITORING***

The smart grid environment requires the upgrade of tools for monitoring at all levels of the grid. These components will provide the data necessary for monitoring the grid. This PUC aims to validate new smart grid technologies and business models and provide two-way communication between distributed generation, storage, demand assets, and the existing grid operator (dispatch center). The measurement techniques may include various device types including smart meters (HL-UC 2\_SUC\_1.1), remote terminal units (RTUs), and phasor measurement units (PMUs). Measurements are captured, stored (HL-UC 2\_SUC\_1.2), and analyzed (HL-UC 2\_SUC\_1.3) in order to determine in every moment the status of the grid. Thanks to these analyses, faults can be detected (HL-UC 2\_SUC\_1.4), thus assuring the correct functioning of the system. Additional tasks for the maintenance of the elements in the grid are considered as well (HL-UC 2\_SUC\_1.5).

#### ***HL-UC 2\_PUC\_2: REAL-TIME DISTRIBUTION SYSTEM AWARENESS***

The grid operation may be characterized by the following states: normal, emergency and restorative, since its operation conditions change due to sudden and unexpected events. If the state changes to emergency, then it is necessary to take suitable corrective measures and bring the state back to normal. The measurements are acquired in suitable concentration structures, such as SCADA, AMI, and PDC (HL-UC 2\_SUC\_1.2). Once the topological data are known (HL-UC 2\_SUC\_2.2) and the network is found to be fully observable (HL-UC 2\_SUC\_2.3), the measurements, together with other data, are processed by the state estimator (HL-UC 2\_SUC\_2.5) which aims at filtering/removing the measurement noise and compute a system state that is as close as possible to the true one. It is possible to use the load flow analysis tool to verify the state estimation calculation or make a comparison (HL-UC 2\_SUC\_2.4). If bad data is detected (HL-UC 2\_SUC\_2.6), then the state estimation process has to be re-executed, otherwise the state estimation result is wrong. The estimated state is passed on to the Energy management system (EMS) and Distribution Management Systems (DMS) applications (HL-UC 2\_PUC\_3), which are related to the real-time grid control and operation.

#### ***HL-UC 2\_PUC\_3: GRID CONTROL***

The main goal of the Distribution System Operator (DSO) is to ensure the network operation and management in a reliable and economic manner under normal and abnormal conditions. Application of grid control is motivated either by the inherent needs of the distribution grid operated by the DSO or by the extraneous needs of the transmission system operated by the Transmission System Operator (TSO). Accomplishing these goals requires continuous monitoring of the prevailing conditions in the MV/LV distribution network (HL-UC 2\_PUC\_1) and identification of the operating state of the distribution network (HL-UC 2\_PUC\_2). Combining



this information, the DSO determines the necessary preventive actions in case the distribution grid state is identified as insecure (inherent needs) or in case the TSO has sent a request for specific actions or a notification regarding the current state of the transmission system (HL-UC 2\_PUC\_3).

#### ***HL-UC 3\_PUC\_1: EVSE AND EV FLEET MONITORING***

This PUC describes the data collection process from the EVSEs and the EVs.

#### ***HL-UC 3\_PUC\_2: INTERACTION OF THE USER WITH EVSE***

This PUC describes the interaction of the EV user (driver) with the charging infrastructure (EVSEs) in order to authenticate, start a charging session or book an EVSE. The user will be able to select (or book in advance) three different types of charging sessions: Charging on user demand, Smart charging, Smart charging with V2G

#### ***HL-UC 3\_PUC\_3: EV CHARGING MANAGEMENT***

This PUC describes all the processes that take place in the WiseEVP to manage the charging sessions of the EVSE and to schedule the charging session according to the EV user preferences

#### ***HL-UC 3\_PUC\_4: INTERACTION WITH THE ENERGY INFRASTRUCTURE***

This PUC describes how the EV charging infrastructure might module its power output to provide flexibility to the grid, to maximize the RES integration and to participate in the house energy management process (V2H).

#### ***HL-UC 4\_PUC\_1: BATTERIES MANAGEMENT AT PROSUMER LEVEL***

To get a more flexible RES generation and more efficient distributed generation system on the grid, it is necessary to set up storage facilities and most feasible would be batteries together with a management system at consumer/prosumer level. This control would facilitate higher energy generated by distributed renewable energy resources and optimize the grid availability at the consumer group level. This system also enables consumers to become prosumers, as active grid-users that would maximize the generation from RES both with balance between generation and consumption but also grid load control.

#### ***HL-CU 4\_PUC\_2: BATTERIES MANAGEMENT AT AGGREGATOR LEVEL***

Batteries enable the grid to become more stable for several reasons. If batteries are managed by a system, they can reduce the grid's fluctuations by means of coordinated control of the grid's voltage and frequency. They can, as well, ensure a quick response in case of a grid outage (fast restoration), reducing the blackout duration and improve the consumer's security of supply. The following services regarding grid support can be provided by battery storage systems: Load frequency control, grid capacity management, voltage support, power quality support, blackstart and backup capabilities.

#### ***HL-UC 4\_PUC\_3: ANCILLARY SERVICES***

Energy Storage Systems can provide services that are important for a satisfactory operation of the network, such as reactive power support, load following, back-up service, peak shaving, power quality (PQ) and disturbance compensation to name a few. Through various control algorithms, such as droop control, virtual inertia, etc., generation and storage units can coordinate their operations offering significant benefits for the utility grid. The aggregation of battery systems based on modern communication, at any level, can offer several services related indirectly with the energy storage as the market regulation. Ancillary services like “active power reserves” and “frequency response”, would be possible based on energy and power availability.

#### ***HL-UC 4\_PUC\_4: COMBINATION OF BATTERY STORAGE SYSTEMS***

With the combination of different storage technologies high power (e.g. ultracapacitors) and energy (e.g. batteries) contents can be achieved at the same system. In common uses, it is necessary to obtain information about the status of every unit by means of a standard of information trading. This information can be used for managing in a coordinated manner the area system for interest. Technical specifications of any battery connected to the system will be available for “grid operators” and “management systems” and used for both administrative and operative (controlling) functions. This information about the specifications of every battery model included in the system must be available for both reading and controlling.

#### ***HL-UC 5\_PUC\_1: THERMAL MONITORING***

This PUC deals with the integration of Cogeneration in WiseCORP and the efficient management of CHPs and Thermal Storage. Three system components (as well as the relevant critical values of thermal storage) are monitored: Gas Consumption in Households, Combined Heat and Power, Buildings.

#### ***HL-UC 5\_PUC\_2: COGENERATION AND HVAC MANAGEMENT***

This PUC is associated with the control of CHP, HVAC and thermal loads of buildings. It must take under consideration the schedules proposed by HL-UC 5\_PUC\_4, without being bound by them (PUC must proceed if deviations are detected. Forecasting of thermal needs (taking into account models from HL-UC 5\_PUC\_3 and measurements from HL-UC 5\_PUC\_1) is part of this process, as well as the alarm management

#### ***HL-UC 5\_PUC\_3: COMFORT-BASED DEMAND FLEXIBILITY MODELS***

This PUC is responsible for the development of models of buildings/households and the associated usage patterns that have an impact on energy demand. A model of thermal behavior will be created, through advanced algorithms using as much information as possible. Apart from this, thermal flexibility and the amount of thermal energy that can be shifted must be estimated. Inputs from HL-UC 5\_SUC\_2.3 are to be included.

#### ***HL-UC 5\_PUC\_4: COGENERATION AND HVAC OPTIMISATION***

In this PUC, the market and business aspects of CHP, HVAC and building management are examined. Firstly, the role of each asset and its participation in the VPP or provision of Ancillary Services to the distribution network is defined. The final business decisions are made by an optimization algorithm, while two different algorithms optimize the participation of the

assets in VPP and the Ancillary Services. As a result, the optimal bids are identified and a set of schedules is produced.

#### ***HL-UC 6\_PUC\_1: VPP MONITORING AND MANAGEMENT***

According to the description already provided in the D2.1, the goal of this PUC is to monitor the state of the re-sources (industrial, domestic and public facilities, EVs, energy storages etc.) belonging to the VPP (current status) (HL-UC 6\_SUC\_1.1) as well as to provide forecasting for RES, demand (HL-UC 6\_SUC\_1.2) and flexibility (HL-UC 6\_SUC\_1.3), and use that information for defining suitable strategies for managing (internal) grid and market issues (HL-UC 6\_SUC\_1.4).

#### ***HL-UC 6\_PUC\_2: VPP MARKET PARTICIPATION***

According to the description already provided in the D2.1, this PUC manages the VPP within energy market participation. It helps the VPP to participate to the energy (day-ahead and intra-day) (HL-UC 6\_SUC\_2.1) as well as to the ancillary services market (HL-UC 6\_SUC\_2.2) and to calculate the most appropriate bid to be submitted in that energy market, where appropriate. Then according to these results, it supports the VPP to define a single strategy for the participation in these types of energy markets (HL-UC 6\_SUC\_2.3).

#### ***HL-UC 6\_PUC\_3: VPP REAL TIME CONTROL***

This PUC aims at providing a real time control on the VPP. In order to do that it is necessary to identify the current available flexibility by taking into consideration the real time measurements (HL-UC 6\_SUC\_3.1), to receive notifications and requests by the local DSO through the ancillary services market in order to implement ancillary services (HL-UC 6\_SUC\_3.2), and to define the appropriate commands that the VPP Operator will send to the VPP Components (HL-UC 6\_SUC\_3.3).

#### ***HL-UC 6\_PUC\_4: VPP USERS RELATIONSHIP MANAGEMENT***

This PUC is about the possibility to manage more efficiently the grid load avoiding peak by means of Demand Side Management (DSM) and Demand Response (DR) mechanisms, which push consumers (in an aggregated way) at VPP level to consume more or less RES according to the need of the grid. In this direction, this PUC describes the functionalities needed by the VPP Operator to manage the portfolio of VPP members. Such functionalities include: describes management of the contractual issues and Service Level Agreement (SLA) (HL-UC 6\_SUC\_4.1), management of member compensation (HL-UC 6\_SUC\_4.2) and DR actions (HL-UC 6\_SUC\_4.3).

#### ***HL-UC 7\_PUC\_1: DYNAMIC MANAGEMENT OF DEMAND SIDE ASSETS IN TERTIARY SECTOR***

To ensure the active engagement of businesses, industries, ESCOs, local communities and public facilities in energy markets and energy management initiatives, a corporate application tool should be available. This is a tool to facilitate the management of large infrastructures and promote the concept of smarter and responsible energy players by giving them more power and protection and also ownership, reducing their energy bill, supporting self-consumption by means of real-time data coming from all their energy devices and by means of demand response and load optimization schemes. To sum up, the goal of this PUC is to facilitate professionals (e.g. Facility Managers) on daily activities.

### ***HL-UC 7\_PUC\_2: DYNAMIC AGGREGATION OF DEMAND SIDE ASSETS AND ACTIVE PARTICIPATION INTO ENERGY MARKET***

To support the active involvement of traditional (Suppliers) and new business (Aggregators, cooperatives) roles in energy markets a portfolio management tool will support the engagement of Consumers and Prosumers in emerging business models (e.g. real-time pricing, demand response). The tool is an application for energy Suppliers, Aggregators, local communities and cooperatives of Consumers and Prosumers (and other intermediary companies) to help domestic and small businesses, Consumers and Prosumers achieve better energy deals: better services, prices and opportunities to participate in ancillary service markets will be offered to the final Consumers/Prosumers. This includes aggregation models such as VPP where the Aggregator (or other intermediate) gathers a portfolio and operates them as a unified and flexible resource on the energy market. In summary, the goal of this PUC is to provide the engine that facilitates energy stakeholders (Aggregators & Suppliers).

### ***HL-UC 7\_PUC\_3: CUSTOMERS ENGAGEMENT FOR ACTIVE MARKET PARTICIPATION***

Towards citizen's empowerment in energy market and reduction of energy poverty, as the main objective of HL-UC 7, we have to ensure that even the small (residential) clients move from passive entities to active elements of the electricity grid. In order to ensure client participation, information about electricity usage and energy market (retail & ancillary services) operation should be available in an appealing but not intrusive way. This can be done with a personalized application for individual domestic Consumers and Prosumers covering different types of functionalities like: real-time monitoring of consumption and production, participating in demand response programs (visualizing DR signals, e.g. price information), alerts, energy saving tips, etc. This is actually the main objective of this PUC: to establish a dynamic channel of communication with the domestic Consumers and Prosumers, enabling their transformation to active grid elements.

#### ***Privacy and Data Protection***

The Privacy and Data Protection is covered within each WiseGRID tool architecture description as specific threats and events to be treated, and also within Chapter 14 where are presented general European regulation aspects, a Data Protection Impact Assessment (DPIA) process and specific national regulation from "site pilots" countries.

The general presentation makes reference to existing requirements (i.e. Regulation EU 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC - shortly: General Data Protection Regulation) that are matching the Privacy and Data Protection and also the resulting obligations within the Project to perform a DPIA in line with existing template as developed by Expert Group 2. Such approach is also in line with WiseGRID Grant Agreement, article 27 Protection of Results and article 39 Processing of Personal Data.

Performance of DPIA is based on Primary data (Questionnaire designed and sent to all WiseGRID pilot sites and tools to evaluate the impact on privacy and data protection), and Secondary data (applicable regulations within privacy and data protection).

DPIA is a legal obligation and a dedicated procedure to evaluate the risks related to privacy and data security to a project or a business, to identify potential risks and enhance data security and protection by applying appropriate mitigation techniques (controls) which in turn create a series of advantages and benefits to the project/business.

According General Data Protection Regulation (GDPR), DPIA is mandatory for technologies and processes that are likely to result in a high risk to the rights of the data subjects.

The starting point for such evaluation and processes is going back to “the right to protection of an individual’s private sphere against intrusion from others, especially from the state”, as laid down in Article 12 of the United Nations Universal Declaration of Human Rights (UDHR) of 1948 on respect for private and family life. The UDHR further influenced the development of other human rights instruments including in Europe. The right became legally binding when incorporated into the International Covenant on Civil and Political Rights.

Main principles on data protection were defined within Convention 108. These were also incorporated into the 1995 EU Data Protection Directive and therefore, currently the GDPR has similarly incorporated the principles applied to any collection or processing of personnel data like: Personal data must be processed lawfully, fairly and transparently; Personal data can only be collected for specified, explicit and legitimate purposes; Personal data must be adequate, relevant and limited to what is necessary for processing; Personal data must be accurate and kept up to date; Personal data must be kept in a form such that the data subject can be identified only as long as is necessary or processing, and Personal data must be processed in a manner that ensures security.

Specific within Energy, related regulation has referred to principles in requirements regarding customers and data management. The DPIA is based on detailed activity performed by main team members as: DPO, Controllers and Processors.

The DPIA performed describes: the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects (identify threats and events), the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data (controls) to demonstrate compliance with EU Regulation. It will also help as appropriate, the National Data Protection Authorities to assess the compliance of the processing and the risks for the protection of personal data of the data subject and the related safeguards, assuming data controllers consult them prior to data processing.

In line with above mentioned, the DPIA was performed using the “Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems (18.03.2014)”, chapters 2 and 3. The DPIA for Smart Grid and Smart Metering systems, specifically WiseGRID tools, was performed in following steps:

#### **Step 1 - Pre-assessment and criteria determining the need to conduct the DPIA;**

The activity was based on 6 criterion that creates a preliminary image of the Project and envisage the need of a DPIA. This was done looking to specific personal data used within WiseGRID tools and also to the motivation of a DPIA process. A survey to collect “personal data” to be considered in WiseGRID was performed.

#### **Step 2 - Initiation;**

This step considered: purposes to execute the DPIA, defining the DPIA team and identifying the resources including the launch of a surveys as: “questionnaire”.

#### **Step 3 - Identification, characterization and description of smart grid systems / applications processing personal data;**

This is looking to identify and understand description of the systems (detailed description, scenarios, main actors, description of primary and supporting assets) as they are processing personal data. Use cases and WiseGRID tools description from deliverable D2.1, and also the architecture from current deliverable D3.1 were considered. It was also applied the survey with a “questionnaire” of 29 questions related to WiseGRID tools predesign.

#### **Step 4 - Identification of relevant risks (events and threats);**

This is a complex activity looking to identify threats and feared events that would compromise the privacy and data protection. The overall idea of risk for the smart grid Applications, looks over two terms: their likelihood of occurrence (likelihood) and the impact of their consequences (severity).



The survey with the 29 questions mentioned under Step 3 was also used. The result of this step was concluded with a tool by tool table realized with feared events and threats associated to each WiseGRID tool.

#### Step 5 - Data protection risk assessment;

In this step the identified feared events and related threats were weighed with the severity of impact on the individuals and likelihood of occurrence. In order to classify the impact and likelihood, for each WiseGRID tool was created a table like below:

Feared events	Threat ID	Related Privacy targets	Affected assets	Impact (Severity)	Likelihood	Risk Level (Impact+Likelihood)
---------------	-----------	-------------------------	-----------------	-------------------	------------	--------------------------------

A complete set of tables together with a mapping of the identified risks (one table and one map graph for each WiseGRID tool) were concluded afterwards.

#### Step 6 - Identification and recommendation of controls and residual risks;

At this step, the aim was based on the risks determined and assessed in the previous step, to identify which controls are planned to be implemented (mitigation measures) in order to reduce the risk at a lower level. Any risk found at unacceptable level, was appropriately mitigated by one or more controls considering their likelihood and impact. The options that can be considered to manage (treat) those risks are as: Risk Modification; Risk Retention; Risk Avoidance and Risk Sharing.

In order to treat (manage) the risks, for each WiseGRID tool was created a table like below:

Feared events	Threat ID	Related Privacy targets	Controls planned or implemented	Risk level	Risk treatment (based on privacy targets)	Residual risk
---------------	-----------	-------------------------	---------------------------------	------------	---	---------------

A complete set of tables together with a mapping risks with implemented/planned controls (one table and one map graph for each WiseGRID tool) were concluded afterwards.

According to ISO 27005, the residual risk is “the risk remaining after the risk treatment”. In this context, it was identified that residual risks remained after implementing controls stays at an acceptable level (Limited or Negligible).

The following resolution was concluded at the end of current DPIA process for WiseGRID applications, still under design:

- **The DPIA is positive:** risks have been assessed and controls addressing those risks properly defined and tuned. Any residuals risks are acceptable, and no further controls have been identified as necessary. The system implementation proceeds.
- **This DPIA report shall be rechecked** within deliverable D3.1 (V2) and further on when the system will be in production or whenever there would be changes in risk evaluation.

It is mentioned that DPIA will be under a continuous improvement process. It therefore requires monitoring changes over time (context, risk, measures...) and updates whenever a significant change occurs.

It is also important to stress that shall be communicated to national data privacy authorities about the data protection activities carried out within WiseGRID and also about the results of DPIA Report and further possible updates.

### *Standards and Interoperable Data Models*

This deliverable includes the main results of the activities carried out in the scope of the task “Standards and interoperable data models” of the WiseGRID project. The main objective of this task was to value the necessary interfaces between actors of components and recommend the appropriate set of standards or new data models based on ontologies.

To cope with this objective, the identification of the main interfaces between WiseGRID products and external agents and resources was a preliminary stage of the standards and data model assessment in order to build a simplified architecture to work in the definition of WiseGRID standards. The next step was mapping all the WiseGRID products with the IEC Smart Grid Standards Map to provide a clear definition of each of them based on the zones (process, station, field, operation, enterprise and/or market) and domains (generation, transmission, distribution, DER, consumption and/or communication) addressed by each tool.

As the final stage for the interfaces identification, each WiseGRID product was represented in a diagram showing the differences between the communications among WiseGRID products, the communications between WiseGRID products and external actors and the communication between these products and external resources that will be managed or integrated in WiseGRID solution.

Once the interfaces were clearly identified, the standards and data models assessment started. The first release of the “WiseGRID architecture, data models, standards and data protection (D3.1) includes the state of the art of the available standards and data models. Using as a reference the WiseGRID tools mapping, the respective includes the standards proposed by the IEC for each functional cluster of the smart grids. The data models state of the art has been mainly focused on the most extended standards for smart grids: IEC 6180 and CIM model. Finally, we have included a review of the new data models based on ontologies that might be applied to the smart grids and specifically to WiseGRID products.

In the second release of this document (D3.2), once the design of the WiseGRID tools is almost finished, this section will be extended to study the applicability of data models and standards to WiseGRID. Based on the state of the art included on this release, for each WiseGRID tool, the most appropriate standards and data models will be selected.

## 1 INTRODUCTION

### 1.1 PURPOSE OF THE DOCUMENT

The purpose of this document is to provide the tools to model the architecture of an interoperable, secure and flexible architecture, which will consider smart grids addressing active networks with high penetration of renewables, integrating distributed and concentrated storage, with e-mobility and with various energy services, including demand response, to optimize the functionality for all actors, including the end-user, with the citizen in the core. The architecture will enable complex markets for energy and energy services, with dynamics from one hour down to one minute and associate quality of service. The Smart grid security, data models, standards and interoperability issues are analyzed in order to detect potential barriers in the future stages of the project.

In addition to the architectural issues associated with the WiseGRID offered services and tools, this document lays also the foundations for aligning the afore mentioned services and tools with all European and regional legislation and laws related to data privacy and data protections issues.

Finally, to ensure a uniform and harmonized approach across all developed services and tools, a thorough analysis of the existing standards is performed and their application in the context of WiseGRID is assessed and analyzed in a structured manner.

### 1.2 SCOPE OF THE DOCUMENT

The scope of the document covers the modeling of the use-cases developed in WP2 using the European SGAM framework, in a systematic manner that is also closely related to the architectures already developed in other H2020 projects, such as NOBEL GRID, Elsa and Success. This modeling also considers local neighborhood transactions for energy delivery, energy storage, demand response and various energy services, either aggregated (e.g. through VPPs) or to stabilize local networks/sub-networks/microgrids or neighborhood bilateral, such as small quotas of energy production, storage and consumptions in MV/LV networks.

Privacy and data protection issues in a multi-actor environment also fall under the scope of this document. To this extent, national and DSO rules regarding the lawful constraints about privacy as well as the will of end-customer to participate have been investigated and analyzed. A DPIA assessment is also carried within this document, which includes bilateral/multilateral contracts agreed with standard and digitally signed versions. Output from WP1 and the ongoing work in the Smart Grid Task Force and its Experts Groups in the field of the regulatory environment for privacy, data protection, cyber security have been considered in this task.

Moreover, standards and interoperable data models to be used in the context of the WiseGRID tools and UCs are analyzed. Furthermore, new data models have been considered in order to allow new reasoning mechanisms in the process of automated decisions and collective awareness.

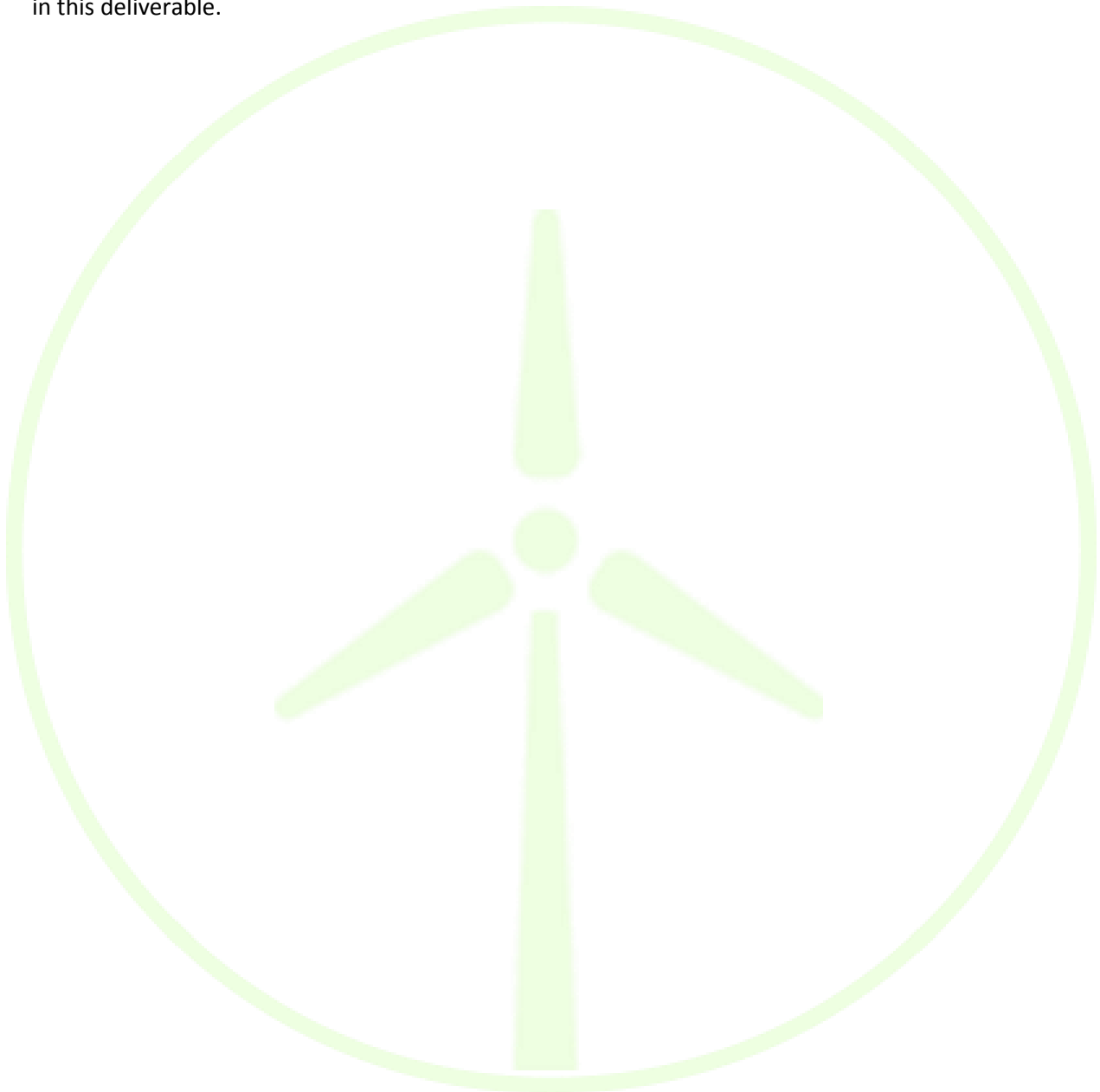
Finally, it should be mentioned that this document implements the first version (V1) of the report related to architecture, data privacy and protection, and data-standards and it would be updated to the second version (V2) at M18 of the project, where the development of the said services and tools will be matured.

### 1.3 STRUCTURE OF THE DOCUMENT

This document is structured as follows. The document starts by introducing the Smart Grid Architecture Model, which will be used as the framework for modelling in a systematic and unified way both the WiseGRID tools and the Use Cases (UCs). An overview of the WiseGRID architecture under the point of view of SGAM is provided in the subsequent chapter. Having become familiar with the overall



structure of the WiseGRID architecture, the architecture for each one of the WiseGRID tools is presented in separate chapters in terms of SGAM Component, Function, Communication, and Information Layers. Aspects related to standards and data models, as well as to data privacy are addressed for each one of the WiseGRID tools in the respective chapter. Additionally, separate chapters with a more in-depth analysis to standards and data privacy issues related to WiseGRID, are dedicated for the interested reader. Finally, a thorough analysis using the SGAM framework is carried out for all WiseGRID PUCs in the form of appendices presented in the end of the document, together with the data gathered from various sources (e.g. pilot sites) for performing the required modeling presented in this deliverable.



## 2 WISEGRID ARCHITECTURE SPECIFICATION

### 2.1 THE SMART GRID REFERENCE ARCHITECTURE

A Reference Architecture (RA) can be defined as a work product used to describe a concrete (standard) architecture, in a more abstract concept. As far as Smart Grids (SG) are concerned, the design of an RA needs to follow some particular standards (requirements) in order to be able to produce flexible, globally accepted models. While capable of describing the current state of a SG, a RA needs to take into account its upgrading prospects, in order to be functional in the years to come. Regarding the different nature of the involved stakeholders, a coherent and flexible framework must be provided, where a proper categorization of all interested parts (as well as their technical equipment, financial transactions, information exchanged etc.) is feasible.

Obviously, the design of a SG-RA can and should not be arbitrary. Consistency with the established M/490 conceptual model, as well as the standard interoperability categories is recommended, in order to produce a universal schema which will be able to provide a view on the SG different structures (domains, zones, layers). Following this principle, the complexity of the UC models produced can be dramatically decreased. However, the criteria according to which the degree of coherence of a RA with an existing architecture is determined may vary and different methods can be applied. At first, the inclusion of the NIST Conceptual Model was considered as an important input in the SG-RA framework, since it can cover most of the SG domains of interest. Subsequently, the proper adjustments were made, especially with regard to the distributed energy resources (DER) domain.

Last but not least, an important scope of an SG-RA is to provide an overall picture of the SG, in combination with the capability of deepening into low-level details. These details may refer to many different aspects of the functionality of a SG or the overall architecture design. Therefore, it is of the utmost importance that a RA is designed to provide an easy to follow link between these viewpoints.

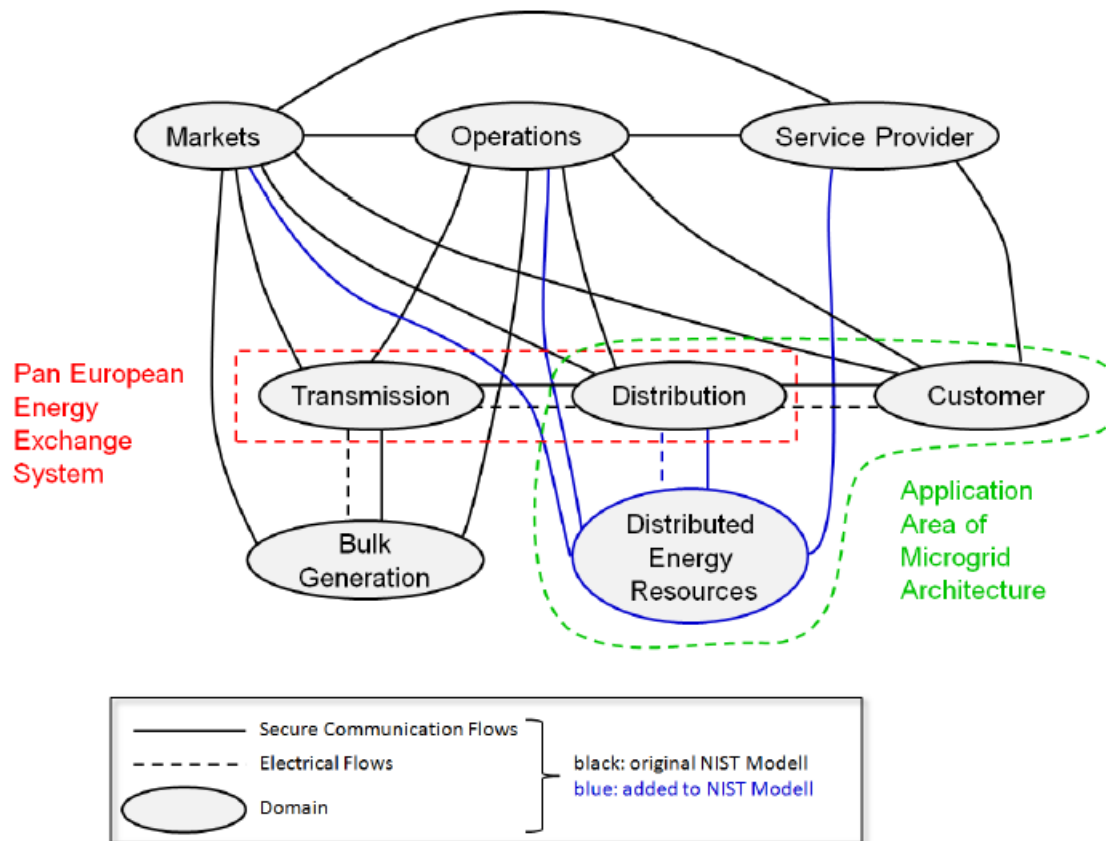
Apart from the requirements presented above, a RA is distinguished by some particular characteristics. First of all, the authorship of the RA should be attributed to the person/party responsible. Apart from this, any newly developed RA must be accompanied by a *recommendation*, aiming to transform the whole modelling process into a more user-friendly experience. Since the final choice will be made by the users, the RA's universality can satisfy only a portion of them, for the acceptance criteria will differ. Of course, the methodology provided should be tested through modelling a wide variety of UC, in order to identify any defects in its central structure.

Taking into account the aforementioned, it is quite obvious that the development of a new reference architecture framework presents quite a challenge. Nonetheless, continuous technological advancement in the micro-grid (MG) structure demands a more sophisticated architectural approach. Following the universal dominance of smart-grids (SG), the integration of ICT and market domain requires a multidimensional architectural structure so as to allow the participation of all stakeholders involved.

As stated earlier, the development of the European Conceptual Model (ECM) is based upon the NIST Smart Grid Conceptual Model (NIST-SG/CM). Referring briefly to the model structure, the NIST-SG/CM constitutes a framework in which seven different domains related to the function of a SG are identified (Bulk Generation, Transmission, Distribution, Customers, Operations, Markets and Service Providers). Beyond the distinction of these domains, communication and energy flows between them are presented.

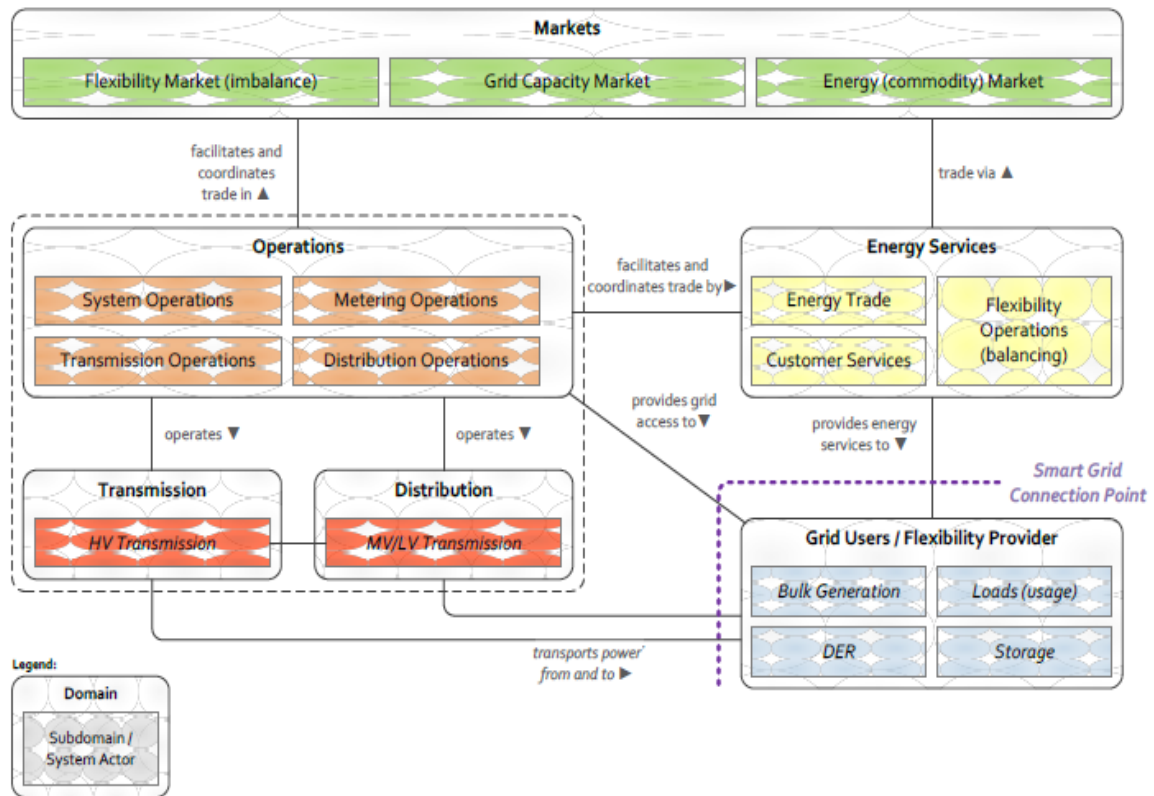
While the NIST-SG/CM should be considered as a very useful tool, describing many different domains of a SG entity, particular attention should be paid at distinguishing the Distributed Energy Resource from Bulk Generation and Customers domain, due to its economic and technical peculiarities. Taking into account that the role of a DER actor can change dynamically (prosumer), as well as the fact that

its operating voltage and control mechanisms differ from these of the actors' involved in the BG and Customer domain, the remodeling process of NIST-SG/CM is deemed necessary. Of course, some other aspects need to be adapted.



**Figure 1 - EU extension of the NIST Model**

As seen in (Figure 1) the EU extension of the NIST Model consists of different domains, with several connections between them in terms of communication and energy flows. In Figure 2 - European Conceptual Model for the Smart Grid (Figure 2) the European Conceptual Model for Smart Grids is presented.



**Figure 2 - European Conceptual Model for the Smart Grid [1]**

Four basic domains can be discriminated (Operations, Grid Users, Markets, Energy Services) each of them consisting of subdomains. While referring to the actors and functions involved in each of them, Operations and Grid Users address the more technical part of the system (that is the physical processes of generation and distribution of electricity and the ICT enabled actors). More specifically, the system, metering, transmission and distribution operations are included in the Operations domain, with the involved equipment also included (transformers, lines, etc.). As far as the Grid Users are concerned, the actors involved deal with the Bulk Generation, storage and consumption of electricity. As expected, the DER subdomain is encapsulated in the Grid Users domain.

Moving onto the other aspects of the system, the Energy Services and Markets domains deal with the transaction processes of the energy produced and the necessary services provided. The former domain involves the actors responsible for the total balance of the system (flexibility operations), in terms of electricity produced-consumed and economical exchanges involved. The latter includes the actors responsible for the actualization of the economical transactions (coordinated by the operations domain).

## 2.2 THE SMART GRID ARCHITECTURE MODEL FRAMEWORK

The Smart Grids Architecture Model (SGAM) framework can be described as the architectural structure of a practical methodology where each particular Use Case (UC) can be modelled and analyzed from different aspects. The most important factor while modelling a UC is the coherency of the whole process, as well as the production of an analytic and detailed object, where the role of each stakeholder is clearly defined. As far as the general presentation of a UC is concerned, three main categories interoperate between each other, while various Cross-cutting issues (referring to relationships between the categories) need to be taken into account.

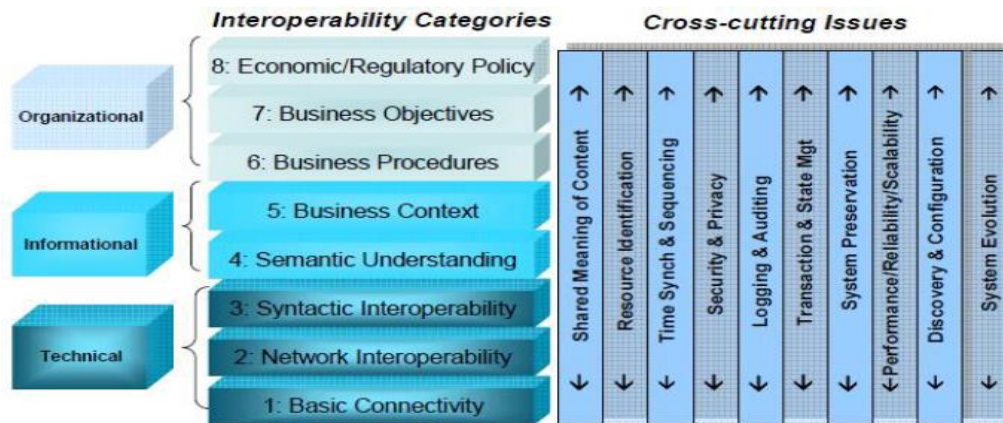


Figure 3 - Interoperability Categories and Cross Cutting Issues [1]

In the SGAM framework these interoperability categories are aggregated into five different levels, the **SGAM layers** Figure 4 - Interoperability Categories and layers . As can be seen, each layer refers to a different aspect of every UC, starting from the **Business layer** (referring to the business usage of the smart grid information exchanged, the involved market partners, business objectives, constraints, etc.), moving step by step to the **Component layer** (physical layer, including all entities of smart grid, such as the system equipment, the network infrastructure and the protection devices). Between these two, lie the **Function**, the **Information** and the **Communication layer**. These layers refer to the functions implemented (functionality of UC), the information object and data models exchanged between functions or actors (devices, applications, persons, organizations) and the protocols/mechanisms used for the exchange of information, respectively.

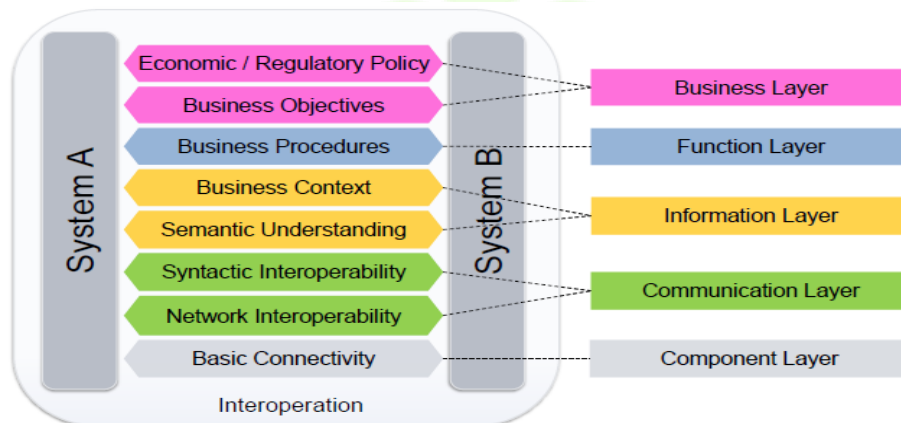


Figure 4 - Interoperability Categories and layers [1]

In succession, the interoperability layers need to be merged with another concept, the smart grid plane, to compose the 3D SGAM framework. In the smart grid plane, an important distinguish is made between the electrical processes (domains) and the information management viewpoints (zones) involved in every UC. The five SGAM domains contain the **Bulk Generation domain** (massive generation of electricity), the **Transmission domain** (infrastructure and organization for the transportation of energy), the **Distribution domain**, the **Distributed Electrical Resources domain** (DER connected to the public distribution grid ranging from 3 kW~10.000 kW) and the **Customer Premises domain** (prosumers of electricity).

Moving on to the six SGAM zones, these are distinguished as follows. The **Process zone** (refers to the transformation of energy and the equipment involved) is followed by the **Field zone** (protection, control and monitor equipment) which, in turn, is succeeded by the **Station zone** (areal aggregation



of previous level). Next comes the **Operation zone** (control operation systems such as DMS/EMS), followed by the **Enterprise zone** (commercial aspect/e.g. logistics, staff training, etc.) and finally the **Market zone** (commercialization of the produced energy).

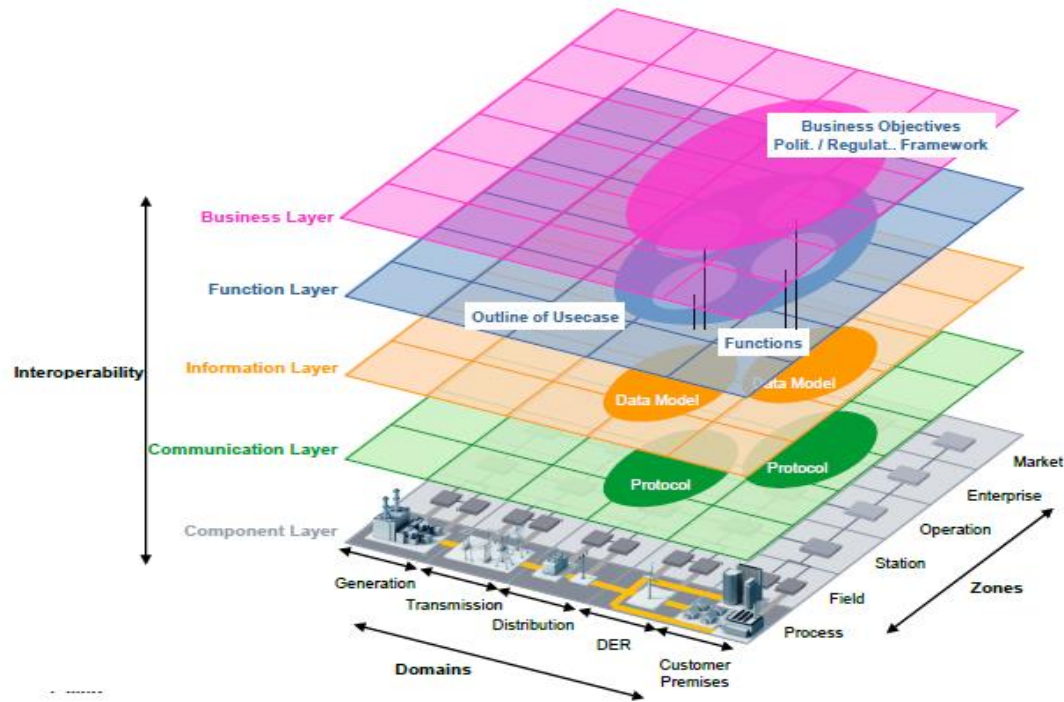


Figure 5 - The SGAM Framework [1]

The basic principles on which the SGAM modelling framework is based upon are universality, localization, consistency, flexibility, scalability, extensibility and interoperability. So, as far as flexibility is concerned, a UC can be analyzed in multiple different ways while many functions or services can be placed in different zones/domains. This feature does not come at the expense of the consistency of the model, since all layers, domains and zones must be specified. In the end the coherency of the final extracted model is guaranteed, since the five SGAM layers are linked and able to interact with each other, as shown in the above figure.

Moving on, the mapping process of every UC, begins with the analysis phase in which needs to be confirmed that the UC description provides the necessary information (objective, UC diagram, actor name and type, precondition and assumptions, steps, information exchanged and requirements). Once this phase is completed, one can proceed with the development of each SGAM layer.

Regarding the peculiarity of the business layer, its architecture must comply with a standard, so as the roles used in business interactions can be consistent. The Harmonized Electricity Market Role Model by ENTSO-E, EFET and ebIX [ENTSO-E] is proposed, since it can fit all European electricity markets. The HEM-RM of ENTSO-E, EFET and ebIX (freely downloadable at <http://www.ebix.org/content.aspx?ContentId=1117&SelectedMenu=8>) can be used for the definition of each business role. Increased attention is recommended during the transition from the business to lower layers. If this is performed correctly, each architectural element of lower layers can be mapped to the appropriate business role, making the most out of the available information. Should this not be the case, further specifications need to be provided.

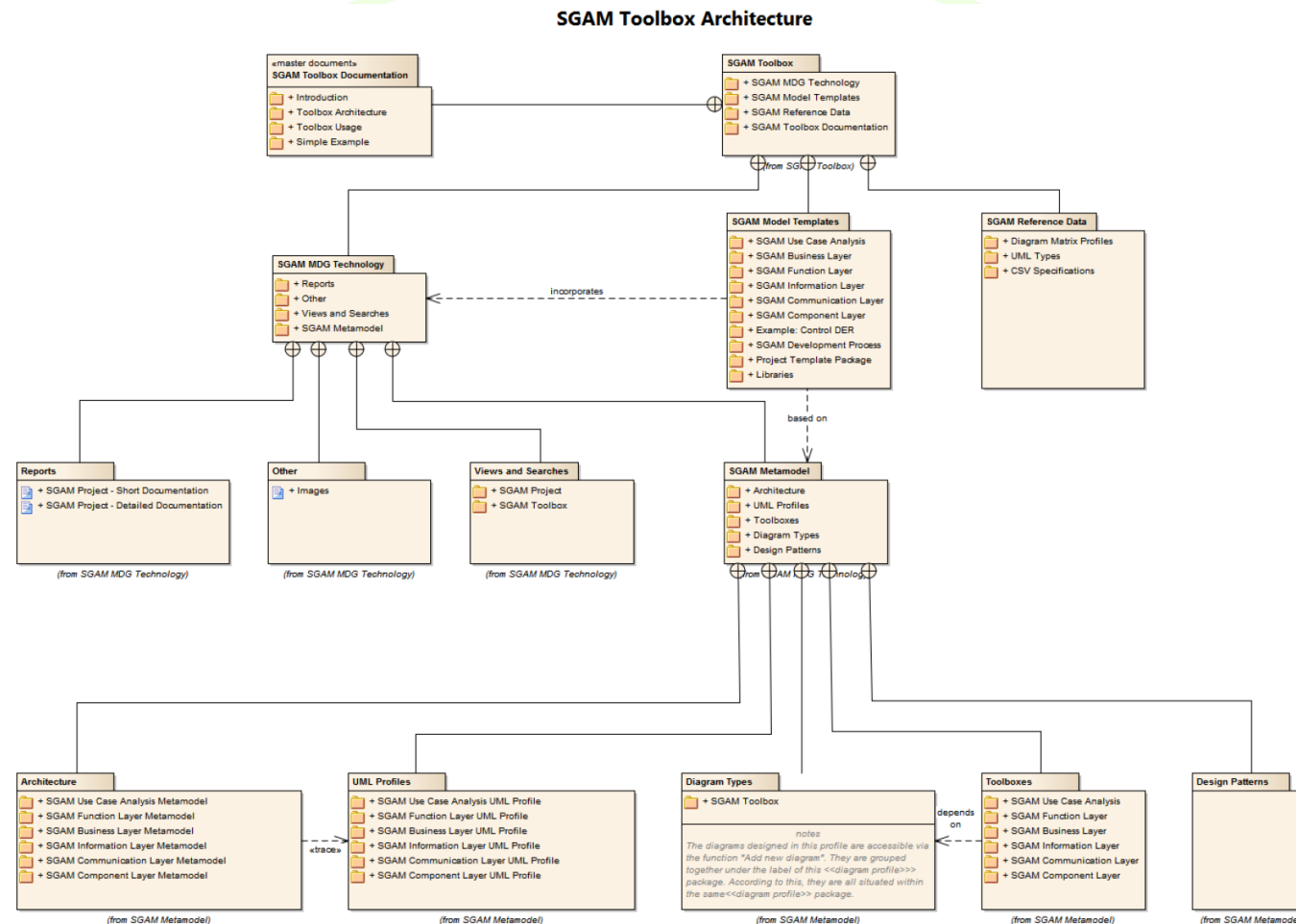
### 2.3 MODEL-DRIVEN ARCHITECTURE SPECIFICATION USING THE SGAM TOOLBOX

In order to proceed with the modelling process use cases, their incorporation into the SGAM Framework is necessary. This can be actualized by the use of the SGAM Toolbox, a caption of its basic architecture (V 0.2.0) being presented below.

As can be seen above, the most important element of the architecture constitutes the SGAM Metamodel, since it provides the necessary outputs such as the layer metamodels, Diagram types, Toolboxes and Design Patterns. The SGAM model templates (used to simplify the use of SGAM) are also based on the SGAM Metamodel. Regarding the description of the SGAM Metamodel, this is extracted from the SGAM MDG (Model Driven Generation) Technologies (i.e. files that allow users to extend Enterprise Architect's modelling capabilities to specific domains and notations. MDG Technologies seamlessly plug into Enterprise Architect to provide additional toolboxes, UML patterns, templates and other modelling resources. The last important component of the Toolbox architecture is the Reference Data, which provides information regarding the Model Import/Export, well as other important elements. In

Figure 8 the structure of the SGAM metamodel can be observed.





**Figure 6 - The SGAM Toolbox Architecture**

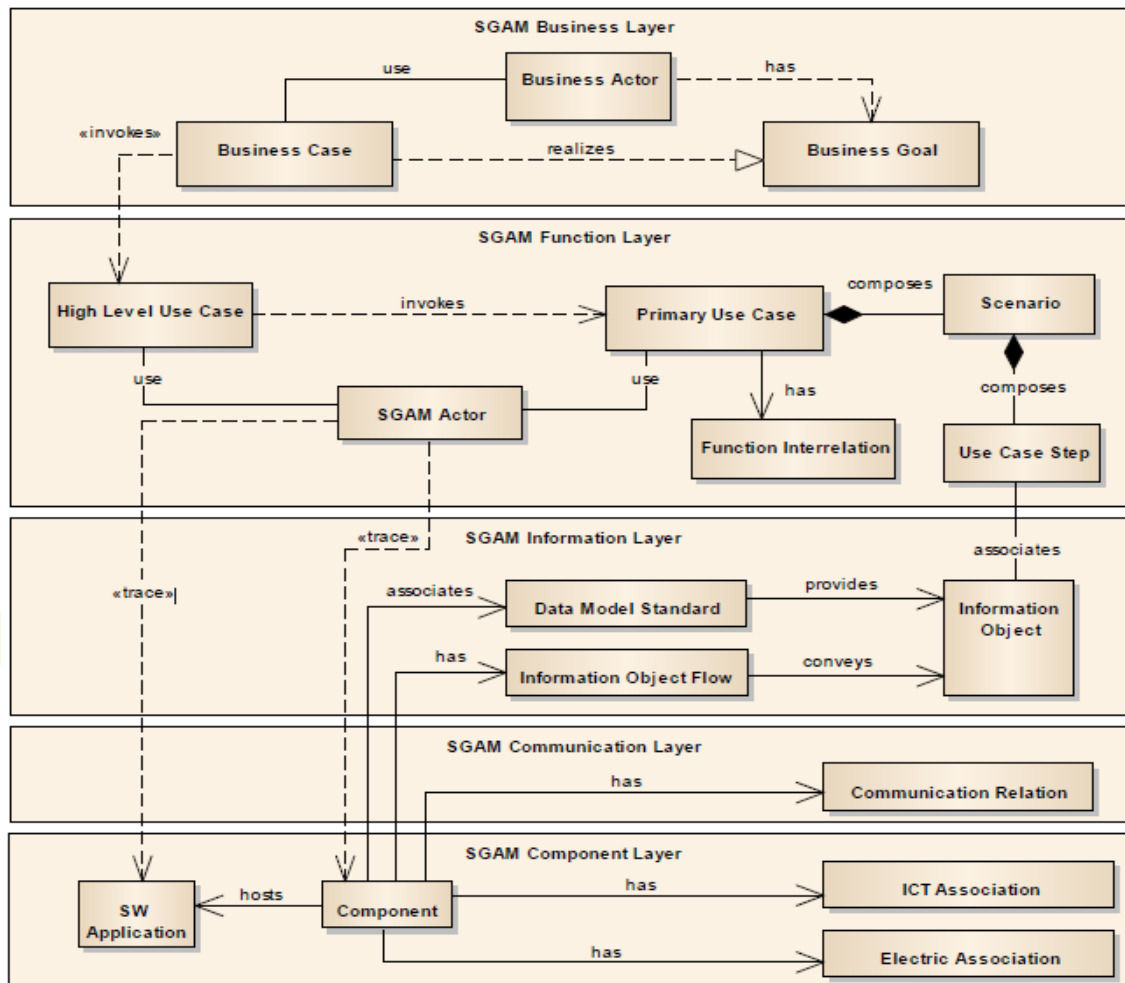


Figure 7 - The SGAM Metamodel [2]

Starting from top, a business actor needs to achieve a goal, while this is only possible through a business case (BC). Moving to the function layer, the High Level Use Case (HLUC), which provides a general description of an idea/requirement, uses the SGAM actors (devices, applications, persons or organizations), while invoking a Primary Use Case (PUC). PUCs are described by specific scenarios, and address the functionality aspect of a business process [3]. While not depicted in the diagram above, a PUC is composed by one or more Secondary Use Cases (SUC). In the information layer, the objects, demanded to compose the scenarios invoked for the description of PUCs (information objects) are defined through the Data Model Standards. These objects contain some type of information exchanged (e.g. a fault report) between actors. Finally, in the SGAM Component layer the components (electric device, software, cables, etc.) related to the ICT and electric domains are included. The communication between two or more components is based on various protocols, defined in the Communication Relation.

One last obstacle that needs to be overcome in order to be able to produce UC models, through the SGAM Toolbox, in accordance with the SGAM Framework is the accurate and detailed transformation of UCs into objects that possess distinct SGAM-based characteristics. In other words, the development/UC mapping process needs to be clearly defined.

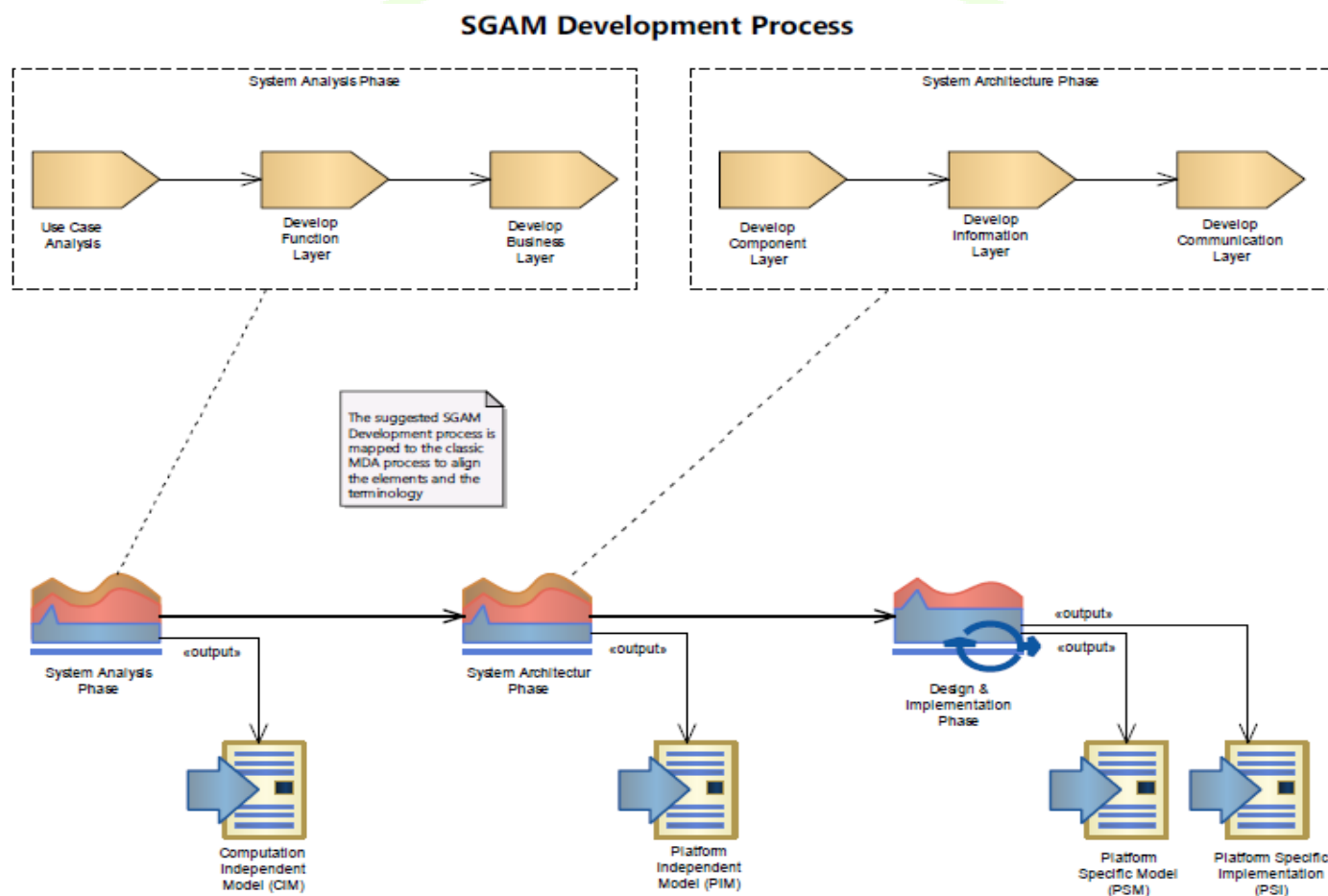


Figure 8 - SGAM Development Process [2]

As shown in the above figure, the process begins with the System Analysis Phase (SAP). During SAP, it needs to be confirmed that the UC description provides the necessary information (objective, UC diagram, actor name and type, precondition and assumptions, steps, information exchanged and requirements), so one can proceed with the development of each SGAM layer. In this phase, the development of the SGAM Function and Business layer is should be implemented so as the business actors/goals/cases can be defined. Next comes the System Architecture Phase where the development of the Component, Information and Communication layer is done. Finally, the Design and Development Phase referring to the realization of individual systems can be actualized by any classic system engineering method, as it does not need to be in compliance with the SGAM Framework. Nonetheless, this methodology is only a recommendation and slight deviations might be observed.

## 2.4 THE SMART GRID ARCHITECTURE CONCEPTS IN WISEGRID

Architecture can be described as the fundamental concepts or properties of a system in its environment embodied in its elements, relationships, and in the principles of its design and evolution [ISO/IEC42010]. The semantics of RA presented earlier (section 2.1) was incomplete, since the different architectural concepts describing the functionality of a SG were not given. Returning to this matter, the most important subject that needs to be addressed before examining the technical aspects of a SG, is the definition of a conceptual architecture framework which can present briefly the role of each stakeholder involved. Subsequently, a more thorough analysis of the functions implemented and the procedures followed in order to be in compliance with the requirements baseline (functional architecture), as well as the description of the related connectivity issues (communication architecture), are deemed necessary. Apart from this, the presence of an architecture field associated with the information exchanged between parties/actors (information architecture), is recommended.

In addition to the aforementioned architecture viewpoints, many more aspects of a SG must be diligently examined to ensure its smooth and efficient operation. Examining a SG from a technological point of view, it is obvious that the involved equipment, as well as the communication between the devices deployed, consist a subject of major importance and many different aspects must be considered (engineering viewpoint, technology architecture viewpoint, computational viewpoint). On the other hand, a SG constitutes an economical entity, and should be studied as such. In other words, the enterprise/business architecture viewpoint should also be addressed properly. As in most modelling tools/frameworks, a compromise must be reached between the detailed description of an entity (each SG sector) and the reduction of complexity of the overall modelling process. In this case, a simple way to achieve this enterprise is the merging of some of the aforementioned architecture concepts into a more general context. Considering the Joint Working Group for Standards for the Smart Grids (JWG-SG 2011) recommendations, the different aspects of SG can be represented through the following architecture concepts.

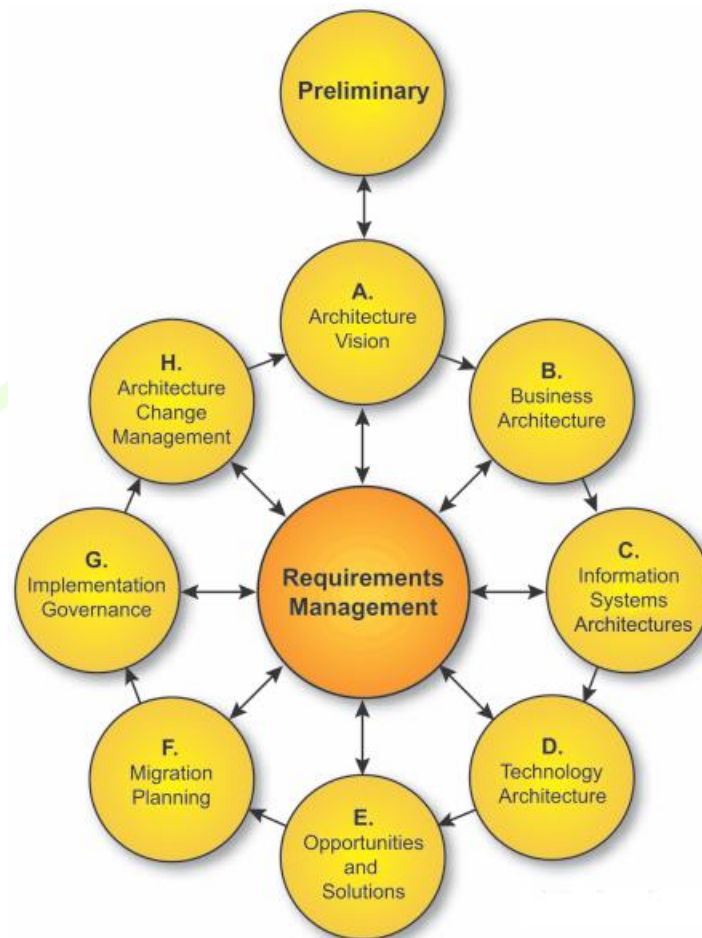
- **Business Architecture:** Describes the business models/processes accepted.
- **Functional Architecture:** Deals with the functional characteristics of SG.
- **Information Architecture:** Refers to the data modelling and interfaces applicable in SGAM model.
- **Communication Architecture:** This architecture concept is responsible for the elimination of any communication standard gaps.

These architecture concepts/layers will be further analyzed in the following chapters.

## 2.5 RELATION OF WISEGRID MODELLING CONCEPTS WITH OTHER PROJECTS

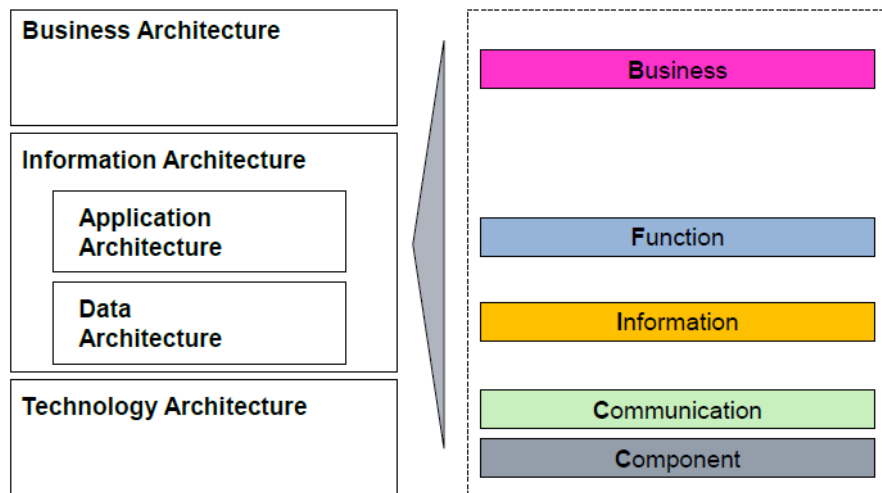
The WiseGRID Modeling Concepts (SGAM Framework/Conceptual Model/Reference Architecture) are derived as the outflow of the combination of many different standards, as well as their extensions. As a result, many of the existing Meta-Models can be mapped into the SGAM model, offering great flexibility and reliability of the total UC modeling process. Of course, all procedures must be actualized in compliance with the European specificities. Especially, as far as the SGAM Framework development is concerned, many aspects defined in the past are taken into account, while much of the classification/categorization of existing Meta-Models is extracted by the First Set of Standards Work Group (FSSWG).

The architecture conceptualization (AC) process was not performed anew, but was based on the ISO/IEC 42010: Systems Engineering - Architecture description. Unfortunately, the transition to a modernized, smarter version of MG has added a lot of complexity in the transition process from the AC meta-model in a clearly defined architectural framework. In other words, while a description of the different sectors where a SG functionality is extended can be easily illustrated, the exact assignment of the individual functions performed, the description of the actors' involved behavior as well as the interaction processes involved, constitute an issue of increased complexity. To overcome this obstacle, an encapsulation of existing architecture development methods (e.g. TOGAF) and Architecture Description Language (ADL) compliant with the ISO/IEC 42010:2007 (e.g. ArchiMate) is considered mandatory.



**Figure 9 - TOGAF ADM Model [1]**

The TOGAF Architecture Development Method (ADM) describes the basic characteristics of an architecture. TOGAF is able to present the different architecture viewpoints, providing also the capability of pointing out the stakeholders' main concerns (Figure 9). This concludes the utility aspects of TOGAF ADM as the detailed description of each concern must be carried out by an ADL. The ArchiMate language is capable of coping with this demand. In fact, it is considered as the ideal option, since it is already used to describe the structure of the ArchiMate Framework, which shares many mutual viewpoints with TOGAF. In (Figure 10) the ArchiMate representation of the architectural viewpoints, as well as the mapping of GridWise Interoperability Context-Setting Framework (March 2008) - (GWAC2008) into ArchiMate can be observed, revealing the application of existing methodologies in conjunction with the SGAM.



**Figure 10 - Archimate representation of the architectural viewpoints and Mapping of GWAC dimensions onto Archimate [1]**

To conclude the first chapter, the alignment of WiseGRID modelling concepts with existing processes/concepts/role models is presented.

- **Alignment with EU flexibility concept:** The EU flexibility concept is closely related to the prosumers subjected into the DER domain of a SG (smart customers). Since the dynamical role exchange of these actors can be actualized (producer to consumer and vice versa), the system is quite flexible in terms of electricity generation, storage and consumption. Of course, this attribute is extended to the technical and commercial aspects of a SG. In the EU Conceptual Model, presented in section 2.1, the smart behavior of the prosumers is reflected into the Grid Users domain. The Flexibility operator (reflected into the service providers' domain) can act as the Resource Provider, Balance Responsible Party, Balance Supplier or the Grid Access Provider. In the market domain, flexibility concept is also addressed by service providers.
- **Alignment with Harmonized Electricity Market Role Model:** While the HEM-RM is picked up for use, new roles might need to be defined.
- **Alignment with SG-CG/SP on Sustainable Processes:** The existing standards identified by the SGAM framework, must be based on the deliverables extracted from the SG-CG/SP WorkGroup on Sustainable Processes. These deliverables refer to the Technical Requirements, the Actors, the Identification and Interaction between them, as well as the procedures involved.
- **Alignment with NIST, SGIP, SGAC:** Due to the fundamental differences between US and EU market models, the outcome of the modeling process must follow specific standards so as not to volatile the interoperability principle. The conceptual models may also differ.
- **Alignment with EU market model developments (EG3):** Refers to the extension of the interactions between the actors involved, into interactions between roles, so that the interactions between market parties can be defined. It is essential that the roles and responsibilities of market parties can be mapped into the HEM-RM roles, in order to clarify the interface standards and business services required.



### 3 SGAM GOALS AND OBJECTIVES

In this section a thorough examination of the business layer, business actors (BAs), business goals (BGs) and business cases (BCs) concepts related to the SGAM framework has been carried out. A brief description of the BCs modeling process is also presented.

#### 3.1 SGAM BUSINESS LAYER OVERVIEW

The business layer can be characterized as the most peculiar layer of the SGAM Framework. While being atop the other four layers, this is where the information provided by each HLUC is combined, into producing the final Business Cases. Because of the significance of the business aspect of every UC function, it is really important for the UC mapping process to be executed carefully. After all, the scope of ICT solutions is the support of the business procedures. Of course, as can be seen below, the objectives and constraints of every UC need to be taken into account.

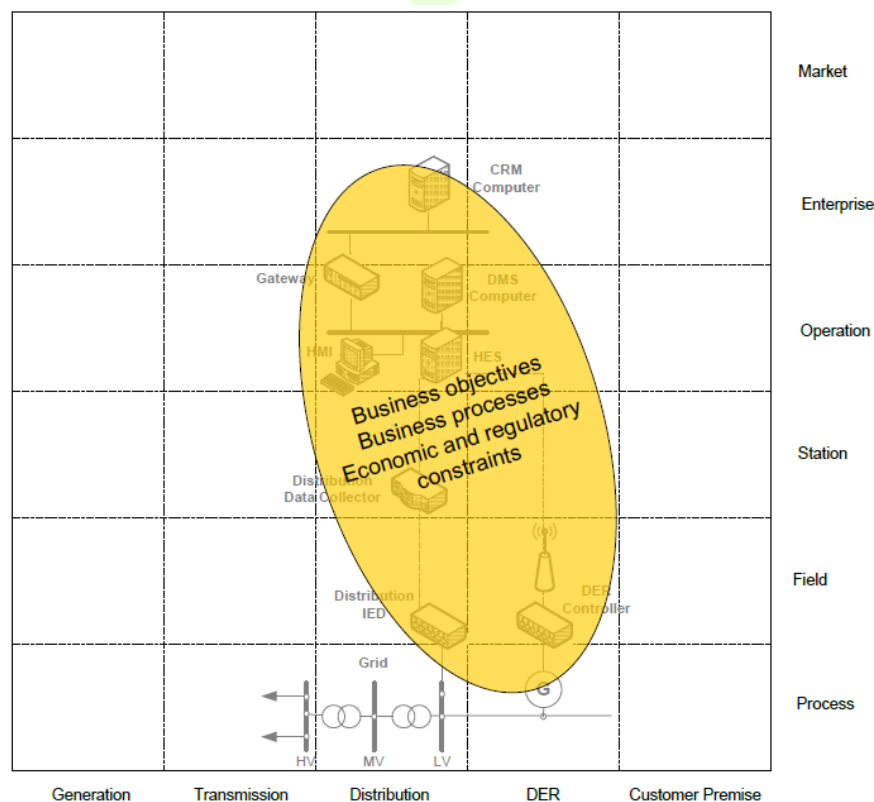


Figure 11 - Business Layer «Control reactive power of DER unit» [1]

In the business layer, every entity is located into the appropriate domains and zones, contributing to the detailed description of each market actor, as well as the economic structures and policies of the parties involved. It should be noted that good interoperability between different market and business models is addressed by the M/490 mandate. As a result, the development of a flexible meta-model (TOGAF 9.1), capable of interpreting the multiple roles of the organizations and architecture aspects involved was considered mandatory. Its depiction, as well as its correspondence with the SGAM Framework is given in Figure 11. As can be observed, the business architecture layer involves business

organizations (parties), actors, roles, functions, processes and services, as well as the interactions between them.

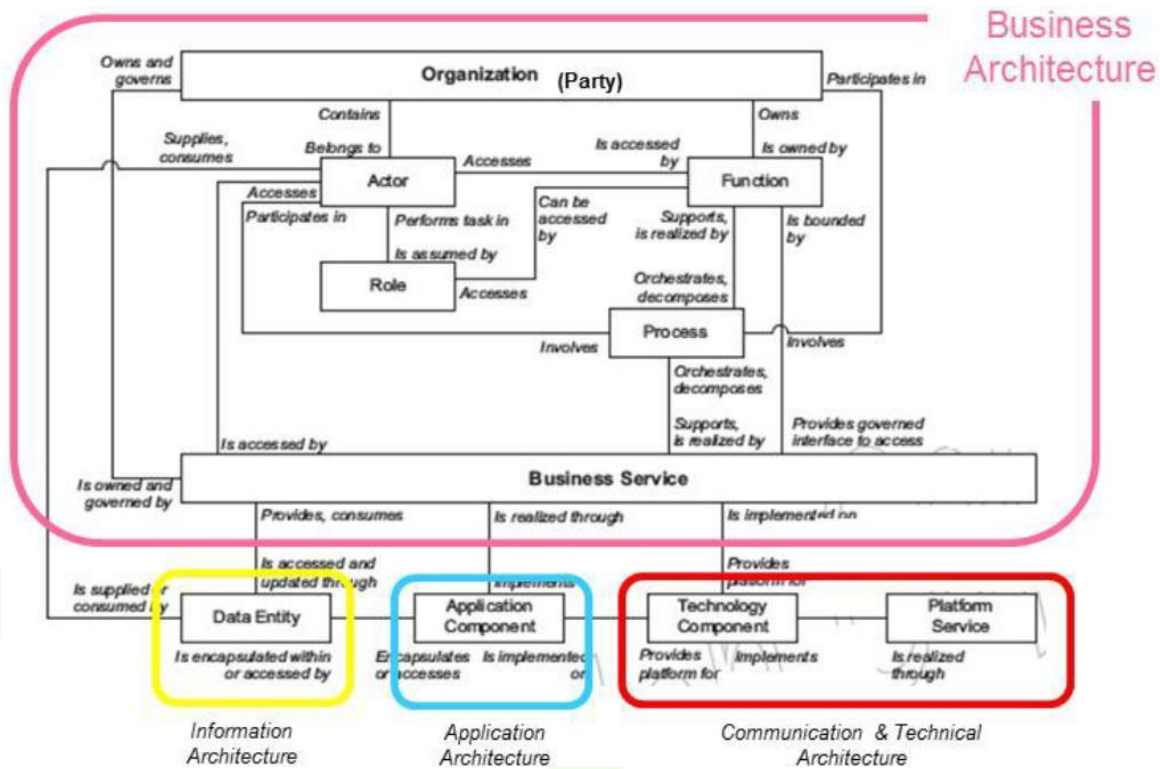


Figure 12 - Relation Meta-Model to SGAM [1]

An organization contains business actors that perform tasks in roles and accesses the business functions (BF). The role of BFs is the delivery of business capabilities, closely related to an organization (TOGAF 9.1). Every function is supported by processes and bounded by business services (BS), where some of the organizations are involved. A BS is in fact a piece of information exchanged between market parties. However, in order for the exchangeable information to be characterized as BS, the involved actors must be represented by applications and the procedure should be completed through application interfaces, crossing the boundaries between different market parties. By prioritizing the BSs between regulated and unregulated environments, the Smart Market concept can be promoted. As seems reasonable, associations between BSs and business products do exist. Summarizing the utility of Business Processes, they are responsible for the orchestration of the BFs as well as the realization of BSs, involving the participation of different actors/parties. They also provide input for the function and information architectures.

The interconnection of the business layer to lower SGAM layers can be a somewhat complex matter. The total procedure should be performed with particular attention, in order to avoid the loss of information exchanged. At first, the market model, as well as the roles of the actors involved, need to be defined (based on the HEM-RM and EG3). Secondly, the business services must be described through the utilization of the information handled. After these two steps have been completed, the necessary inputs are available, allowing the mapping of business roles into elements of the lower SGAM layers. Should this not be the case, further investigation needs to be performed.

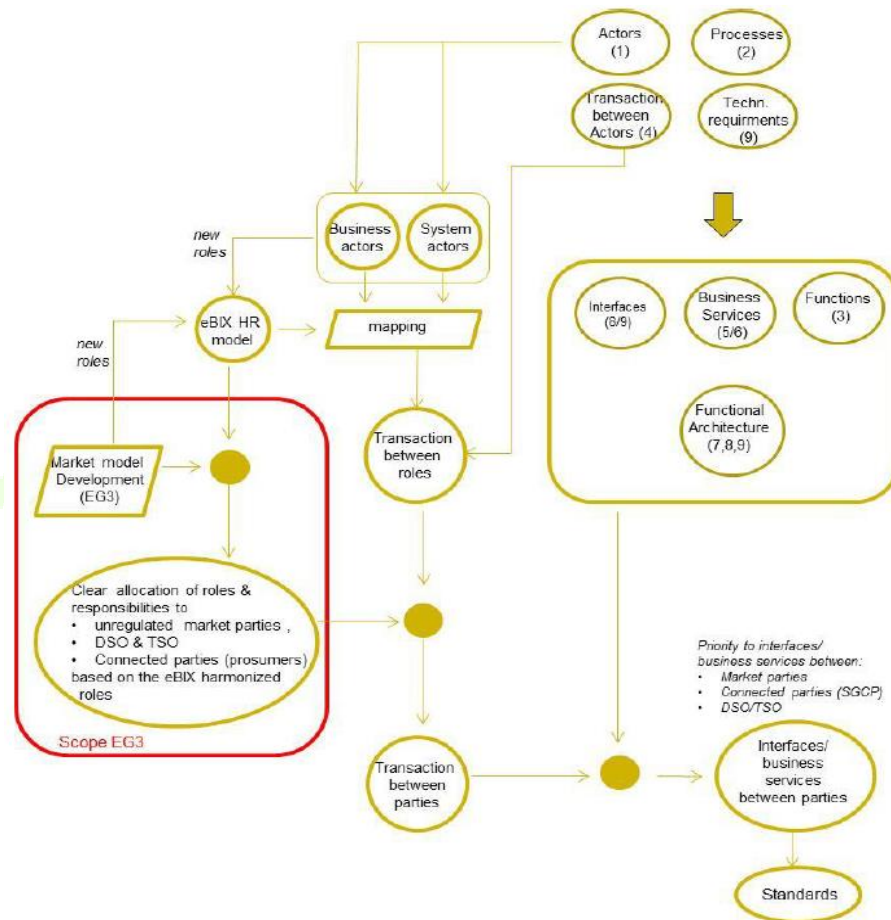


Figure 13 - Alignment process between market model developments and ICT architecture [1]

### 3.2 SGAM BUSINESS ACTOR ANALYSIS

The term **actor** may refer to any of the entities associated with the technical and economical aspect of a SG function (people, devices, management systems etc.). In general, two categories of actors can be distinguished (IEC TC8):

- **System Actors:** This category involves the devices or systems, which perform a task under a specific role.
- **Business Actors:** Here an actor may specify a "Role", as roles are specified according to the eBIX HEM-RM. New roles may be added.

From another perspective, an actor is actually the representative of a party, in a business transaction. Each party is defined as a legal entity performing one or more roles (NIST 2009). In order to express the interests of each party involved, a brief presentation of the most important business roles as defined from [ENTSO-E 2011] is considered necessary.

- **Balance Responsible Party/BRP:** Party responsible for providing financial security and identifying a party's capability to operate in the market.
- **Balance Supplier:** Party responsible for the financial transactions regarding the difference between energy bought and consumed.
- **Billing Agent:** Takes care of the billing processes of a party.

- **Block Energy Trader:** Seller/Buyer of energy.
- **Capacity Coordinator:** Party responsible for the establishment of a standard offered capacity
- **Capacity Trader:** Party participating in capacity market.
- **Consumer**
- **Consumption Responsible Party:** Regulates the imbalances between energy nominated and energy consumed.
- **Market Information Aggregator:** Party providing information relevant to the energy market.
- **Market Operator:** Determines the market energy price in coordination with the System Operator.
- **Party Connected to the Grid**
- **Producer**
- **Production Responsible Party:** A type of Balance Responsible Party accountable for the imbalances between energy nominated and energy produced.
- **Reconciliation Accountable:** Party financially responsible for the reconciled volume of energy products for an Accounting Point.
- **Reconciliation Responsible:** Party responsible for the regulation of the imbalance settlement process for profiled Accounting Points.
- **Reserve Allocator:** A party that informs the market of reserve requirements, also being responsible for the reception and assignment of tenders.
- **Scheduling Coordinator:** Party responsible for information exchanges on behalf of a BRP.
- **System Operator:** Probably the most important role in the list. The System Operator party has many responsibilities, such as the stable power system operation, the regulation of cross border capacity and exchanges as well as additional obligations imposed by the local markets.
- **Trade Responsible Party:** Is a type of Balance Responsible Party that deals with the imbalances between energy nominated and consumed for the associated Accounting Points.
- **Transmission Capacity Allocator:** Allocates transmission capacity for an Allocated Capacity Area, in consultation with the market and individual capacity traders.

Of course, some of the roles mentioned above can extend to more than one SGAM layers, while also referring to different domains (grid operator/access provider, meter administrator party etc.). These roles can be, and usually are, performed by number of different actors. As far as business actors are concerned, the following entities can be distinguished:

- **Producer/Consumer:** Actors responsible for the production/consumption of electricity
- **Prosumer:** This business actor may produce or consume electricity, while the dynamic exchange of its role is possible. The presence of a big number of prosumers reinforces the flexibility of the SG. The Active-Demand and supply (ADS) role is realized through this category.
- **Supplier:** Actor responsible to supply and invoice energy of its customers, while being in consultation with the prosumers, in order to maximize the flexibility potential of the system.

- **Balance Responsible Party (BRP):** In addition to the definition presented earlier, a BRP aims at finding the most economical solution for the requested energy to be supplied, by maintaining the balances between energy produced/consumed.
- **Transmission System Operator (TSO):** Deals with the transportation of energy from producers to the distribution grid operators.
- **Distribution System Operator (DSO):** Actor responsible for the cost-effective distribution of the transported energy, as well as the connection with the transmission grid.
- **Energy Service Company (ESCO):** Offers a plurality of services to the prosumers (information/notification or energy management services)
- **Retailer:** A very important business actor. A retailer invoices energy consumption from consumers and manages the financial interactions between the other business actors (DSO, Aggregator, Prosumer).
- **Aggregator:** Acts as the intermediate between the Prosumers/ADS and the BRP/DSO. Through the aggregator the flexibility offered by the prosumers is transferred to the BRPs. This actor's main target is the maximization of system flexibility, through the exploitation economic and technological information available.

### 3.3 WISEGRID ACTORS

As mentioned above, every business actor must achieve a goal, related to a business transaction. While a close correlation between the goals to be achieved and the role that an actor undertakes exists, the majority of actors aim at the achievement of a multiple number of goals. For example, while a prosumer wants to minimize the energy bills, the minimization of emissions produced, is also to his benefit. As a more general business goal, the optimization of the energy that is produced/consumed could be considered. A presentation of the actors that we are considering in WiseGRID is listed below.

Table 1 - WiseGRID Actors

Actor name	Description	Actor type
Aggregator	Accumulates flexibility from Prosumers and Consumers and sells it to the Supplier, the DSO or the TSO.	Organization
AMI	<i>Advanced Metering Infrastructure.</i> A set of systems that monitor, collect and analyze electricity consumption, and have two-way communication capabilities.	System
Balance Responsible Party	A party that has a contract proving financial security and identifying balance responsibility with the Market Operator entitling the party to operate in the market. [The meaning of the word "balance" in this context signifies that the quantity contracted to provide or to consume must be equal to the quantity really provided or consumed.]	Organization
Battery Operator	An entity responsible for operating a set of Storage Units connected to the electricity grid.	Organization

Actor name	Description	Actor type
Building Management System	An automated system that monitors and controls the equipment of a building (ventilation, lighting, electricity infrastructure, etc.)	System
CHP	<i>Combined Heat and Power</i> . A system that simultaneously generates electricity and useful thermal energy in one process from a single source of energy.	Device
Consumer	An entity connected to the grid, which consumes energy, i.e. a Prosumer without any production capabilities.	Person
Data Provider	Independent entity responsible for undertaking and coordinating the information exchange and translation of the data of various sources into a common data model.	Organization
Distributed Energy Resource	Any type of generation units, storage units and load flexibility resources connected to the distribution network.	System
DMS	<i>Distribution Management System</i> . A system that monitors, controls and analyzes in real-time or near real-time the electricity distribution system.	System
DSO	<i>Distribution System Operator</i> . The entity responsible for: the distribution network planning and development; the safe and secure operation and management of the distribution system; for data management associated with the use of the distribution system; for procurement of flexibility services.	Organization
Electronic Meter	A physical device containing one or more registers.	Device
Energy Management System	A system that monitors, controls and optimizes the operation of the energy system under supervision.	System
ERP	<i>Enterprise Resource Planning</i> . A system that offers integrated management and automation of business processes. It is also used to refer to the Customer Relationship Management (CRM) system.	System
ESCO	<i>Energy Service Company</i> . Offers auxiliary energy-related services to Prosumers.	Organization
EV	<i>Electric Vehicle</i> . A vehicle that uses stored electricity as a source of energy.	Device
EV Fleet Manager	<i>Electric Vehicle Fleet Manager</i> . An organization that operates and controls an EV fleet.	Organization
EV User	<i>Electric Vehicle User</i> . The user of an EV.	Person
EVSE	<i>Electric Vehicle Supply Equipment</i> . The infrastructure external to the EV that provides connection to a power source for charging the EV.	Device
EVSE Operator	<i>Electric Vehicle Supply Equipment Operator</i> . The entity responsible for managing and operating the EV charging infrastructure.	Organization
Facility Manager	An entity responsible for the management of one or more buildings or other facilities in general.	Organization



Actor name	Description	Actor type
Forecast Provider	The organization that provides, upon demand, forecasts regarding certain variables (e.g. electricity demand, RES production, weather conditions, etc.)	Organization
Gas Distribution Company	The organization responsible for the distribution of natural gas to final consumers.	Organization
Gas Meter	A device that measures and records the amount of gas (natural gas) consumed in residential, commercial, and industrial buildings.	Device
GIS	<i>Geographical Information System.</i>	System
Harbour Operator	An organization that manages and operates the harbour infrastructure.	Organization
HVAC	<i>Heating, ventilation and air conditioning.</i> An HVAC system maintains desired environmental conditions in a space.	System
Inverter	A power electronic device that converts DC electricity to AC and vice versa.	Device
Load Controller	A device that communicates with on-site electricity loads and has capabilities of sending control signals for increasing/decreasing the electricity demand.	Device
Market Operator	The unique power exchange of trades for the actual delivery of energy that receives the bids from the Balance Responsible Parties that have a contract to bid. Determines the market energy price taking into account the technical constraints from the Transmission System Operator.	Organization
P2G Unit	<i>Power to Gas Unit.</i> A unit that converts electrical power to a gas fuel.	Device
PDC	<i>Phasor Data Concentrator.</i> Receives and time-synchronizes phasor data from multiple phasor measurement units (PMUs) to produce a real-time, time-aligned output data stream.	Device
Producer	An entity connected to the grid that injects electricity to the grid.	Person
Prosumer	An entity that consumes and produces energy. There is no distinction between residential end-users, small and medium-sized enterprises or industrial users.	Person
Public Authority	Governmental organization that administrates the public life on the level of a municipality.	Organization
RES Unit	<i>Renewable Energy Source Unit.</i> A type of Producer that transforms energy from renewable energy sources (e.g. sun, wind, etc.) to electricity and injects it to the grid.	Device
RESCO	An ESCO that delivers energy to Consumers from renewable energy sources. (Not to be confused with WG RESCO)	Organization
SCADA	<i>Supervisory Control And Data Acquisition system</i>	Device



Actor name	Description	Actor type
Sensor	A device that monitors and processes specific input from the physical environment (e.g. light, heat, motion, etc.).	Device
Smart Meter	An Electronic Meter with two-way communication capabilities.	Device
Storage Unit	A device that stores energy.	Device
Supplier	Supplies and invoices energy to its customers.	Organization
TSO	<i>Transmission System Operator.</i> A party that is responsible for a stable power system operation (including the organisation of physical balance) through a transmission grid in a geographical area. The System Operator will also determine and be responsible for cross border capacity and exchanges. If necessary, he may reduce allocated capacity to ensure operational stability.	Organization
VPP Component	<i>Virtual Power Plant Component.</i>	Device
VPP Operator	<i>Virtual Power Plant Operator.</i>	Organization

## 4 GENERAL WISEGRID ARCHITECTURE SPECIFICATION

The WiseGRID general architecture specification is presented in this section. In subsection 4.1 the architecture mainly associated with the conceptual model, the RA and the overall concept of the SGAM Framework are included. Subsequently, a description of the SGAM different layers' architecture, as well as the interoperability principles adhered to is provided.

### 4.1 WISEGRID ARCHITECTURE PRINCIPLES

The WiseGRID general (Reference) architecture is mainly based on already existing standards. As noted in section 2.5, many of these «standards» (NIST SGCM, GWAC2008, ISO/IEC42010, TOGAF, ArchiMate, GridWise, ebIX and others) are developed upon specific architectural principles, which are also met in the WiseGRID architecture. However, the constant decentralization of the Electrical Grid, in addition to the transition to a more sophisticated form (Smart Grid), with the ICT domain clearly present, has imposed a lot of new principles that need to be addressed so that all different levels of decentralization of the system can be taken under consideration.

The most important principle that must not be breached by any means while developing an architectural model is that of the **interoperability** (i.e. the meeting of the necessary conditions that enable the interaction) between the different architectural levels (layers) included. In Figure 6 the Smart Grid functionality categories that need to address the interoperability principle are presented. As mentioned before, these categories are mapped into the five SGAM layers.

**Universality** is also really important when describing the multiple aspects of a SG, as the final models produced should be accessible by many different architecture frameworks. However, **localization** should also be respected, as all SG entities must be placed in the appropriate domains/zones/layers, in order to provide a systematic view of the UC to be mapped. This way, the principles of **consistency** (i.e. the clear connection of SGAM layers) and **scalability** (i.e. the possibility of viewing the grid from a top level, as well as a close view) are also reinforced. As far as the evolution of the Smart Grids is concerned, the **extensibility** of layers, domains and zones of the SGAM Framework might need to be developed in the future.

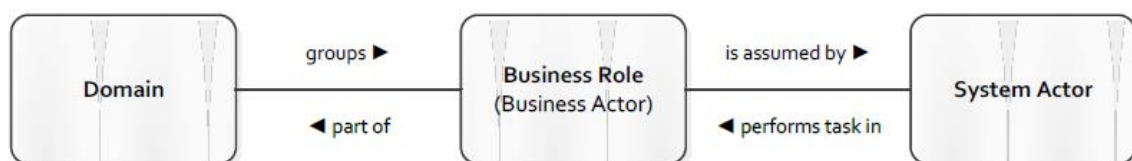
Most importantly, the **flexibility** principle should be adhered to. While supporting some of the previously mentioned characteristics (extensibility, scalability) of an architectural model, flexibility also provides alternative designs of UCs, while allowing a more thorough examination of all associated important issues. In order to comply with this principle, the different mapping of all UCs, functions and services should be allowed, especially as far as the information and communication layers are concerned. This process must also be independent of the SGAM zone-allocation process. Additionally, the nesting capability of functions/services in different components involved in individual UCs is desirable.



**Figure 14 - Flexibility Concept (result of WGSP) [1]**

In Figure 14, a depiction of the general flexibility concept, in respect to the technical and commercial operations of a SG, is presented. As can be seen, the Smart Grid Connection Point (SGCP) constitutes a common hub, where all flexible parties (in terms of electricity generation, consumption and storage) are connected. It is here that, commercial and technical flexibilities related to the market (e.g. pricing) and grid operations (e.g. information exchange) are identified.

Moving onto the principles associated with the development of the EU Conceptual Model, five important issues must be dealt with. First of all, the general philosophy of the extended NIST conceptual model, as far as business roles are concerned, (being part of the different domains and performed by the system actors/Figure 15) must be preserved. Additionally, alignment with the European electricity market is mandatory, since the definition of business roles is based on the European Harmonized Electricity Market Role Model.



**Figure 15 - Meta-model for the European conceptual model for Smart Grids [1]**

Apart from the aforementioned, the mapping of fully centralized/distributed and hybrid power systems must be supported, not only as far as the electrical energy produced is concerned, but grid infrastructure must be considered as well. Meeting this requirement is essential, because of the constant transition of electrical power systems from the traditional centralized to a more decentralized form (Figure 16). Finally, the Conceptual model should be able to describe the functionality of a power system both from a microgrid and a Pan European Energy Exchange System (dealing with the energy balance between different regions) perspective. While optimizing each power system function through a microgrid perspective is quite common, a more large-scale approach is necessary, so that the transport, generation and distribution systems, as well as the relations between them, can be studied as a whole.

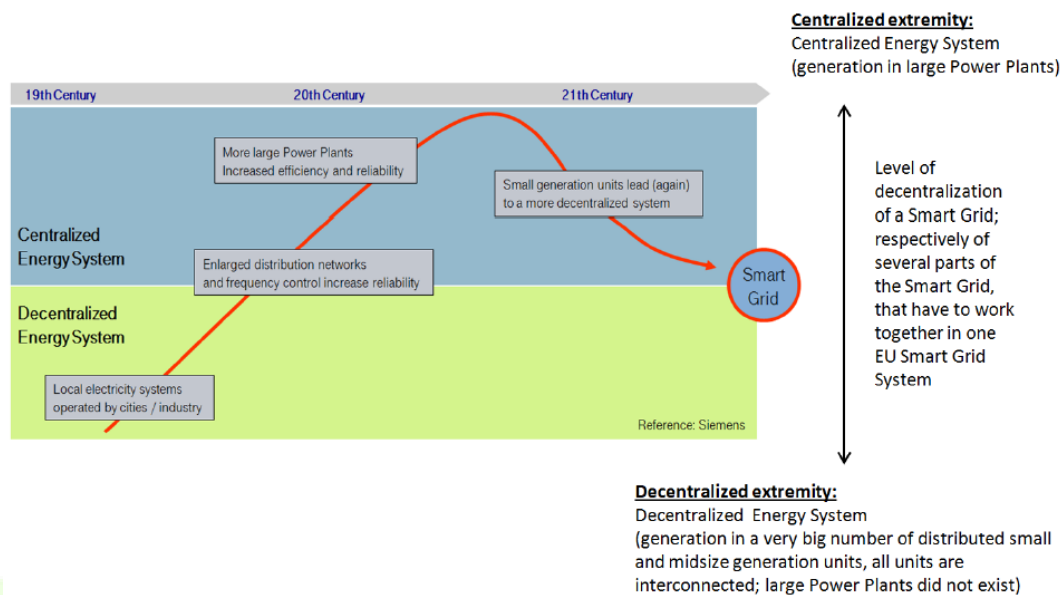


Figure 16 - Evolution of centralized/decentralized power systems deployments [1]

## 4.2 WISEGRID SGAM FUNCTION LAYER

The SGAM Function Layer is a way to incorporate the Functional Architecture (FA) viewpoint into the Smart Grid Use Case modelling process. The FA does not deal with the physical implementation of the SG elements, the technological aspects, or the actors involved, but with the description of the functions implemented. In Figure 17 the functional architecture meta-model is depicted, where the **Interactions** (realized by the information exchanged) between different **Functions** (logical entities performing a dedicated function) can be observed. The functions may (or may not) be part of a Function Group (logical aggregation of one or more functions or FGs).

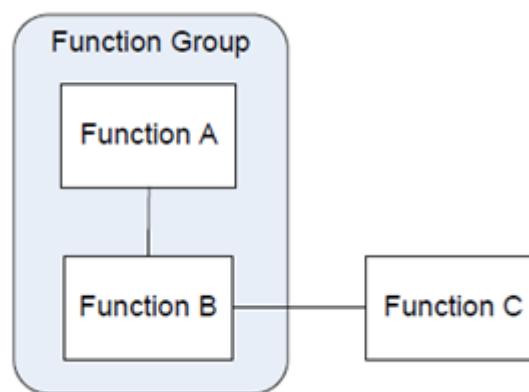


Figure 17 - Functional Architecture meta-model [1]

Summarizing the utility aspect of the Function Layer, this is where each HLUC functionality is described. Functionality is then translated into separate functions, interrelated between each other, which are placed in the appropriate domains and zones. As mentioned earlier, a HLUC consists of several Primary UCs (PUCs). In this layer the location of each PUC, as well as the actors involved in a HLUC, are described. Also, it should be noted that every HLUC model demands the development of a different function layer.

The creation process of the Function layer is quite simple and involves the arrangement of all PUCs and Actors, associated with a particular HLUC, to the corresponding domains and zones. More specifically, the first step involves the identification of different actors involved into the HLUC. The UC is then placed into the appropriate sectors of the SGAM model and transformed into a utility graph. In this graph the information exchanged between actors is highlighted. The final result should be somewhat similar to the one depicted below.

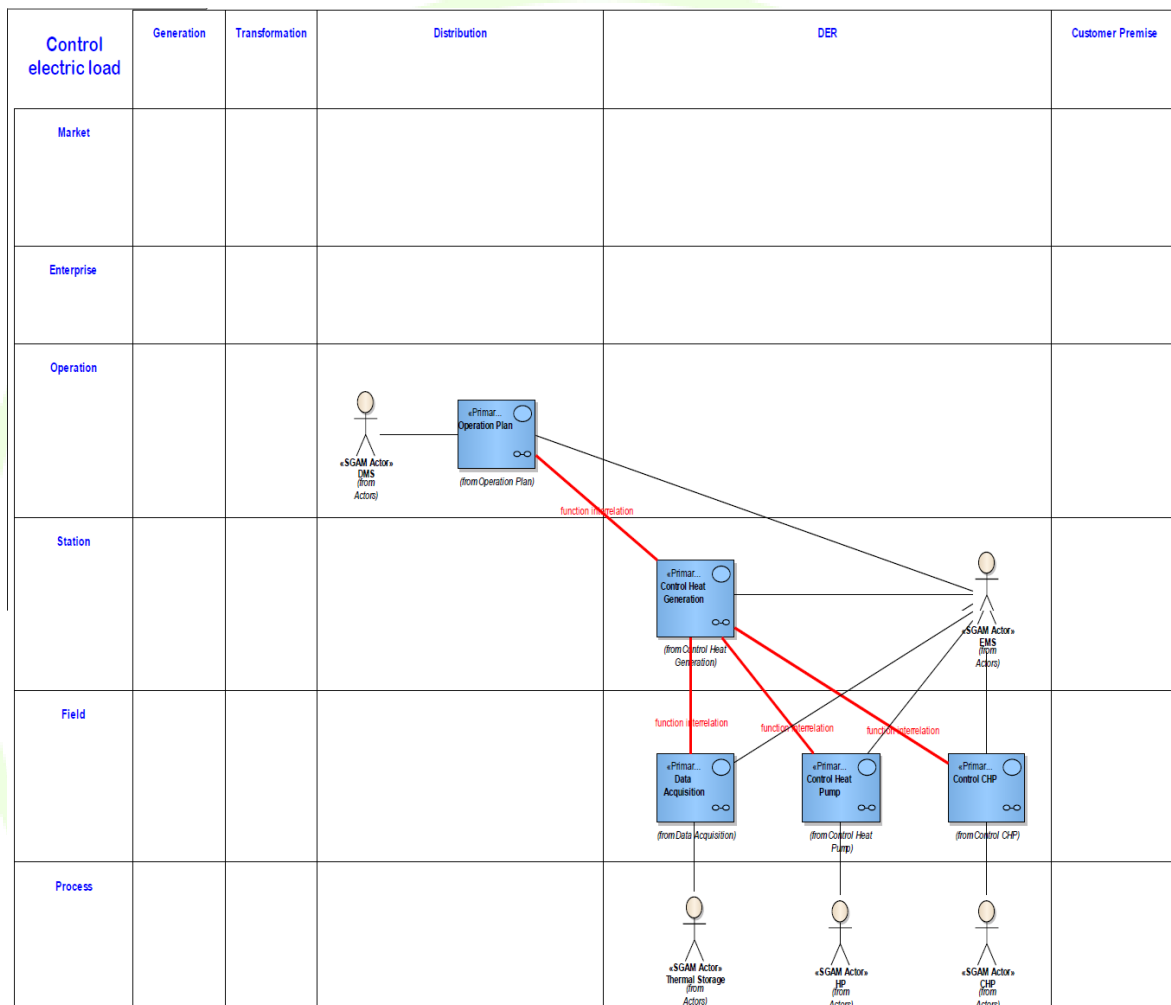


Figure 18 - SGAM Function Layer (example) [2]

### 4.3 WISEGRID SGAM COMPONENT LAYER

In the SGAM Component Layer the model transformation from the Computational Independent Model (reflecting system and software knowledge from a business perspective) to the Platform Independent Model (model of a system independent of the specific technological platform used to implement it) is represented. Firstly, logical actors have to be mapped into physical components (applications, power system equipment, protection devices, network infrastructures, computers) which must, in turn, be distributed properly among the different SGAM domains and zones. This way, the functional information of the system is turned into an architectural model. So, in the end, the use case actors are transformed into a hardware form and each UC functionality can be examined.

Explaining further the actor mapping process, while inside the SGAM Component Layer, a physical component must be created for each actor involved in the UC. Of course additional components need to be included, such as ICT-Networks or individual devices (e.g. a transformer). Subsequently, the relations between the components selected above have to be described and represented into the SGAM component layer. An example of the final result of a component layer development process is presented in Figure 20.

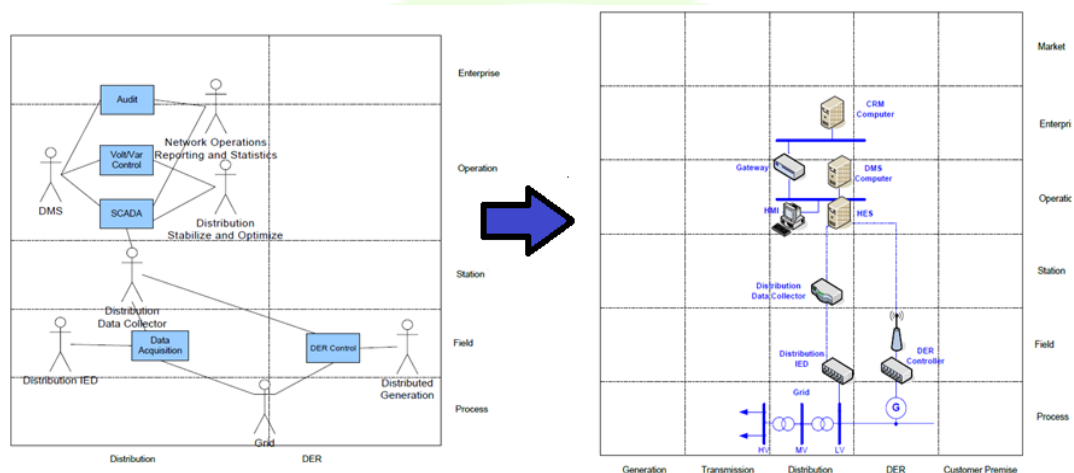


Figure 19 : Actor Mapping Model (example) [1]

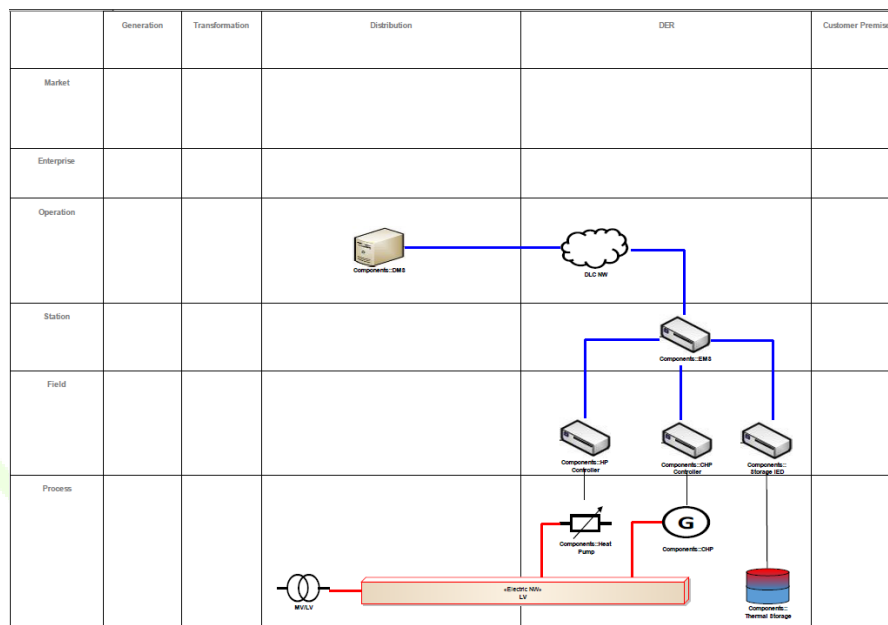


Figure 20 - SGAM Component Layer (example) [2]

#### 4.4 WISEGRID SGAM COMMUNICATION LAYER

The communication field is closely associated with the operational procedures of a SG. While each actor/component has to implement its own separate functions, the communication between them is essential, so that the individual processes can be coordinated. The information collected must also be sent to a central server so that the optimal operation of the SG may be achieved. For the

abovementioned reasons, a separate SGAM layer is dedicated to the communications sector.

While no gaps are identified in the existing communications standards (referring to the OSI model), general profiling (description of how to use different options and capabilities within a set of standards) and interoperability specifications need to be developed. All things considered, the following recommendations were made. First of all, specific communication profiles must be developed (in consultation with IETF, IEEE, ETSI, CEN and CENELEC), describing the exact way of utilizing the existing communication standards as well as providing the necessary interoperability test specifications. Due to the fact that **wired** and **wireless** technologies will be used, the spectrum to be committed must be clearly defined. It is also recommended that the **IP** protocol is employed. Last but not least, the support of specifications established through consortia, particularly with regard to the development of open standards, is suggested.

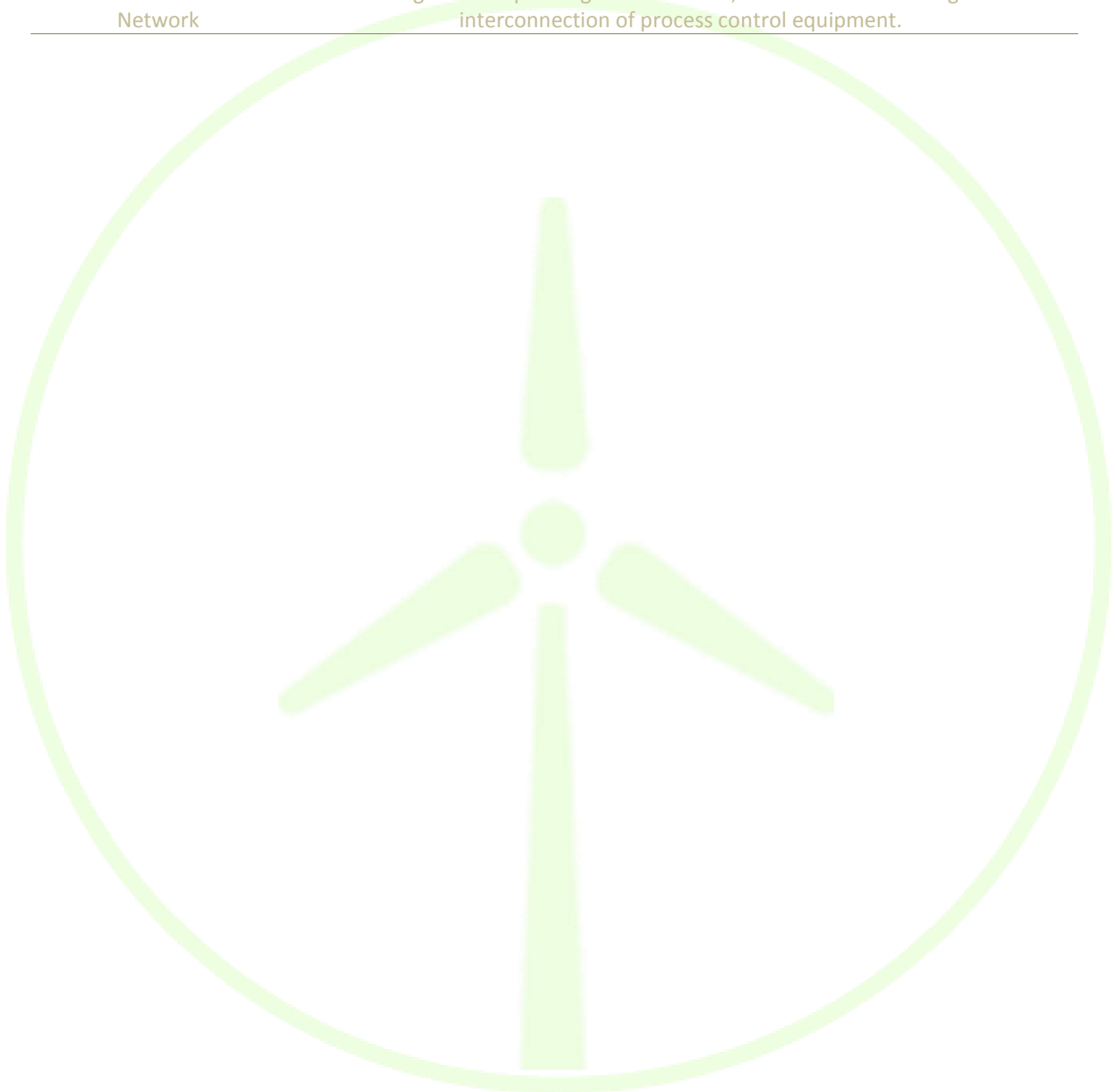
Before describing more in detail the utility and development process of the SGAM communication layer, the networks included in the overall communication architecture should be identified. In Figure 21 the individual mapping the sub-network technologies to the categories presented in Table 1 is depicted.

**Table 2 - Mapping of sub-network technologies**

Network Name	Description
Subscriber Access Network	While not being part of the utility infrastructure, devices and systems interacting with it are included (e.g. commercial facilities).
Neighbourhood Network	Interposed between distribution substations and end users, these networks can implement a lot of functions (service metering, distribution automation, public infrastructure).
Field Area Network	Located at the distribution level upper tier, this Network integrates various sub layer networks and provides backhaul connectivity. Can also provide P2Pw or hub and spoke connectivity.
Low-end intra-substation Network	Network inside secondary substations or MV/LV substations, connecting the different electronic components.
Intra-substation network	Network involved in low latency critical functions (e.g. tele-protection). It is located inside primary distribution substations.
Inter substation network	These networks are used for the connection of different substations and control centres. They serve SCAD, SIPS event messaging, remote asset monitoring telemetry traffic and P2P connectivity for teleprotection and distributed intelligence.
Intra-Control Centre / Intra-Data Centre network	While being at the same logical tier level, these are not the same networks, since they have different connection requirements and capabilities.
Enterprise Network	Involve enterprise, campus and inter control centre networks.
Balancing Network	As stated by its name, this network manages the interconnection and energy balance between generation operators and independent power producers.
Interchange Network	Interconnects regional reliability coordinators with operators as well as electricity markets to different stakeholders (providers, traders, operators retailers).
Trans-Regional / Trans-National Network	The most recently evolved concept in electric networking, these networks deal with the interconnection of regional, national or even continental scale



Network Name	Description
	networks.
Wide and Metropolitan Area Network	Defined through Service Level Agreements, these networks interconnect network devices over long areas. They are distinguished by the other categories, since they can be managed by multiple stakeholders and provide different levels of security.
Industrial Fieldbus Area Network	Dealing with the power generation field, these networks manage the interconnection of process control equipment.



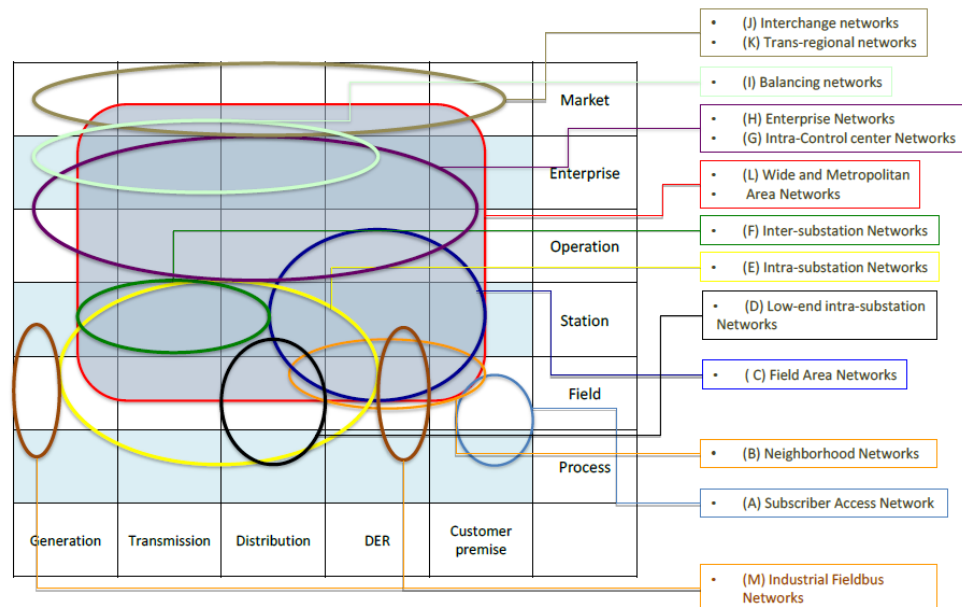


Figure 21 - Mapping of communication networks on SGAM Communication Layer [1]

	Subscriber access network	Neighbourhood Network	Field area	Low-end intra substation	Intra-substation	Inter-substation	Intra control centre	Intra data centre	Enterprise	Balancing	Interchange	Trans regional	Trans national	WAN	Industrial Fieldbus
	A	B	C	D	E	F	G	H	I	J	K	L	M		
Narrow band PLC (Medium and Low voltage)	x	x	x												
Narrow band PLC (High and very High voltage)					x	x									
Broadband PLC	x	x													
IEEE 802.15.4	x	x	x												
IEEE 802.11	x	x		x	x										
IEEE 802.3/1				x	x		x	x	x						x
IEEE 802.16	x	x	x												
ETSI TS 102 887		x	x												
IPv4	x	x	x	x	x	x	x	x	x	x	x	x	x	x	
IPv6	x	x	x	x	x	x	x	x	x	x	x	x	x	x	
RPL / 6LowPan	x	x	x												
IEC 61850		x	x	x	x	x								x	
IEC 60870-5				x	x	x								x	
GSM / GPRS / EDGE	x	x												x	
3G / WCDMA / UMTS / HSPA	x	x					x	x	x	x	x	x	x	x	
LTE/LTE-A	x	x	x	x		x	x	x	x	x	x	x	x	x	
SDH/OTN	x	x	x	x	x	x	x	x	x	x	x	x	x	x	
IP MPLS / MPLS															
TP	x	x	x	x	x	x	x	x	x	x	x	x	x	x	
EN 13757		x													
DSL/PON	x	x				x								x	

Figure 22 - Applicability statement of the communication technologies to the smart grid sub-networks [1]

The communication layer aims at the description of the protocols and technology involved, so that the information exchange between different UC actors or components can be achieved. The protocols and mechanisms included in the overall process must be mapped to the appropriate zones

and domains. As far as the development of the SGAM Communication Layer is concerned, this is organized in three simple steps. Firstly, the components are mapped in the Communication Layer diagram. Subsequently, communication paths relations are used to connect the different components. Last but not least, the appropriate protocols, as well as the involved technology, are defined, in respect to every communication path. An example of the final implemented model is presented in Figure 23

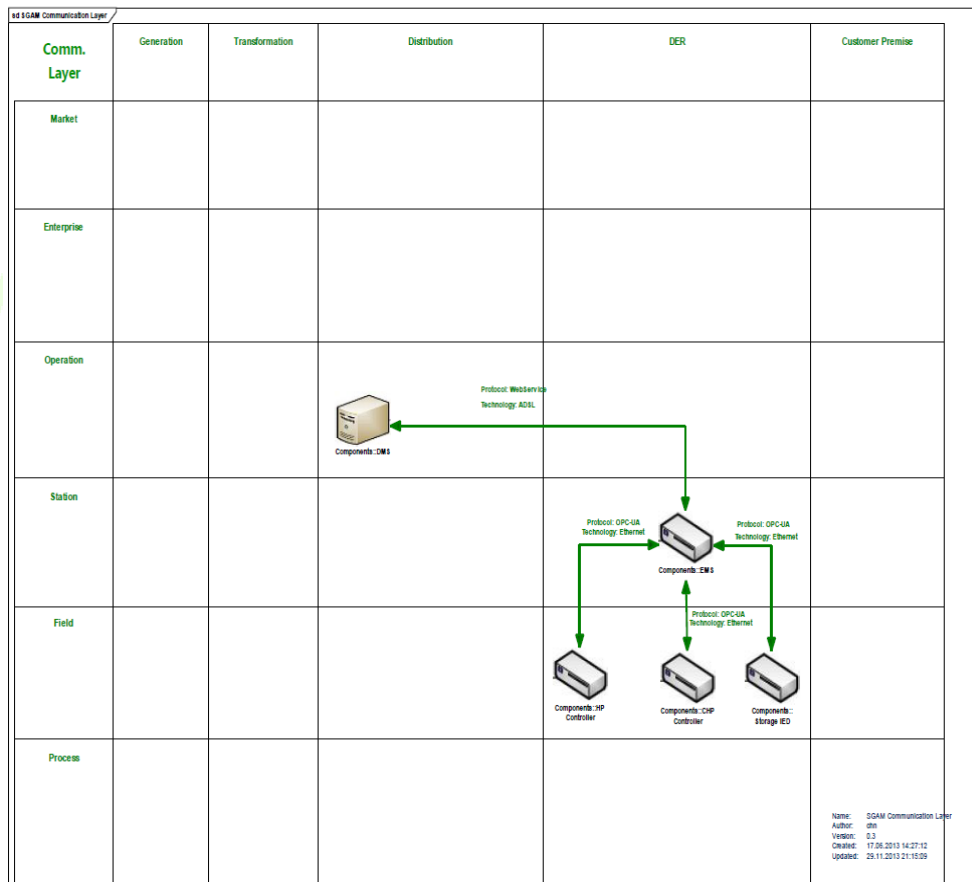


Figure 23 - SGAM Communication Layer (Example) [2]

## 4.5 WISEGRID SGAM INFORMATION LAYER

The functionality of a SG is based upon the exchange of data between the actors/components involved. The representation of important information related to the SG elements is the main reason of existence of the SGAM Information Layer. As seems logical, its architectural structure must support the inclusion of all interrelated entities, as well as the relationships between them and the different ways of interaction. This can be achieved by addressing three basic concepts:

### 4.5.1 INTEGRATION TECHNOLOGY

The smooth operation of a SG demands the individual contribution of many different systems and applications. These systems can be described as sources of information production and must be connected, for the optimization of the SG functionality. Consequently, a coupling of these separate systems has to be performed, while the preservation of their individuality (in terms of functionality and performance) is desired. In order for these requirements to be met, the development of new

interfaces, which can guarantee the semantic and syntactic interoperability between the different systems and applications involved, is considered. In addition to this, the presence of an integration platform is essential, so that the new interfaces can be implemented upon and are able to communicate between each other. The final scope of the information layer is the provision of a link between different SGAM layers, or fields.

The whole information trading process is based upon the exchange of multiple messages between the information layer's components. The rationale behind the information architecture is based upon the Enterprise Application Integration (EAI) Framework. In an abstract concept, the EAI makes use of software systems to enable data integration across applications, while simplifying the involved business processes. This concept is also adopted by Service Oriented Architecture (SOA) which provides transactional data transfers, without requiring the assistance of a third party solution. The term «service», in this case, can be interpreted in different ways, depending on the related stakeholders. Since no other parties need to participate, services are self-contained, while the integration of different services is recommended since it can provide additional flexibility to business and technical processes. A more complex software architecture concept, providing integration of enterprise application and services for complex architectures, is the Enterprise Service Bus (ESB), acting much like a router to control the data transferred. For the great majority of data production sources (prosumers, storage, etc.) SOA and EAI are employed.

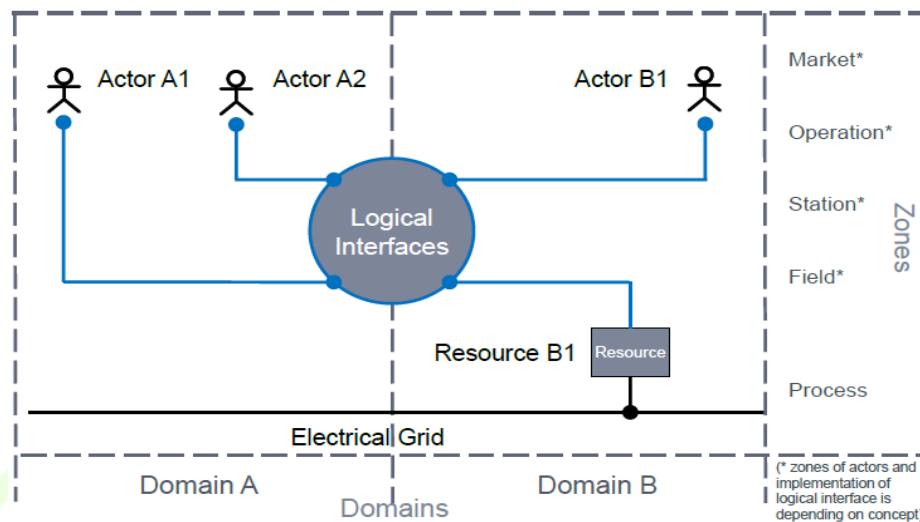
#### 4.5.2 DATA MODELS

Data models can be characterized as the core of the information layer architecture. In data models business data are contained and organized in respect to the information included, through which the communication between different SG entities can be performed. As far as the data description language is concerned, a top-down approach is recommended, since it provides a plurality of advantages (such as the avoidance of useless translations or misunderstandings between different stakeholders and the increase of system flexibility). The most prominent data models are the CIM (IEC 61968, 61970 62325) and IEC 61850 data model.

#### 4.5.3 INTERFACES

Technology independent interfaces (ETSI M2M, IEC 61850 ACSI, CIM profiles) are necessary, so that the communication and data model exchange between different SGAM layers, domains and zones can be possible. While many different standards have been developed, only some of them are recommended, taking into consideration that the semantics and syntax should be stable as long as the system is considered functional.

Since the definition of new interfaces between different SGAM layers can prove quite a challenge, the concept of **logical interfaces** was developed, aiming to the simplification of the whole process by providing a systematic way of developing the interfaces' specifications in regard to the logical relations (excluding any physical or technical characteristics).



**Figure 24 - Concept of logical interfaces in the context of domains and zones [1]**

The development of logical interfaces can be summarized into three basic steps. At first, every UC must be properly analyzed. The mapping of UC actors to the appropriate domains and zones is performed in this step. Subsequently, the identification of exchangeable information is performed, a process involving the assignment of each piece of information to the associated logical interface (indicated by the dots in the logical interface circle). Finally, all different specifications are merged. As can be seen in Figure 24, the actors can communicate through logical interfaces, providing information packages of specific characteristics. Any element related to physical implementation of the aforementioned actions is absent from this modelling concept, since the whole process is addressed from a theoretical/logical point of view.

Moving from the architectural structure to the utility aspect of the information layer, the main target is the exchange of information between different functions, services and components. In particular, information objects (derived from the UC descriptions), as well as the associated canonical data models (identified through the examination of available standards related to the support of information objects) are exchanged. As far as the mapping process of the information layer is concerned, three different steps must be completed: the development of the **Business Context View** (modelling the information object flows between individual components/Figure 25), the **Standard and Information Object Mapping** (stating the relations between Data Model Standards and Information Objects/Figure 26) and the development of the **Canonical Data Model View** Figure 27.

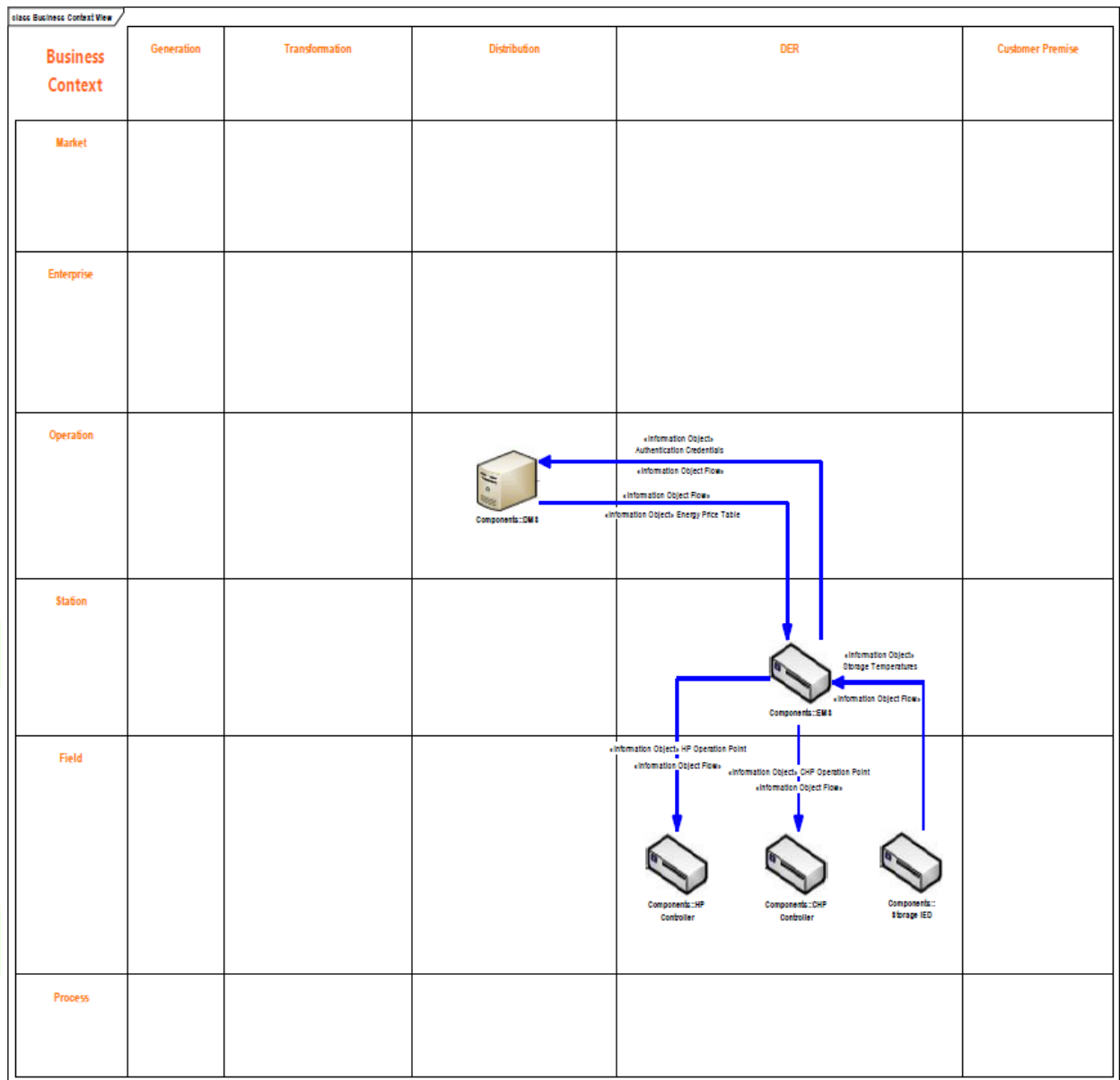


Figure 25 - Business Context View (example) [2]





#### 4.6 SGAM FRAMEWORK IN THE CONTEXT OF WISEGRID

The SGAM framework and underlying methodology have been applied to analyze and design the architecture of the WiseGRID services, tools, and use cases. More specifically the following design and analysis process has been followed.

5. Definition of the various WiseGRID-related use cases
6. Modelling of the use cases using the SGAM methodology and framework
7. Identification of proper WiseGRID applications to tackle the respective use cases
8. Modelling of the WiseGRID tools and services using the SGAM methodology and framework after the detailed analysis of the related use cases.

This analysis, design, and implementation are shown graphically in the following diagram.



**Figure 28: WiseGRID UCs and tools analysis and design process**

## 5 WG INTEROPERABLE PLATFORM (IOP)

The WG IOP in the WiseGRID project aims to provide a scalable, secure and open ICT platform, with interoperable interfaces, for real-time monitoring and decentralized control to support effective operation of the energy network.

The objective of the platform is to manage and process the heterogeneous and massive data stream coming from the distributed energy infrastructure deployed. This platform should enable new services and reduce ICT costs for prosumers and smaller players, whilst it will facilitate cross-network and cross-entity interoperability. It will enable the cooperation and synergies among the different actors targeted by the different WiseGRID technological solutions.

In order to increase adoption and speed up deployment, this platform will have open interfaces to the relevant energy, Internet of Things (IoT) and Smart City standards. In addition, proper data model standards will be considered for fostering the interoperability of energy field solutions.

### Features

The relevant features considered for the general WiseGRID Work Package IOP can be summarized in the set of features depicted in the following picture:

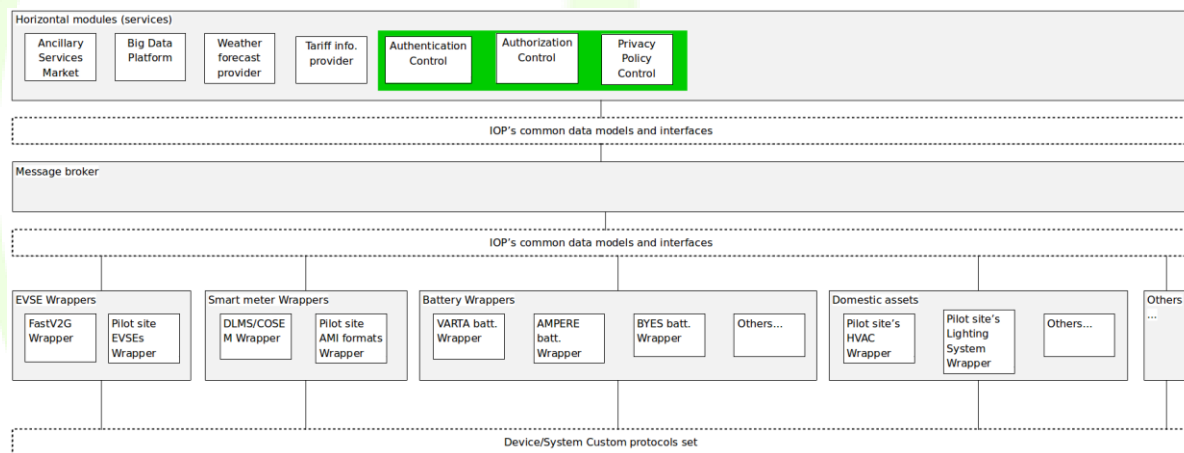


Figure 29 - WG IOP structure

According to this picture the IOP will include the following software modules

- Message broker (core feature)
- Some horizontal general purpose feature (ancillary services market, weather forecast provider, tariff info...)
- Field device/system wrapper modules (USM, batteries, EVSEs, AMI, SCADA...), operating thanks common data models and interfaces to be defined per field device / system type based on existing standards (work started on WP3).

The picture depicts also a Big Data platform (for its general nature, but such a result will be the result of WP5).

## 5.1 WG INTEROPERABLE PLATFORM SGAM COMPONENT LAYER

The IOP SGAM component layer depicts the modules considered in order to implement the functionalities strictly related to the message brokering. Those functionalities under the SGAM domains/zones matrix will span the Distribution, DER and Customer premise SGAM domains - as IOP message brokering features will relate with both managing communications among devices and among other major WiseGRID Tools.

Since most, if not all, WiseGRID devices and tools will eventually communicate by relying their messages through the IOP, those details are described in the corresponding sections of the remaining WiseGRID applications.

The following modules are envisaged to be developed in order to implement the required functionalities.





The following table details the different modules composing the message brokering component of the WG IOP.

**Table 3 - Modules of message brokering component of WG IOP**

Component	Description
On-site components	Existing components (under DSO premises or control) that will be integrated with WG IOP
Storage	Energy Storage related controller
RES	RES equipment related controller
Load Controller	Variable load related controller
RES Controller	RES equipment related controller
Storage Controller	Energy Storage related controller
Generic Wise-GRID product	Any product resulting from WiseGRID
Specific components	Components composing WiseIOP (Message Brokering functionalities)
Message Broker	Module implementing the core messaging functionalities on the basis of the RabbitMQ middleware.
Authentication and authorization	Module implementing the Authentication and authorization policies to access the core messaging functionalities
Near real time sub IOP	If scalability and performance so requires a hierarchical structure of message brokers may be considered (or necessary). The Near real time sub IOP components will deal with such hierarchical communications (if necessary)

## 5.2 WG INTEROPERABLE PLATFORM SGAM COMMUNICATION LAYER

The WG IOP will interconnect the different modules in a fast and reliable way. The main protocols envisaged to implement these communication flows are MQTT and AMQP.

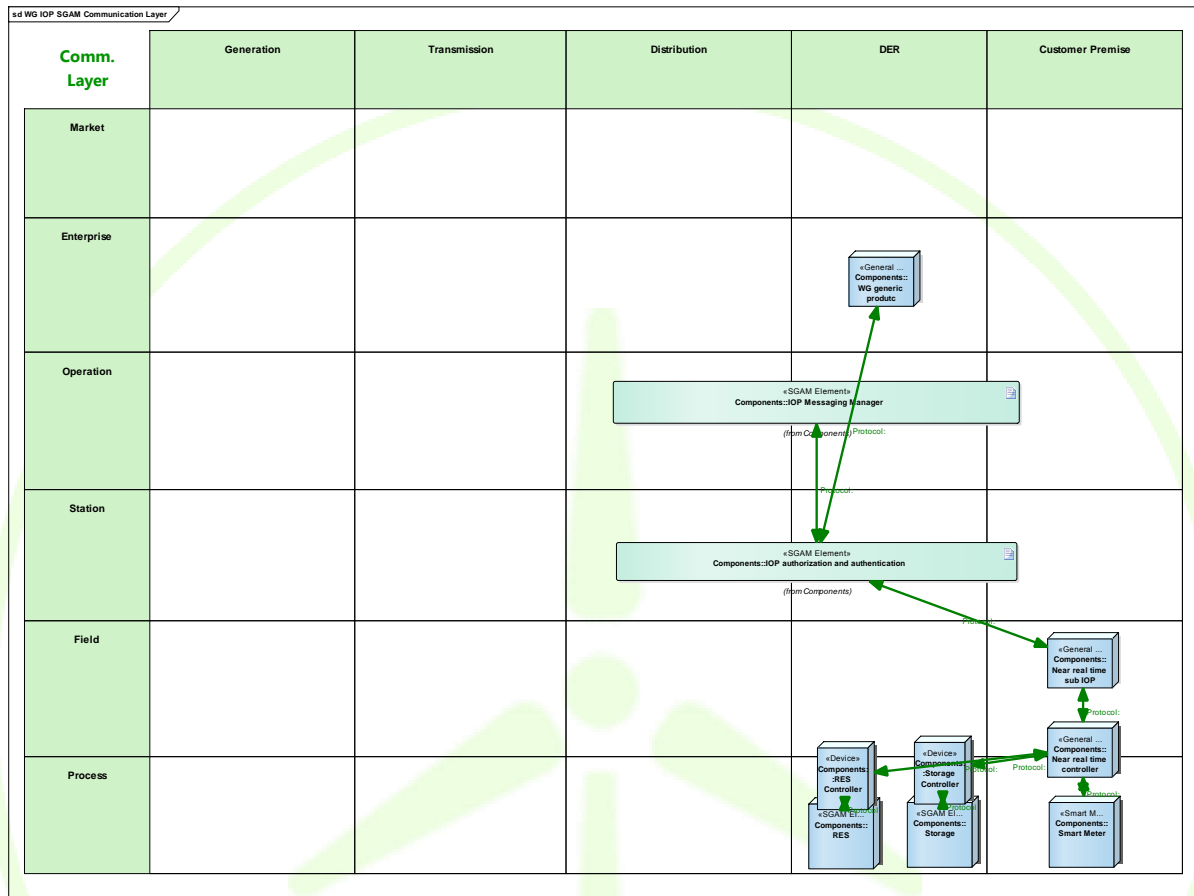


Figure 31 - SGAM Communication Layer of WG IOP

### 5.3 WG INTEROPERABLE PLATFORM SGAM INFORMATION LAYER

The WG IOP information layer will mirror the logical flows of data among the different modules. This first identification of data items will be useful for the identification and selection of proper common data models and standard interfaces to be used during the implementation phase.

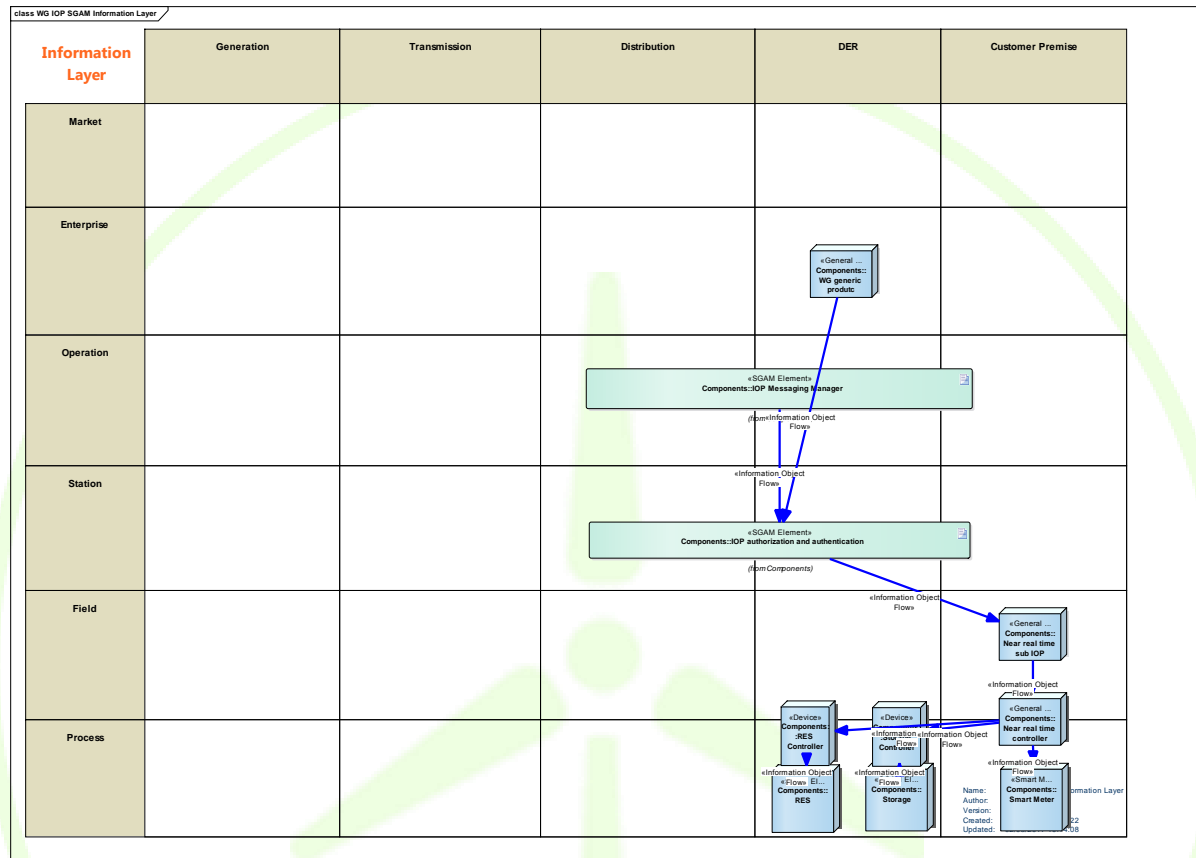


Figure 32 - SGAM Information Layer of WG IOP

In order to integrate other common functionalities a larger picture of the WP IOP results, encompassing both the core message brokering functionalities and is depicted in the diagram.

#### Related standards

Table 4 - Data item - model matching

Data item	Related data model or standard
Energy metering	CIM - DLMS/COSEM
Weather forecast	CIM
Flexibility offer	USEF
Retail electricity price	OpenADR



## 5.4 WG INTEROPERABLE PLATFORM PRIVACY AND DATA PROTECTION

The WiseGRID Interoperable Platform (WG IOP) serves as the “heart” of the WiseGRID platform when it comes down to services orchestration and data exchange. Since WG IOP will be handling sensitive data (and in some cases critical data) coming flowing from the systems and applications of the various parties participating in the WiseGRID ecosystem, a detailed investigation of the threats and associated risks related to the WG IOP are presented below. It should be mentioned that a similar investigation and analysis has been carried out for all WiseGRID tools.

Tables for the results of the assessment related to the WG IOP are presented below.

**Table 5 - Threat and feared events identification for WG IOP**

Feared events	Threat ID	Threat name	Brief explanation why relevant
Change in processing: it deviates from what was originally planned (diversion of the purpose, excessive or unfair collection)	II	Incomplete information	The information provided to the data subject on the purpose and use of data is not complete
Disappearance of personal data: they are not or no longer available	ED	Eavesdropping of computer channels	Interception of Ethernet traffic; acquisition of data sent over a Wi-Fi network, etc
	Pobj	Prevention of objections	Data subjects have the right to object to the processing of data. If they want to execute this right it must be (technically) possible.
Diverting of personal data to other users: they are distributed to people that have no need	DoS	Denial of service	Denial of service will lead to unavailability of computing system
	IISC	Insufficient information security controls	Unauthorized parties obtain access to personal information by breach of security or lack of security implementation.
Illegitimate access to personal data: they are known by unauthorized persons	HL	Hardware loss	Retrieval of a discarded storage device or hardware; loss of an electronic storage device
	IACP	Insufficient access control procedures	Access rights are not revoked when they are no longer necessary.
Unavailability of legal processes: they do not or no longer exist or work	NL	Non legally based personal data processing	Processing of personal data is not based on consent, a contract, legal obligation, or other relevant legal ground as per Article 7 of Directive 95/46/EC.
	SA	Software alteration	Errors during updates, configuration or maintenance; infection by malicious code; replacement of components, etc.
Unwanted change in personal data: they are altered or changed	LQD	Lack of quality of data for the purpose of use	If data is used for certain processes it should be adequate.

## 6 WG COCKPIT SGAM ARCHITECTURE SPECIFICATION

WiseGRID Cockpit is the WiseGRID technological solution targeting DSOs and microgrid operators, allowing them to control, manage and monitor their own grid, improving flexibility, stability and security of their net-work. Taking into account the goals of the project, the features to be implemented within WiseGRID cockpit consider a scenario of increasing share of distributed renewable resources and services provided by communities of prosumers (aggregated in the form of VPPs or cooperatives in order to achieve higher participation and environmental, social and economic benefits).

The main purpose of the WiseGRID Cockpit is to enable DSOs to manage the fundamental changes that distribution grids are facing nowadays, some remarkable ones of those being the transition towards a grid with high penetration of distributed renewable energy resources and the presence of additional significant loads coming from electric vehicles among others. In addition, this particular outcome of the WiseGRID project aims at approaching the benefits that new technologies (such as big data or unbundled smart meters) and algorithms (such as state estimation or fault detection) bring to the operation of the grid. Finally, since one of the objectives of the project is the empowerment of the citizens in the energy field, the WiseGRID Cockpit will also demonstrate how that empowerment can be beneficial for several actors - including DSOs -, and how the whole ecosystem of actors can contribute to reach an environmentally and economically sustainable energy system.



Figure 33 - WiseGRID Cockpit

### Features

An analysis of the different use cases where WiseGRID Cockpit plays a lead role shows the need for the following features to be implemented:

- Asset portfolio management: DSO has the need of managing in a clear way the different elements connected to the grid, including smart meters, distributed RES production, grid-support batteries, etc. Management includes:
  - Real time monitoring of status of assets
  - Maintenance management
  - Dynamic identification and retrieval of basic information of assets on
    - GIS: showing elements' location, and their connection to MV/LV lines
    - Topology: showing elements' connection in the single-line schema of the grid

- Grid metering: it is mandatory to have a proper observability of the grid in near real time. This includes:
  - Real-time monitoring (retrieval of information from field devices and SCADA)
  - Alert monitoring: being able to detect anomalous behavior of assets
  - Alert triggering: evaluate the data coming from the grid and trigger alerts upon operational thresholds violation or observation of abnormal measurements
  - Load flow calculation and state estimation: allow a complete observability of the grid
- Grid control: this application shall facilitate the actions to be taken by the DSO operator when a problem is detected:
  - Trigger actions on assets under direct control of DSO (reconfiguration)
  - Integration of ancillary services market, allowing third parties to provide support upon congestion or voltage problems
- Grid planning: simulation of “what-if” scenarios in order to evaluate impact of high penetration ratios of RES and EVs to the distribution grid

## 6.1 WG COCKPIT SGAM COMPONENT LAYER

The WG Cockpit SGAM component layer presents the set of modules that can cooperate in order to achieve the functionalities required to the WG Cockpit. Those are represented under the SGAM domains/zones matrix. As expected, most of the modules integrating the WG Cockpit fall under the *distribution* SGAM domain - as distribution is the core business of DSOs - and under the operation zone - since most of the features of WG Cockpit deal with the near real-time monitoring and evaluation of the status of the grid and support to identified problems.

The main elements of the DSO to be integrated within the WG Cockpit include:

- Advanced Metering Infrastructure: refers to the current system in place on pilot sites to retrieve information from the smart meters of the installation. The architecture contemplates the readout and further processing of this data in the WG Cockpit
- Unbundled Smart Meters: refers to the field devices that can be deployed to get additional metering information with advanced capabilities - the main of those its capability to provide data at higher rates than usual AMIs
- SCADA system: software in charge of performing real-time monitoring of the electric parameters at certain critical points distribution grid, as well as allowing control of assets under domain of DSO

The presented modules retrieve and process the information provided by these elements in order to implement the advanced functionalities foreseen and described in the use cases.

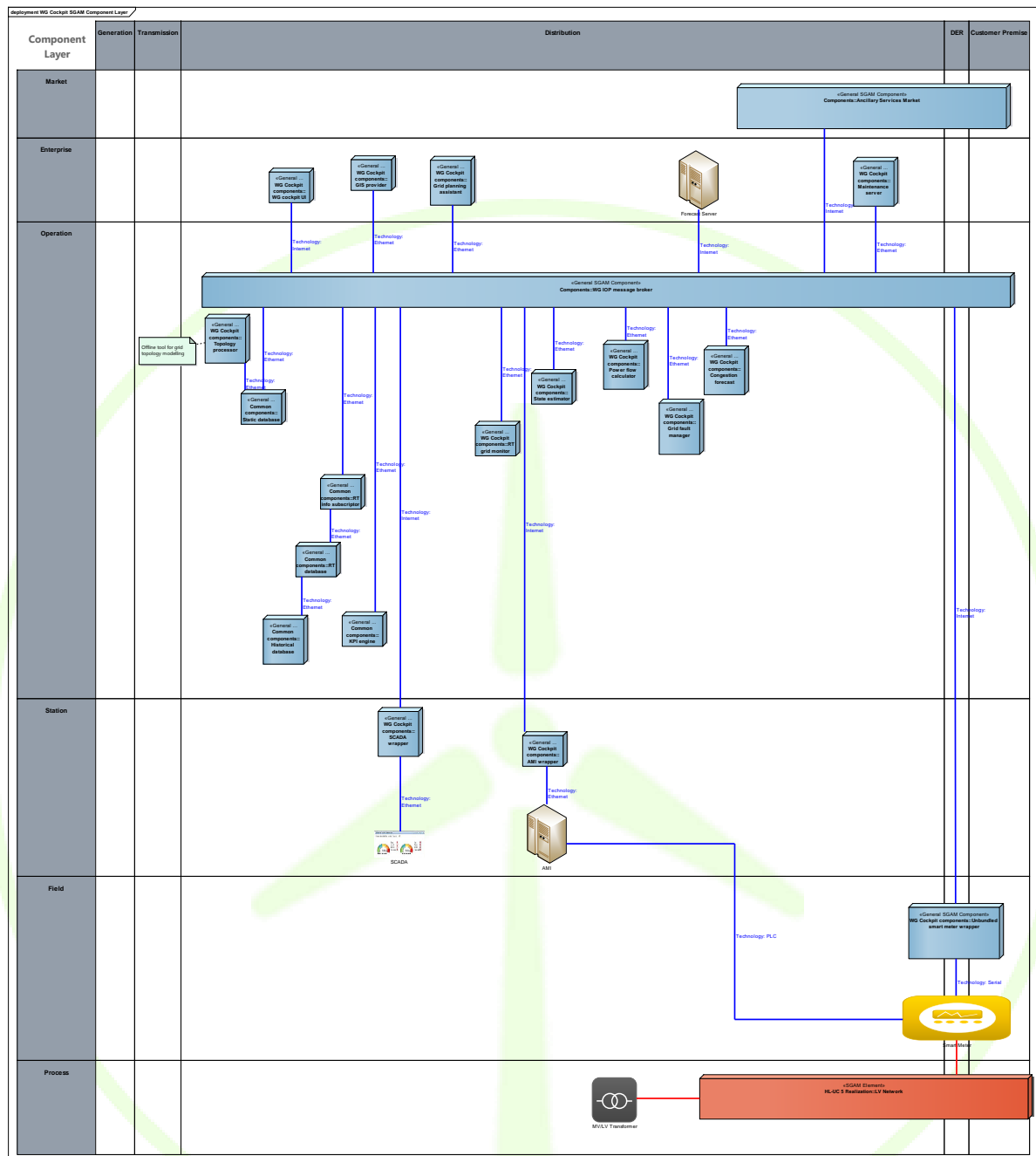


Figure 34 - WG Cockpit SGAM Component Layer

The following table details the different modules composing the WG Cockpit:

Table 6 - Modules composing the WG Cockpit

Component	Description
On-site components	Existing components (under DSO premises or control) that will be integrated with WG Cockpit

Component	Description
Smart meter	Refers to the existing smart meters currently deployed at pilot sites, integrated with an AMI system in charge of collecting data - mainly with billing purposes -, as well as unbundled smart meters to be deployed as part of the execution of the project. The architecture envisages the read-out of this data in order to provide DSOs an overall vision of the status of the distribution grid, also including the low voltage lines
AMI	Refers to the existing systems in charge of retrieving data from the currently deployed smart meters - via concentrators and a dedicated data collection system. The architecture envisages the integration of these systems in order to gain access to the information produced by currently deployed smart meters
SCADA	Refers to the existing SCADA systems utilized by the DSOs to monitor and control their distribution grids - mainly HV/MV substations, MV/LV substations and MV lines. The architecture envisages the integration of these systems in order to provide DSOs an overall vision of the status of the distribution grid, including the MV lines and elements, as well as allowing the execution of advanced control policies enabled by WG Cockpit
Horizontal modules	Components that will be reused among different WiseGRID applications
Forecast server	Module supporting the calculation of forecasts required by the WG Cockpit, such as congestion forecasts - estimation of power flow limits exceeded at a certain point of the distribution grid
Ancillary Services Market	Binding module between WG Cockpit - which will demand support upon the detection or forecast of certain problems in the distribution grid - and the rest of WiseGRID applications - which may be able to support the operation of the DSO in preventing and solving those problems, mainly by modulating their demand or activating specific voltage control support features. This module will be in charge of the orchestration of these supporting services
Big data platform	Suite of modules specified within the WiseGRID project in order to support big-data related functionalities, including long-term storage and data-mining algorithms
Specific components	Components composing WG Cockpit
Topology processor	Offline tool for converting the topology of the distribution grid - which is typically stored in raster formats - into an interoperable and actionable format to be further used by other modules
GIS provider	Module for converting the GIS data of the distribution grid - for which several different data models exist - into a common data model (e.g. GeoJSON) that can be further used by other modules
Static database	Database holding structural data of the WG Cockpit - including topology, GIS, asset portfolio...
Unbundled smart meter wrapper	Module in charge of publishing data from unbundled smart meters into the WiseGRID application ecosystem via the WG IOP. Unbundled smart meters will be installed at some of the pilot sites - both at MV and LV levels - allowing advanced capabilities and faster data rates
AMI wrapper	Module in charge of publishing data from the existing AMI systems into the WiseGRID application ecosystem via the WG IOP. In principle, this wrapper will respect current configuration of those AMIs, with the objective of having the minor possible impact with those operational systems

Component	Description
SCADA wrapper	Module in charge of publishing data from the existing SCADA systems into the WiseGRID application ecosystem via the WG IOP. In principle, this wrapper will respect current configuration of those systems, with the objective of having the minor possible impact with those operational systems. In particular pilot sites, this wrapper will allow triggering commands to the SCADA as well
RT info. subscriber	Module subscribed to the proper flows of data of the WG IOP - Unbundled smart meters, AMI and SCADA - and in charge of collecting that data and pushing it into the proper databases
RT (short-term) database	Specific database focused in daily operation, holding short-term data
Historical (long-term) database	Specific database, supported by the big data platform, focused in long-term storage of data for data-mining purposes
KPI engine	Data-mining algorithm, supported by the big data platform, in charge of calculating and updating KPIs of particular interest to the DSO
Power flow / State estimator	Using the formal definition of the topology and the set of measurements retrieved from field devices - triggered into the WG Cockpit by the RT info. subscriber - this module will calculate the measurements of the remaining nodes of the grid, thus providing a complete observability of the distribution grid
RT grid monitor	Module in charge of detecting alerts based on the abnormality of the data being collected from the field devices - and complete with the results of the power flow/state estimator module. These analysis will include threshold exceeding control and anomalous pattern detection in the incoming data
Congestion forecast	Module in charge of performing analysis on historical data, together with forecast of context information - including weather, type of day and forecasts provided by other Wise-GRID applications - with the objective of detecting future congestion in advance, thus allowing the execution of preventive policies
Grid fault manager	<p>Upon reception of different types of alerts, triggered by other modules, the grid fault manager will implement the business logic to be executed in order to solve or prevent those problems. Depending on the nature of the problem, the actions to be initiated by this module will include:</p> <ul style="list-style-type: none"> <li>Informing DSO operator and scheduling a service for the maintenance staff, with as much details as possible - e.g. upon a failure detected in a device and needing manual assistance</li> <li>Initiating negotiation in the ancillary services market with third parties in position of delivering support to the DSO. These services mainly use demand response mechanisms in order to achieve demand modulation of the prosumers of the grid - in order to avoid congestion problems- or activate voltage support features of elements under third party control</li> <li>Triggering self-healing algorithms - e.g. in case of outages. These algorithms have the purpose of analyzing the grid topology and possible reconfigurations in order to detect the most adequate one, establish the proper steps to be executed, and proceed with the execution of the reconfiguration commands - by interfacing with the SCADA - in order to apply the best identified solution as fast as possible</li> </ul>
Maintenance server	Module in charge of optimally managing the work of the maintenance staff, both including preventive maintenance and corrective maintenance. Corrective maintenance will be

Component	Description
	triggered by the output of the grid fault manager among other possibilities, such as calls received by the customer service or problems manually identified by the maintenance staff
Grid planning assistant	Module implementing the capability to simulate and evaluate the effects of having extra demand on the distribution grid - e.g. evaluate the possible impact of high penetration of RES or EVs in the grid. For this purpose, historical data will be evaluated together with models of demand and production of different RES and EV technologies
WG Cockpit UI	Implements the DSO operator interface of the WG Cockpit. Based on web technologies, will provide different visualizations accordingly to the different features implemented by the WG Cockpit, including an appropriate selection of real-time information displayed over GIS georeferenced data and over single-wire diagrams of the topology, detailed views of the data and sensors being managed by the WG Cockpit, information about problems detected in the grid and actions taken or proposed by WG Cockpit... One main objective of this user interface is to provide an homogeneous view of all considered aspects of the grid management, offering in a single application all necessary features to ease the daily work of the DSO operators

## 6.2 WG COCKPIT SGAM COMMUNICATION LAYER

The architecture envisaged for the WG Cockpit puts the WG IOP message broker in the centre of the main communication flows. Since this technology will offer a reliable, fast and open mechanism to interconnect different modules within the WiseGRID application ecosystem, efforts will be put in reusing the same technological solution also for internal communication within the different modules of the WG Cockpit. The identified advantages of this approach include:

- Active promotion of reusable modules across different developments of the project: by using a common technology for interfacing the modules, their potential to be reused by other developments of the project - or even by future developments based on this work - are strengthened
- Loose coupling between data sources and data sinks: by adopting a common interfacing technology based on open standards, inclusion of new data sources or delivery of information to new processing modules gets easier
- Fosters adoption of common data models: this approach, with open interfaces, also encourages the adoption of common data models for the exchange of information among the modules, which in fact also facilitates the extension of the application with future modules implementing extra features





- Include access control mechanisms: while some communication flows will be kept internal to the WG Cockpit - and therefore may traverse a custom independent instance of the message broker, just dedicated to this application - other flows will include communication with

external elements, such as smart meters and SCADA. The technology employed for messaging needs to assure that information from those elements only reaches the proper actors and modules of the architecture

- Advanced routing capabilities: since the technology will be employed for interconnecting several different modules and data flows, the chosen technology needs to provide flexibility in the way those routing rules are defined

Last but not least, in the architecture we already propose some applicable application-level protocols that are well-known for their use in data-centric and micro-service-based architectures similar to proposed for the WG Cockpit:

- Advanced Message Queuing Protocol (AMQP): open standard application layer protocol for message-oriented middleware. The defining features of AMQP are message orientation, queuing, routing (including point-to-point and publish-and-subscribe), reliability and security [4]
- Message Queue Telemetry Transport (MQTT): ISO standard (ISO/IEC PRF 20922) [5] publish-subscribe-based lightweight messaging protocol for use on top of the TCP/IP protocol designed for connections with remote locations where a small code footprint is required or the network bandwidth is limited

### 6.3 WG COCKPIT SGAM INFORMATION LAYER

The WG Cockpit information layer shows the logical flows of data among the different modules, also detailing the information items that are conveyed within each one of those flows. This first identification of data items present in the operation of the WG Cockpit will further support the evaluation and selection of the proper common data models and standard interfaces to be used not only within the WG Cockpit itself, but also for interoperability with other applications of the WiseGRID ecosystem.



### D3.1 WiseGRID Architecture, Data Models, Standards and Data Protection (V1)

### Setup and offline processes

This section includes the modules dealing with offline processes - i.e. required to setup the WG Cock-pit and perform analysis purely based on historical data.

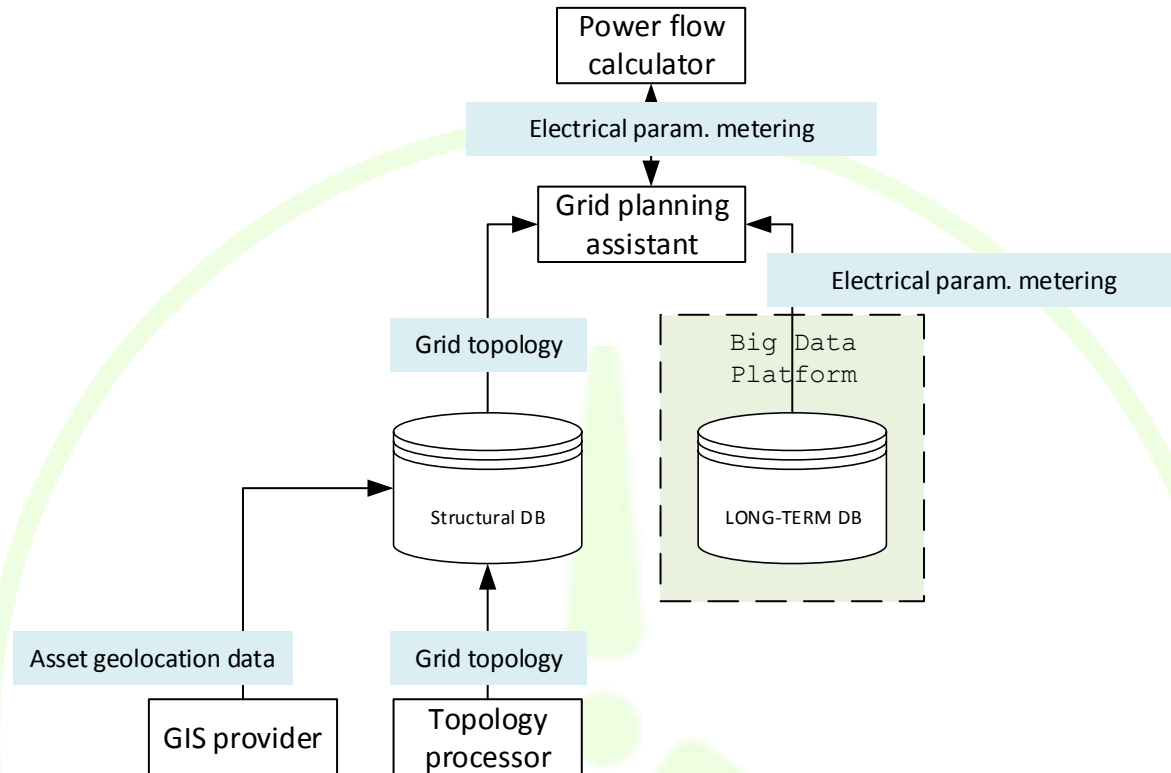


Figure 37 - Offline Processes diagram

Table 7 - Data item Description

Data item	Description
Asset geolocation data	MV/LV asset - e.g. substation, lines, switches... - metadata, including georeferenced description of the item - i.e. point, polygon or polyline representation linked to a location
Grid topology	Formal definition of the assets under control of the DSO, including equipment information, relationships and connections between those elements. This model shall include all information needed to perform further calculations of grid parameters, such as power flow and state estimation calculations
Electrical parameter metering	Electrical measurements (voltage, phase angle, current, active/reactive power)

### Grid monitoring

This section includes the modules dealing with the real time retrieval of information from field devices and DSO systems for grid monitoring purposes.

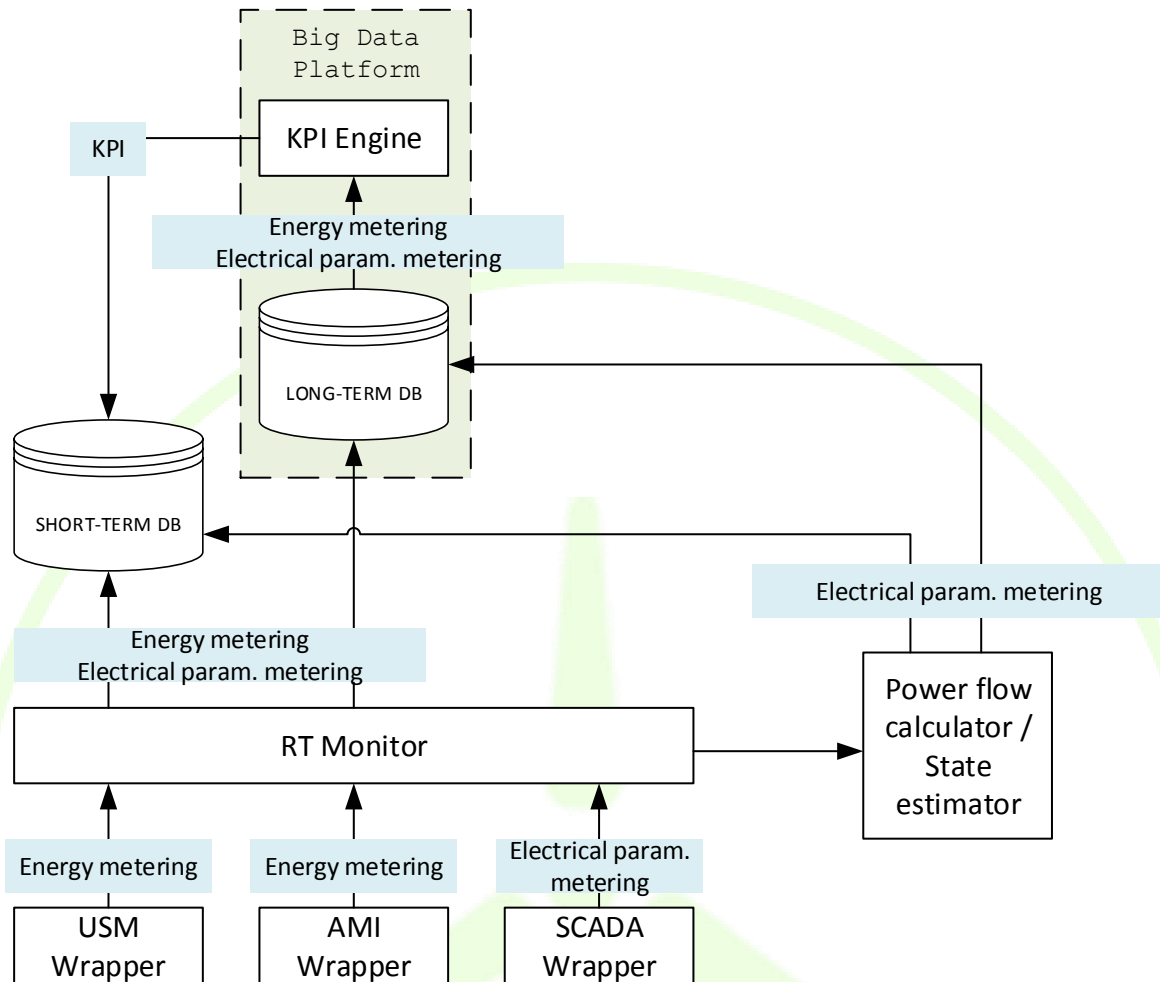


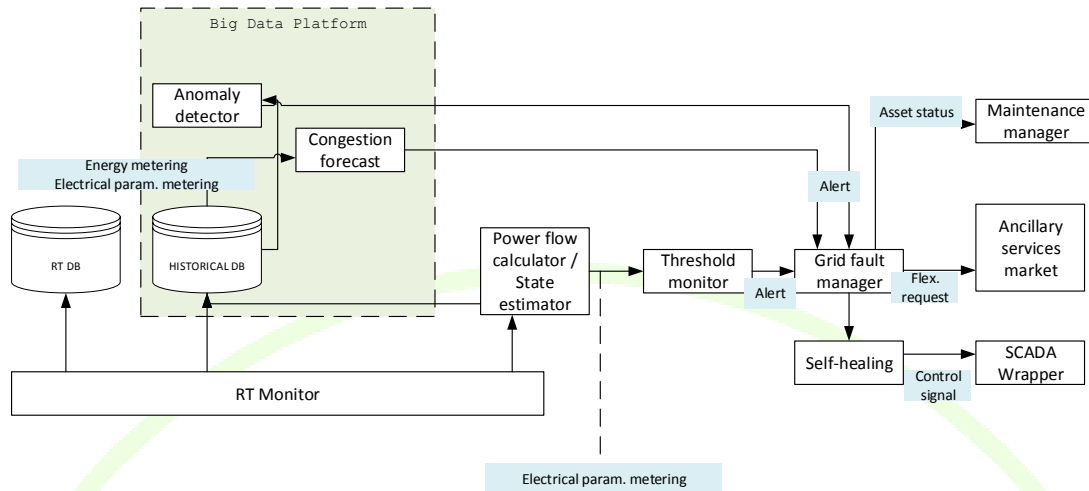
Figure 38 - Information retrieval diagram

Table 8 - Data item description

Data item	Description
Electrical parameter metering	Electrical measurements (voltage, phase angle, current, active/reactive power)
Energy metering	Measurements of energy consumption or production
KPI	Numeric values summarizing the state or evolution of certain variables of interest to the DSO

### Problem detection and reaction

This section includes the modules in charge of analyzing the data flows in order to evaluate the occurrence - or likelihood of future occurrence - of problems in the grid for whose the WG Cockpit can execute mitigation actions.



**Figure 39 - Problem detection diagram**

**Table 9 - Data item description**

Data item	Description
Electrical parameter metering	Electrical measurements (voltage, phase angle, current, active/reactive power)
Energy metering	Measurements of energy consumption or production
Alert	Formal description of an identified problem in the grid, including outage, operational threshold violation, anomaly on the data pattern...
Asset status	Metadata of an equipment of the grid (id, location, type, description...), also including details of its current status and identified problems
Flexibility request	Formal description of the request of the DSO to third parties for modulating their demand/production curves (flexibility in their consumption patterns)
Control signal	Formal description of a state or set point to be applied by the SCADA at a particular asset of the grid (e.g. open/close MV substation switch)

### Related standards

The following table summarizes some of the relevant standards and data models identified for the data to be handled by WG Cockpit

**Table 10 - Items and related data models**

Data item	Related data model or standard
Asset geolocation data	GeoJSON
Grid topology	CIM
Electrical parameter metering	CIM - DLMS/COSEM
Energy metering	CIM - DLMS/COSEM
KPI	CIM
Alert	CIM
Asset status	CIM
Flexibility request	USEF
Control signal	IEC61850

## 6.4 WG COCKPIT PRIVACY AND DATA PROTECTION

Tables for the results of the assessment related to the WiseGRID Cockpit are presented below. There are no personal data handled within WG Cockpit.

**Table 11 - Threat and feared events identification for WiseGRID Cockpit**

Feared events	Threat ID	Threat name	Brief explanation why relevant
Change in processing: it deviates from what was originally planned (diversion of the purpose, excessive or unfair collection)	II	Incomplete information	The information provided to the data subject on the purpose and use of data is not complete
Disappearance of personal data: they are not or no longer available	ED	Eavesdropping of computer channels	Interception of Ethernet traffic; acquisition of data sent over a Wi-Fi network, etc.
	Pobj	Prevention of objections	Data subjects have the right to object to the processing of data. If they want to execute this right it must be (technically) possible
Diverting of personal data to other users: they are distributed to people that have no need	DoS	Denial of service	Denial of service will lead to unavailability of computing system
	IISC	Insufficient information security controls	Unauthorized parties obtain access to personal information by breach of security or lack of security implementation.
Unavailability of legal processes: they do not or no longer exist or work	SA	Software alteration	Errors during updates, configuration or maintenance; infection by malicious code; replacement of components, etc.



Feared events	Threat ID	Threat name	Brief explanation why relevant
Unwanted change in personal data: they are altered or changed	MEP	Missing erasure policies or mechanisms; excessive retention periods	Data is retained longer than necessary to fulfil the specified purpose or to comply with legal obligations.
	LQD	Lack of quality of data for the purpose of use	If data is used for certain processes it should be adequate.



## 7 WISECOOP ARCHITECTURE SPECIFICATION

WiseCOOP is the WiseGRID technological solution targeting aggregators of consumers and prosumers - particularly focused on domestic and small businesses -, supporting them in their roles of energy retailers, local communities and cooperatives - which may have different objectives.

The main goal of the solution is helping consumers and prosumers to work together in order to achieve better energy deals while relieving them from administrative procedures and cumbersome research. In the particular scenario of increasing share of distributed renewable resources, this goal can be achieved by pursuing several objectives:

- Net-metering: supporting the operation of communities of prosumers that invest in renewable energy sources aiming at reducing their environmental impact
- Member profiling: clusters of consumers and prosumers with common energy usage patterns may be identified, allowing the aggregator to negotiate special terms (as for instance energy tariffs) particularly beneficial for those groups
- Demand forecasting: by allowing aggregator (in its retailer role) to forecast the demand of its customers, optimized purchase of energy at the wholesale market is enabled
- Tariff comparison: by offering members a tool for comparing their particular consumption with different available tariffs, those will have access to very valuable information to reduce their energy bills
- Implicit price-based demand response towards modulating the overall demand of the group to achieve a common objective (as, for instance, maximize usage of renewable energy sources produced within the group or minimize deviations between actual demand and energy purchased at the wholesale market)
- Providing clear information to members to raise awareness on efficient energy usage and environmental awareness



Figure 40 - WiseCOOP

## Features

An analysis of the use cases focused on the WiseCOOP shows the need for the following features of the tool:

- The tool will be able support different business cases implying different optimization objectives
  - Solidarity motivations (maximize green energy usage among the community, promote self-consumption...)
  - Economic motivations (optimize energy purchase, minimize costs)
- Portfolio profiling: having a clear insight of the energy usage patterns of the members of the portfolio can be very beneficial for the aggregator, since it will allow:
  - Tariff advisory mechanisms
  - Properly addressing the market by providing proper information to cooperatives (e.g. decision support for negotiating bilateral energy supply contracts directly with producers)
  - Addressing the proper set of members under a demand-response campaign with a particular objective and context
- Portfolio management: the tool shall facilitate regular operations of the aggregator, including:
  - Designing and triggering implicit (price-based) demand response campaigns, in order to shift demand towards periods where energy bought by the cooperative is more affordable or cleaner, or to reduce deviations of actual consumption from the forecasted one
  - Billing energy supply, considering rewards for active participation in demand response campaigns

### 7.1 WISECOOP SGAM COMPONENT LAYER

The WiseCOOP SGAM component layer presents the set of modules that are considered in order to include all required functionalities of the tool. The modules are represented under the SGAM domains/zones matrix. Most modules fall under the *Customer premise* SGAM domain - as WiseCOOP features relate with the business of the aggregator of prosumers - and under the *operation* zone - since most features are intended to provide services to those prosumers.

The main external elements to be integrated with WiseCOOP are the following ones:

- Smart meters: main data required by aggregators and retailers is the metering information - both demand and production - provided from the smart meters. From the perspective of most functionalities of WiseCOOP, prosumers members of the portfolio can be seen as assets with certain demand/production patterns, and with a potential to provide a certain flexibility. Detailed information defining their energy usage is therefore the most important input for the aggregator
- WiseCORP and WiseHOME: WiseGRID applications targeting the different prosumer profiles (tertiary and domestic) of the aggregator portfolio. The demand response campaigns initiated by the aggregator will be reflected in actions taken and information presented by those two applications

The following modules are candidates to be developed in order to achieve the required functionalities.

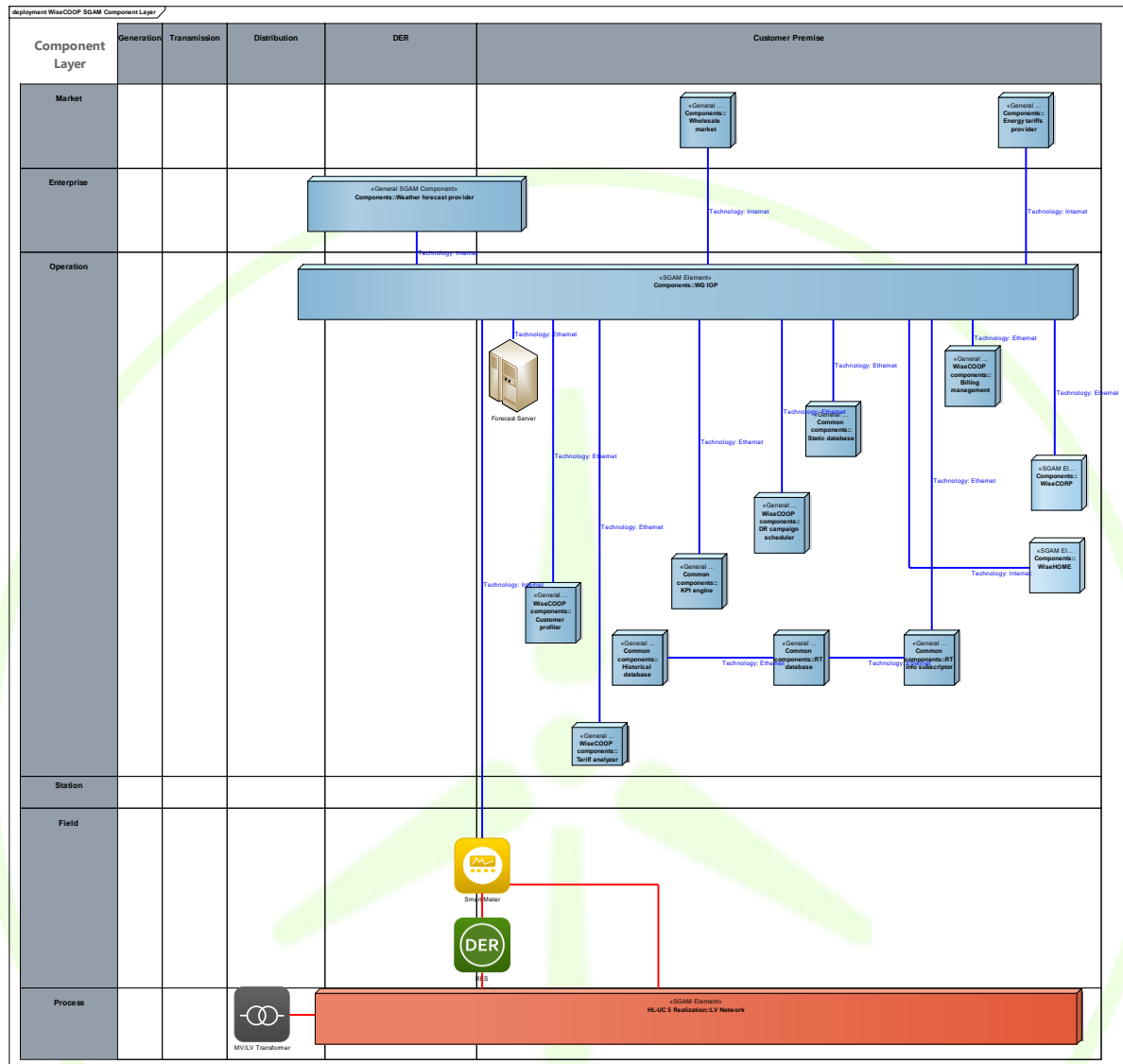


Figure 41 - WiseCOOP SGAM Component layer

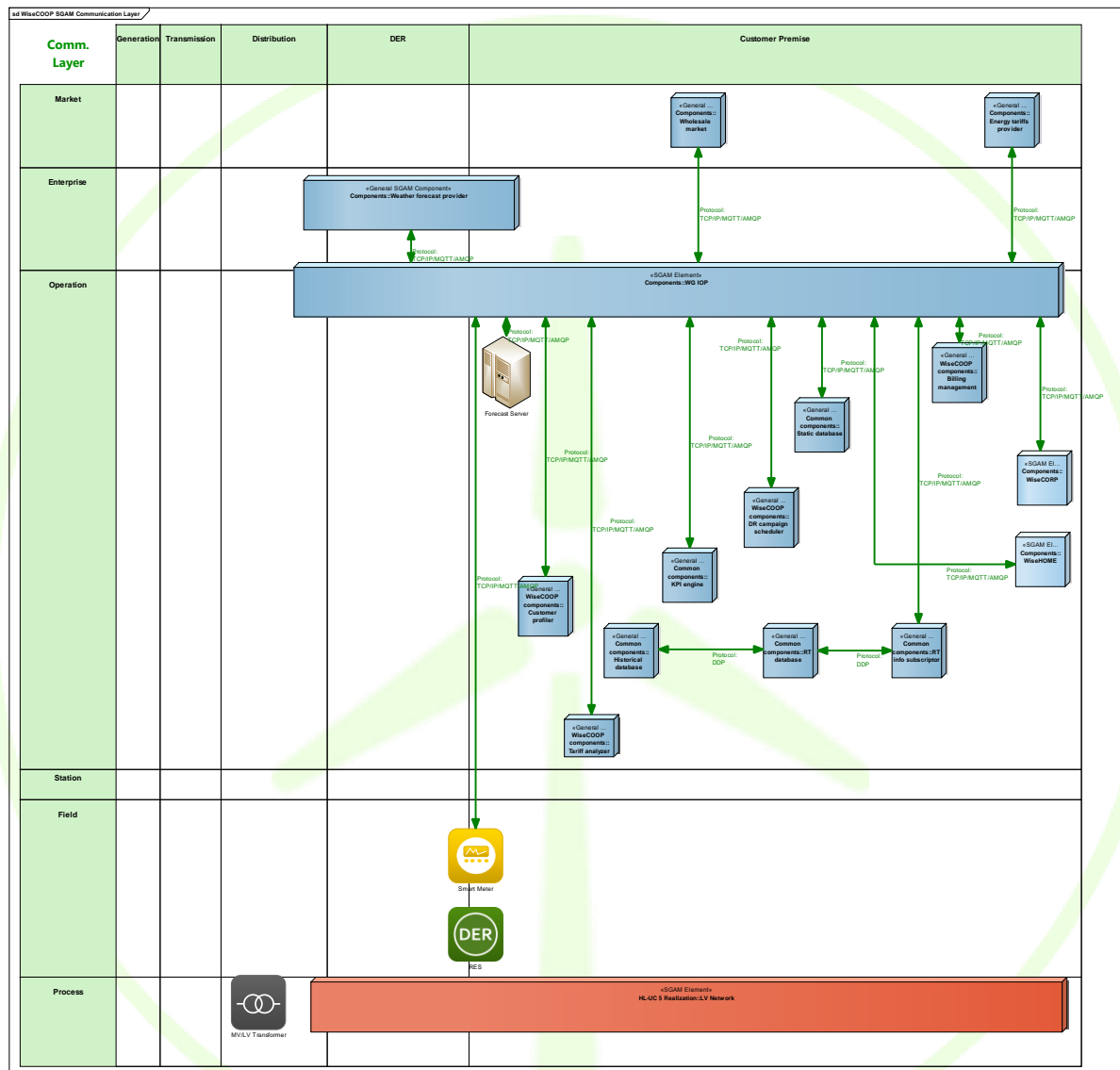
The following table details the different modules composing the WiseCOOP:

Table 12 - WiseCOOP modules

Component	Description
On-site components	Existing components (under DSO premises or control) that will be integrated with WiseCOOP
Smart meters	Smart meters measuring demand and production at members' sites. The application will use the wrappers developed within the project to retrieve energy metering data from those devices.

Component	Description
Horizontal modules	Components that will be reused among different WiseGRID applications
Wholesale market	Module representing the wholesale market. Its purpose is to demonstrate that WiseCOOP is able to produce all information needed by a retailer in order to purchase energy in the wholesale market
Weather forecast provider	Module in charge of providing representative weather forecast and historical data, retrieved from an external specialized provider
Big data platform	Suite of modules specified within the WiseGRID project in order to support big-data related functionalities, including long-term storage and data-mining algorithms
Energy tariff provider	Module providing formal definition of energy tariffs, including economic details and source of the energy (green, renewable resources)
Forecast server	Module supporting the calculation of forecasts required by the WiseCOOP, such as demand and production forecast of the prosumer portfolio
Specific components	Components composing WiseCOOP
RT info. subscriber	Module subscribed to the proper flows of data of the WG IOP - smart meters - and in charge of collecting produced data and pushing it into the proper databases
RT (short-term) database	Specific database focused in daily operation, holding short-term data
Historical (long-term) database	Specific database, supported by the big data platform, focused in long-term storage of data for data-mining purposes
KPI engine	Data-mining algorithm, supported by the big data platform, in charge of calculating and updating KPIs of particular interest to the aggregator
Customer profiler	Module in charge of analyzing different perspectives of the energy usage of the portfolio members (demand, production, flexibility, price elasticity...) and classifying those into groups with similar characteristics, thus allowing the aggregator to operate on sections of the portfolio that share relevant characteristics
Tariff analyzer	Module in charge of handling the work of the retailer related to tariffs. It will consider two main functionalities: facilitating the definition of new tariffs, and simulate the energy costs faced by different members of the portfolio under different tariffs.
Demand response campaign scheduler	Module in charge of scheduling the demand response campaigns over the portfolio, by taking into account forecasted data (production, demand, flexibility, etc.) and other external information. Its output is translated into commands (either automated or manual) to WiseCORP and WiseHOME.
Billing management	Module allowing the aggregator to operate the billing of its customer portfolio, including billing of energy supplied and rewards for the energy produced and active participation on demand response campaigns
WiseCOOP UI	Implements the WiseCOOP operator interface. Based on web technologies, will provide different visualizations accordingly to the different features implemented by the WiseCOOP, including appropriate visions of the managed portfolio, interactions with the wholesale market, real-time monitoring of the energy usage of the portfolio, and graphical tools for designing tariffs and demand response campaigns

Similarly to the architecture presented for other WiseGRID tools, the architecture of the WiseCOOP plans to take advantage of the message brokering technology of the WG IOP to foster the interconnection of the WiseCOOP internal modules as well as its interaction with external actors. The main protocols envisaged to implement these communication flows are MQTT and AMQP.



**Figure 42 - WiseCOOP SGAM Communication layer**

### 7.3 WISECOOP SGAM INFORMATION LAYER

The WiseCOOP information layer represents the logical flows of data among the different modules, also detailing the information items that are conveyed within each one of those flows. This first identification of data items will be useful for the identification and selection of proper common data models and standard interfaces to be used during the implementation phase.

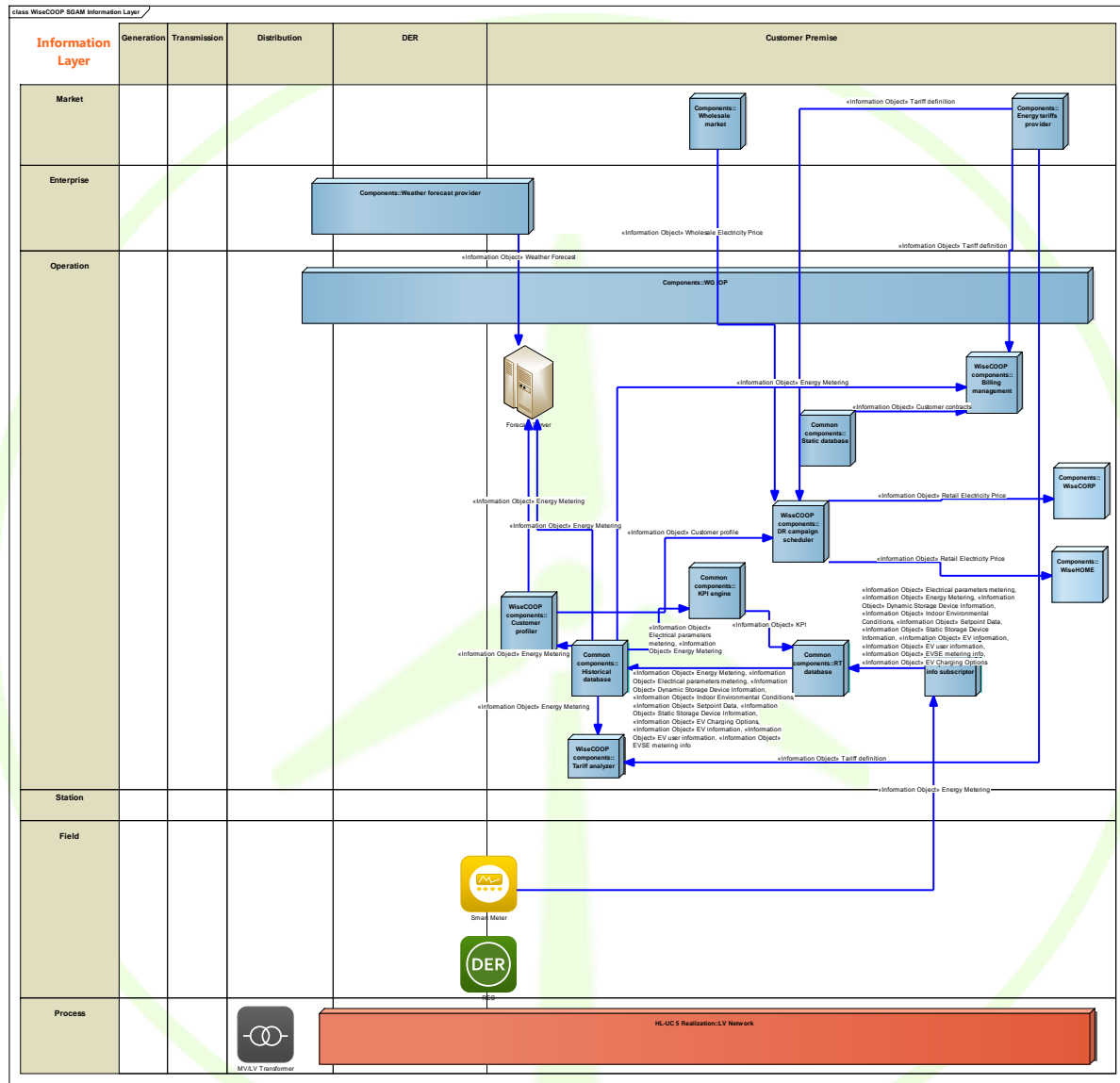


Figure 43 - WiseCOOP SGAM Information layer

In order to facilitate the readout of the details of the information flows, the following simplified diagram depicts the most relevant elements and exchanged data items.



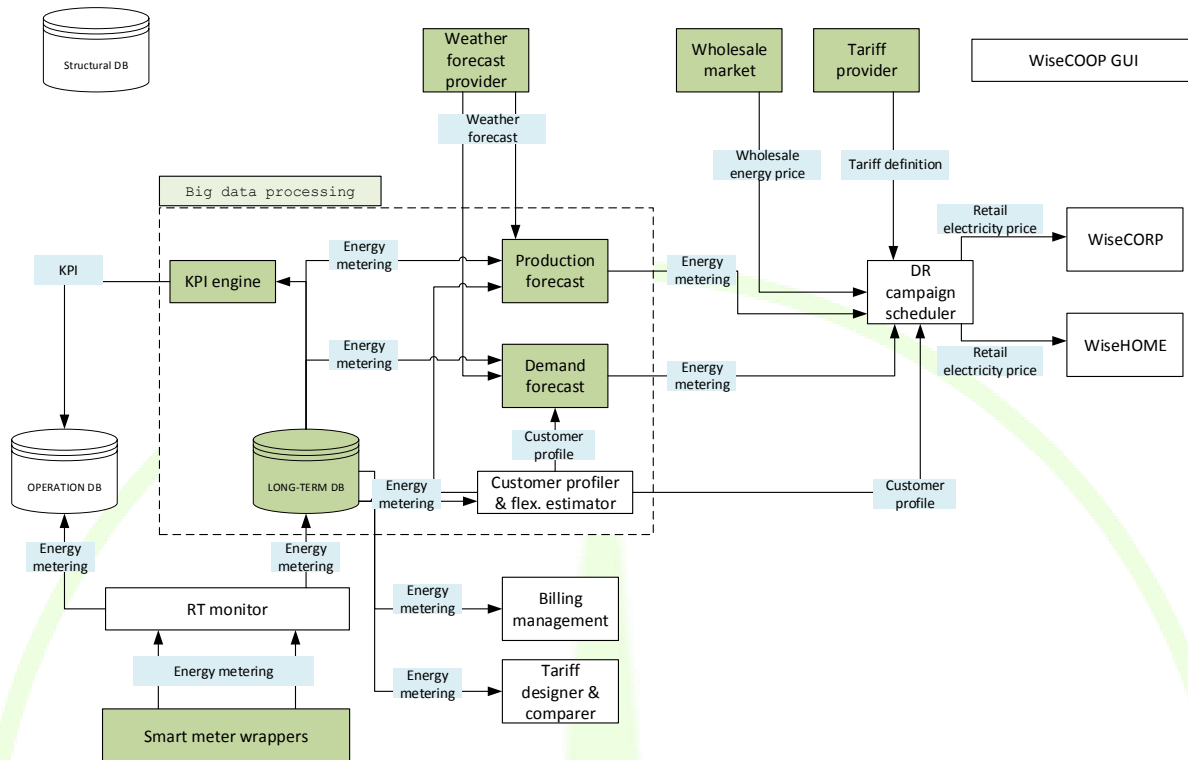


Figure 44 - Important elements and exchanged data items

Table 13 - Data item description

Data item	Description
Energy metering	Energy demand/supply measurements, provided by the smart meters
KPI	Numeric values summarizing the state or evolution of certain variables of interest to the aggregator
Weather forecast	Weather forecast (and historical data) delivered by external provider
Wholesale energy price	Daily curves of price of energy available for purchase at the wholesale market
Tariff definition	Formal definition of the energy tariffs used by the aggregator, including both economic and energy source details
Customer profile	Formal definition of the groups identified within the prosumer portfolio of the aggregator, sharing relevant properties (demand patterns, production patterns, price elasticity), together with their size and members list. Those profiles allow the aggregator to operate the demand response campaigns over groups of similar, whose response is expected to be aligned with the purpose of the campaign
Retail electricity price	Formal definition of the (dynamic) prices to be applied by the aggregator to its customers. Facilitates the execution of implicit demand response campaigns

The following table summarizes some of the relevant standards, data models and open protocols identified for the data to be handled by WiseCOOP

**Table 14 - Items and related data models**

Data item	Related data model or standard
Energy metering	CIM - DLMS/COSEM
Weather forecast	CIM
Flexibility forecast	USEF
Retail electricity price	OpenADR

## 7.4 WISECOOP PRIVACY AND DATA PROTECTION

Tables for the results of the assessment related to the WiseCOOP are presented below.

**Table 15 - Threat and feared events identification for WiseCOOP**

Feared events	Threat ID	Threat name	Brief explanation why relevant
Disappearance of personal data: they are not or no longer available	ED	Eavesdropping of computer channels	Interception of Ethernet traffic; acquisition of data sent over a Wi-Fi network, etc
Diverting of personal data to other users: they are distributed to people that have no need	DoS	Denial of service	Denial of service will lead to unavailability of computing system
	IISC	Insufficient information security controls	Unauthorized parties obtain access to personal information by breach of security or lack of security implementation.
Unwanted change in personal data: they are altered or changed	LQD	Lack of quality of data for the purpose of use	If data is used for certain processes it should be adequate.

## 8 WG STAAS ARCHITECTURE SPECIFICATION

WiseGRID STaaS/VPP is a platform developed in WiseGRID context to manage a communication and information flow of many system to get an improvement on the behavior of the whole system.

The main goal of this platform is to establish a communication way to exchange information about every single system for becoming these individual energy storage system as more complex system with better efficiency and capacity.

### Features

An analysis of the use cases focused on the WiseSTaaS/VPP shows the need for the following features of the tool:

- Many kinds of generation must be supported:
  - Generation by means large power plants
  - Generation by means intermediate RES power plants
  - Distributed generation by means several types of renewable energy sources.
- The platform must be able to control several information fluxes from market requirements, user consumption and ever generation.
- WiseSTaaS/VPP tool must be focused on ancillary services market as a mainly operation objective. This option becomes the energy storage system as a new actor type, due to is able to work behind-the-meter and helping the system to improve grid stability.
- Forecast info it is no necessary to be gotten by WiseSTaaS//VPP platform, but the system must have access to this information in order to plan next actions.

### 8.1 WG STAAS SGAM COMPONENT LAYER

In order to include all required functionalities of the tool the modules are represented under the SGAM domains/zones matrix. Most modules fall under the *Customer premise* SGAM domain - as WG STaaS/VPP features relate with the business of the aggregator of prosumers - and under the *operation* zone - since most features are intended to execute a monitoring and control of the energy-demanding assets.

The main external elements to be integrated with WG STaaS/VPP are the following ones:

- Smart meters: Measurement of prosumers consumption and production. It is one of the most important information in this process, due to it is an essential input to algorithm.
- Storage controller: The mainly actor in this process. Ever Energy Storage System must incorporate one for controlling its processes.
- Forecast server: Provides information about consumption, production and forecast capabilities.
- WiseCORP, WiseCOOP WG Cockpit following different goals everyone. The information fluxes can be shared between them to improve the performance of the whole system.

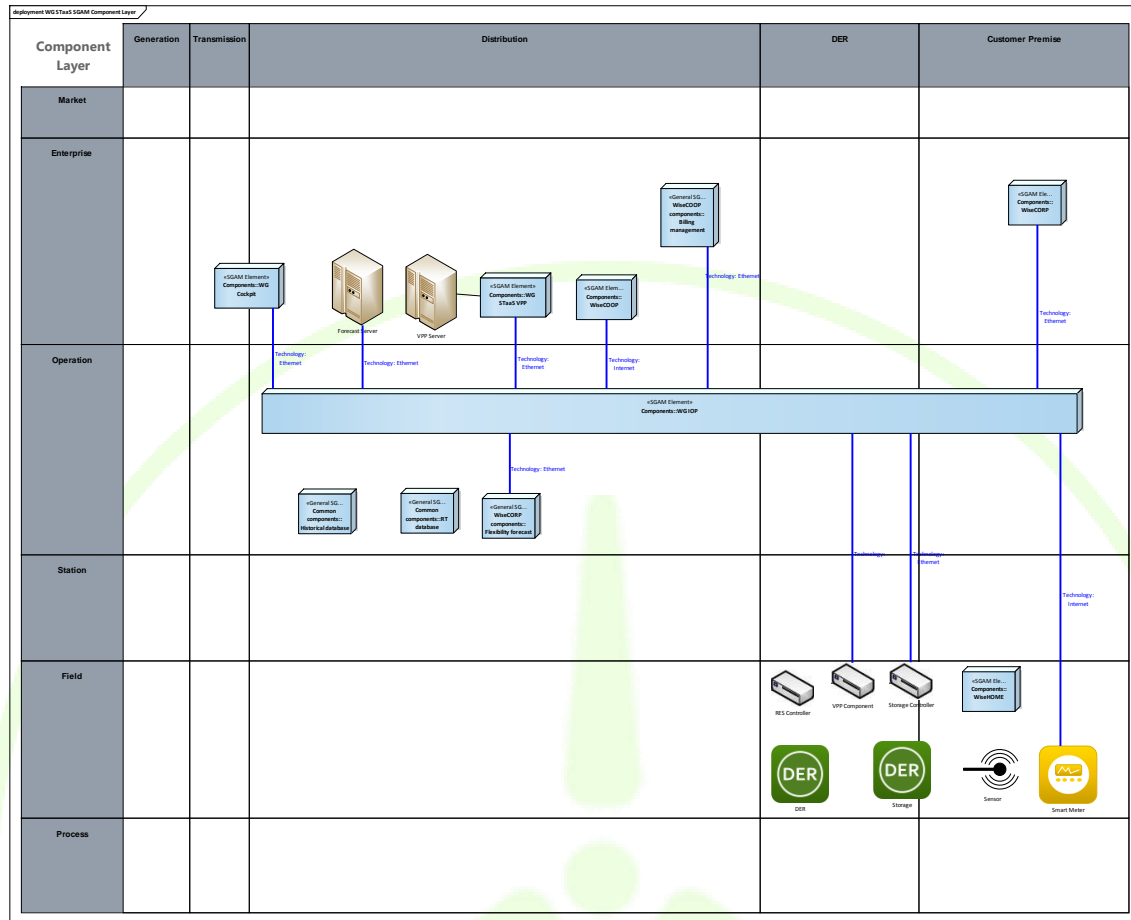


Figure 45 - WG StaaS Component Layer

Table 16 - WG StaaS Components

Component	Description
On-site components	Existing components (under 3 <sup>rd</sup> party premises but RESCO control) that will be integrated with WGRESco
VPP component	VPP related info exchanger
RES Controller	RES equipment related controller
Storage Controller	Energy Storage related controller
Storage	Energy Storage related controller
DER	DER equipment related controller
Forecast Server	Forecast information provider
VPP Server	VPP info exchanger platform

## 8.2 WG STAAS SGAM COMMUNICATION LAYER

Similarly to the architecture presented for other WiseGRID tools, the architecture of the WiseSTaaS/VPP takes advantage of the message brokering technology of the WG IOP to interconnect the different modules in a fast and reliable way. The communication architecture of WiseSTaaS/VPP is based on the communication between user and market, with the Interoperable platform and main control of WiseSTaaS/VPP platform as a center of this information.

The other large communication channel is established between Ancillary Services Market and WiseIOP and WiseSTaaS/VPP. This communication set the operation point based on market requirements, as a voltage control or frequency regulation.

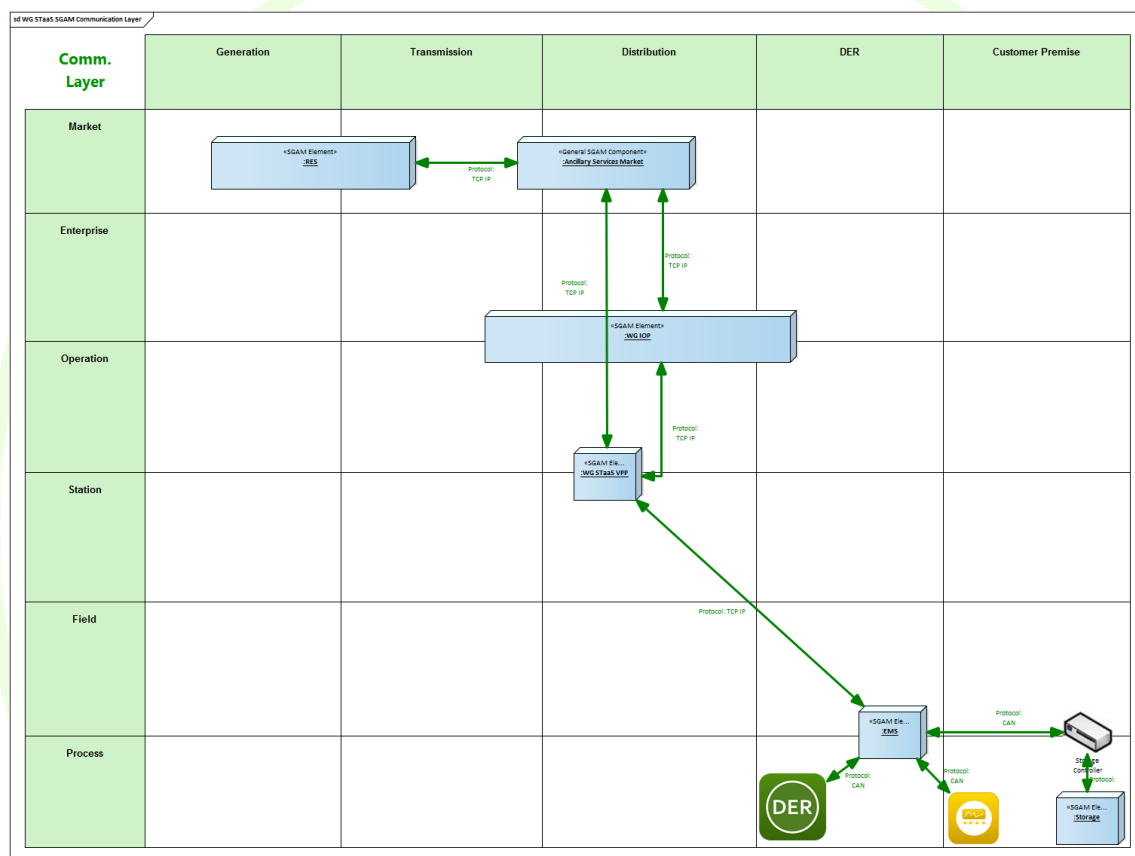


Figure 46 - WG StaaS Communication Layer

## 8.3 WG STAAS SGAM INFORMATION LAYER

The WiseSTaaS/VPP information layer represents the logical flows of data among the different modules, also detailing the information items that are conveyed within each one of those flows. This first identification of data items will be useful for the identification and selection of proper common data models and standard interfaces to be used during the implementation phase.

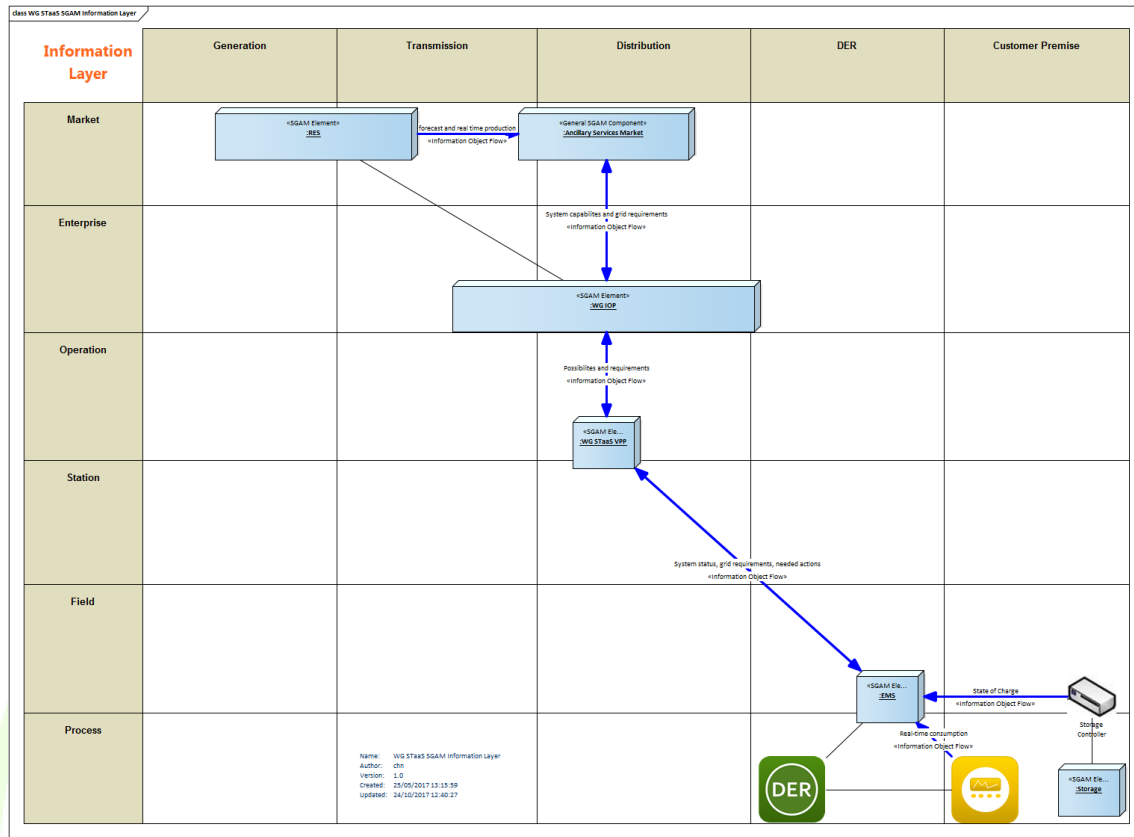
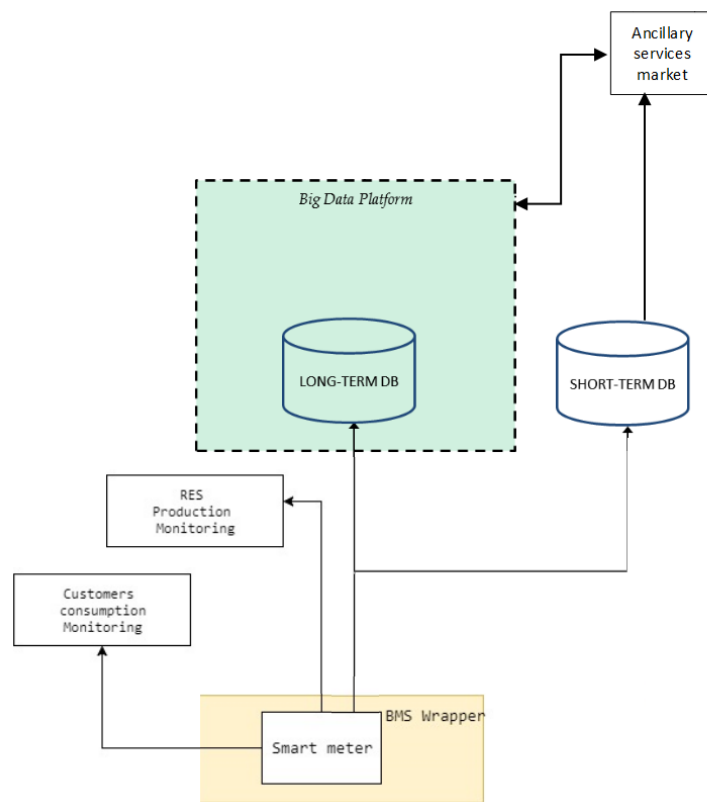


Figure 47 - WG STaaS Information Layer

## Related standards

Figure 48 - Items and related data models

Data item	Related data model or standard
Consumption	OpenADR
Dynamic Storage Device Information	OpenADR
Energy Metering	DLMS/COSEM
Market requirements	DLMS/COSEM



**Figure 49 - Important elements and exchanged data items**



## 8.4 WG STaaS PRIVACY AND DATA PROTECTION

Tables for the results of the assessment related to the WG STaaS are presented below.

**Table 17 - Threat and feared events identification for WiseGRID STaaS**

Feared events	Threat ID	Threat name	Brief explanation why relevant
Disappearance of personal data: they are not or no longer available	ED	Eavesdropping of computer channels	Interception of Ethernet traffic; acquisition of data sent over a Wi-Fi network, etc
Diverting of personal data to other users: they are distributed to people that have no need	DoS	Denial of service	Denial of service will lead to unavailability of computing system
Diverting of personal data to other users: they are distributed to people that have no need	CDEEA	The protection of data is compromised outside the European Economic Area (EEA).	There is a risk that smart metering data may be at risk if sent outside of the EEA.

## 9 WISEEVP ARCHITECTURE SPECIFICATION

WiseEVP is the WiseGRID technological solution for

- Vehicle-sharing companies or electric vehicle fleet managers and
- Electric vehicle infrastructure (EVSE) operators

In order to optimize the activities related with smart charging and discharging of the EVs including V2G (vehicle to grid, energy injection in the distribution network) and V2H (vehicle to home, energy injection in the household electric installation).

The management of the EVSEs charging and discharging processes will meet the following objectives:

- Reduce the EV charging energy bill.
- Follow flexibility requests from DSO to help the electric distribution network operation in exchange for an economic compensation.
- Follow flexibility requests to increase injection of RES production reducing curtailment in exchange for an economic consideration compensation.
- Contribute in the household energy management system with the main objectives of reducing the energy bill and maximize local RES production.

All the aforementioned objectives will be subordinated to the EV user preferences: desired state of charge (SOC) at the time of unplugging the EV.



Figure 50 - WiseEVP

### Features

An analysis of the different use cases focused on WiseEVP shows the need for the following features to be implemented:

- Management of EVSE portfolio: the tool shall facilitate the access to the metadata and real-time status of the deployed EVSEs, including
  - Static characteristics (model, location, max. power...)

- Dynamic characteristics (status, supplied power...)
- Management of EV portfolio: similarly, the tool shall provide access the details about the vehicles that compose the fleet, including
  - Static characteristics of the vehicles (model, connector model, battery model, capacity, max. admissible power...)
  - Dynamic characteristics (state of charge, location, energy in the battery...)
- Operational management of charging sessions: refers to the core functionality of the WiseEVP, which is its ability to manage the charging sessions in a dynamic way in order to optimize the objective of the organization - minimize economic costs, maximize green energy usage - while fulfilling the constraints imposed by the requirements of the organization - availability and min. charge of the vehicles. This management implies the implementation of the following capabilities:
  - User authentication
  - Process charging session requests and booking
  - Monitor load demand and perform forecasting
  - Smart charging scheduling (optimized towards costs or source of energy)
- Operational management of ancillary services and V2G: refers to the capability of the operator to provide ancillary services to the DSO through the execution of demand response campaigns. WiseEVP will need to handle with rescheduling of the charging sessions upon requests of demand modulation, considering also the possibility to inject energy back to the grid if required (V2G). This management requires the following functionalities:
  - Flexibility estimation according to current plan and demand forecast
  - Participation in ancillary services market (through reschedule of charging sessions, taking into account V2G possibility)
    - Active power reserve (voltage support)
    - Grid outage fast restoration support
    - Peak-shaving, load harmonization (congestion support)
    - Backup power

## 9.1 WISEEVP SGAM COMPONENT LAYER

The WiseEVP SGAM component layer presents the set of modules that are deemed necessary in order to implement all functionalities required by the use cases. The modules are represented under the SGAM domains/zones matrix. Most modules fall under the *Customer premise* SGAM domain - as WiseEVP handles assets that are owned by organizations that are consumers of energy supplied by DSOs - and under the *operation* zone - since most features are intended to execute a monitoring and control of the energy-demanding assets.

The main external elements to be integrated with WiseEVP are the following ones:

- Charging Stations (EVSEs): are used by the operator of WiseEVP to charge the vehicles of the fleet. In fact, these elements are the ones that handle the charge operation, and therefore any actuation of WiseEVP towards optimizing the energy required from the grid to charge

the vehicles needs to command those elements. Depending on its capabilities, the optimization algorithms will have different degrees of freedom:

- Most basic EVSEs will just allow static charging - i.e. once the charge session starts, vehicle is charged as fast as possible). Control strategies in these cases will include smart activation/deactivation of the supply
- Advanced EVSEs will allow dynamic charging - i.e. the power supplied to the vehicles can be modulated. Control strategies in these cases will include the ability to change the supplied power without pausing the charge process
- EVSEs with V2G capabilities: within the project, WG FastV2G will provide V2G capabilities, thus enabling the execution of advanced ancillary services to other actors of the grid and more advanced optimization algorithms considering, for instance, transferring energy from one vehicle to another if required
- Electric vehicles: conform the fleet of the operator. Minimum information to be retrieved from those includes the state of charge upon connection to the EVSE - which determines the amount and time needed by the charge process - and required availability. In addition, the operator may get benefit if online information about the fleet - real-time location and SoC, battery health indicators... - can be retrieved as well

The following modules are candidates to be developed in order to achieve the required functionalities.

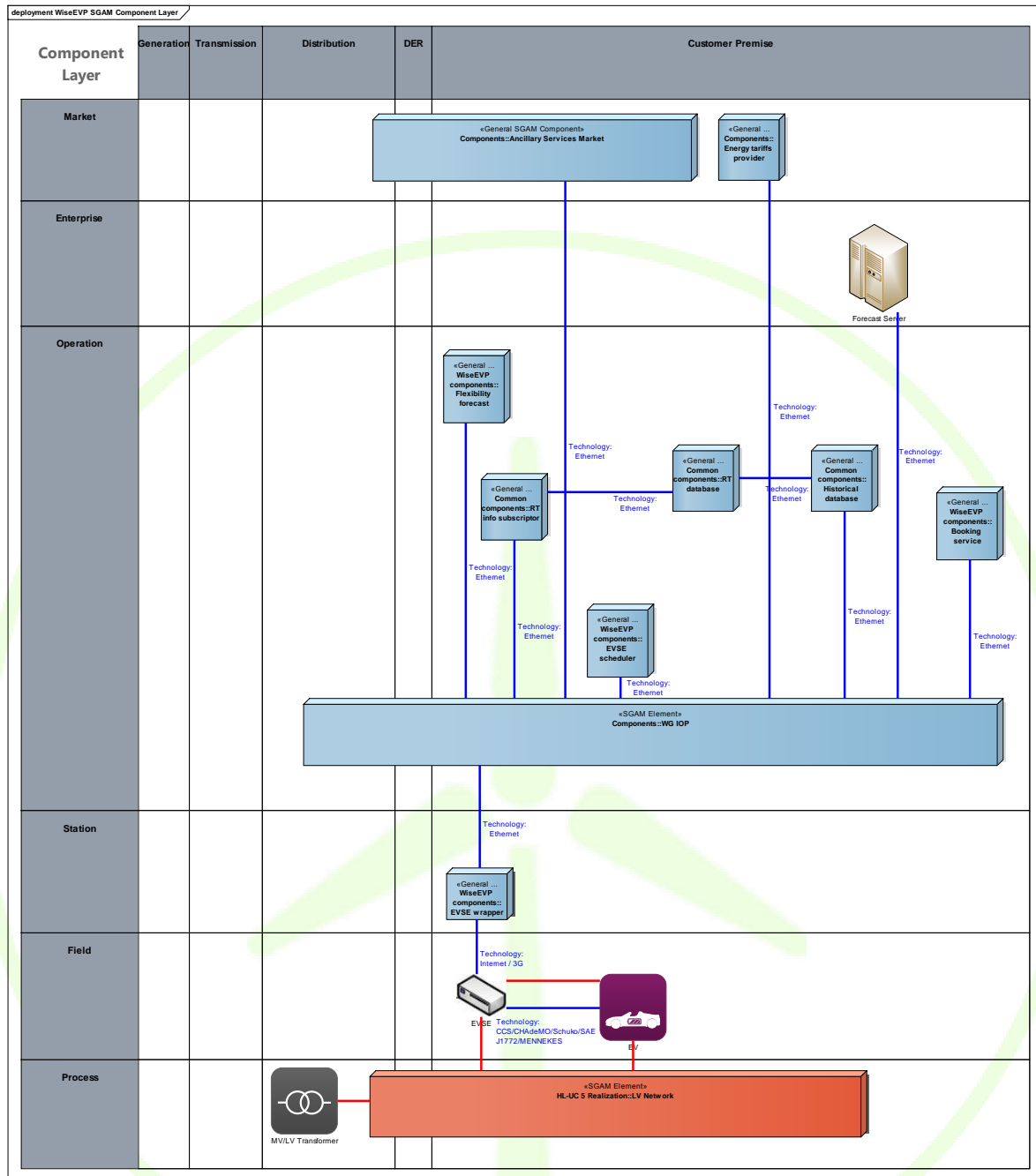


Figure 51 - WiseEVP SGAM Component layer

The following table details the different modules composing WiseEVP:

**Table 18 - WiseEVP modules**

Component	Description
On-site components	Existing components (under DSO premises or control) that will be integrated with WiseEVP
EVSE	Charging stations, in charge of supplying energy to the vehicles (or retrieving it from the vehicle in V2G scenarios) as required by the central control system
Electric Vehicle	Core asset of the WiseEVP operator, imposing energy demand and availability requirements
Horizontal modules	Components that will be reused among different WiseGRID applications
Forecast server	Module supporting the calculation of forecasts required by the WiseEVP, such as demand forecast accordingly to historical data and current charge processes scheduled
Ancillary Services Market	Binding module between WG Cockpit - which will demand support upon the detection or forecast of certain problems in the distribution grid - and the rest of WiseGRID applications - including WiseEVP, which may be able to support the operation of the DSO in preventing and solving those problems, mainly by modulating their demand or activating specific voltage control support features. This module will be in charge of the orchestration of these supporting services
Big data platform	Suite of modules specified within the WiseGRID project in order to support big-data related functionalities, including long-term storage and data-mining algorithms
Energy tariff provider	Module providing formal definition of energy tariffs, including economic details and source of the energy (green, renewable resources)
Specific components	Components composing WiseEVP
EVSE Wrapper	Module in charge of publishing data from the EVSEs into the WiseGRID application ecosystem via the WG IOP, as well as exposing the required EVSE functionalities with a common interface, independently of the custom communication protocol of the underlying EVSE
RT info. subscriber	Module subscribed to the proper flows of data of the WG IOP - EVSEs and EVs - and in charge of collecting produced data and pushing it into the proper databases
RT (short-term) database	Specific database focused in daily operation, holding short-term data
Historical (long-term) database	Specific database, supported by the big data platform, focused in long-term storage of data for data-mining purposes
Booking service	Module allowing customers of the EVSE/Fleet manager to book particular EVSEs and vehicles for future use
EVSE scheduler	Core of the system, implementing most of the business logic. This module is in charge of scheduling the operation of all EVSEs operated by the system, by taking into account operational constraints (operator preferences) and other constraints imposed by external actors (e.g. congestion constraints triggered by DSO). It also has to optimize energy cost/CO2 emissions (tariffs analysis)
Flexibility forecast	Taking into account historical information and currently scheduled charging sessions, will forecast the flexibility that can be offered to the ancillary services market

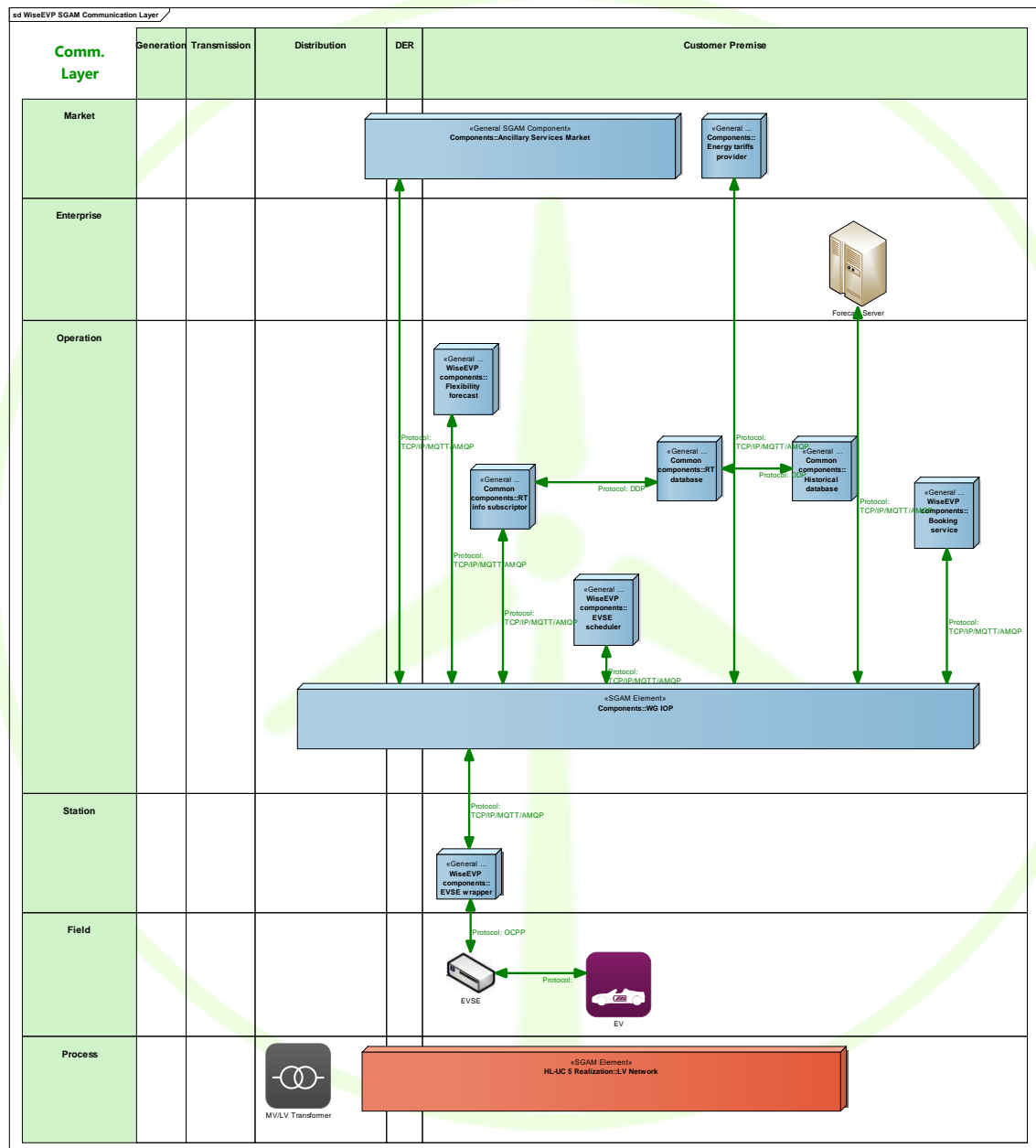
Component	Description
WiseEVP UI	Implements the WiseEVP operator interface. Based on web technologies, will provide different visualizations accordingly to the different features implemented by the WiseEVP, including an appropriate selection of real-time information displayed over GIS georeferenced data and over a dashboard, detailed views of the data and assets being managed, including information about ongoing charge sessions, problems detected, etc.





## 9.2 WISEEVP SGAM COMMUNICATION LAYER

Similarly to the architecture presented for other WiseGRID tools, the architecture of WiseEVP puts the WG IOP message broker in the center of the main communication flows, in order to take advantage of the features that will be delivered by this technology - reliable, fast and open mechanism to interconnect different modules within the WiseGRID application ecosystem. WiseEVP communication among the different submodules will be based on the open standards offered by the WG IOP (mainly, AMQP and MQTT are envisaged).



**Figure 52 - WiseEVP SGAM Communication layer**

The WiseEVP information layer shows the logical flows of data among the different modules, also detailing the information items that are conveyed within each one of those flows. This first identification of data items present in the operation of WiseEVP will further support the evaluation and selection of the proper common data models and standard interfaces to be used during the implementation.



### D3.1 WiseGRID Architecture, Data Models, Standards and Data Protection (V1)

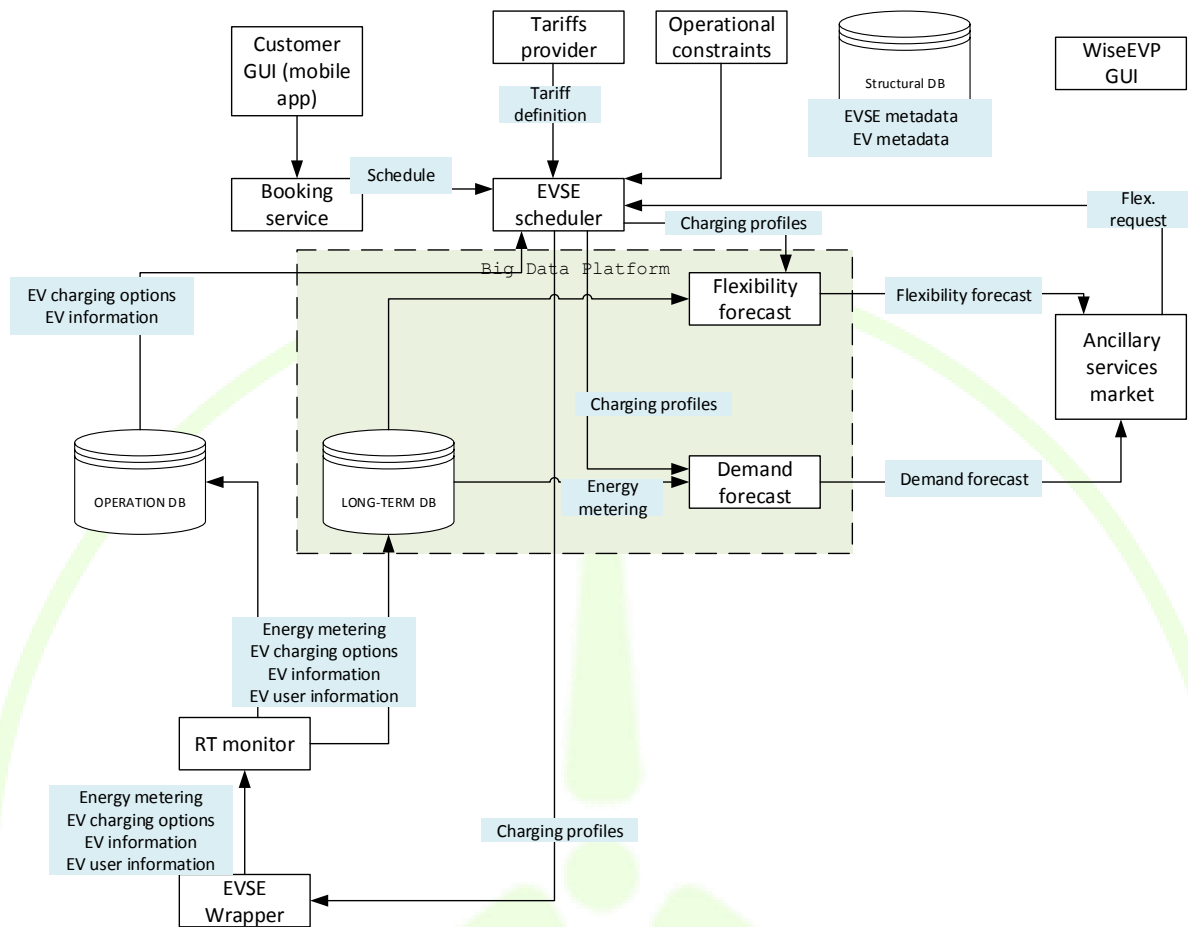


Figure 54 - Important elements and exchanged data items

Table 19 - Data item description

Data item	Description
EVSE metadata	Relevant data of the EVSEs managed by the system (id, model, location, max. power...)
EV metadata	Relevant data of the EVSEs managed by the system (id, model, battery model, SoC...)
Energy metering	Energy demand/supply measurements, provided by the EVSEs
EV information	Upon connection of a vehicle to an EVSE, details of the currently connected EV (id, SoC)
EV user information	Upon connection of a vehicle to an EVSE, details of the user requesting the charge session (id)
EV charging options	Upon connection of a vehicle to an EVSE, restrictions imposed to the current charging operation (energy required, time available, supply constraints)
Schedule	Formal definition of a future charge operation requested at the booking service module

Data item	Description
Charging profiles	Optimum charging profiles calculated by the EVSE scheduler. Those are defined by temporal curves that set the power to be supplied by each one of the EVSEs
Tariff definition	Formal definition of the energy tariffs used by the EVSE operator, including both economic and energy source details
Demand forecast	Temporal curves defining the expected energy demand of the system in the future, per regulation area
Flexibility forecast	Temporal curves defining up to which extent the current and expected charging profiles can be modified in order to provide ancillary services to third party actors, per regulation area
Flexibility request	Activation of flexibility as requested by third party actors. Includes a temporal curve of the requested demand reduction, together with a temporal curve informing of the available grid capacity, thus allowing the scheduler to properly reorganize the charging profiles

The following table summarizes some of the relevant standards, data models and open protocols identified for the data to be handled by WiseEVP

**Table 20 - Items and related data models**

Data item	Related data model or standard
Asset geolocation data	GeoJSON
Energy metering	CIM - DLMS/COSEM
Demand forecast	USEF
Flexibility forecast	USEF
Flexibility request	USEF
EVSE metadata	OCPP
Charging profiles	OCPP
EV information	OCPP
EV user information	OCPP

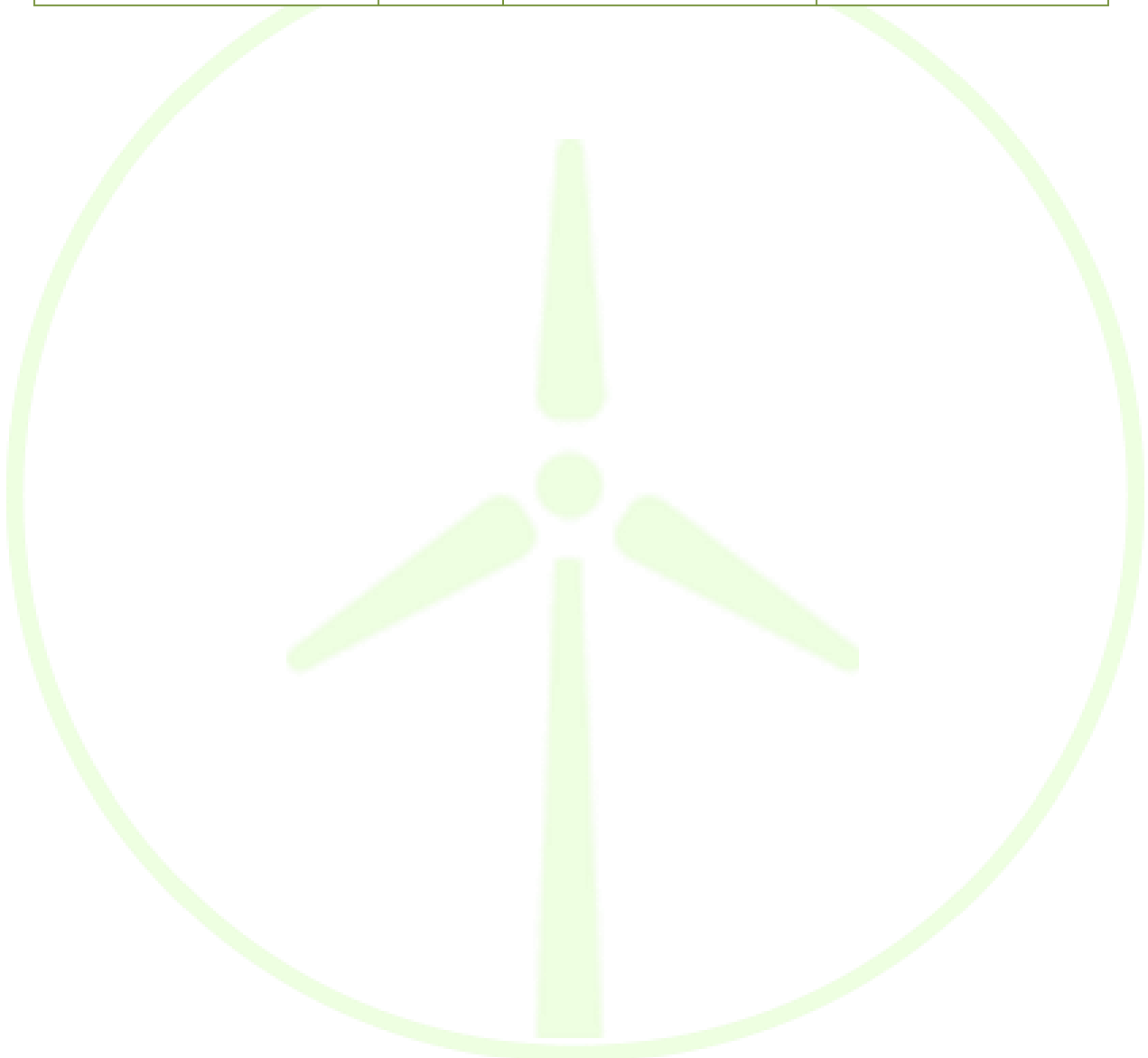
## 9.4 WISEEVP PRIVACY AND DATA PROTECTION

Tables for the results of the assessment related to the WiseEVP Cockpit are presented below.

**Table 21 - Threat and feared events identification for WiseEVP**

Feared events	Threat ID	Threat name	Brief explanation why relevant
Disappearance of personal data: they are not or no longer available	ED	Eavesdropping of computer channels	Interception of Ethernet traffic; acquisition of data sent over a Wi-Fi network, etc

Feared events	Threat ID	Threat name	Brief explanation why relevant
Diverting of personal data to other users: they are distributed to people that have no need	DoS	Denial of service	Denial of service will lead to unavailability of computing system
Unwanted change in personal data: they are altered or changed	ADNI	Access to data that was not intended (not necessary for the purpose of collection)	The subjects could access data not owned by them.



## 10 WG FASTV2G ARCHITECTURE SPECIFICATION

WG FastV2G is the WiseGRID technological solution to use EVs as dynamic distributed storage devices. Under smart grid environment, where two-way instantaneous communication is available, the energy flow from EVs to the grid is feasible. Energy stored in the batteries of available vehicles runs back to the grid when needed (fast V2G supply) to support ease up domestic peak load.

Therefore, the main goal of this solution is make possible the energy transfer from the vehicle to the grid (V2G) as proactive method of balancing utility supply and demand. In V2G, the grid operator communicates directly with individual EVs regarding their availability for services such as providing peak power, spinning reserves and frequency regulation, or makes use of real time markets to deliver these services

V2G could provide the distributed resource the utility grid and infrastructure needs to supplement generating capacity and alleviate transmission grid bottlenecks today and into the future. Most EVs are in actual operation for few hours per day; so, vehicles could be connected to the utility grid for the majority of the day. Thus, the energy stored in the vehicle's battery could be used for other purposes as long as the vehicle battery is sufficiently charged for the EV owners commute.



Figure 55 - WiseFASTV2G

### Features

An analysis of the use cases focused on the WG FASTV2G shows the need for the following features of the tool:

- Management of EVSE portfolio: the tool shall facilitate the access to the metadata and real-time status of the deployed EVSEs, including
  - Static characteristics (model, location, max. power...)
  - Dynamic characteristics (status, supplied power...)
- Management of EV portfolio: similarly, the tool shall provide access the details about the vehicles that compose the fleet, including
  - Static characteristics of the vehicles (model, connector model, battery model, capacity, max. admissible power...)
  - Dynamic characteristics (state of charge, location, energy in the battery...)
- Operational management of charging sessions: refers to the functionality of the WG FastV2G, which is to communicate EVs status to grid Operator. This management implies the implementation of the following capabilities:

- Monitor load demand and perform forecasting
- Smart charging scheduling (optimized towards costs or source of energy)
- Operational management of ancillary services: refers to the capability of the operator to provide ancillary services to the DSO support the stable operation of the electric system from EVs batteries. This management implies the implementation of the following capabilities:
  - Flexibility estimation according to current plan and demand forecast
  - Participation in ancillary services market (through reschedule of charging sessions, taking into account V2G possibility)
    - Active power reserve (voltage support)
    - Grid outage fast restoration support
    - Peak-shaving, load harmonization (congestion support)
    - Backup power

### 10.1 WG FASTV2G SGAM COMPONENT LAYER

The WG FastV2G SGAM component layer presents the set of modules that are considered in order to include all required functionalities of the tool. The modules are represented under the SGAM domains/zones matrix. Most modules fall under the *Customer premise* SGAM domain - as WG FASTV2G features relate with the business of the aggregator of prosumers - and under the *operation* zone - since most features are intended to execute a monitoring and control of the energy-demanding assets.

The main external elements to be integrated with WG FASTV2G are the following ones:

- Charging Stations (EVSEs): are used by the operator of WiseEVP to charge the vehicles of the fleet. In fact, these elements are the ones that handle the charge operation, and therefore any actuation of WiseEVP towards optimizing the energy required from the grid to charge the vehicles needs to command those elements. According, WG FastV2G functionalities the optimization algorithms related to enabling the execution of advanced ancillary services to other actors of the grid and more advanced optimization algorithms considering, for instance, transferring energy from one vehicle to another if required.
- Electric vehicles: conform the fleet of the operator. Minimum information to be retrieved from those includes the state of charge upon connection to the EVSE - which determines the amount and time needed by the charge process - and required availability. In addition, the operator may get benefit if online information about the fleet - real-time location and SoC, battery health indicators... - can be retrieved as well
- WG STaaS/VPP and WiseHOME: WiseGRID applications targeting the different profiles (tertiary and domestic) of the DSO portfolio. The demand response operations will be reflected in actions and information presented by those two applications.

The following modules are candidates to be developed in order to achieve the required functionalities.

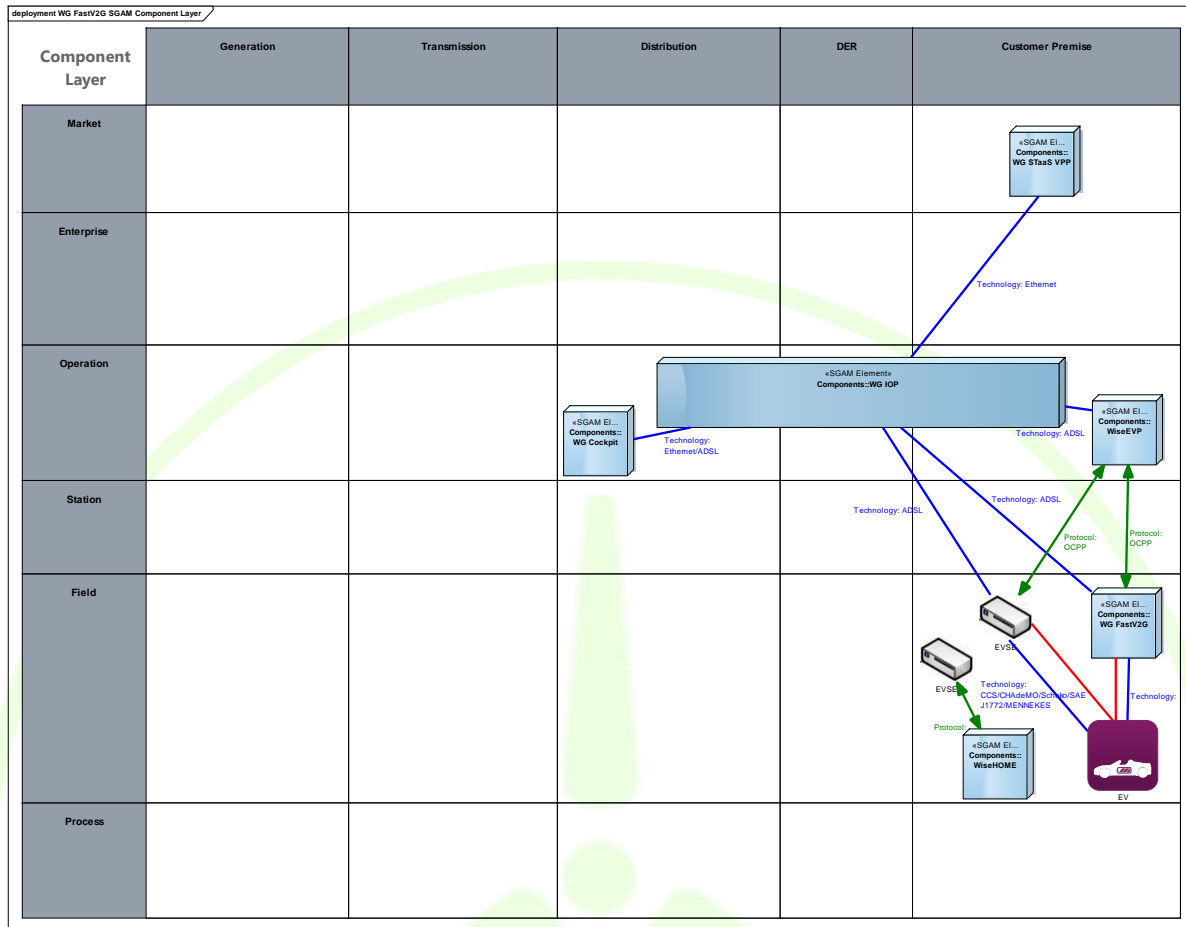


Figure 56 - SGAM Component Layer of WG FastV2G

The following table details the different modules composing the WG FastV2G.

Table 22 - WG FastV2G modules

Component	Description
On-site components	Existing components (under DSO premises or control) that will be integrated with WG FastV2G
Horizontal modules	Components that will be reused among different WiseGRID applications
Specific components	Components composing WG FastV2G
Big data platform	Suite of modules specified within the WiseGRID project in order to support big-data related functionalities, including long-term storage and data-mining algorithms
WG FastV2G UI	Implements the WG FASTV2G operator interface. Based on web technologies, will provide different visualizations accordingly to the different features implemented by the WG FASTV2G, including appropriate visions of the managed portfolio, interactions with the wholesale market, real-time monitoring of the energy usage of the portfolio, and graphical tools for designing tariffs and demand response campaigns
EVSE	Charging stations, in charge of supplying energy to the vehicles (or retrieving it from the vehicle in V2G scenarios) as required by the central control system



Electric Vehicle	Core asset of the WiseEVP operator, imposing energy demand and availability requirements
------------------	--

## 10.2 WG FASTV2G SGAM COMMUNICATION LAYER

Similarly to the architecture presented for other WiseGRID tools, the architecture of WG FASTV2G devises to take advantage of WG IOP message broker functions to develop a reliable, fast and open mechanism to interconnect WG FastV2G internal modules as well as its interaction with external actors. WG FastV2G communication flow among the different submodules will be based on the open standards envisage by the WG IOP (mainly, AMQP and MQTT).

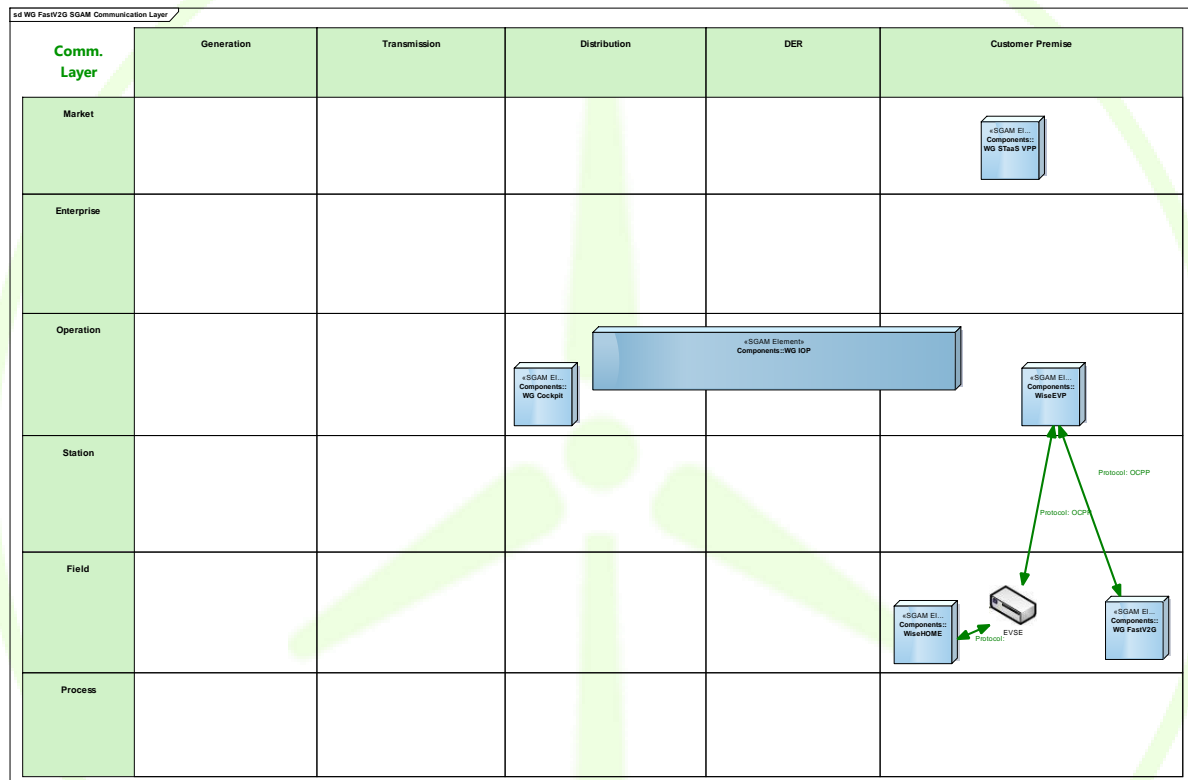


Figure 57 - SGAM Communication Layer of WG FastV2G

### 10.3 WG FASTV2G SGAM INFORMATION LAYER

The WG FastV2G information layer represents the logical flows of data among the different modules, also detailing the information items that are conveyed within each one of those flows. This first identification of data items will be useful for the identification and selection of proper common data models and standard interfaces to be used during the WG FastV2G implementation phase.

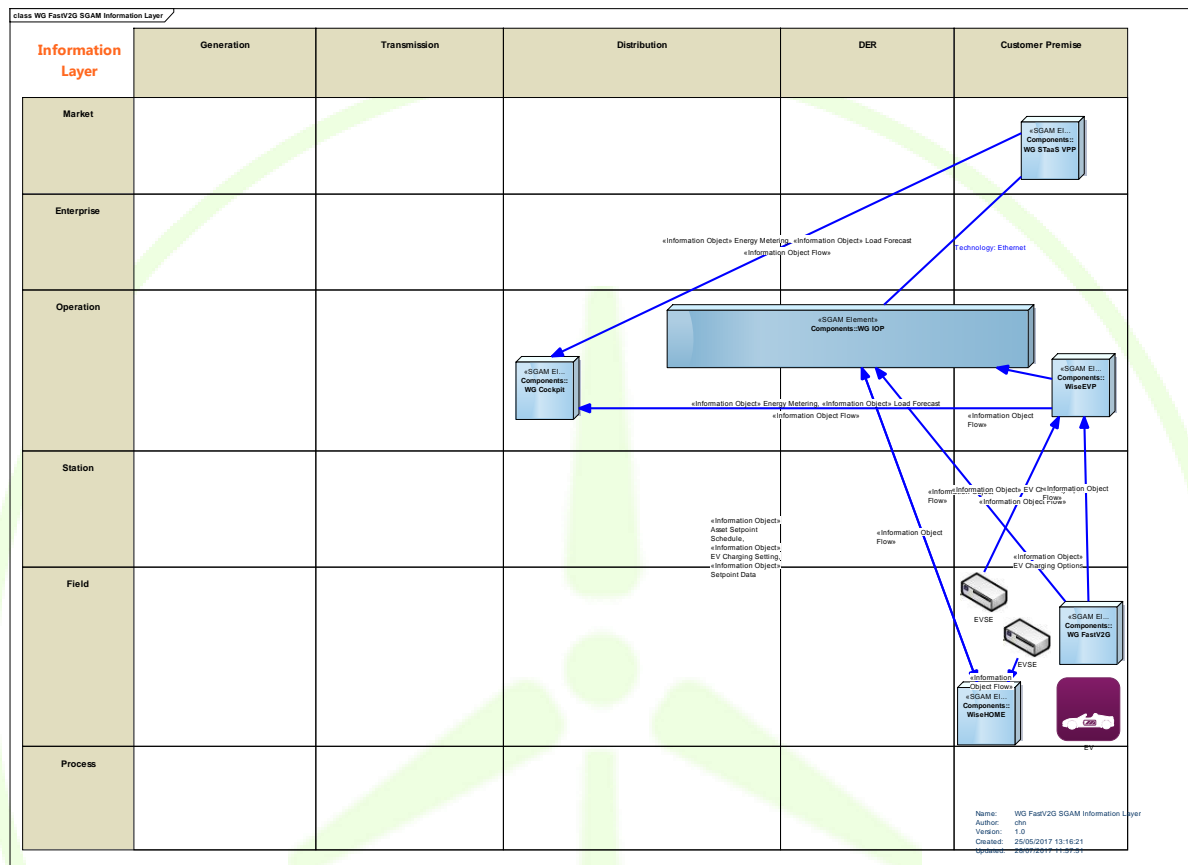
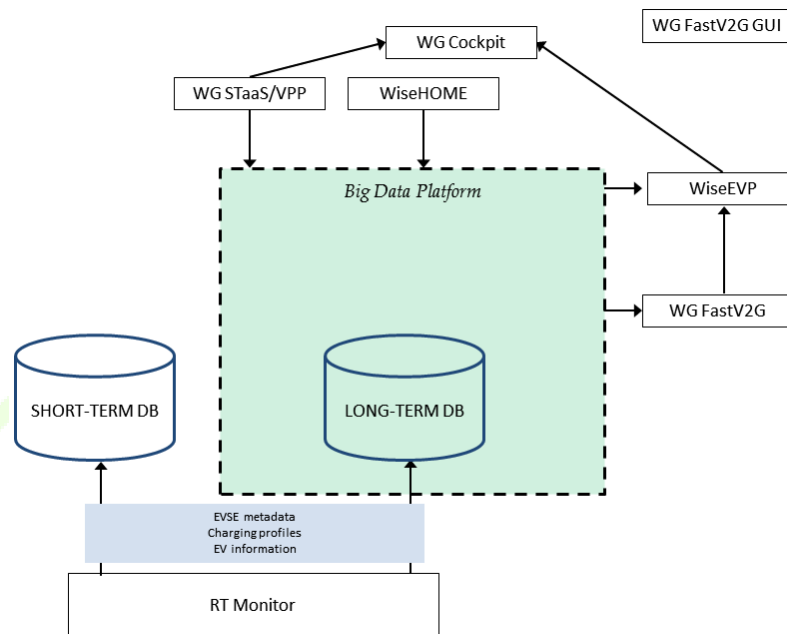


Figure 58 - SGAM Information Layer of WG FastV2G

In order to facilitate the readout of the details of the information flows, the following simplified diagram depicts the most relevant elements and exchanged data items.



**Figure 59 - Information flow for the WG FastV2G tool**

**Table 23 - Data item description**

Data item	Description
EVSE metadata	Relevant data of the EVSEs managed by the system (id, model, location, max. power...)
EV information	Upon connection of a vehicle to an EVSE, details of the currently connected EV (id, SoC)
Charging profiles	Upon connection of a vehicle to an EVSE, restrictions imposed to the current charging operation (energy required, time available, supply constraints)

The following table summarizes some of the relevant standards, data models and open protocols identified for the data to be handled by WG FastV2G.

**Table 24 - Items and related data models**

Data item	Related data model or standard
EVSE metadata	OCPP
Charging profiles	OCPP
EV information	OCPP

## 10.4 WG FASTV2G PRIVACY AND DATA PROTECTION

Table with the result of the risk assessment for the WG FastV2G tool is presented below.

**Table 25 - Threat and feared events identification for WiseGRID FastV2G**

Feared events	Threat ID	Threat name	Brief explanation why relevant
Disappearance of personal data: they are not or no longer available	ED	Eavesdropping of computer channels	Interception of Ethernet traffic; acquisition of data sent over a Wi-Fi network, etc
	Pobj	Prevention of objections	Data subjects have the right to object to the processing of data. If they want to execute this right it must be (technically) possible.
	HLPL	Hardware loss and Loss of Power	Retrieval of a discarded storage device or hardware; loss of an electronic storage device, etc. Loss of power can harm hardware and software and lead to unavailability
Diverting of personal data to other users: they are distributed to people that have no need	DoS	Denial of service	Denial of service will lead to unavailability of computing system
	IISC	Insufficient information security controls	Unauthorized parties obtain access to personal information by breach of security or lack of security implementation.
Change in processing: it deviates from what was originally planned (diversion of the purpose, excessive or unfair collection)	II	Incomplete information	The information provided to the data subject on the purpose and use of data is not complete
Unwanted change in personal data: they are altered or changed	ADNI	Access to data that was not intended (not necessary for the purpose of collection)	The subjects could access data not owned by them.
Illegitimate access to personal data: they are known by unauthorized persons	IACP	Insufficient access control procedures	Access rights are not revoked when they are no longer necessary.

## 11 WISEHOME ARCHITECTURE SPECIFICATION

WiseHOME is the WiseGRID IT solution that aims to raise the awareness of residential energy users regarding their energy consumption, and more importantly to provide them with detailed analytics that lead to actionable triggers so that they start realizing the benefits of modifying their demand profile. Its ultimate aim is to serve as the user interface that will transform conventional, passive energy consumers in households into active participants of the energy system through modulation of their demand according to the needs of the network and energy supply.

A key factor towards achieving these objectives is the adequate retrieval and analysis of energy usage data, and visualization of meaningful information extracted from it. This information may include:

- Detailed visualization of energy demand at different areas of the home or at different times when other activities are ongoing, helping dwellers to identify opportunities for enhancing energy efficiency;
- Energy tariff comparison, enabling a direct economic cost reduction by shifting to a more profitable tariff;
- Energy demand forecast, enabling medium to long term cost estimations and supporting operative decisions about the usage of the facilities;
- Demand flexibility estimation, allowing the execution of optimization algorithms that will - either automatically or by providing alerts and triggers - shift demand in order to minimize economic costs - by maximizing self-consumption or moving demand to off-peak periods - or minimize environmental impact - by shifting demand to periods where green energy is available.

### Features

The relevant use cases targeted by WiseHOME can be summarized in the following set of features:

- Local monitoring and control of home assets: dwellers need a clear overview and monitoring of the status of the controllable assets, including
  - Demand (electricity and gas)
  - Production (e.g. PV)
  - Controllable loads (space/water heating, space cooling, lighting, etc.)
  - Storage (batteries, EVs)
- Visual analytics for dwellers: smart analysis of the data is needed to assist users in the decision making process:
  - Analysis of evolution of energy usage patterns
  - Energy usage KPIs
  - Energy cost analysis (both economic and environmental)
  - Tariff comparison
- Local optimization: the application will facilitate the execution of local optimization policies, while taking comfort models into account, towards
  - Increasing self-consumption

- Energy cost optimization
- Peak-shaving
- Integration with WiseCOOP: home dwellers - using WiseHOME - will be able to participate in dynamic price schemes.

### 11.1 WISEHOME SGAM COMPONENT LAYER

WiseHOME constitutes the main user interface that enables residential users to become more aware of electricity usage in their household and to leverage novel tariff schemes - e.g. real-time pricing - to reduce their energy costs. One of its main functionalities is monitoring electricity usage - in an as-fine-as-possible granularity - and generating insightful visualizations for the dweller that can lead her to actionable interpretations of energy usage. Examples include usage patterns against price fluctuations (ToU) that can lead to demand shifting, or understanding consumption of idle/standby devices. Once such fundamental aspects become part of people's everyday routine, they can start engaging in more innovative concepts such as revealing and exploiting demand flexibility or participating in the energy markets through real-time pricing tariff plans. The WiseGRID project also includes functionalities for the estimation of demand flexibility within the home. They are not strictly part of the WiseHOME application, but they constitute necessary infrastructure tools for the achievement of the project/WiseHOME objectives.

To achieve its purpose, the WiseHOME relies on information from a number of sources. They include:

- HEMS: home energy management system - if available - that can become the facilitator of information flows between sensors/home devices and the relevant WiseGRID tools (incl. IOP, WiseHOME, etc.). Devices of interest include energy-hungry assets such as the following. In the absence of a HEMS, individual interfaces will be needed (Space heating, water heating, space cooling, lighting, etc.).
- Storage: any electricity storage devices are extremely useful for energy cost optimization strategies
- Space heating/cooling: Technologies can vary greatly from heat-pumps to storage radiators and so on. Regardless of technology, space heating is one of the primary energy consumers in the household.
- Water heating: typically electricity-consuming water tanks. They consume significant electricity and have significant potential for demand shifting.
- Lighting: dimmable lights can offer potential for demand shedding. In combination with occupancy sensing, the flexibility potential is significant.
- Sensors: devices that monitor and process specific input from the physical environment (e.g. light, indoor air quality, temperature, humidity, motion/occupancy, etc.)
- The following modules are envisaged to be developed in order to implement the required functionalities.

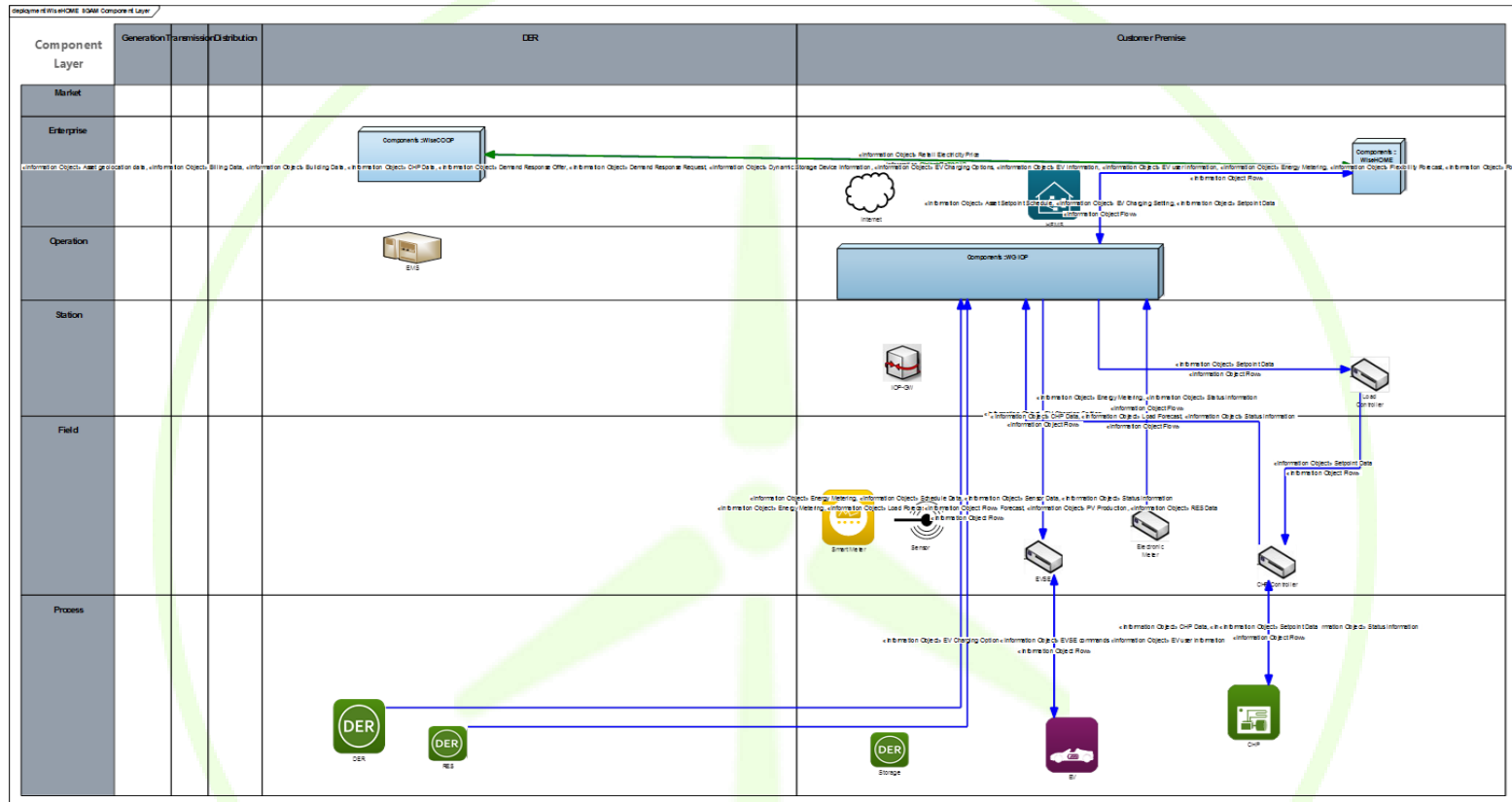


Figure 60 - SGAM Component Layer of WiseHOME

WiseHOME is the application that will be used by residential users in order to monitor their consumption and various Key Performance Indicators of their choice as well as to be informed about energy price spikes that can have a detrimental impact on their energy cost.

To achieve these aims, WiseHOME needs to interact with two other WiseGRID products:

- WG IOP: the interoperable platform will serve as the main system middleware component, responsible for bi-directional data transmission to and from the aforementioned residential field devices, among others. This tool will provide the interoperability perspective that is required to simplify the integration effort of all other WiseGRID products.
- WiseCOOP: the IT tool of the retailer/supplier will be a key element in the participation of residential users in demand response schemes. It will provide the price signal that is needed to trigger a reaction from the user.

## 11.2 WISEHOME SGAM COMMUNICATION LAYER

Similarly to the architecture presented for other WiseGRID tools, the architecture of the WiseHOME takes advantage of the message brokering technology of the WG IOP to interconnect the different software modules and physical assets/field devices in a fast and reliable way. The main protocols envisaged to implement these communication flows are MQTT and AMQP.



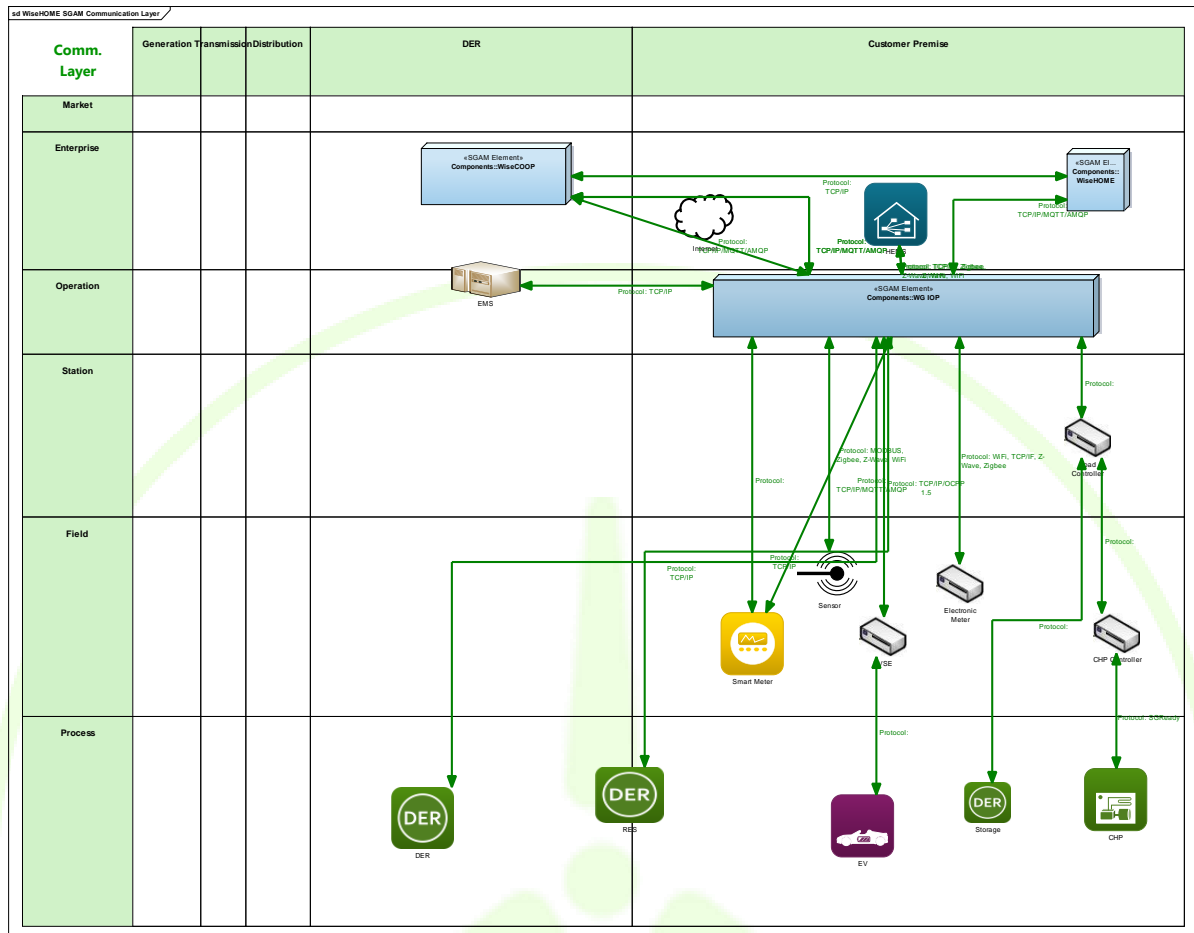
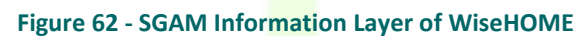


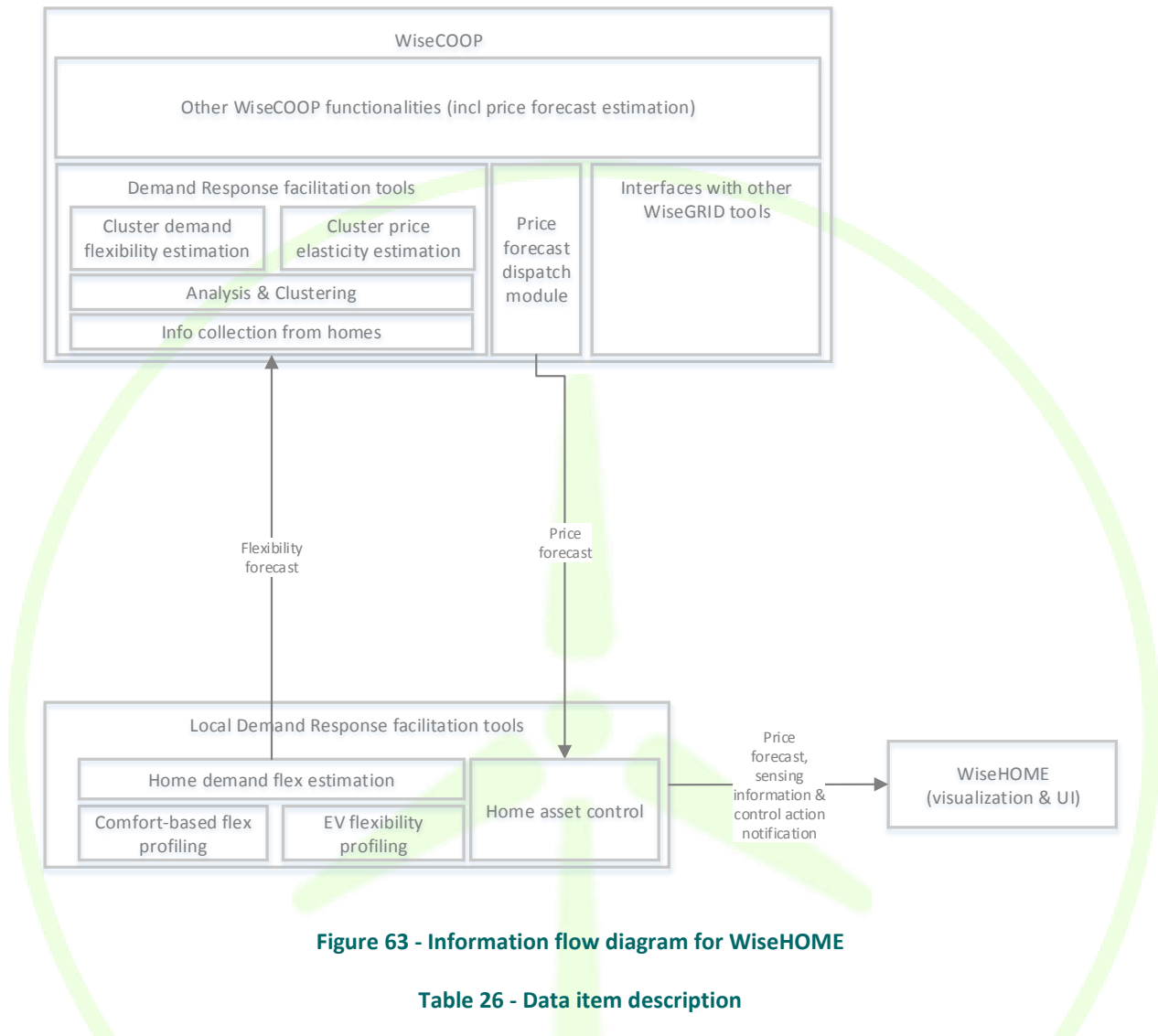
Figure 61 - SGAM Communication Layer of WiseHOME

### 11.3 WISEHOME SGAM INFORMATION LAYER

The WiseHOME information layer represents the logical flows of data among the different modules, also detailing the information items that are conveyed within each one of those flows. This first identification of data items will be useful for the identification and selection of proper common data models and standard interfaces to be used during the implementation phase.



In order to facilitate the readout of the details of the information flows, the following simplified diagram depicts the most relevant elements and exchanged data items.



**Table 26 - Data item description**

Data item		Description
Flexibility forecast	fore-	A forecast of the available demand - or supply - side flexibility that can be made available from the home assets to the aggregator/retailer. It is necessary for the aggregator to estimate its portfolio wide flexibility that can be bid in markets.
Retail electricity price forecast	electricity	Formal definition of the (dynamic) prices to be applied by the retailer to its customers. Facilitates the execution of implicit demand response campaigns
Sensing information	infor-	Real-time information about conditions within the home, including environmental conditions, occupancy, etc. This information is necessary for the reliable estimation of flexibility.
Control action notification	action	Information about automated control actions undertaken by the system. The user should be notified in order to provide e priori permission or a posteriori acceptance, depending on the use case.

### Related standards

The following table summarizes some of the relevant standards, data models and open protocols identified for the data to be handled by WiseHOME.

**Table 27 - Items and related data models**

Data item	Related data model or standard	Comments
Energy metering	CIM - DLMS/COSEM	May be needed for billing purposes
Weather forecast	CIM	External information required for flexibility estimation
Flexibility forecast	USEF	
Retail electricity price	OpenADR	

## 11.4 WISEHOME PRIVACY AND DATA PROTECTION

Tables for the results of the assessment related to the WiseHOME are presented below.

**Table 28 - Threat and feared events identification for WG HOME**

Feared events	Threat ID	Threat name	Brief explanation why relevant
Disappearance of personal data: they are not or no longer available	ED	Eavesdropping of computer channels	Interception of Ethernet traffic; acquisition of data sent over a Wi-Fi network, etc
	Pobj	Prevention of objections	Data subjects have the right to object to the processing of data. If they want to execute this right it must be (technically) possible
Diverting of personal data to other users: they are distributed to people that have no need	DoS	Denial of service	Denial of service will lead to unavailability of computing system
	IISC	Insufficient information security controls	Unauthorized parties obtain access to personal information by breach of security or lack of security implementation.
Unavailability of legal processes: they do not or no longer exist or work	AUS	Abnormal use of software	Unwanted modifications to data in databases; erasure of files required for software to run properly; operator errors that modify data, etc.
	NL	Non legally based personal data processing	Processing of personal data is not based on consent, a contract, legal obligation, or other relevant legal ground as per Article 7 of Directive 95/46/EC.
Change in processing: it deviates from what was originally planned (diversion of the purpose, excessive or unfair collection)	ADNI	Access to data that was not intended (not necessary for the purpose of collection)	Unjustified data access after Change of Tenancy (CoT) or Change of Supply (CoS).

## 12 WISECORP ARCHITECTURE SPECIFICATION

WiseCORP is the WiseGRID technological solution targeting businesses, industries, ESCOs and public facility consumers and prosumers, with the objective of providing them the necessary mechanisms to become smarter energy players. By means of energy usage monitoring and analysis, proper information can be given to facility managers helping them to reduce energy costs and environmental impact.

A key factor towards achieving these objectives is a proper retrieval and analysis of energy usage data, and visualization of meaningful information extracted from it. This information may include:

- Detailed visualization of energy demand at different areas of the building, helping facility managers to identify opportunities for enhancing energy efficiency
- Energy tariff comparison, enabling a direct economic cost reduction by shifting to a more adequate tariff
- Energy demand forecast, enabling medium to long term cost estimations and supporting operative decisions about the usage of the facilities
- Demand flexibility estimation, allowing the execution of optimization algorithms that will - either automatically or by providing advices - shift demand in order to minimize economic costs - by maximizing self-consumption or moving demand to off-peak periods - or minimize environmental impact - by shifting demand to periods where green energy is available.



Figure 64 - WiseCORP

## Features

The relevant use cases targeted by WiseCORP can be summarized in the following set of features:

- Local monitoring and control of building assets: facility managers need a clear overview and monitoring of the status of the controllable assets, including
  - Demand (electricity and gas)
  - Production (PV, CHP...)
  - Controllable loads (HVAC, lighting)
  - Batteries
- Decision support system for facility manager: smart analysis of the data is needed to assist the facility manager in the decision making process:
  - Analysis of evolution of energy usage patterns
  - Energy usage KPIs
  - Energy cost analysis (both economic and environmental)
  - Tariff comparison
- Local optimization: the application shall facilitate the execution of local optimization policies, while taking comfort models into account, towards
  - Increasing self-consumption
  - Peak-shaving
  - Time-of-use optimization
- Integration with WiseCOOP: facility managers - using WiseCORP - can collaborate and participate of aggregators' programs - using WiseCOOP - for mutual benefit. Features in this direction may include:
  - Aggregator information displayed to facility managers (e.g. advises, comparison with peers...)
  - Provide local flexibility estimation to aggregator, taking comfort models into account
  - Enable participation in demand response campaigns

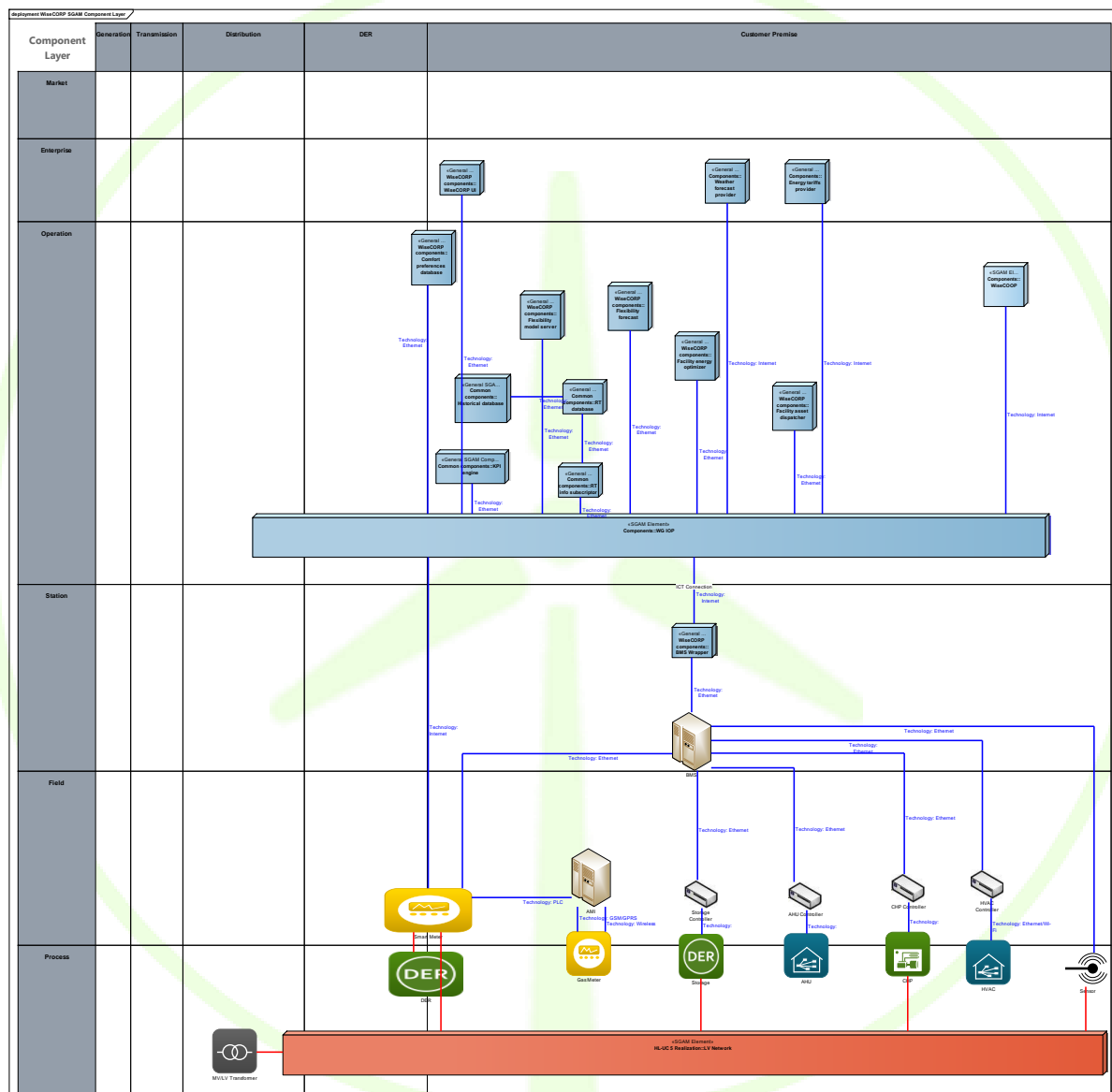
### 12.1 WISECORP SGAM COMPONENT LAYER

The WiseCORP SGAM component layer depicts the set of modules that are considered in order to implement all required functionalities of the tool. Those modules are represented under the SGAM domains/zones matrix. Most modules fall under the *Customer premise* SGAM domain - as WiseCORP features relate with the business of facility managers - and under the *operation* zone - since most features are intended to optimize energy usage of facility premises.

There are a number of elements in the facility premises that may be integrated with WiseCORP to achieve its objectives. The list includes:

- BMS: automated system that monitors and controls the equipment of a building (ventilation, lighting, electricity infrastructure, etc.)
- Storage: devices capable of storing energy
- AHU: Air Handling Units

- The following modules are envisaged to be developed in order to implement the required functionalities.



**Figure 65 - SGAM Component Layer for WiseCORP**

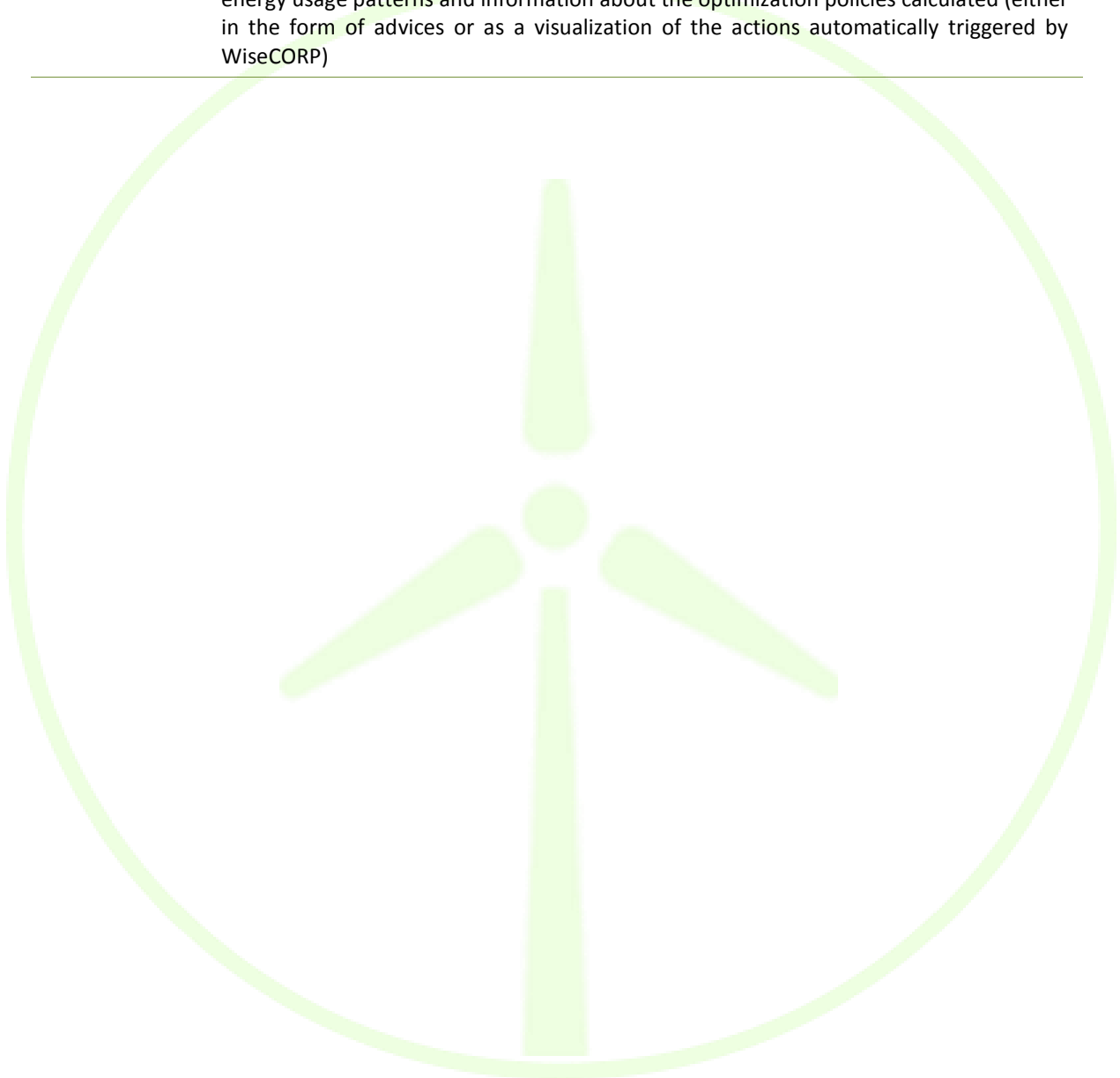
The following table details the different modules composing the WiseCORP.

**Table 29 - WiseCORP modules**

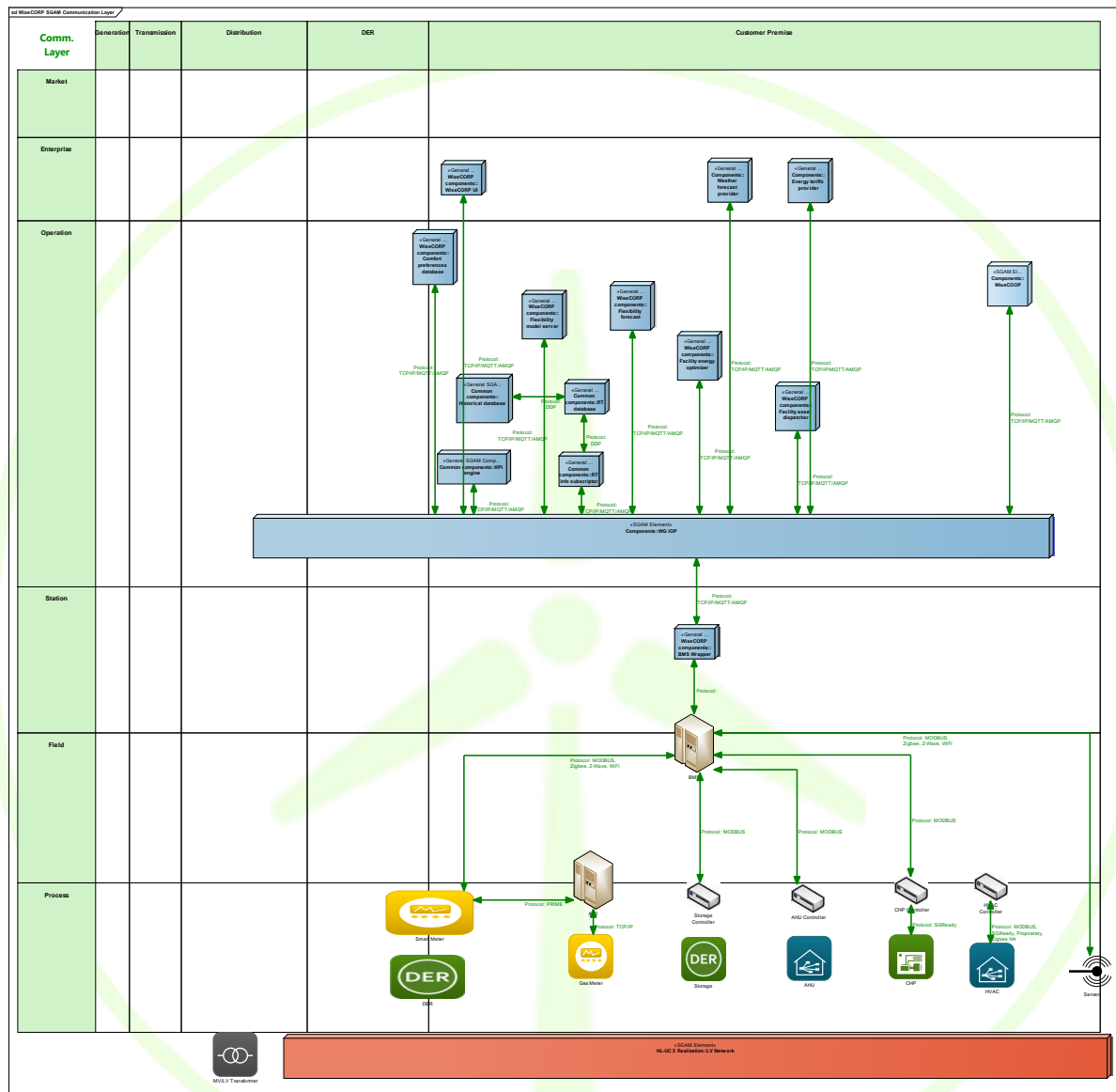
Component	Description
On-site components	Existing components (under DSO premises or control) that will be integrated with WiseCORP
Smart meters	Smart meters measuring demand and production at different areas/sections of the facility premises. The application will use the wrappers developed within the project to retrieve energy metering data from those devices.
BMS	Automated system that monitors and controls the equipment of a building, also offering control capabilities over part of the controlled assets
Horizontal modules	Components that will be reused among different WiseGRID applications
Weather forecast provider	Module in charge of providing representative weather forecast and historical data, retrieved from an external specialized provider
Big data platform	Suite of modules specified within the WiseGRID project in order to support big-data related functionalities, including long-term storage and data-mining algorithms
Energy tariff provider	Module providing formal definition of energy tariffs, including economic details and source of the energy (green, renewable resources)
Specific components	Components composing WiseCORP
BMS Wrapper	Module interacting with the BMS of the facility and offering the proper information to the rest of the modules in a common data format. This module will also encapsulate the commands that can be executed on those assets (setting setpoints)
RT info. subscriber	Module subscribed to the proper flows of data of the WG IOP - BMS-controlled assets - and in charge of collecting produced data and pushing it into the proper databases
RT (short-term) database	Specific database focused in daily operation, holding short-term data
Historical (long-term) database	Specific database, supported by the big data platform, focused in long-term storage of data for data-mining purposes
KPI engine	Data-mining algorithm, supported by the big data platform, in charge of calculating and updating KPIs of particular interest to the facility manager
Comfort preferences database	Module holding the constraints of the facility manager to the actions that may be taken by WiseCORP, including parameters such as building occupancy schedules, desired temperature ranges, etc.
Flexibility model server	Module holding models of the energy-related behavior of different asset types (HVACs, batteries, CHPs). Those flexibility models allow WiseCORP to derive the necessary set-points to be scheduled in order to activate a certain flexibility (modulate energy demand) on that particular device
Flexibility forecast	Taking into account information on forecasting, flexibility models, and user preferences/constraints, generates forecasts of the overall flexibility that can be offered to the aggregator
Facility energy optimizer	Considering the available flexibility of the system, energy prices and possible external constraints (e.g. demand response restrictions), this module calculates the optimal usage of each controllable asset in the system



Component	Description
Facility asset dispatcher	Module in charge of translating the output of the energy usage optimizer into commands considering the type of asset to be controlled. These commands are eventually sent to the BMS wrapper, which will deal with their specific implementation
WiseCORP UI	Implements the facility manager interface. Based on web technologies, will provide different visualizations accordingly to the different features implemented by the WiseCORP, including a dashboard with the energy used by the facility and its different areas, KPIs, energy usage patterns and information about the optimization policies calculated (either in the form of advices or as a visualization of the actions automatically triggered by WiseCORP)



Similarly to the architecture presented for other WiseGRID tools, the architecture of the WiseCORP takes advantage of the message brokering technology of the WG IOP to interconnect the different modules in a fast and reliable way. The main protocols envisaged to implement these communication flows are MQTT and AMQP.

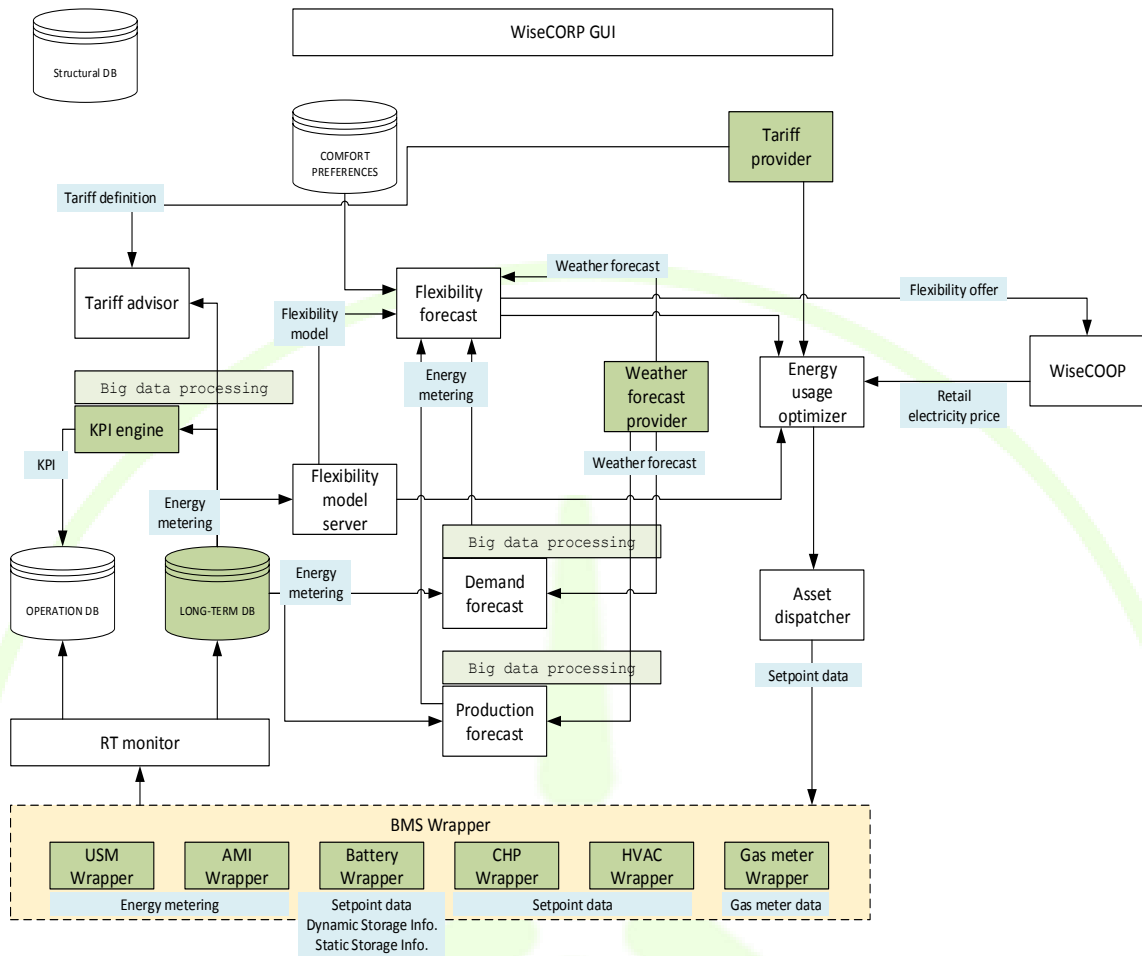


**Figure 66 - SGAM Communication Layer of WiseCORP**

The WiseCORP information layer represents the logical flows of data among the different modules, also detailing the information items that are conveyed within each one of those flows. This first identification of data items will be useful for the identification and selection of proper common data models and standard interfaces to be used during the implementation phase.



### D3.1 WiseGRID Architecture, Data Models, Standards and Data Protection (V1)



**Figure 68 - Information flows for WiseCORP**

**Table 30 - Data item description**

Data item	Description
Energy metering	Energy demand/supply measurements, provided by the smart meters
Setpoint data	Setpoint of asset (battery, CHP, HVAC) currently executed or programmed
Static storage info.	Metadata of the storage assets (model, capacity)
Dynamic storage info.	Current status of storage assets (state of charge)
KPI	Numeric values summarizing the state or evolution of certain variables of interest to the facility manager
Weather forecast	Weather forecast (and historical data) delivered by external provider
Tariff definition	Formal definition of the energy tariffs used by the facility manager, including both economic and energy source details

Data item	Description
Flexibility model	Model of the energy-related behavior of different asset types (HVACs, batteries, CHPs) including relationships between setpoints and flexibility activated (energy demand modulation) on a particular set of device types
Retail electricity price	Formal definition of the (dynamic) prices to be applied by the aggregator to its customers. Facilitates the execution of implicit demand response campaigns
Flexibility offer	Temporal curve of flexibility (adjustable demand) of the building

### Related standards

The following table summarizes some of the relevant standards, data models and open protocols identified for the data to be handled by WiseCORP.

**Table 31 - Items and related data models**

Data item	Related data model or standard
Energy metering	CIM - DLMS/COSEM
Weather forecast	CIM
Flexibility offer	USEF
Retail electricity price	OpenADR

## 12.4 WISECORP PRIVACY AND DATA PROTECTION

Tables for the results of the assessment related to the WiseCORP are presented below.

**Table 32 - Threat and feared events identification for WiseCORP**

Feared events	Threat ID	Threat name	Brief explanation why relevant
Disappearance of personal data: they are not or no longer available	ED	Eavesdropping of computer channels	Interception of Ethernet traffic; acquisition of data sent over a Wi-Fi network, etc
	Pobj	Prevention of objections	Data subjects have the right to object to the processing of data. If they want to execute this right it must be (technically) possible
Change in processing: it deviates from what was originally planned (diversion of the purpose, excessive or unfair collection)	ADNI	Access to data that was not intended (not necessary for the purpose of collection)	Unjustified data access after Change of Tenancy (CoT) or Change of Supply (CoS).
Illegitimate access to personal data: they are	IACP	Insufficient access control procedures	Access rights are not revoked when they are no longer necessary.

Feared events	Threat ID	Threat name	Brief explanation why relevant
known by unauthorized persons			

### 13 WG RESCO ARCHITECTURE SPECIFICATION

The WiseGRID RESCO will be a tool conceived for RESCOs - Renewable Energy Service Companies and ESCOs that want to provide RES services to end-users (households or businesses) that do not own nor wish to maintain the necessary equipment. In this perspective, three potential scenarios are envisaged:

- RESCO pays a fee to end-users using their premises (e.g. for installing PVs on their roof), installs and maintains the RES assets and markets all produced energy;
- RESCO provides to customers the supply of energy coming from RES owned by the RESCO (i.e. allowing self-consumption) and markets the production surplus;
- RESCO provides to customers the installation of RES equipment (e.g. PV panels) which are owned and maintained by the RESCO but fully exploited by the end customers (renting business model).

According to that, the WG RESCO tool will support RESCOs in managing the relationship with their customers and the provision of energy to the consumers from renewable energy sources, usually PV, wind power or micro hydro. Since the generation equipment will be owned, serviced and operated by the RESCO itself, the WG RESCO will have a central feature in supporting the maintenance management of those assets.



Figure 69 - WG RESCO

#### Features

The relevant features targeted by WiseGRID RESCO can be summarized in the following two major set of features:

- Electrical management
- Maintenance management

The set of features around the former will be specified in the following months.

As far as the Maintenance management is concerned we are in the position to already provide more

specific detail. The WG RESCO Maintenance management will deal mainly with two physical entities: Plant of Interest (POI) and Items of Interest (IOIs). A Plant of Interest (POI) is a specific point location or area hosting a RES plant that the RESCO needs to manage. The plant may be modelled with a single point on Earth representing a specific location, or more precisely with an area. The WG RESCO data model for a POI, will need at a minimum, the latitude and the longitude of the POI, a name and a description. All other information such as altitude, site manager in charge, contact number etc.... will be optional and may or may not be specified.

Any plant is composed of specific technical parts or components. To deal with them the WGRESO tool introduces the concept of IOIs. An Item of Interest (IOI) is a specific item (e.g. a circuit breaker, an inverter, a PV panel) that is part of the larger plant. Such items may be located indoor or outdoor. The indoor position implies that GPS coordinates will not be useful to pinpoint the IOI location, but even for outdoor located IOIs close proximity among items, e.g. two adjacent PV panels may not be enough to allow their position to be discriminated by using GPS, because of insufficient GPS precision. To allow additional positioning the WG RESCO platform will support additional technologies (Bluetooth Low Energy emitters, QR codes) to locate IOIs.

In WG RESCO, any POI can be linked to any other POI. This logical relation may in theory represent any logical relationship in the real world. Please notice that the concept of proximity is already represented by GPS coordinates, it is hence advisable to link POIs that share some other type of relationship e.g. being managed for the same customer (or partner), or be linked electrically in the same VPP etc.

Any given POI will generally be composed of many Items of Interest (IOIs).

Generally plants have a precise technical sub-structure (e.g. for a PV plant inverters, several channel linked to the power inputs of each inverter, strings of PV panels linked to a specific channel of a specific, single PV panels, ... ) that is highly variable across different plants. In fact, in addition to the previous example we may cite other examples, such as the presence or the absence of local electric storage, of wind turbines.

To deal with all this different possibilities WG RESCO introduces the general concept of Equipment of Interest (EOI). An EOI is a real physical subsystem of a POI that may contain IOIs or, recursively other EOIs. This flexible concept allows WGRESO to describe in a powerful and flexible manner any level of complexity of a POI internal structure. POIs EOI and IOIs all will have digital resources that describe them and help with their maintenance management.

### 13.1 WG RESCO SGAM COMPONENT LAYER

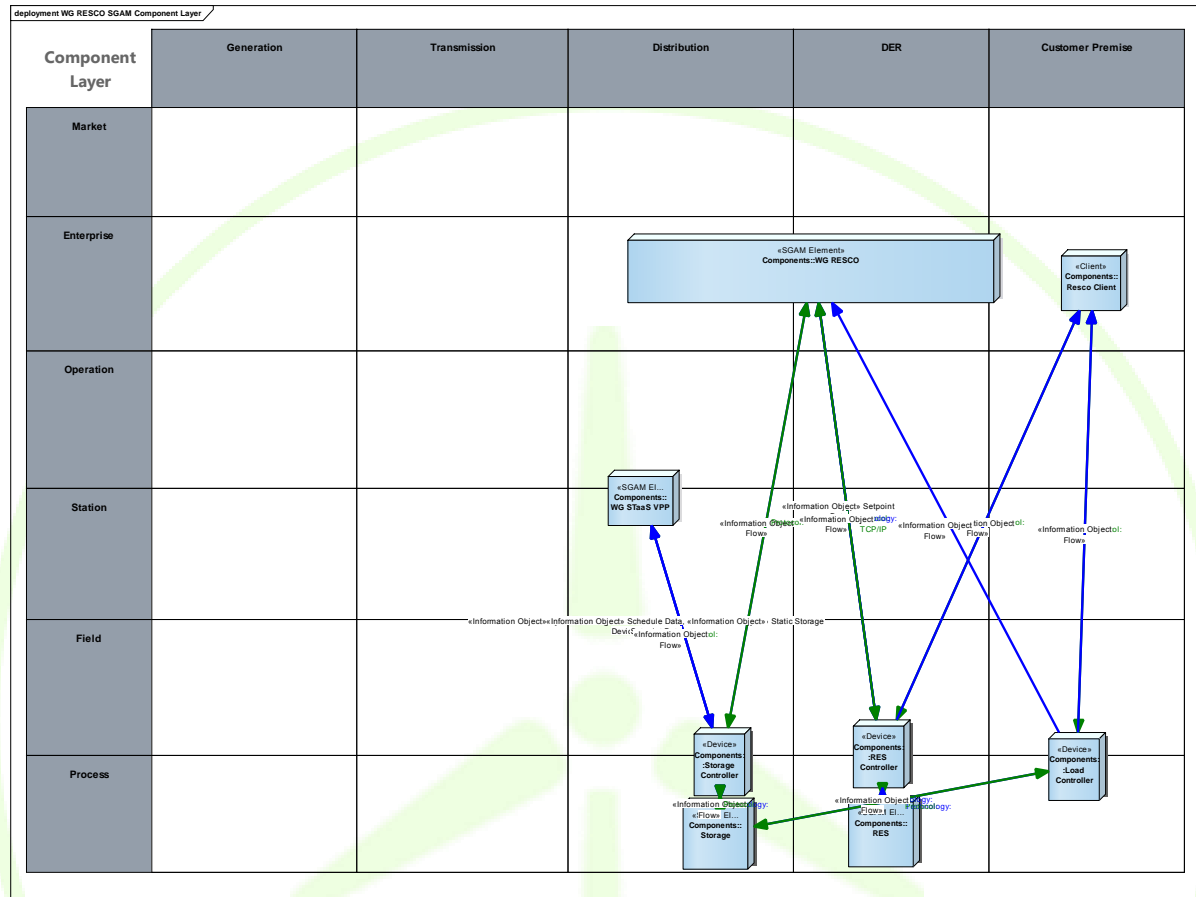
The WG RESCO SGAM component layer on the other hands depicts the set of modules that are considered in order to implement the electrical related functionalities of the tool. Those modules, represented under the SGAM domains/zones matrix, fall under the Customer premise SGAM domain - as WG RESCO features relate with equipment of any kind installed in third part premises- and under the operation zone - since most features are intended to manage energy usage on such premises.

There are a number of different equipment types that may be integrated with WG RESCO. The list includes:

- Storage: devices capable of storing energy
- Controllable loads: loads capable of being controlled in instantaneous power demand
- RES: renewable energy equipment installed

In a theoretical point of view RESCO of the future may well install and manage on 3rd party premises non only RES equipment but also other types of useful equipment.

In that aspect most core functionalities of RESCO will bear resemblance to similar functionalities of a VPP.



**Figure 70 - SGAM Component Layer for WG RESCO**

The following table details the different modules composing the WG RESCO.

**Table 33 - WG RESCO modules**

Component	Description
On-site components	Existing components (under 3 <sup>rd</sup> party premises but RESCO control) that will be integrated with WG RESCO
Storage	Energy Storage related controller
RES	RES equipment related controller
Load Controller	Variable load related controller
RES Controller	RES equipment related controller
Storage Controller	Energy Storage related controller



Component	Description
Specific components	Components composing WG RESCO
WG RESCO electrical management	Module interacting with the BMS of the facility and offering the proper information to the rest of the modules in a common data format. This module will also encapsulate the commands that can be executed on those assets (setting setpoints)
WG RESCO maintenance management	Implements the maintenance manager interface. Based on web technologies, will provide different visualizations accordingly to the different features implemented by the WG RESCO, about the distributed “fleet”, a structure builder module for every facility and its different components, maintenance material energy and information about the maintenance policies calculated

### 13.2 WG RESCO SGAM COMMUNICATION LAYER

Similarly to the architecture presented for other WiseGRID tools, the architecture of the WG RESCO takes advantage of the message brokering technology of the WG IOP to interconnect the different modules in a fast and reliable way. The main protocols envisaged to implement these communication flows are MQTT and AMQP.

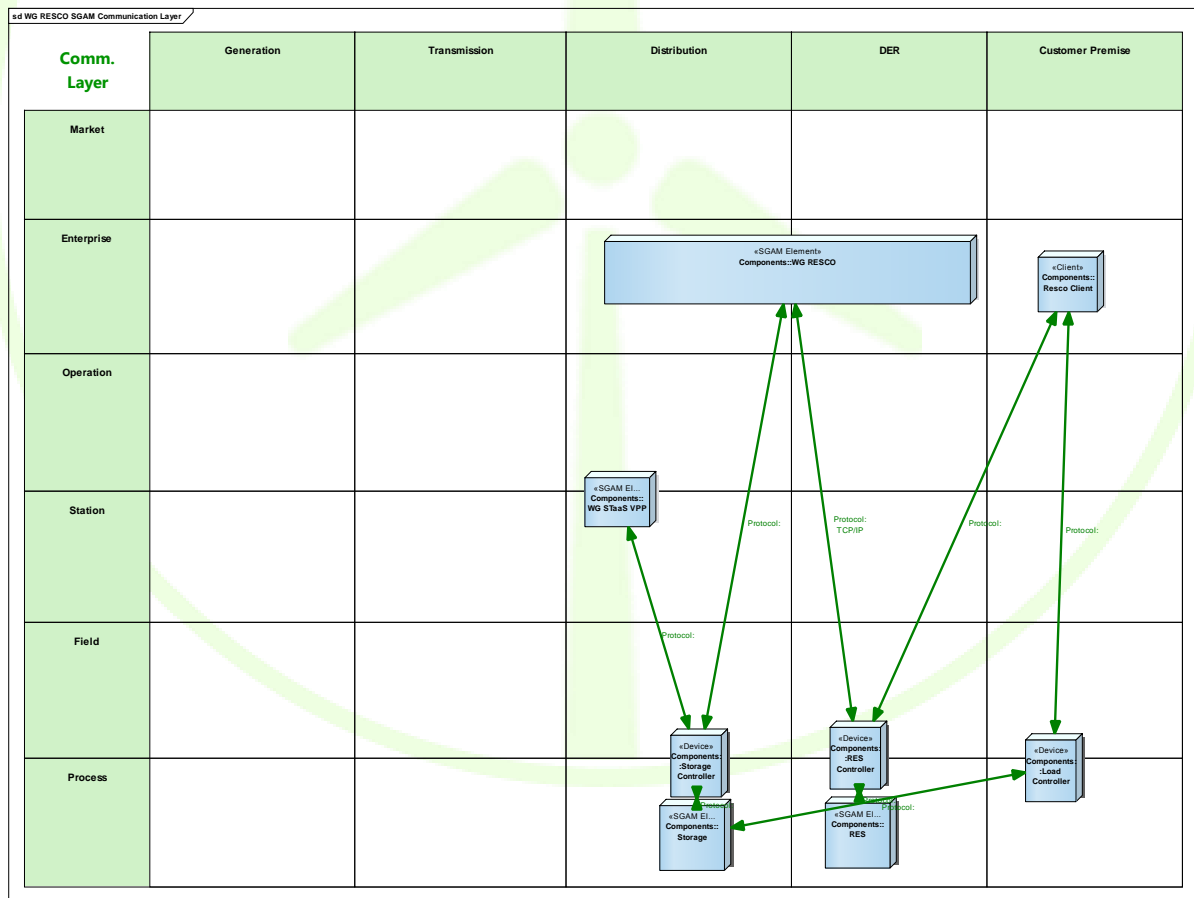


Figure 71 - SGAM Communication Layer of WG RESCO

### 13.3 WG RESCO SGAM INFORMATION LAYER

The WG RESCO information layer represents the logical flows of data among the different modules, also detailing the information items that are conveyed within each one of those flows. This first identification of data items will be useful for the identification and selection of proper common data models and standard interfaces to be used during the implementation phase.

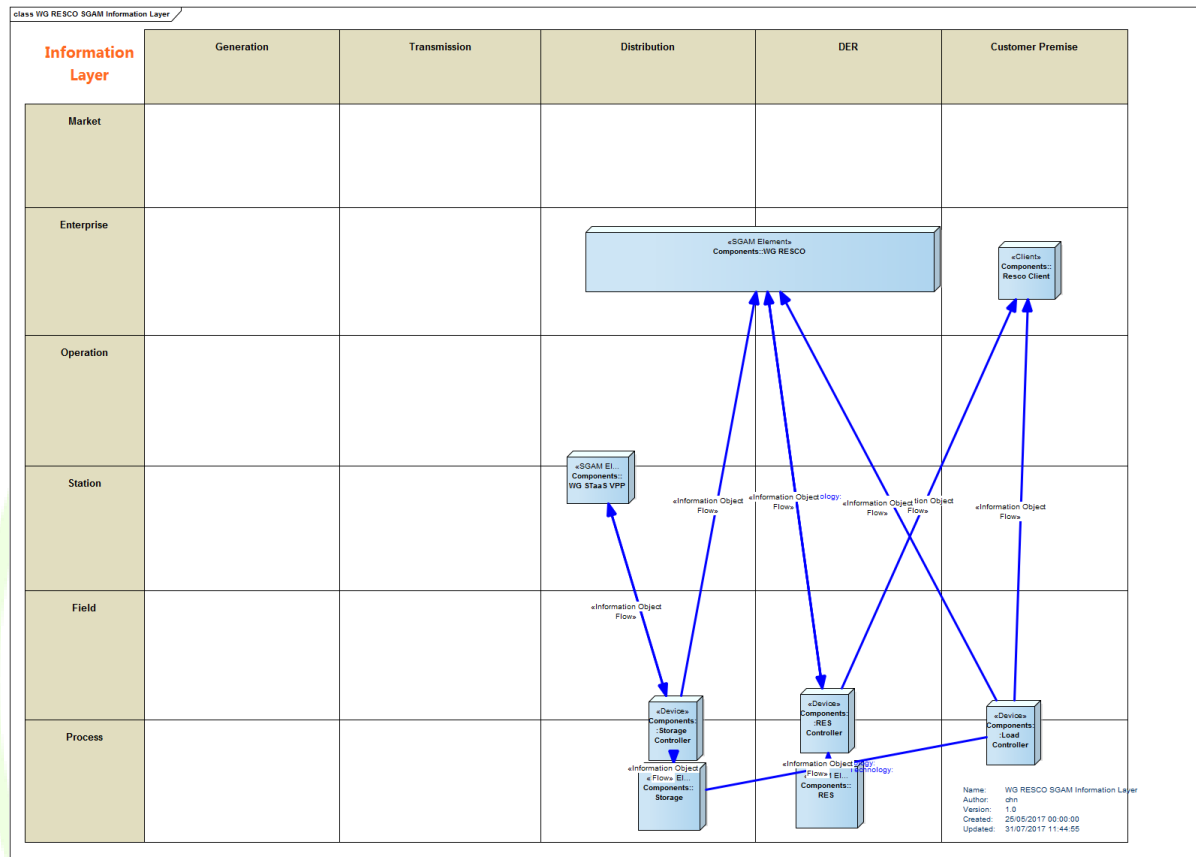


Figure 72 - SGAM Information Layer of WG RESCO

In order to facilitate the readout of the details of the information flows, the following simplified diagram depicts the most relevant elements and exchanged data items.

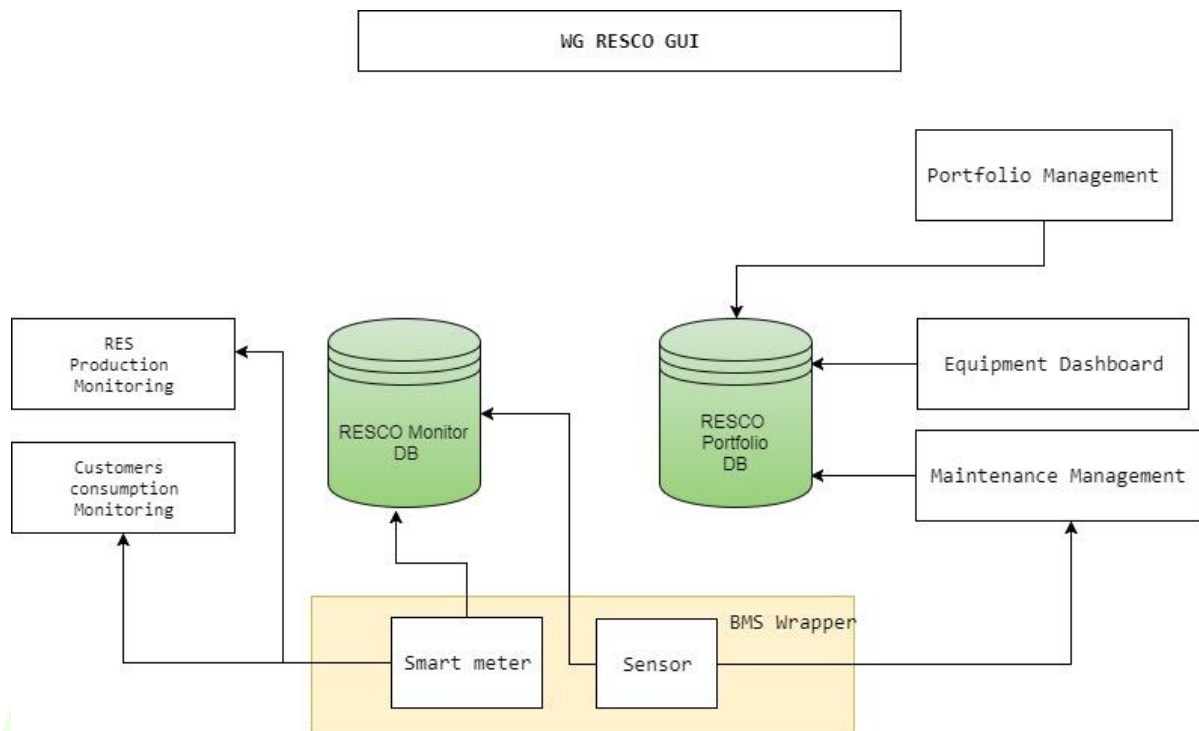


Figure 73 - WG RESCO component process diagram

### Related standards

The following table summarizes some of the relevant standards, data models and open protocols identified for the data to be handled by WG RESCO.

Table 34 - Items and related data models

Data item	Related data model or standard
Energy metering	CIM - DLMS/COSEM
Weather forecast	CIM
Flexibility offer	USEF
Retail electricity price	OpenADR

## 13.4 WG RESCO PRIVACY AND DATA PROTECTION

Tables for the results of the assessment related to the WG RESCO are presented below.

Table 35 - Threat and feared events identification for WG RESCO

Feared events	Threat ID	Threat name	Brief explanation why relevant
Illegitimate access to personal data: they are	UDC	Undeclared data collection	Some data is secretly recorded and thus unknown to the data subject.

Feared events	Threat ID	Threat name	Brief explanation why relevant
Disappearance of personal data: they are not or no longer available	ED	Eavesdropping of computer channels	Interception of Ethernet traffic; acquisition of data sent over a Wi-Fi network, etc
	Pobj	Prevention of objections	Data subjects have the right to object to the processing of data. If they want to execute this right it must be (technically) possible
Diverting of personal data to other users: they are distributed to people that have no need	DoS	Denial of service	Denial of service will lead to unavailability of computing system
	IISC	Insufficient information security controls	Unauthorized parties obtain access to personal information by breach of security or lack of security implementation.
Unavailability of legal processes: they do not or no longer exist or work	SA	Software alteration	Errors during updates, configuration or maintenance; infection by malicious code; replacement of components, etc.

## 14 PRIVACY AND DATA PROTECTION IN WISEGRID

### 14.1 GENERAL CONSIDERATIONS

This “Privacy and Data Protection chapter” as well as D3.1 deliverable as a whole is in accordance with the WiseGRID Grant Agreement, more specifically with article 27 *Protection of Results* and with article 39 *Processing of Personal Data*. Moreover, this report follows the national and DSO specific rules<sup>1</sup> on privacy and data protection, where applicable, as country specificities might apply on top of European directives and regulations which attempt to harmonize the data protection framework across the EU.

In the area of privacy, the only risks to consider are those that processing of personal data pose to privacy. Those risks are composed by one feared event (what do we fear?) and all the threats that make it possible (how can this occur?).

For the development of this deliverable, the following secondary and primary data have been used:

- A. **Secondary data:** European data protection legal framework:
  - *Regulation EC no 45/2001* on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data
  - *Regulation EC no 679/2016* on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) – *entering into force in May 2018*
  - *Directive EC no 680/2016* on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA – *entering into force in May 2018*
  - *Directive EC no 58/2002* on processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)
  - *NIS Directive no 1148/2016* on security of network and information systems
- B. **Primary data:** Questionnaire designed and sent by the Romanian Energy Center (CRE). In order to evaluate the impact on privacy and data protection of WISEGRID pilot sites and tools, CRE disseminated a comprehensive questionnaire to all responsible parties (ETRA, ENG, ASM, ECO, ENER, HYP, AMP, ITE, ICCS, HEDNO, VS), with the purpose to identify threats that may jeopardize personal data and associated confidentiality, integrity and availability. The same questionnaire was considered to find out criteria for an acceptable DPIA with specific implications of privacy and data protection to WISEGRID products.

The entire set of resulted data was considered for the identification of feared events, risks and mitigation measures, for all components specific to WISEGRID project.

---

<sup>1</sup> Ask all partners on country specific legislation on data protection that complements the European directives and legislations

#### 14.1.1 THE SCOPE OF THE DATA PROTECTION IMPACT ASSESSMENT (DPIA)

The Data Protection Impact Assessment (DPIA) within the WiseGRID project and specifically within this deliverable D3.1 covers the data protection impact assessment by focusing on WiseGRID tools and pilot sites, as privacy and data security is highly project and sector specific.

- *WISEGRID tools*: WG IOP, WG Cockpit, WiseHOME, WiseCORP, WiseCOOP, WiseEVP, WG Fast V2G, WG STaas/VPP, WG RESCO.
- *WISEGRID pilot sites*: Crevillent, Flanders, Terni, Mesogia, Kythnos.

**Table 36 – WISEGRID Tools and Pilot sites**

Item/Component	Description
WISEGRID Pilot Sites (Crevillent, Flanders, Terni, Mesogia, Kythnos)	How each individual pilot site will use the data
WISEGRID Tools (WG IOP, WiseHOME, WiseCORP, WiseCOOP, WG Cockpit, WiseEVP, WG Fast V2G, WG STaas/VPP, WG RESCO)	How each individual tool will collect, process, analyze and store the data
Type of data (metering – consumption and power quality, billing, SCADA specific data, demographics, etc.)	The management of personal/user specific data
Type of users (residential, industrial, commercial, public authorities, education facilities, etc.)	How the data will be used according to type of user

DPIA is a legal obligation and a specific procedure to evaluate the risks to privacy and data security to a project or a business, in order to assess potential risks and enhance data security and protection by promoting appropriate mitigation techniques which in turn create a series of advantages and benefits to the project/business. Organizations can take adequate measures in order to reduce these risks and, as such, reduce the potential impact of the risks on the data subject, the risk of non-compliance, legal actions and operational risk, or to take a competitive advantage by providing trust. Consequently, the contribution of DPIA on the WISEGRID project is to highlight potential risks and threats as well as to point-out appropriate mitigation techniques and ensure the design of a data security infrastructure.

Advantages and benefits of conducting a DPIA [6]:

- alleviating privacy and data protection risks results in costly adjustments in processes or system redesign by mitigating;
- timely understanding of the major risks results in preventing the suspension of a project ;
- mitigating the impact of law enforcement and oversight involvement;
- enhancing the personal data quality (minimization, accuracy);
- enhancing service and operation processes;
- enhancing the data protection decision-making processes.
- encouraging and increasing privacy awareness within the organization;
- enhancing projects' feasibility ;

- consolidating the confidence of consumers, employees or citizens in the way which personal data are processed and privacy is respected;
- improving communication about privacy and the protection of personal data

The DPIA shall have a clear description of all the smart grid actors, components and interactions so that the Data Protection Authority (DPA) is able to clearly identify the sensitivity of information being exchanged as well as all privacy-related concerns. When analysing a DPIA, the DPA should be able to verify all identified risks and evaluate if correspondent controls are adequate for mitigation or minimization of the identified risks [7].

#### 14.1.2 LEGAL BASIS FOR DPIA

Addressing the legal basis for a DPIA concerning the WISEGRID project, several questions should be addressed:

- Is there a legal obligation to conduct a Data Privacy Impact Assessment?
- Is the legal basis for processing of consumer data still unidentified?
- Is there a legal framework for the application of the tools or of the pilot cases?
- Do you anticipate that the public will have any privacy concerns regarding the proposed tools?

Under the General Data Protection Regulation (GDPR), DPIA is mandatory for technologies and processes that are likely to result in a high risk to the rights of the data subject. The template is related to the protection of personal data as defined in Directive 95/46/EC [8]. The DPIA definition includes the fundamental rights defined in Articles 7 and 8 of the European Union Charter of Fundamental Rights (the 'Charter') [9]; respectively the right to privacy and the right to the protection of personal data.

In 2012 the EU Commission stated that data protection impact assessments should make it possible to identify data protection risks in smart grid developments from the start, following the principle of data protection by design [10]. The European Commission Recommendation on Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems was adopted on 10 October 2014 [11]. The Recommendation 2012/148/EU further indicates that the Data Protection Impact Assessment Template should guide data controllers in conducting a thorough data protection impact assessment which describes the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with Directive 95/46/EC, taking into account the rights and legitimate interests of data subjects concerned [12]. The Smart Grids Task Force undertook a two-year test phase of the DPIA Template to see if it can be fine-tuned to improve its efficiency and user-friendliness.<sup>2</sup>

Member States should cooperate with industry, civil society stakeholders and national data protection authorities to stimulate and support the use and deployment of the Data Protection Impact Assessment Template at an early stage in the deployment of smart grids and the roll-out of smart metering systems.

---

<sup>2</sup> The text phase ran from March 2015-March 2017

Moreover, the EU GDPR replaces the 1995 Data Protection Directive from the 25 May 2018. The Regulation 'lays down the rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data' [13]. Under the GDPR DPIA will be mandatory for technologies and processes that are likely to result in a high risk to the rights of the data subject. It aims to continue to uphold the fundamental rights and freedoms including the right to the protection of personal data but also to ensure that the free movement of personal data is neither restricted nor prohibited for reasons connected with the protection of peoples' rights and the processing of their personal data [14].

### **14.1.3 THE POLICY OF PRIVACY AND DATA PROTECTION**

The policy and laws on privacy and data protection have built upon fundamental international rights and evolved with advances in information and communication technologies (ICT). The following sub-sections provide an overview of the international and EU laws before outlining how these are applied to smart grids and the WiseGRID project more specifically.

#### **14.1.3.1 THE FUNDAMENTAL RIGHTS TO PRIVACY AND DATA PROTECTION (PERSONAL DATA, THE PROTECTION OF PRIVACY)**

A right to protection of an individual's private sphere against intrusion from others, especially from the state, was laid down in Article 12 of the United Nations Universal Declaration of Human Rights (UDHR) of 1948 on respect for private and family life. The UDHR influenced the development of other human rights instruments including in Europe. The right became legally binding when incorporated into the International Covenant on Civil and Political Rights [15].

Recognizing the need to protect computer processed information the international Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) was adopted in 1981 [16]. Convention 108 applies to all data processing carried out by both the private and public sector, such as data processing by the judiciary and law enforcement authorities. It protects the individual against abuses, which may accompany the collection and processing of personal data, and seeks, at the same time, to regulate the trans-border flow of personal data. As regards the collection and processing of personal data, the principles laid down in the convention concern, in particular, fair and lawful collection and automatic processing of data, stored for specified legitimate purposes and not for use for ends incompatible with these purposes nor kept for longer than is necessary. They also concern the quality of the data, in particular that they must be adequate, relevant and not excessive (proportionality) as well as accurate [17].

In addition to providing guarantees on the collection and processing of personal data, it outlaws, in the absence of proper legal safeguards, the processing of 'sensitive' data, such as on a person's race, politics, health, religion, sexual life or criminal record. The convention also enshrines the individual's right to know that information is stored on him or her and, if necessary, to have it corrected. Restrictions on the rights laid down in the convention are possible only when overriding interests, such as state security or defense, are at stake.

Although the convention provides for free flow of personal data between State Parties to the convention, it also imposes some restrictions on those flows to states where legal regulation does not provide equivalent protection [18]. In order to further develop the general principles and rules laid down in Convention 108, the Committee of Ministers of the Council of Europe has adopted several recommendations that are not legally binding. All EU Member States have ratified Convention 108. In 1999, Convention 108 was amended to enable the EU to become a Party. In 2001, an Additional



Protocol to non-parties, so-called third countries, and on the mandatory establishment of national data protection supervisory authorities.

With the entry into force of the Treaty on the Functioning of the European Union (TFEU) in December 2009, the Charter of Fundamental Rights of the EU became legally binding. The right to the protection of personal data was elevated to the status of a separate fundamental right. The right to protection of personal data forms part of the rights protected under Article 8 of the European Convention of Human Rights (ECHR), which guarantees the right to respect for private and family life, home and correspondence and lays down the conditions under which restrictions of this right are permitted [19]. Article 8 of the ECHR not only obliged states to refrain from any actions which might violate this Convention right, but that they were in certain circumstances also under positive obligations to actively secure effective respect for both private and family life.

#### 14.1.3.2 THE EU LEGAL FRAMEWORK ON PERSONAL DATA APPLICABLE TO THE SMART GRID

The legal basis for data protection in Europe is contained in Article 16 TFEU which provides that everyone has the right to the protection of personal data concerning him or her. The EU primary law also contains a general EU competence to legislate on data protection matters [20]. Freedom of information according to Article 11 of the Charter and Article 10 of the ECHR protects the right not only to impart but also to receive information. Article 8 of the EU Charter of Fundamental Rights provides specifically for the protection of personal data. The Charter not only explicitly mentions a right to data protection in Article 8 (1), but also refers to key data protection principles in Article 8 (2). Finally, Article 8 (3) of the Charter ensures that an independent authority will control the implementation of these principles.

It is important to note that the fundamental right to the protection of personal data under Article 8 of the Charter is not an absolute right, but must be considered in relation to its function in society [21]. Article 52 (1) of the Charter specifies that limitations can be imposed on the exercise of rights set out in both Articles 7 and 8 of the Charter. The limitations need to be provided for by law, respect the essence of those rights and freedoms and, subject to the principle of proportionality. The limitations should be necessary and genuinely meet objectives of general interest recognized by the European Union or the need to protect the rights and freedoms of others. The fundamental right to the protection of personal data under Article 8 of the Charter is not, however, an absolute right, but must be considered in relation to its function in society.

Data subject rights will be much greater under the EU GDPR than under the previous Data Protection Directive. The GDPR aims to protect information of 'natural persons, whatever their nationality or place of residence'. It applies to all persons resident in the EU, not just EU citizens, including refugees, people on work and travel visas and those with residency. It can also apply to non-EU residents whose personal data is held and/or processed within the EU. As such EU organizations bound by the GDPR must protect personal data about anyone from anywhere in the world. This is a significant point – that the GDPR does not distinguish between data subjects on the basis of nationality or location.

The personal data that the GDPR refers to is much broader than was protected under the previous Data Protection regulation.<sup>3</sup> In an attempt to provide greater protection with developments in new

---

<sup>3</sup> The definition according to the Directive of 1995 is the following: 'personal data' mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity - Directive 95/46/EC

technologies such as the Internet of Things and Big Data analytical capacity the GDPR altered the scope. As such the GDPR states that:

*‘any information relating to an identified or identifiable natural person (‘data subject’); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, location data, an online identifier or to one or more factors, specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person’ [22].*

#### **14.1.3.3 THE ECHR AND EU CHARTER ON FUNDAMENTAL RIGHTS (PRIMARY LAW)**

The Charter of Fundamental Rights of the European Union (2000) incorporates the civil, political, economic and social rights of European citizens. It brings together the constitutional traditions and international obligations common to the Member States. The rights described in the Charter are divided into six sections: dignity, freedoms, equality, solidarity, citizens’ rights and justice. Although originally only a political document, the Charter became legally binding [23] as EU primary law with the coming into force of the Lisbon Treaty on 1 December 2009.<sup>4</sup> Article 7 of the EU Charter of Fundamental Rights protects the fundamental right of everyone to the respect for his or her private and family life, home and communications.

#### **14.1.3.4 THE EU PRIVACY AND DATA PROTECTION LEGAL FRAMEWORK (SECONDARY LAW)**

Prior to 2016 the EU legal instrument on data protection was Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive) [24]. It was adopted in 1995, at a time when several Member States had already adopted national data protection laws. The aim of the Data Protection Directive was harmonization of data protection law at the national level.<sup>5</sup> The General Data Protection Regulation is replacing the Data Protection Directive as of 25 May 2018.

Other complimentary EU regulations on privacy and data protection include the Regulation 45/2001/EC on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data; Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters and the Directive 2002/58/EC concerning processing of personal data and the protection of privacy in the electronic communication sector (Directive on privacy and electronic communication). The regulations post-1995 were the result of the changes in information and communication technologies scope as well as growing national security and social privacy concerns. These will be adapted where necessary to ensure consistency with the new GDPR.

#### **14.1.3.5 RELEVANT REQUIREMENTS FROM EU DATA PROTECTION LAW FOR THE DEVELOPMENT OF WISE GRID COUNTERMEASURES**

---

<sup>4</sup> See consolidated versions of European Communities (2012), Treaty on European Union, OJ 2012 C 326; and of European Communities (2012), TFEU, OJ 2012 C 326.

<sup>5</sup> See, for example, Data Protection Directive, Recitals 1, 4, 7 and 8.

Risk-treatment measures must be determined. This is done by linking existing or planned measures (identified earlier in the study or the applicable guidelines) to the risk(s) they help to treat. Subsequent measures are added until the risk level is finally considered acceptable.

Additional measures may be created from scratch or taken from good practices issued by recognized institutions or international standards. Generally, they shall be adapted to the specific context of each WiseGRID tool processing operation under consideration.

Additional measures that will cover:

1. **The primary assets:** measures designed to prevent security breaches, to detect such breaches or to restore security (informing data subjects, keeping personal data to a minimum, anonymization of personal data, etc.).
2. **The potential impacts:** measures designed to prevent the consequences of risks from occurring, to identify and limit their effects or to curb them (making of backups, integrity checks, management of personal data breaches, etc.).
3. **The risk sources:** measures designed to prevent risk sources from acting or making a risk real, to identify and limit their impact or to cause them to backfire (physical and logical access control, activity tracking, management of third parties, protection against malicious codes, etc.);
4. **The supporting assets:** measures designed to prevent the exploitation of vulnerabilities, to detect and limit threats that do occur or to restore the normal operating condition (reducing the vulnerabilities of software, hardware, individuals, paper documents, etc.).

The higher the capabilities of the risk sources, the more robust measures should be in order to withstand them. Moreover, any incidents that may have already occurred (especially personal data breaches) as well as any difficulties in implementing certain measures, may be used to improve the security system. Measures specified shall be formally set out, implemented, regularly audited and continually improved.

#### 14.1.3.6 DATA PROTECTION PRINCIPLES

Convention 108 established several key principles on data protection. These were incorporated into the 1995 EU Data Protection Directive. The GDPR has similarly incorporated the principles. Article 5 of the GDPR outlines the six principles that are to be applied to any collection or processing of personnel data.

1. Personal data must be processed lawfully, fairly and transparently.
2. Personal data can only be collected for specified, explicit and legitimate purposes.
3. Personal data must be adequate, relevant and limited to what is necessary for processing.
4. Personal data must be accurate and kept up to date.
5. Personal data must be kept in a form such that the data subject can be identified only as long as is necessary or processing.

6. Personal data must be processed in a manner that ensures security.

Energy related regulation has referred to principles in requirements regarding customers and data management. In the 2012 Energy Efficiency Directive for example the data extracted from smart metering shall be made available in an 'understandable format' [25]. There is however no expansion on what this might mean in practice. Further guidance on this as well as the realization of other principles is required for data controllers in smart grids so they can fulfill their legal obligations.

#### 14.1.3.7 FUNDAMENTAL NOTIONS AND ROLES

**Consent** is necessary from the data subject to ensure that collection and processing is lawful [26]. The GDPR defines consent as 'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action signifies agreement to the processing of personal data relating to him or her' [27]. The conditions for consent include the requirement that the data controller has consented to the processing of his or her personal data; that a data subject can withdraw consent at any time and that this should be easy to do [28]. Any contract where a service is provided, such as supplying energy, should where data processing is necessary to fulfil the contract meet the conditions for consent outlined in Article 7. The GDPR Recitals underscore that consent is considered not to be freely given if the data subject had no genuine and free choice or is unable to easily refuse consent without detriment. If consent is given but data is to be used for direct marketing, then the data subject needs to have a right to object which is explicit and which they are made aware of.

**Data protection by design and default** is a fundamental notion within the GDPR [29]. The emphasis is to be placed on incorporating forward thinking data protection into the design phase of an application of process. The concept of 'privacy by design' as it is often referred to is not new but the GDPR makes it a mandatory requirement. The concept applies to both applications as well as processes. As such liability will fall on those who design the processes should there be a data breach. The requirements are not prescribed in any detail in the GDPR. The Regulation merely requires that application designers and system processors 'implement appropriate technical and organizational measures' [30].

**Data portability** comes in two parts. It includes the right of data subjects to receive, store and transmit personal data for personal use, without transmitting it to another data controller. This right to data portability for data subjects is empowering rebalancing the relationship data subjects have with the data controller. Yet the right to data portability also gives data controllers the right to transmit data between one controller and another. But the data subject is included in the process. This prevents the data subject from being excluded from the process however because of the requirement that all data controllers and processors fulfill their legal obligations according to the principles contained in the GDPR. Data anonymization is part of this process whereby processors remove any traces to the data subject. Once anonymized data is no longer considered 'personal data'. Less rigorous is the concept of pseudonymization. This process means that the data subject's name and other identifying features are replaced by an alias. Explicit consent is not then required for processing pseudonymized data.

**Right to be forgotten**, also known as the right to erasure, under Article 17 gives the data subject the right to obtain from the controller the erasure of personal data. The personal data should no longer be necessary for the purpose it was collected; the data subject withdraws consent according to Article 6(1)a; and/or the data subject objects to the processing; the personal data was processed unlawfully [31]. Complimentary to the right to be forgotten is the right to restriction of processing.

#### 14.1.3.8 DATA CONTROLLERS AND PROCESSORS IN WISEGRID

Responsibilities for the control of data can be shared between several actors [32]. That is primarily data controllers and processors. The most important consequence of being a controller or a processor is legal responsibility for complying with the respective obligations under data protection law. Only those who can be held responsible under the applicable law can therefore assume these positions. In the private sector, this is usually a natural or legal person.

Data controllers have significant legal responsibilities to fulfil. Data controllers are defined in EU legislation as a *'natural or legal person, public authority, agency or any other body which, alone or jointly with others determines the purposes and means of the processing of personal data'* [33]. The data controller is responsible legally to demonstrate that principles contained in the GDPR are met, and ensure that external data processors with which they may have a contract have similarly met the requirements [34]. This may be challenging, especially as the meaning of certain terms is exceptionally broad, e.g. 'processing'. They must also ensure that fair processing notices are applied to ensure transparent information to data subjects. This obligation is more onerous, and arguably costlier, than the previous 1995 Data Protection Directive requirements. There can be joint controllers who determine the purposes and means of processing [35].

The data processor is the actor actually processing the data and under the GDPR have direct obligations for the first time.<sup>6</sup> Market actors including Distribution System (network) Operators (DSOs), Suppliers, Cooperatives, Service Providers, will be considered a data processor. The main obligation of a processor is to report to the controller and the supervising authority [36]. A data processor should look to design the data processing system in such a way as to minimize the possibility of privacy breaches though following the concept of 'privacy by design' [37].

A processor cannot engage a second processor without the controller's explicit authorization. The second, and any subsequent, processor must meet the same requirement that 'sufficient guarantees implement appropriate technical and organizational measures' are met [38]. Ultimately the actors who deliver the data processing services need to design a secure system. Ultimately however processors are not permitted to process data except on instructions from the controller [39].

A processor is defined under EU law as someone who processes personal data on behalf of a controller. The activities entrusted to a processor may be limited to a very specific task or context or may be quite general and comprehensive.

Under EU law, a controller is defined as someone who "alone or jointly with others determines the purposes and means of the processing of personal data". A controller's decision lays down why and how data shall be processed. The definition of 'controller' mentions additionally that a controller decides which categories of personal data should be stored.

The controller is defined as the one who determines the purposes and the means of processing. If the power to determine the means of processing is delegated to a processor, the controller shall nonetheless be able to interfere with the decisions of the processor regarding the means of processing. Overall responsibility still lies with the controller, who shall supervise the processors to ensure that their decisions comply with data protection law.

Data processors are required to keep a written record of processing activities carried out on behalf of each controller. The new requirements are likely to have implications for how commercial service

---

<sup>6</sup> EU GDPR 2016 Article 4 (8) defines the processor as a 'natural or legal person, public authority, agency or another body to which personal data are disclosed, whether a third party or not.'



contracts are drafted. However European Union organizations and member states are encouraged to consider the specific needs faced by micro, small and medium sized enterprises in the application of the GDPR. For enterprises with fewer than 250 organizations the GDPR includes derogation with regard to record keeping. This will reduce the costs but also legal obligations placed on smaller enterprises [40].

Controllers can appoint Data Protection Officers (DPO). Although DPOs are only required under the GDPR where 'special categories of data' are being managed it may be prudent to appoint a DPO. Data processors, along with groups of controllers and processors may appoint a DPO. The DPO should be easily accessible to all establishments. A DPO can be employed on a service contract [41]. The DPO needs to be an expert in data protection law and policies, being able to meet the requirements as stated under Article 39, hence it is likely that new DPO consultancies will manage several portfolios, perhaps specializing in particular sectors [42].

#### **14.1.3.9 TRANSFERRING DATA ACROSS BORDERS**

Not only does the GDPR apply to all organizations within the EU but it also applies to any external organizations that are trading with the EU [43]. This can be any organization in the world. The responsibility for ensuring that external data processors meet the GDPR lies with the EU data controller with whom the external provider has a contract [44]. However both the data controller and the data processor are liable in the event of a data breach. Arguably this could be a disincentive for EU organizations to work with external data processors who may be riskier in terms of the GDPR principles. It is important to document data responsibilities clearly between actors. Certifications to international standards, such as ISO/IEC 27001 can demonstrate that appropriate technical and organizational measures have been implemented by the data processors.

The E-commerce Directive looks to 'contribute to the proper functioning of the internal market by ensuring the free movement of information society services between the Member States' [45]. The GDPR operates without prejudice to the e-commerce Directive similarly seeking to contribute to the proper functioning of the internal market by ensuring the free flow of information services between Member states [46].

#### **14.1.3.10 NOTIFICATION TO SUPERVISORY AUTHORITY IN DIRECTIVE 95/46/EC**

The supervisory authority is an independent public authority that Member States are obliged to establish under Article 51 of the GDPR. The supervisory authority builds on the original agency established under the 1995 Data Protection Directive. The supervisory authority is responsible for monitoring the application of the GDPR to protect the fundamental rights and freedoms of natural persons in relation to the processing and to facilitate the free flow of personal data within the Union [47]. Members of the supervisory authority are appointed using transparent procedures by the government, head of state, parliament or independent body appointed by the members state, all members needed to have appropriate qualifications, experience and skills in the area of the protection of personal data [48].

The heads of Members States supervisory authorities were to be appointed to a newly established European Data Protection Board (EDPB) [49]. The EDPB was charged with monitoring and ensuring the application of the GDPR across the EU. Yet it is the supervisory authority at the Member State level that is charged with the responsibility to impose fines. The fines vary according to the gravity, nature and duration of an infringement [50].

Data controllers are obliged to inform the supervisory authority of personal data breaches [51]. Processors are party of the chain of responsibility with an obligation to inform the data controller if a breach occurs [52]. Documentation of data breaches should be recorded in writing by the data controller so it can be verified for the supervisory authority. Where the data breach is likely to result in a high risk to the rights and freedoms of natural persons the controller has to communicate the data breach to the data subject without any delay in a clear format [53].

## 14.2 IDENTIFICATION OF SENSITIVE DATA SOURCES FOR DSOS

The task of identifying the sensitive data sources for DSOs involved all partners as required to complete the below table. The full set of data are presented in the Appendixes under Appendix M. (They are also available on the WiseGRID project repository (redmine) as “data sources for DSOs”) and refer to all relevant WiseGRID tools.

**Table 37 – Data Sources for DSOs**

Data type (focus on your use-case specific data)	Actor who needs data (DSO, supplier, ESCO, aggregator, etc.)	Source of data (device or entity)	Time series – data granularity, data accuracy	Why is data needed	Privacy status
--	--	--------------------------------------	---	-----------------------	----------------

## 14.3 IDENTIFICATION OF SENSITIVE DATA SOURCES FOR NON-DSOS

The task of identifying the sensitive data sources for non-DSOs involved all partners as required to complete the below table. The full set of data are presented in the Appendixes under Appendix N. (they are also available on redmine as “data sources for non-DSOs”) and refer to all relevant WiseGRID tools.

**Table 38 – Data Sources for non-DSOs**

Data type (focus on your use-case specific data)	Actor who needs data (DSO, supplier, ESCO, aggregator, etc.)	Source of data (device or entity)	Time series – data granularity, data accuracy	Why is data needed	Privacy status
--	--	--------------------------------------	---	-----------------------	----------------

## 14.4 SURVEY OF PRIVACY AND DATA PROTECTION RISKS

The use of smart grids creates new risks for data subjects and brings potential impact in various areas (price, profiling, security) that were not present in the energy sector before, but rather usual in other environments (telecoms, e-commerce).

Regarding privacy and data protection, the mandate of EG2 (2<sup>nd</sup> Expert Group) defined by the SGTF (Smart Grid Task Force) was to provide a Smart Grid Data Protection Impact Assessment (DPIA) template. The current (third) version of the DPIA template has been prepared by an editorial team which has constructively addressed latest recommendations and was finalized by the EG2 members on 10 of March 2014.

The purpose of the DPIA template is to provide guidance on how to perform a *Data Protection Impact Assessment (DPIA) to Smart Grid and Smart Metering systems*.

The DPIA definition includes the fundamental rights defined in Articles 7 and 8 of the European Union Charter of Fundamental Rights ([http://www.europarl.europa.eu/charter/pdf/text\\_en.pdf](http://www.europarl.europa.eu/charter/pdf/text_en.pdf)); respectively the right to privacy and the right to the protection of personal data. It is noted that the template is related to the protection of personal data as defined in Directive 95/46/EC.

By conducting this DPIA the following goals will be achieved:

- The DPIA shall describe the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with Directive 95/46/EC.
- The DPIA shall also help as appropriate, the national Data Protection Authorities assess the compliance of the processing and, in particular, the risks for the protection of personal data of the data subject and the related safeguards, when data controllers consult them prior to data processing, as provided for by the Commission Recommendation. DPIAs, thus, should also assist the data controller in demonstrating compliance with Directive 95/46/EC.

Distribution System Operators (DSOs) are responsible for energy distribution in high voltage (usually below 60 kV), medium voltage (usually between 1 kV and 30 kV) and low voltage grids.

The term DSO is defined within the Electricity Directive (2009/72/EC) to be “a natural or legal person responsible for operating, ensuring the maintenance of and, if necessary, developing the distribution system in a given area and, where applicable, its interconnections with other systems and for ensuring the long-term ability of the system to meet reasonable demands for the distribution of electricity”.

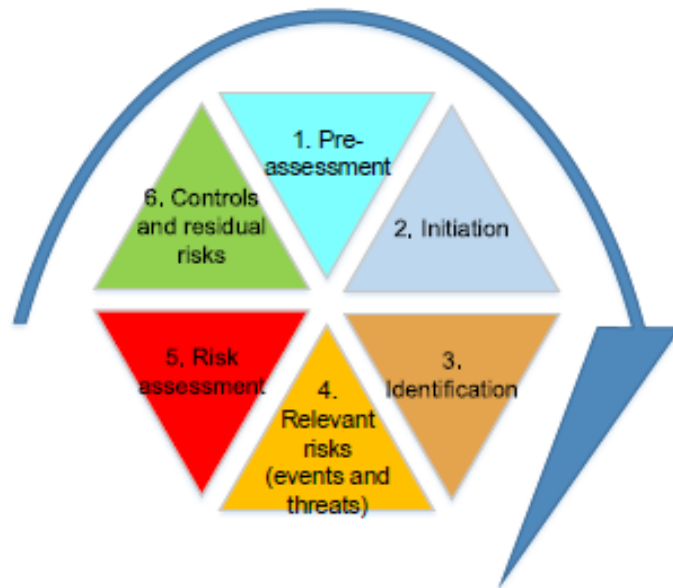
In most European markets, the role of a DSO is also the data hub for metering data; and this role will be extended by the task to manage an active power grid network that interacts with Renewable Energy Source (RES) and Distributed Generation (DG).

DSOs are involved in the processing of personal data originated from smart grids or smart metering.

Carrying out this DPIA, the templates from “*Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems* (18.03.2014)”, from chapters 2 and 3 [54] have been used. The performance of the *Data Protection Impact Assessment (DPIA) for Smart Grid and Smart Metering systems* comprises the following important steps:

- Step 1 - Pre-assessment and criteria determining the need to conduct the DPIA;
- Step 2 - Initiation;
- Step 3 - Identification, characterization and description of smart grid systems / applications processing personal data;
- Step 4 - Identification of relevant risks (events and threats);
- Step 5 - Data protection risk assessment;
- Step 6 - Identification and recommendation of controls and residual risks;





**Figure 74 - DPIA iterative cycle**

Further on the results are “Documented and drafting of the DPIA Report” and also followed by “Review and maintenance”.

For the evaluation of data privacy and risk assessment were considered the partners from the Project that are either “pilot site” or “WiseGRID tool developers”. The evaluation is based on a comprehensive set of questions (under a questionnaire form) and subsequent table of data sources to be used within the tools. These data sources are further split under DSO and non-DSO formats as appropriate.

#### **14.4.1 PRE-ASSESSMENT AND CRITERIA DETERMINING THE NEED TO CONDUCT THE DPIA**

##### ***Criterion 1 – Personal data involved***

Within this section we get an initial insight of the data collected and used within WG Tools and the potential necessity to execute a DPIA. The concept of personal data is as defined in article 2 of the Directive 95/46/10. More guidance regarding this definition can be found in WP136 opinion of the Article 29 Working Party on the concept of personal data ([http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf)).

It is underlined that when processing personal data, it was considered whether it was absolutely necessary for operational purposes. If not absolutely necessary, personal data processing are avoided whenever possible.

For smart grid applications within WG Tools, examples of personal data are:

- Household and organizations consumption;
- Consumer registration data: names and addresses of data subjects, etc.;
- Usage data (energy consumption, demand information and time stamps) - provide insight in the daily life of the data subject;

- Amount of energy and power (e.g. kW) provided to the grid (energy production), - provide insight into the amount of available sustainable energy resources of the data subject;
- Locally produced weather forecast – consumption prediction / forecasts;
- Demand forecast of building, campus and organization;
- Technical data (tamper alerts) - might change how the data subject is approached;
- Profile of types of consumers - might influence how the consumer is approached;
- Data and function of individual consumers / loads;
- Facility operations profile data (e.g. hours of use, how many occupants at what time and type of occupants);
- Frequency of transmission of data (if bound to certain thresholds) - might provide insight in the daily life of the data subject;
- Billing data and consumer's payment method

### ***Criterion 2 – data controller/data processor***

The data controllers are specialists and/or partners from the Consortium. As smart grid application makes determinations related to the collection or use of personal data, its role is similar to that of the Data Controller as defined in Directive 95/46/EC and is the natural or legal person, which jointly with others, determines the purposes, conditions and means of operating such smart grid application with impacts on personal data.

The application owner (tool developer) is considered as the data processor who conducts the identified processing operations on behalf of the data controller.

These two roles are defined by article 2 d) and e) of Directive 95/46 and further guidance can be found in WP 169 opinion<sup>12</sup> of the Article 29 Working Party on the concepts of controller and processor.

### ***Criterion 3 – Impact on rights and freedom***

Within this preliminary step we do not conduct a full risk assessment as foreseen in step 3 of the DPIA process, but only list the ones which could already be envisaged considering the nature of the personal data processing.

The following risks can be considered as specific ones which do trigger the need for a DPIA:

For the individual,

- Loss of independence (e.g. by preventing to provide own energy supply);
- Loss of equality (e.g. by difference in approaching individuals based on consumption or production);
- Stigmatization (e.g. by judging if someone has a clean/green energy supplier or not);
- Loss of freedom to move (e.g. not able to load an electric car);
- Interference with private life (e.g. incidentally cut-off energy supply by wrong decision based upon quality of data);

- Manipulation (e.g. by threat to cut off energy supply by individual or organization);
- Loss of Autonomy (e.g. by not being able to live by their own standards).

#### ***Criterion 4 - When to perform a DPIA (right timing and motivation)***

##### ***Right timing:***

As we develop new applications, in compliance with the principle of privacy by design, the DPIA is executed from the start of the idea throughout the design and implementation phases. This enables a Privacy-by-Design approach guaranteeing that potential risks are identified and that appropriate controls will be built into the systems.

With already existing applications the following criteria are considered envisaging the DPIA:

- Significant changes in the smart grid application, such as material changes that expand beyond the original purposes;
- Processing of new types of information;
- Unexpected personal data breach with significant impact and the occurrence of which had not been identified in the residual risks of the application identified in the first DPIA;
- The system owner in accordance with the risk management policy shall evaluate if to define periods of regular reviews of the DPIA report;
- Substantive or significant internal or external stakeholder feedback or inquiry;
- Use of cloud based services for processing personal data issued from the smart grid system;
- In the context of change management procedures such as material changes that expand beyond the original purposes (e.g., secondary purposes): throughout the lifetime of the Smart Grid application, a new or revised DPIA Report shall be warranted if there will be technological-related changes in applications.

##### ***Motivation:***

The DPIA process is motivated by the following elements:

- The wish to prevent costly re-design and control risks when designing and implementing smart grid (components);
- The necessity to ensure compliance with data protection and security legislation as well as other relevant legal obligations. See: Reform of the General Data Protection legislation (Article 33 of the Regulation);
- As part of a wider risk management process (e.g. ISO 27005);
- In line with corporate rules and culture;
- For accountability and communication policy sometimes related to the previous point with the aim of obtaining certification/seal.

### ***Criterion 5 – The nature of the system/application exercise***

The main question is: what is the nature of the application or system?

What components/functions of the application will be considered in the scope?

By this criterion we provide a first overview of the possible perimeter of the application at stake. This step provides an initial insight in the system and potential necessity to execute a DPIA.

### ***Criterion 6 - Legal base and public concern***

The processing of personal data is regulated by the EU legal framework (Directive 95/46/EC) transposed by Member States. The word “processing” means any operation or set of operations performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, erasure or destruction. The system owner of the application needs to determine if at least one of these operations is implemented and how far the organization has control on it (see also criterion 2).

The choice of the legal basis for these processing operations has been carefully selected and duly justified. Article 7 of Directive 95/46/EC offers the possible legal basis which are applied. Further guidance on the processing of smart metering data and compliance with the Data Protection Directive was found in Article 29 Working Party opinion WP183 ([http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp183\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp183_en.pdf)) on smart metering.

The list below provides possible situations within WiseGRID applications of processing of personal data.

- Reading out a meter manual/remote, entering data into database;
- Storage of meter data in meter or telecommunication device incl. intermediate storage;
- Adding meter data to tariff registers in the meter and/or back end systems,
- Transfer of meter data / tariff register data via WAN to a back end system naming addressing, encryption, data plausibility mechanism (e.g. detecting tampered data);
- Applying tariffs to the meter data, e.g. multiplication of annual consumption with price/kWh in the back end system;
- Creating a bill out of the aforementioned data (Billing data).
- Reading meter data for the local production of a PV, if the PV is behind the meter and an automation ensure a setpoint of injected power towards the distribution grid (e.g. zero injection). If so, the fine-grained data from the local production may be used to infer consumption profile through simple formulas such as  $P_{CONS} = P_{SETPOINT} - P_{PV}$  or for its corresponding energy with small timeframe load-profiles (15 minutes or less)

Reading PV data in the case of a prosumer with combined RES production, storage and consumption has very good grounds to “hide” the end-user behavior even in the situation that PV production and the PCC (point of common connection) are both read and transferred to an external actor. It is however better to measure only the power and energy on PCC meter, thus personal data is better protected and only rules as such presented below apply.

Following the Article 29 Working Party opinion WP205 ([http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp205\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp205_en.pdf)), it is stated that the following processing operations do not request user consent and may be triggered by the legal obligations of the smart grid operator:

- the provision of energy,
- the billing thereof,
- detection of fraud consisting of unpaid use of the energy provided,
- Preparation of aggregated data necessary for energy-efficient maintenance of the grid (forecasting and settlement).

It is obvious that tracking and profiling processing operations for the purpose of targeted advertisement, require a freely given, specific, informed and explicit consent.

Storage behind the meter is a very good tool to increase the privacy and data protection. It is advisable that power and energy related to the storage resource are not measured and sent to external actors, unless the end-user is participating to an energy storage related service, thus the consent being given through the service agreement.

Accordingly, the WiseGRID tools were assessed by the use of a questionnaire as presented under Appendixes in Appendix L.

## 14.4.2 INITIATION

Initiating the DPIA, different elements were considered.

The tables below do help by documenting the necessary information.

**Table 39 – DPIA team**

Aim of the DPIA			
The DPIA shall describe the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with Directive 95/46/EC.			
Team member name	Partner	Role	Responsibility
Rafael Leal-Arcas	QMUL	DPO	Manage the Privacy and Data Protection activities
Mihai Sanduleac	CRE	Deputy technical director	Supervise DPIA performance
Catalin Chimirel	CRE	Leader task 3.2	Perform survey and data evaluation
Mihai Macarie	CRE	Team member	Data evaluation
Ioannis Vlachos	ICCS	Leader deliverable D3.1	Coordinate overall D3.1 deliverable
Alberto Zambrano	ETRA	Processor	Tools WG Cockpit and WG EVP
Diego Garcia	ETRA	Processor	Tools WG COOP and WG CORP
Aitor Ubierna	ITE	Processor	Tool WG WG FastV2G
Massimo Magaldi (ENG)	ENG	Processor	Tool WG IOP
Antonis Papanikolaou	HYP	Processor	Tool WG HOME
Kraft Benjamin	VS	Processor	Tool WG STaas/VPP
Massimo Magaldi	ENG	Processor	Tool WG RESCO
Irene Aguado	ITE	Controller	Tool WG WG FastV2G
Konstantinos Tsatsakis	HYP	Controller	Tool WG HOME
Controller Site	HEDNO	Controller Site	Messogia, Kythnos
Controller Site	ENERCOOP	Controller Site	Crevillent
Controller Site	ASM TERNI	Controller Site	Terni
Controller Site	ECOPOWER	Controller Site	Flanders

The most important consequence of being a controller or a processor is legal responsibility for complying with the respective obligations under data protection law. Only those who can be held responsible under the applicable law can therefore assume these positions. In the private sector, this is usually a natural or legal person.

A processor is defined under EU law as someone who processes personal data on behalf of a controller. The activities entrusted to a processor may be limited to a very specific task or context or may be quite general and comprehensive.

Under EU law, a controller is defined as someone who “alone or jointly with others determines the purposes and means of the processing of personal data”. A controller’s decision lays down why and how data shall be processed. The definition of ‘controller’ mentions additionally that a controller decides which categories of personal data should be stored.

The controller is defined as the one who determines the purposes and the means of processing. If the power to determine the means of processing is delegated to a processor, the controller shall nonetheless be able to interfere with the decisions of the processor regarding the means of processing. Overall responsibility still lies with the controller, who shall supervise the processors to ensure that their decisions comply with data protection law.

**Table 40 – DPIA resources**

Inventory of necessary resources		
Questionnaires	Data sources	Other resources
Collected under survey and available under Consortium Library	Collected under survey and available under Consortium Library	Use cases description (see deliverable D2.1)
		WiseGRID Tools description (see deliverables D2.1 and D3.1)

#### 14.4.2.1 PURPOSES TO EXECUTE THE DPIA

Use of the DPIA provides answers to questions as addressed below.

##### ***For Investor / Management / Project initiator / system owner:***

- Will the investment be realistic from the viewpoint of data protection?
- Are the risks known and can they be mitigated?

##### ***Project management:***

- Are non-functional requirements sufficiently dealt with?
- Are the risks known and are we (still) dealing with them?

##### ***Compliance and oversight functions:***

- Is the risk assessment properly executed?
- Are all stakes of stakeholders dealt with and balanced?

##### ***System developers / project executions:***

- What measures do we need to take?

- What are the boundaries for performing the work?

#### 14.4.2.2 THE DPIA TEAM

There are three possible options for the management of the DPIA:

1. A dedicated team within the organization but not the one in charge of the application. The Data Protection Officer should be involved or contribute to this team from an evaluation or an operational point of view:
  - a. Persons with knowledge of the automation environment (hardware, software, networks and network components);
  - b. Persons in the user environment;
2. A third party providing external expertise needed for the DPIA;
3. The persons in charge of the application/system which is the target of the DPIA. This is similar with the case of SMEs with limited resources.

For WiseGRID, the 3<sup>rd</sup> option was considered.

The DPIA team has strong understanding of the project itself, knowledge of privacy, data protection and cyber security and expertise in the performance of risk assessments generally and privacy impact assessment in particular.

To conduct the DPIA we had a small and multidisciplinary team where the following expertise are combined:

- Risk assessment;
- IT architecture and system engineering;
- Information security;
- Privacy and data protection;
- Legal;
- Organizational design;
- Project management.

#### 14.4.3 THE RESOURCES

The DPIA was performed within the Consortium with members from all “Pilot Sites” and WiseGRID Tools” developers. We covered:

- Project documents like project plan, project initiation document, and business cases;
- IT Architectures,
- Requirements documentation, like functional, technical and non-functional requirements;
- Type of data to be generated and its purpose of use;
- System design documentation, like interface design and communication protocols.

Main target was to find good understanding and description of the data flow and the parties and systems involved in that data-flow as well as the data protection and security measures envisaged.



#### 14.4.4 IDENTIFICATION, CHARACTERIZATION AND DESCRIPTION OF SMART GRID SYSTEMS / APPLICATIONS PROCESSING PERSONAL DATA

The standard architecture for WiseGRID tools was considered as diagram indicated below. This is a general considered architecture that would be considered at this stage of the DPIA.

The idea is that each tool can directly purchase data (the bottom part of the diagram), which it can store directly in the big data (top part of the diagram).

If a business needs someone else's data and they are in big data, they need to be exchanged through IOP, which has to manage the market chains in terms of data security and privacy.

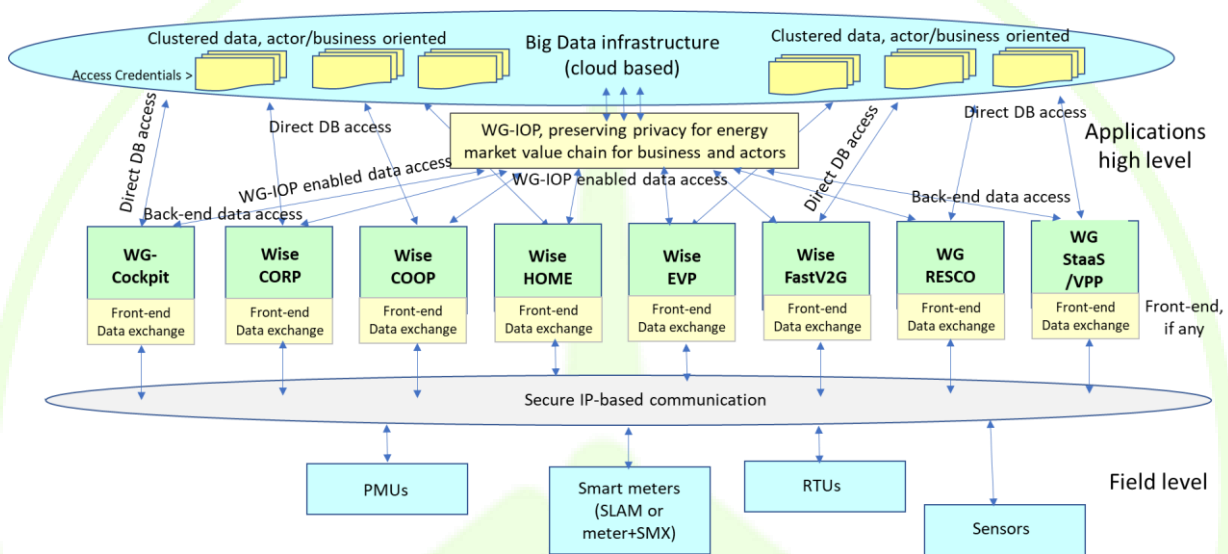


Figure 75 - Architecture for DPIA

The achieved structures were considered during the assessment. Details of the each WG tools specifications are presented in Chapters 5 to 13.

Table 41 – Correlation between WG tools and HLUCs

WG Tool	Related HLUCs
WG IOP	HLUC1, HLUC2, HLUC3
WG Cockpit	HLUC1, HLUC2, HLUC3
WG COOP	HLUC4, HLUC7
WG STaaS	HLUC3, HLUC4, HLUC6
WG EVP	HLUC3
WG FAST V2G	HLUC3
WG CORP	HLUC2, HLUC4, HLUC5, HLUC7
WG HOME	HLUC1, HLUC3, HLUC7

WG Tool	Related HLUCs
WG RESCO	HLUC1

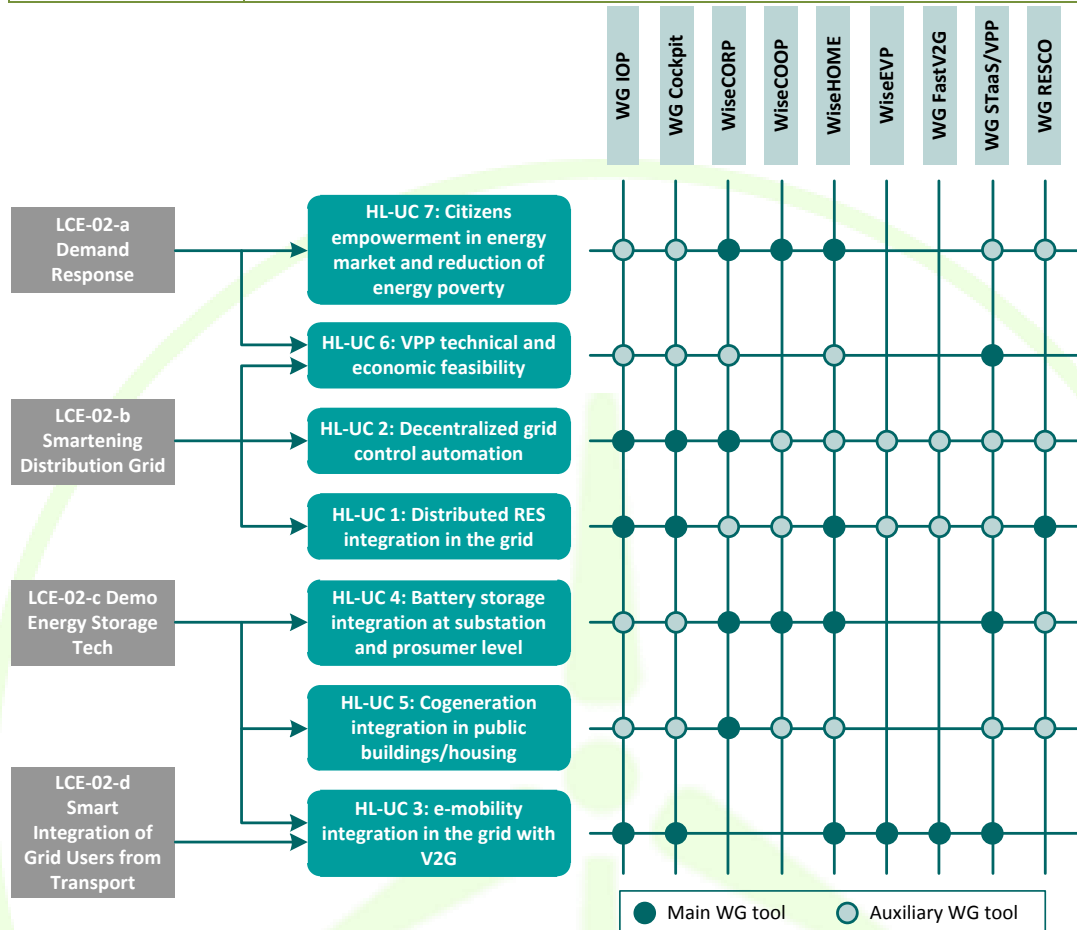


Figure 76 – HL-UCs mapping to project objectives and WiseGRID tools

See also: [Figure 118 - OpenADR communication architecture schema ..](#)

#### 14.4.4.1 DETAILED DESCRIPTION OF SMART GRID PROGRAM/CHANGE ACCORDING TO M/490 SMART GRID COORDINATION GROUP USE CASE TEMPLATE

Based on delivered “Use cases” according deliverable: D2.1, we have a comprehensive and full picture of the applications, its environment, processed data and systems boundaries. The application design, its adjacent interfaces with other systems, and information flows are also described.

Data flow diagrams that show processing of primary and secondary data are designed to visualize origin, locations and destination of data. Data structures are documented too, so that potential links could have been analyzed.

HLUCs diagrams are also presented within the SGAM Modelling (see Chapters 18 to 24 referred also as: Appendixes A, B, C, D, E, F and G)

Summary description of WG products and associated interface are presented under Chapters 14 and 15 below.

The use cases were built in line with the document prepared by M/490 smart grid coordination group for assistance.

All roles and responsibilities in relation to personal data processing operations were clearly documented and communicated.

#### 14.4.4.2 SCENARIOS OF THE SMART GRID USE CASE

The tools developers defined characterization of the targeted smart grid applications.

The 4 scenarios are presented under deliverable D2.1 are:

**Innovative and advanced demand-response mechanisms:** The loads to be considered would have an appropriate capacity to provide demand flexibility; hence WiseGRID focuses on HVAC devices as the most appropriate and favorable with respect to automated DR capacity.

**Smartening of the distribution grid:** In this purpose, will be considered the development of new intelligent monitoring equipment (smart meters, Phasor Measurement Units, modern fault detectors) and also new data concentration structures to support the existing SCADA systems and enable the smooth transition to the Active Distribution Networks by assisting in real-time monitoring. Additional basic component of Active Distribution Networks is the Virtual Power Plant.

**Integration of renewable energy storage systems in the network:** As we have more increasing ratio of distributed RES, with volatile and hardly controllable production, the imbalance between demand and production becomes significant. Energy storage systems would enable some features to fix this imbalance, by charging and discharging the batteries to diminish the deviation between production and demand.

**Smart integration of electricity mobility services:** This scenario is looking to integration of the electric vehicle (EV) and its electric vehicle supply equipment (EVSE) to provide flexibility to the distribution network operation. This would include participating in the household energy management processes (V2H) and also the possibility of power injection in the electrical network (V2G). All these could also improve the local RES integration, avoiding curtailment.

#### 14.4.4.3 MAIN ACTORS OF THE SYSTEM

The Actors identified under the Project are according detailed "Actors List" annexed to deliverable D2.1. (20170731\_iccs\_WiseGRID\_D2.1\_WiseGRID\_requirements\_Use\_cases\_and\_pilot\_sites\_analysis\_pu\_v1.0).

#### 14.4.4.4 USE CASE MAPPED TO A SMART GRID BUSINESS AND ICT ARCHITECTURE (E.G. M/490 SGAM)

Mapping of Use cases to the SMART GRID Business is detailed under Chapters 17 to 24 referred also as: Appendixes A, B, C, D, E, F and G.

#### 14.4.4.5 DESCRIPTION OF PRIMARY AND SUPPORTING ASSETS OF THE SYSTEM

Each system identified for each of the WiseGRID tools was evaluated, including workflows of personal data (the categories of data subjects and category, nature of the process, the recipient to whom data

may be disclosed, how information is provided to the data subject, retention policy, technology uses, communication protocols uses, etc. ).

For each processing of personal data, primary assets are the following:

- processes: those of the processing operations specific to smart grid management dealing with personal data and those required by Directive 95/46 and listed in Annex I “Privacy and data protection targets”.
- personal data: those directly concerned by the processing operations necessary for the management of the smart grid and those concerned by the processes required by the Directive 95/46.

The primary assets rely on various information system components considered as supporting assets. Risk sources would act, accidentally or deliberately, on the various information system components, on which the primary assets rely. These supporting assets do include:

- Hardware: computers, communications relay, USB drives, hard drives, sensors, smart meters, remote terminal units (RTU), intelligent electrical devices (IED), actuators, data concentrators, servers, front-ends, work stations
- Software: operating systems, messaging, databases, business applications, Advanced Metering Infrastructure (AMI) Head-end.
- Networks: electricity and data cable, wireless, fiber optic, routing and switching devices
- People: users, administrators, top management...
- Paper media: printing, photocopying, invoices, delivery contracts...
- Paper transmission channels: mail, workflow, personalized web-portals

## 14.4.5 IDENTIFICATION OF RELEVANT RISKS AND EVENTS

### 14.4.5.1 INTRODUCTION

In the area of privacy, the only risks to consider are those that processing of personal data pose to privacy. Those risks are composed by one feared event (what do we fear?) and all the threats that make it possible (how can this occur?).

Under this step were identified the conditions and potential risks that may threaten or compromise personal data of the data subject and impact his/her privacy using the EU Directive as a reference for important hallmarks of privacy and data protection targets to protect.

The risk assessment process considers the risks of the smart grid Applications in terms of their likelihood of occurrence (likelihood) and the impact of their consequences (severity). These privacy risks are constituted by a feared event and the threats which might trigger these events (several threats can trigger the same feared event).

The feared events represent the following situations to be avoided:

- Unavailability of legal processes: they do not or no longer exist or work;
- Change in processing: it deviates from what was originally planned (diversion of the purpose, excessive or unfair collection...);
- Illegitimate access to personal data: they are known by unauthorized persons;
- Unwanted change in personal data: they are altered or changed;
- Disappearance of personal data: they are not or no longer available.
- Diverting of personal data to other users: they are distributed to people that have no need.

Whenever these events could take place, they would impact on the privacy of the data subjects and these impacts need to be properly and systematically assessed and ultimately mitigated.

For a feared event to occur there must be one or more **risk sources** causing it, accidentally or deliberately. Risk sources may include:

- Insider: persons who belong to the organization: user, system operator, grid operator, service operator, call center operator, commercial service employee
- Outsider: persons from outside the organization: recipient, provider, competitor, authorized third party, government organization, human activity surrounding, external/sub-contracted maintenance
- Machine: non-human sources: corrupt sensor, computer virus, natural disaster such as lightning, energy imbalance, energy disruption an outage.

### 14.4.5.2 DATA PROTECTION THREAT IDENTIFICATION

Starting from the analysis performed in step 3 (description of the systems), threats were identified for each feared event described above. The aim was to establish, for the systems that are under the scope of this assessment, a detailed and prioritized list of all threats that would trigger these feared events.

In order to facilitate the identification of threats, a non-exhaustive list of generic threats is provided below in line with [7]. They are grouped according to their impact on confidentiality, integrity and availability of the data.

#### 14.4.5.2.1 Threats that may jeopardize confidentiality

The following table presents the generic threats that can lead to:

- Illegitimate access to personal data,
- Compromise of processing (as this feared event is considered).

**Table 42 - Generic threats that may jeopardize confidentiality**

Generic threats	Explanation of threats	Specific Energy industry examples of supporting asset vulnerabilities	Questions for guidance	Controls
Viewing of paper documents	Reading, photocopying, photographing, Interception of Ethernet traffic;	Unauthorized parties obtain access to personal information by breach of security or lack of security implementation.	Are special categories of personal data processed (such as data concerning health, biometric data, facial images, ideology, sexual habits, etc.)?	anonymization
Hardware loss	Retrieval of a discarded storage device or hardware; loss of an electronic storage device	Every device which contains sensitive data about the smart grid environment will cause unacceptable risk of alteration and abuse of those data.	How do you ensure the security of data?	Reducing hardware vulnerabilities
Eavesdropping of computer channels	Interception of Ethernet traffic; acquisition of data sent over a Wi-Fi network, etc.	Observation of metering and technical data between the smart meters and the central system with a false GSM base station by unauthorized person.	If personal data are transmitted, please describe the network and the connections between the devices that are used. Is this network isolated from public networks or nodes?	Reducing the vulnerabilities of computer communications networks

#### 14.4.5.2.2 Threats that may jeopardize integrity

The following table presents the generic threats that can lead to:

- Changes in processing,
- Unwanted changes of personal data,
- Alterations to legal processes (as this feared event is considered).

**Table 43 - Generic threats that may jeopardize integrity**

Generic threats	Explanation of threats	Specific Energy industry examples of supporting asset vulnerabilities	Questions for guidance	Controls
Abnormal use of software	Unwanted modifications to data in databases; erasure of files required for software to run properly; operator errors that modify data, etc.	Unauthorized changes of personal data, metering data, etc. make the system unreliable.	Are the processing operations documented? How is the documentation of the processing operations maintained? Are there considered for instance logs to memorize these operations?	Reducing software vulnerabilities
Abnormal use of software	Unwanted modifications to data in databases; erasure of files required for software to run properly; operator errors that modify data, etc.	Unauthorized changes of personal data, metering data, etc. make the system unreliable.	Do you maintain logs to track authorised (or unauthorised) access to personal data for a specific time period?	Reducing software vulnerabilities
Incomplete information	The information provided to the data subject on the purpose and use of data is not complete	Information provided to consumers only consists of usage data, information about other information (such as the ability to detect communication disruptions) gathered is not provided.	How do you inform the data subjects (clients, end-users) about the intended data processing operations?	Clear and consistent communication of purpose and goals of data collection
Access to data that was not intended (not necessary for	Unjustified data access after Change of Tenancy	In case the tenant changes, the data	Are there some unpredictable purposes in the final	Destruction schedules for personal information

Generic threats	Explanation of threats	Specific Energy industry examples of supporting asset vulnerabilities	Questions for guidance	Controls
the purpose of collection)	(CoT) or Change of Supply (CoS).	from previous tenant is made available to the new tenant	architecture of WISEGRID?	
Access to data that was not intended (not necessary for the purpose of collection)	The subjects could access data not owned by them.	In case of change of supply, old supplier still has access to data.	Does the system provide data subjects with the option to exercise the right to data portability (i.e. to have a copy of personal data related to personal users in a machine-readable format and, if technically feasible, transmit them to another data controller)?	Active measure to preclude the use of particular data-items in the making of particular decisions
Insufficient information security controls	Unauthorized parties obtain access to personal information by breach of security or lack of security implementation.	Load profile not end-to-end encrypted and could be read & processed by unauthorized third party, e.g. a network provider.	What is the interplay of "personal data breach" definition with Threat definitions under WISEGRID?	Anonymizing personal data. Encrypting personal data.
Lack of quality of data for the purpose of use	If data is used for certain processes it should be adequate.	A comma is used as a separator where a full-stop is intended.	What measures of interoperability of format exist for providing personal data to users?	Introduction of automated controls on the data quality
Prevention of objections	Data subjects have the right to object to the processing of data. If they want to execute this right it must be (technically) possible	Consumers cannot opt out to reading of detailed energy load profiles because read-out schemes are not configurable: There are no technical or operational means to allow compliance with a data subject's objection.	Is it applied a digital signature process for getting the acceptance of certain data processing?	Certify the processing of the data to be more transparent



Generic threats	Explanation of threats	Specific Energy industry examples of supporting asset vulnerabilities	Questions for guidance	Controls
Software alteration	Errors during updates, configuration or maintenance; infection by malicious code; replacement of components, etc.	Changing smart meter software can lead to changes of metering data which will damage the integrity of the consumption profile.	Is it applied a set of measures to avoid or detect software alteration, such that changes can be detected in time in order not to alter data integrity and confidentiality?	Reducing software vulnerabilities
Insufficient access control procedures	Access rights are not revoked when they are no longer necessary.	Employees who change job positions are still authorized to access data, not necessary for their new job.	Is it applied a Role based Access Control at different levels of data storage (at meter level, at IOP, big data and Wise-GRID Apps level)?	Managing persons within the organization who have legitimate access
The protection of data is compromised outside the European Economic Area (EEA).	There is a risk that smart metering data may be at risk if sent outside of the EEA.	Data protection standards outside the EEA may not be secure and robust as those countries are not subject to the obligations within the Data Protection Directive.	Is it considered the protection of data for not being transmitted outside the European Economic Area?	Limiting personal data transfer to countries that provide an adequate level of protection according to the article 25 of the Directive 95/46/EC

#### 14.4.5.2.3 Threats that may jeopardize availability

The following table presents the generic threats that can lead to:

- Unavailability of legal processes,
- Disappearance of personal data.

**Table 44 - Generic threats that may jeopardize availability**

Generic threats	Explanation of threats	Specific Energy industry examples of supporting asset vulnerabilities	Questions for guidance	Controls
Denial of service	Denial of service will lead to unavailability of computing system	DoS attacks can lead to unavailability. Consumers cannot reach websites of supplier. Smart grid components cannot communicate, which leads to disruption of the self-healing opportunities of the grid.	Do you have a “personal data breach reaction plan” and “reporting protocol”? Or is there a designated data protection officer?	Reducing hardware vulnerabilities
Hardware loss and Loss of Power	Retrieval of a discarded storage device or hardware; loss of an electronic storage device, etc. Loss of power can harm hardware and software and lead to unavailability	Every device which contains sensitive data about the smart grid environment will cause unacceptable risk of alteration and abuse of those data.	Will be considered measures for hardware loss (e.g. theft, physical intrusion) and loss of power (leading e.g. to system unavailability)?	Reducing hardware vulnerabilities
Denial of service	Denial of service will lead to unavailability of computing system	Smart grid components cannot communicate, which leads to disruption of the self-healing opportunities of the grid.	Is unavailability due to attacks leading to Denial of service considered? Please explain measures.	Reducing the vulnerabilities of computer communications networks

#### 14.4.5.2.4 Threats that may jeopardize personal data

The following table presents the generic threats that can lead to:

- Breaches of legal processes,
- Breach of use of personal data

**Table 45 - Generic threats that may jeopardize personal data**

Generic threats	Explanation of threats	Specific Energy industry examples of supporting asset vulnerabilities	Questions for guidance	Control
Undeclared data collection	Some data is secretly recorded and thus unknown to the data subject.	The DSO does remote meter readings of detailed load profile without consumer's awareness.	Are the subjects well informed about the data which is collected from them?	Informing data subjects
Collection exceeding purpose	More personal data is collected than what is necessary to achieve a specified purpose.	Collecting more detailed load profile data for the purpose of monthly billing, where much less detailed data would be sufficient to achieve the same objective.	Are the processed data accurate and relevant?	Minimizing the amount of personal data
Non legally based personal data processing	Processing of personal data is not based on consent, a contract, legal obligation, or other relevant legal ground as per Article 7 of Directive 95/46/EC.	A smart grid operator shares collected information with a third party without notice, consent or as otherwise legally allowed.	If the processing of personal data is based on the consent of the data subject, how do you guarantee that it was informed, specific and freely given?	Obtaining the consent of data subjects
Missing erasure policies or mechanisms; excessive retention periods	Data is retained longer than necessary to fulfil the specified purpose or to comply with legal obligations.	Metering data in energy systems is retained for x period in line with generic Archive Laws but is should only be retained in line with data retention policy, because it is not needed for the purpose anymore.	Is the end date of the processing period set (how long is the personal data retained)? What will happen with the personal data afterwards? Would it be possible that you as operator could reuse these data or transmit them to others (e.g. data brokers)?	Managing personal data retention periods
Missing erasure policies or mechanisms; excessive retention periods	Data is retained longer than necessary to fulfil the specified purpose	Metering data in energy systems is retained for x period in line with generic Archive	How do you ensure data subjects (data owners) are able to use their rights (such as	Minimisation of personal data retention by destroying it as soon as the transaction for

Generic threats	Explanation of threats	Specific Energy industry examples of supporting asset vulnerabilities	Questions for guidance	Control
	or to comply with legal obligations.	Laws but is should only be retained in line with data retention policy, because it is not needed for the purpose anymore.	right to access to data related to them, the right to erase data related to them, rectify such data, restrict or block the processing)?	which it is needed is completed
Combination exceeding purpose	Personal data is combined to an extent that is not necessary to fulfil the specified purpose.	Information in smart metering load profile used for billing is combined with personal data obtained from a third party to provide (third party) additional targeted services or products (e.g. insurance for stability in energy supply)	Are any data fully automatically processed? In such case, you must communicate the user meaningful information about the LOGIC under the algorithm, including the reason for combining it with other data. How would you explain such logic?	Minimizing the amount of personal data

#### 14.4.5.3 DATA PROTECTION THREAT IDENTIFICATION - OUTCOME OF THE QUESTIONNAIRE;

The questionnaire was designed for all 9 WG tools and relevant answers were received from responsible partners.

The answers are collected via a questionnaire (as presented under Appendixes in Appendix L and results are available under Consortium Library.

Finally, a tool by tool table was realized with events and threats associated in all cases. Tables for the results of the assessment related to each WG tool are listed in the respective WiseGRID Tools related Chapters 5 to 13 within WiseGRID tools architecture description for the 4 layers: Component, Communication, Information and Privacy and Data Protection.

#### 14.4.6 DATA PROTECTION RISK ASSESSMENT

In this step the identified feared events and related threats are weighed with *the severity of impact* on the individuals and *likelihood of occurrence*. In order to classify the impact and likelihood, an illustrative model was used, mainly based on ISO 31 000, EBIOS methodology and the synthesis produced by the CNIL<sup>19</sup> (the French data protection authority).

##### 14.4.6.1 IMPACT OF FEARED EVENTS

**Impact (Severity)** represents the magnitude of a risk. It essentially depends on *the level of identification of personal data* and *the level of consequences of the potential impacts*.

The feared events were ranked by determining their impact and severity based on the *level of identification of personal data* and the *prejudicial effect* of these potential impacts. This potential impact was defined by the consequences each feared event could have on a data subject's privacy and other fundamental rights and freedoms, including e.g. crime related risks such as identity theft and fraud, or freedom to move, independence, equal treatment, social relationships, financial interests, etc. due to e.g. profiling, unsolicited marketing, discrimination or individual decisions on wrong information. The consequences of feared events do not impact all data subjects equally.

When assessing the impact and severity of a certain identified feared event, the following elements were considered:

- The privacy targets (the complete list of targets is according Table below concluded from *Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems*)
- Crime related risks such as identity theft and fraud
- Impact on other privacy principles such as freedom to move, loss of independence, loss of equality etc. due to e.g. profiling, unsolicited marketing, discrimination or individual decisions based on wrong information.
- The potential impact from feared events may extend beyond those consumers who are directly affected and this should also be considered in the impact assessment.

**Table 46 – Description of privacy targets**

Description of privacy targets	
Safeguarding quality of personal data	Data avoidance and minimization, purpose specification and limitation, quality of data and transparency are the key targets that need to be ensured.
Legitimacy of processing personal data	Legitimacy of processing personal data must be ensured either by basing data processing on explicit consent, contract, legal obligation, etc.
Legitimacy of processing sensitive personal data	Legitimacy of processing sensitive personal data must be ensured either by basing data processing on explicit consent, a special legal basis, etc.
Compliance with the data subject's right to be informed	It must be ensured that the data subject is informed about the collection of his data in a timely manner.
Compliance with the data subject's right of access to data, correct and erase data	It must be ensured that the data subject's wish to access, correct, erase and block his data is fulfilled in a timely manner. Implementation of the right to be forgotten and the right to data portability should be encouraged
Compliance with the data subject's right to object	It must be ensured that the data subject's data is no longer processed if he or she objects. Transparency of automated decisions vis-à-vis individuals must be ensured especially in the case of profiling.
Safeguarding confidentiality and security of processing	Preventing unauthorized access, logging of data processing, network and transport security and preventing accidental loss of data are the key targets that need to be ensured. Breach notification procedure should be promoted

Description of privacy targets	
Compliance with notification requirements	Notification about data processing, prior compliance checking and documentation are the key targets that need to be ensured. DPIA shall be considered as a determinant tool for this target
Compliance with data retention requirements	Retention of data should be for the minimum period of time consistent with the purpose of the retention or other legal requirements.
Privacy by design	Having regard to the state of the art and the cost of implementation, technical and organizational measures and procedures shall be designed both at the time of the determination of the means for processing and at the time of the processing itself in such a way that they fully respect privacy and data protection rights of the data subject.
Privacy by default	Mechanisms shall be implemented for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage.

The Impact (Severity) evaluation starts with assessing the level of identification of all personal data established beforehand in the list of primary assets (see data sources tables under Appendixes in Appendix M and Appendix N. In other words, how easy is it to identify data subjects?

This is done answering the question: “How easy is it to identify data subjects with the available data processed by the system?”. Following answers are considered:

1. Negligible: Identifying an individual using their personal data appears to be virtually impossible (e.g. searching throughout a Member State population on one meter reading or searching throughout the EU population using only an individual's first name).
2. Limited: Identifying an individual using their personal data appears to be difficult but is possible in certain cases (e.g. searching throughout a Member State population using an individual's 1 day history of meter readings or searching throughout the EU population using an individual's full name).
3. Significant: Identifying an individual using their personal data appears to be relatively easy (e.g. searching throughout a Member State population using an individual's history of meter readings of multiple days or searching throughout the EU population using an individual's full name and date of birth).
4. Maximum: Identifying an individual using their personal data appears to be extremely easy (e.g. searching throughout a Member State population using an individual's history of meter readings or searching throughout the EU population using an individual's full name, date of birth and mailing address).

The value of the level that best match the personal data identified was then selected. Any existing or planned measures that reduce the identification are documented and will be taken into account in the next step (Step 6 on controls and final risk level).

The prejudicial effect of each feared event was then estimated. In other words, how much damage would be caused by all the potential impacts? We answered the following question: “How much damage would be caused by all the potential impacts?”

1. Negligible: Data subjects either will not be affected or may encounter a few inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.).
2. Limited: Data subjects may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.).
3. Significant: Data subjects may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by banks, property damage, loss of employment, subpoena, worsening of state of health, etc.).
4. Maximum: Data subjects may encounter significant, or even irreversible, consequences, which they may not overcome (financial distress such as substantial debt or inability to work, long-term psychological or physical ailments, death, etc.).

The value of the level that best match the potential impacts identified was then selected. Any existing or planned measures that reduce the prejudicial effect shall be documented and will be taken into account in the next step (Step 6 on controls and final risk level).

The last step of this process was to determine the severity/impact of the feared events and their related threats. The severity is determined by adding the respective personal data *level of identification* and *prejudicial effects of potential impacts* values obtained and locating the sum in the table below.

**Table 47 – Determination of Severity/Impact level**

Level of identification + prejudicial effects	Level of identification	Prejudicial effect	Severity/impact
< 5			1. Negligible
= 5			2. Limited
= 6			3. Significant
> 6			4. Maximum

#### 14.4.6.2 LIKELIHOOD OF THREATS

Likelihood represents the probability of a risk to occur. It essentially depends on the level of vulnerabilities of the supporting assets facing the level of capabilities of the risk sources to exploit them.

The likelihood was assessed by the combination of the *level of vulnerability of the supporting assets* and the *capability of the risk source for the exploitation of this vulnerability*.

Since a threat is a possible action by risk sources on supporting assets, the supporting assets are identified and estimated for each threat.

First, the vulnerabilities of the supporting assets are estimated for each threat. In other words, to what degree can the properties of supporting assets be exploited in order to carry out a threat?



Following question was considered: “To what degree can the properties of supporting assets be exploited in order to carry out a threat?”

1. Negligible: Carrying out a threat by exploiting the properties of supporting assets does not appear possible (e.g. theft of paper documents stored in a room protected by a badge reader and access code).
2. Limited: Carrying out a threat by exploiting the properties of supporting assets appears to be difficult (e.g. theft of paper documents stored in a room protected by a badge reader).
3. Significant: Carrying out a threat by exploiting the properties of supporting assets appears to be possible (e.g. theft of paper documents stored in offices that cannot be accessed without first checking in at reception).
4. Maximum: Carrying out a threat by exploiting the properties of supporting assets appears to be extremely easy (e.g. theft of paper documents stored in a lobby).

The value of the level that best match the supporting asset vulnerabilities identified was then selected. Control measures which are already implemented or planned for the applications and which is in principle reducing these vulnerabilities and impact the value of this level are taken into account in the next step (Step 6 on controls and final risk level).

Then the capabilities of risk sources to exploit vulnerabilities (skills, available time, financial resources, proximity to system, motivation, feeling of impunity, etc.) were estimated for each threat.

1. Negligible: Risk sources do not appear to have any special capabilities to carry out a threat (e.g. software function creep by an individual acting without malicious intent and who has limited access privileges).
2. Limited: The capabilities of risks sources to carry out a threat are limited (e.g.: software function creep by a malicious individual with limited access privileges).
3. Significant: The capabilities of risk sources to carry out a threat are real and significant (e.g. software function creep by an individual acting without malicious intent and who has unlimited administration privileges).
4. Maximum: The capabilities of risk sources to carry out a threat are definite and unlimited (e.g. software function creep by a malicious individual with unlimited administration privileges).

The values of the level that best match the risk sources identified were then selected. Any existing or planned measures that reduce the capabilities of risk sources shall be documented and taken into account in the next step (Step 6 on controls and final risk level).

Finally, the likelihood of the threats is determined by adding the values obtained for the vulnerabilities of the supports and the capabilities of the risk sources and locating the sum according the table below:

**Table 48 – Determination of Likelihood level**

Supporting asset vulnerabilities + risk source capabilities	Vulnerabilities of the supporting assets	Capabilities of risk sources	Likelihood
< 5			1. Negligible
= 5			2. Limited
= 6			3. Significant
> 6			4. Maximum



Summary:

The process described above can be synthesized according to the following diagram.

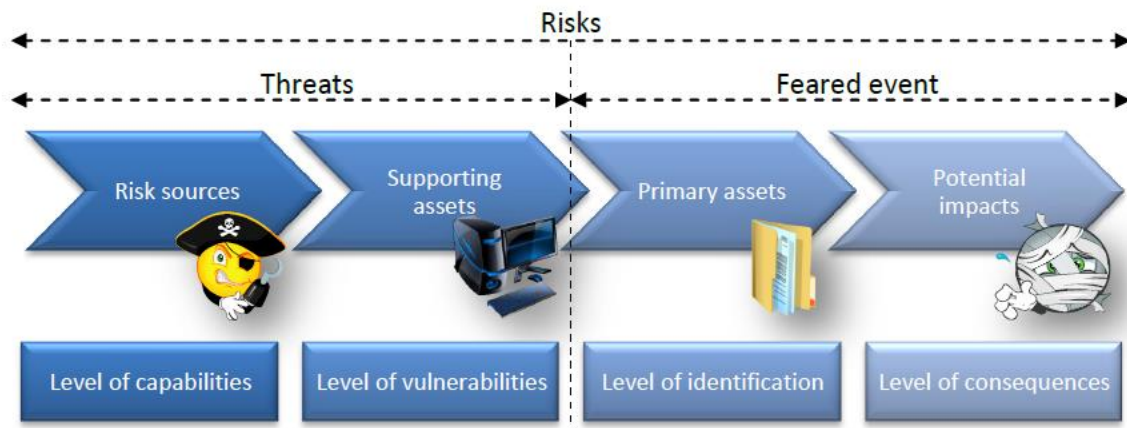


Figure 77 – Threats/Events identification process

#### 14.4.6.3 FINAL RISK LEVEL / VALUE AND PRIORITY

Once the relevant threats have been identified, their quantification did lead us to risks related to the feared events which are considered from the point of view of their impact/severity and likelihood (as highlighted above).

The order of priority for the identified and quantified risks did lead to the following statement:

1. **Risks with a high severity and likelihood** will strictly be avoided or reduced by implementing security measures that reduce both their severity and their likelihood. First option is to ensure that these risks are treated by independent measures of prevention (actions taken prior to a damaging event), protection (actions taken during a damaging event) and recovery (actions taken after a damaging event).
2. **Risks with a high severity but a low likelihood** will be avoided or reduced by implementing security measures that reduce either their severity or their likelihood. Main purpose is on preventive measures.
3. **Risks with a low severity but a high likelihood** will be reduced by implementing security measures that reduce their likelihood. Main purpose is on recovery measures.
4. **Risks with a low severity and likelihood** may be taken, especially since the treatment of other risks could also lead to their treatment.

A table was defined for each WG tool with evaluation results and also a resulting “Risk map” as below.

#### 14.4.6.3.1 WG IOP

Table 49 – Risk evaluation for WiseGRID IOP

Feared events	Threat ID	Related Privacy targets	Affected assets	Impact (Severity)			Likelihood			Risk Level (Impact+ Likelihood)
				level of identification (how easy?)	prejudicial effect (how much damage?)	I	vulnerabilities of the supporting assets	capabilities of risk sources	L	
Change in processing	II	Legitimacy of processing personal data	Processes	2	2	4	1	3	4	
Disappearance of personal data	ED	Compliance with data retention requirements	Personal data	2	2	4	3	2	5	
	Pobj	Compliance with data retention requirements	Personal data	2	1	3	NA	NA	NA	
Diverting of personal data to other users	DoS	Legitimacy of processing personal data	Personal data	1	2	3	3	2	5	
	IISC	Legitimacy of processing personal data	Personal data	1	2	3	3	3	6	
Illegitimate access to personal data	HL	Privacy by default	Personal data	2	3	5	3	3	6	
	IACP	Privacy by default	Personal data	2	3	5	3	2	5	

Feared events	Threat ID	Related Privacy targets	Affected assets	Impact (Severity)			Likelihood			Risk Level (Impact+Likelihood)
				level of identification (how easy?)	prejudicial effect (how much damage?)	I	vulnerabilities of the supporting assets	capabilities of risk sources	L	
Unavailability of legal processes	NL	Compliance with notification requirements	Processes	1	3	4	NA	NA	NA	
	SA	Compliance with notification requirements	Processes	1	3	4	1	3	2	
Unwanted change in personal data	LQD	Safeguarding quality of personal data	Personal data	3	3	6	NA	NA	NA	

The aim of this step is to obtain a risk map in order to determine the order in which they should be treated.

Since a risk consists of a feared event and all the threats that may allow it to occur:

- its severity equals that of the feared event,
- its likelihood equals the highest likelihood value of the threats associated with the feared event.

The risks can then be mapped:

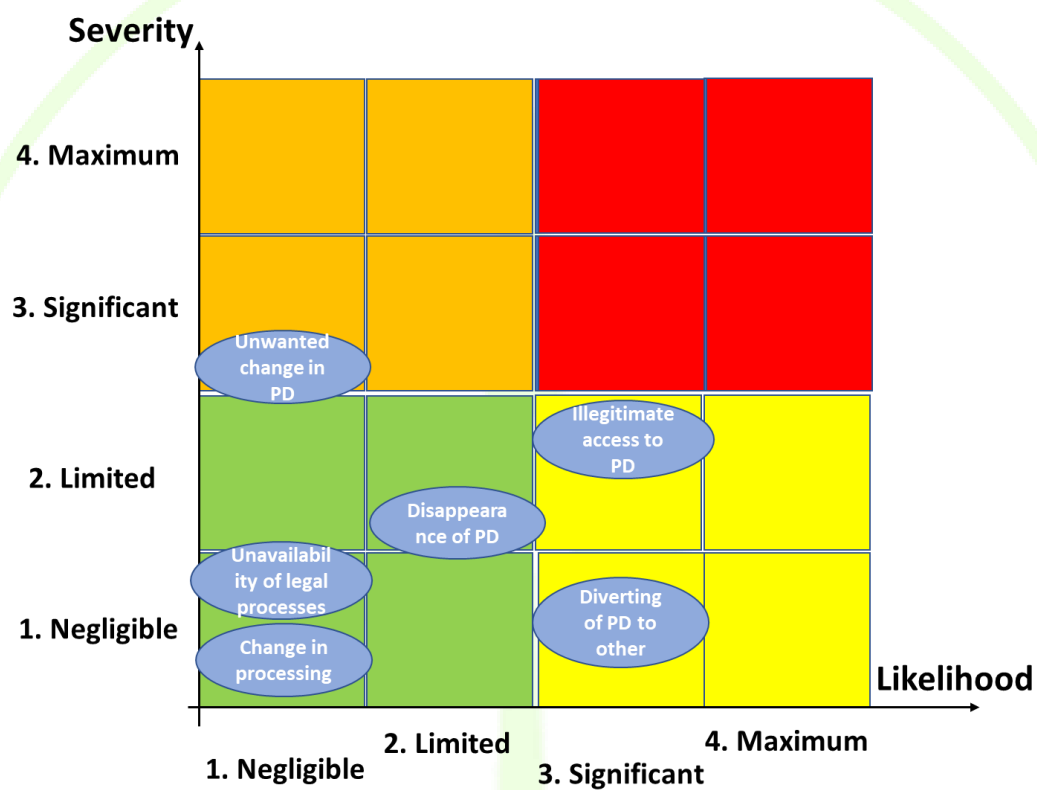


Figure 78 - Risk map for WG IOP

#### 14.4.6.3.2 WG Cockpit

Table 50 – Risk evaluation for WG Cockpit

Feared events	Threat ID	Related Privacy targets	Affected assets	Impact (Severity)			Likelihood			Risk Level (Impact+ Likelihood)
				level of identification (how easy?)	prejudicial effect (how much damage?)	I	vulnerabilities of the supporting assets	capabilities of risk sources	L	
Change in processing	II	Legitimacy of processing personal data	Processes	2	2	4	1	3	4	
Disappearance of personal data	ED	Compliance with data retention requirements	Personal data	1	1	2	NA	NA	NA	
	Pobj	Compliance with data retention requirements	Personal data	1	1	2	NA	NA	NA	
Diverting of personal data to other users	DoS	Legitimacy of processing personal data	Personal data	1	1	2	NA	NA	NA	
	IISC	Legitimacy of processing personal data	Personal data	1	1	2	NA	NA	NA	
Unwanted change in personal data:	MEP	Safeguarding quality of personal data	Personal data	1	1	2	NA	NA	NA	

Feared events	Threat ID	Related Privacy targets	Affected assets	Impact (Severity)			Likelihood			Risk Level (Impact+Likelihood)
				level of identification (how easy?)	prejudicial effect (how much damage?)	I	vulnerabilities of the supporting assets	capabilities of risk sources	L	
they are altered or changed	LQD	Safeguarding quality of personal data	Personal data	1	1	2	NA	NA	NA	
Unavailability of legal processes: they do not or no longer exist or work	SA	Compliance with notification requirements	Processes	2	3	5	3	2	5	

The results are reasonable as long as Cockpit does not process “personal data”.

The risks can then be mapped:

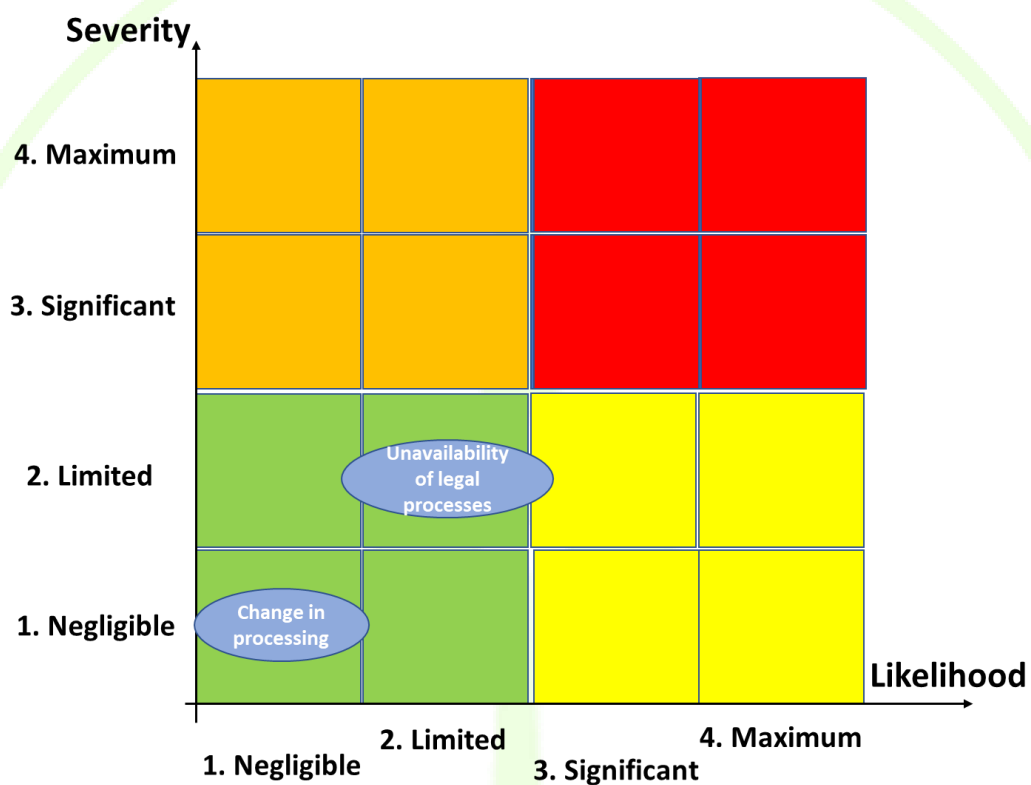


Figure 79 - Risk map for WG Cockpit

#### 14.4.6.3.3 WiseCOOP

Table 51 – Risk evaluation for WiseCOOP

Feared events	Threat ID	Related Privacy targets	Affected assets	Impact (Severity)			Likelihood			Risk Level (Impact+ Likelihood)
				level of identification (how easy?)	prejudicial effect (how much damage?)	I	vulnerabilities of the supporting assets	capabilities of risk sources	L	
Disappearance of personal data	ED	Compliance with data retention requirements	Personal data	2	3	5	3	2	5	
Diverting of personal data to other users	DoS	Legitimacy of processing personal data	Personal data	1	2	3	3	2	5	
	IISC	Legitimacy of processing personal data	Personal data	1	2	3	3	3	6	
Unwanted change in personal data	LQD	Safeguarding quality of personal data	Personal data	3	3	6	NA	NA	NA	



The risks can then be mapped:

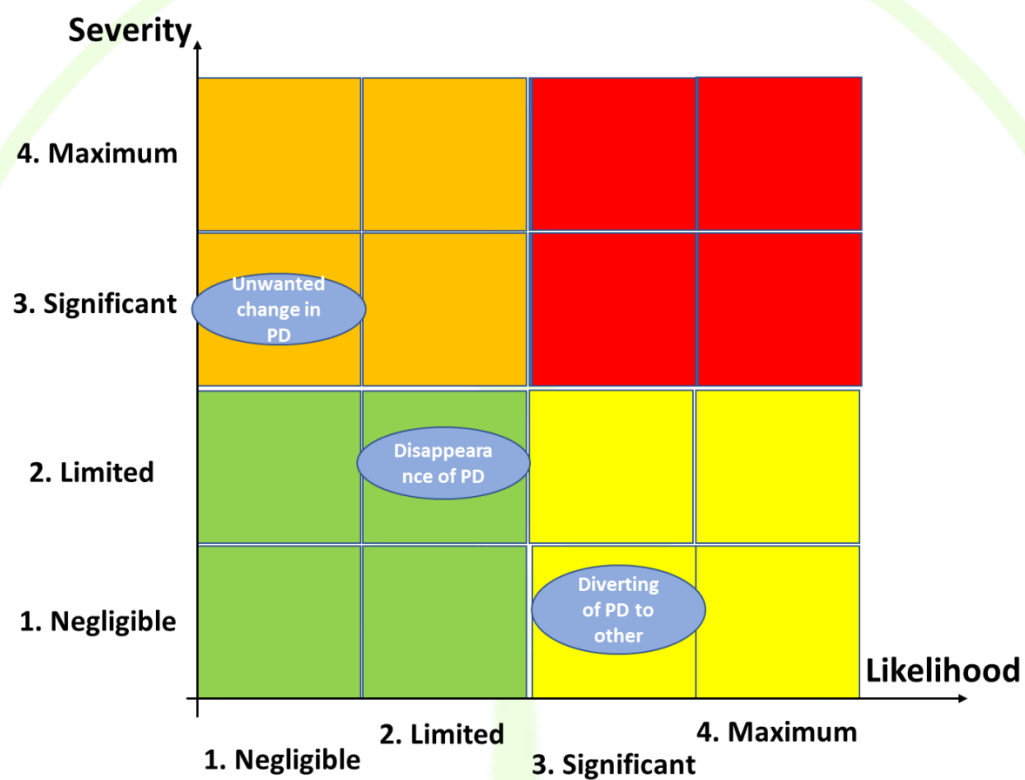


Figure 80 - Risk map for WiseCOOP

#### 14.4.6.3.4 WG STaaS

Table 52 – Risk evaluation for WG STaaS

Feared events	Threat ID	Related Privacy targets	Affected assets	Impact (Severity)			Likelihood			Risk Level (Impact+ Likelihood)
				level of identification (how easy?)	prejudicial effect (how much damage?)	I	vulnerabilities of the supporting assets	capabilities of risk sources	L	
Disappearance of personal data	ED	Compliance with data retention requirements	Personal data	2	3	5	3	3	6	
Diverting of personal data to other users	DoS	Legitimacy of processing personal data	Personal data	1	2	3	3	2	5	
	CDEEA	Legitimacy of processing personal data	Personal data	2	2	4	3	3	6	

The risks can then be mapped:

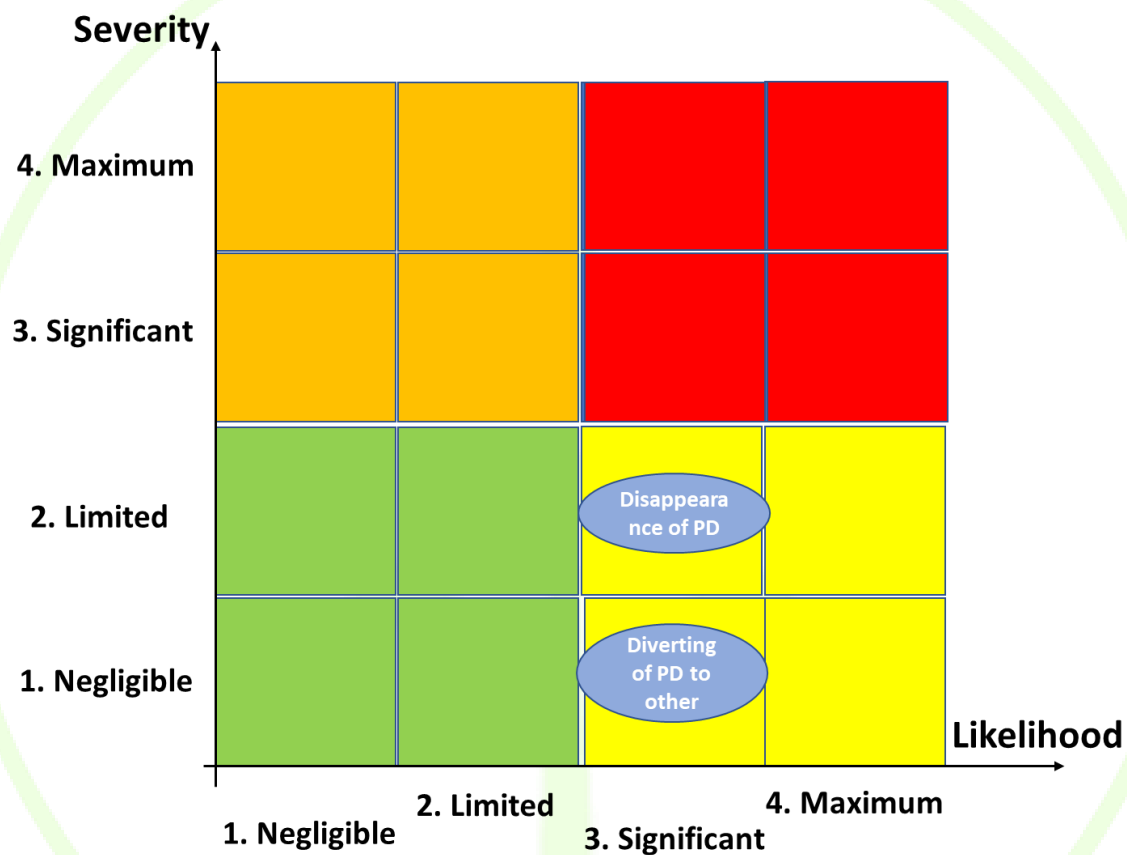


Figure 81 - Risk map for WG STaaS

#### 14.4.6.3.5 WiseEVP

Table 53 – Risk evaluation for WiseEVP

Feared events	Threat ID	Related Privacy targets	Affected assets	Impact (Severity)			Likelihood			Risk Level (Impact+ Likelihood)
				level of identification (how easy?)	prejudicial effect (how much damage?)	I	vulnerabilities of the supporting assets	capabilities of risk sources	L	
Disappearance of personal data	ED	Compliance with data retention requirements	Personal data	2	3	5	3	2	5	
Diverting of personal data to other users	DoS	Legitimacy of processing personal data	Personal data	2	3	5	3	3	6	
Unwanted change in personal data	ADNI	Safeguarding quality of personal data	Personal data	3	3	6	NA	NA	NA	

The risks can then be mapped:

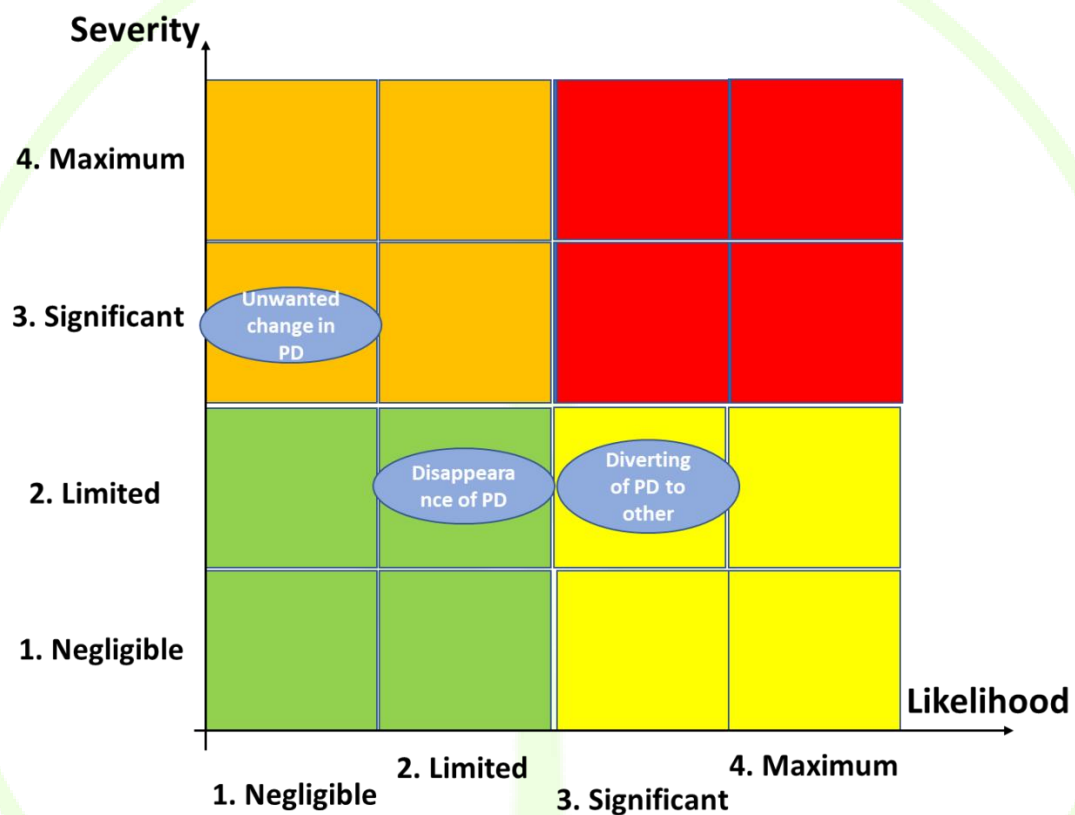


Figure 82 - Risk map for WiseEVP

#### 14.4.6.3.6 WG FastV2G

Table 54 – Risk evaluation for WG V2G

Feared events	Threat ID	Related Privacy targets	Affected assets	Impact (Severity)			Likelihood			Risk Level (Impact+ Likelihood)
				level of identification (how easy?)	prejudicial effect (how much damage?)	I	vulnerabilities of the supporting assets	capabilities of risk sources	L	
Change in processing	II	Legitimacy of processing personal data	Processes	1	2	3	1	3	4	
Disappearance of personal data	ED	Compliance with data retention requirements	Personal data	1	2	3	2	1	3	
	Pobj	Compliance with data retention requirements	Personal data	3	2	5	2	3	5	
	HLPL	Privacy by design	Personal data	2	2	4	2	3	5	
Diverting of personal data to other users	DoS	Legitimacy of processing personal data	Personal data	2	3	5	3	3	6	
	IISC	Legitimacy of processing personal data	Personal data	1	2	3	3	3	6	
Unwanted change in personal data	ADNI	Safeguarding quality of personal data	Personal data	3	3	6	NA	NA	NA	

Feared events	Threat ID	Related Privacy targets	Affected assets	Impact (Severity)			Likelihood			Risk Level (Impact+ Likelihood)
				level of identification (how easy?)	prejudicial effect (how much damage?)	I	vulnerabilities of the supporting assets	capabilities of risk sources	L	
Illegitimate access to personal data	IACP	Privacy by default	Personal data	2	3	5	3	2	5	

The risks can then be mapped:

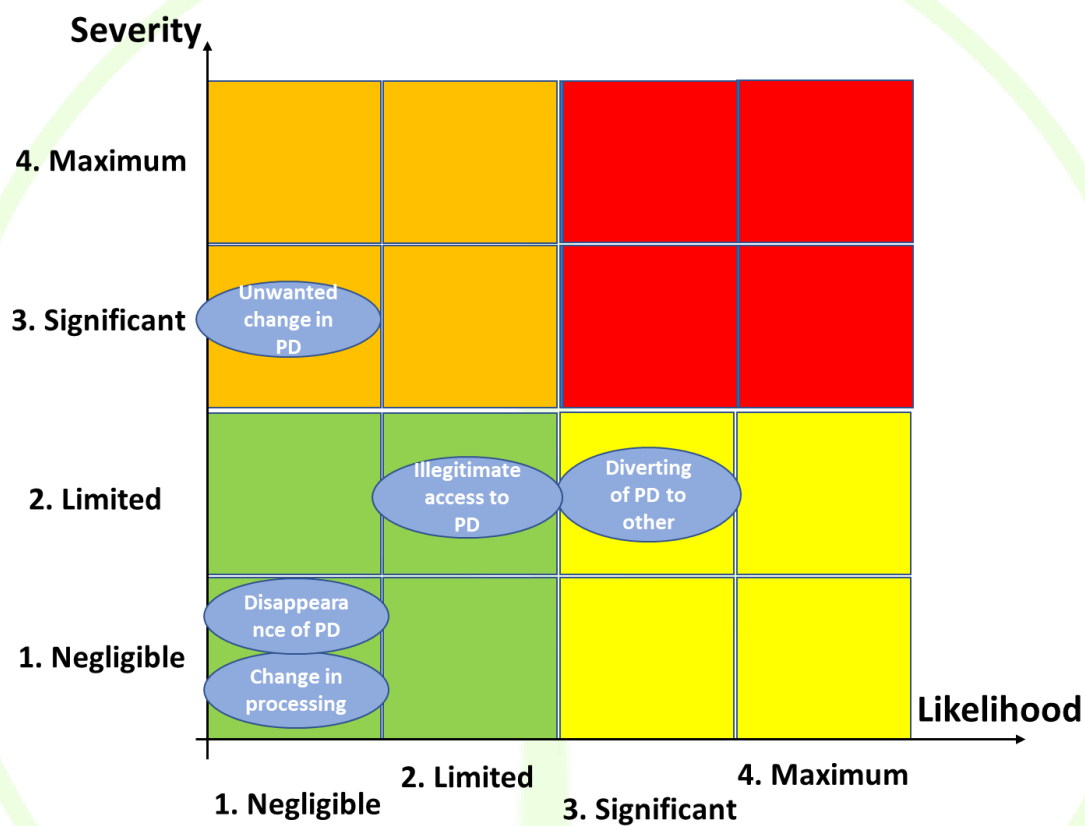


Figure 83 - Risk map for WG FastV2G



#### 14.4.6.3.7 WiseCORP

Table 55– Risk evaluation for WiseCORP

Feared events	Threat ID	Related Privacy targets	Affected assets	Impact (Severity)			Likelihood			Risk Level (Impact+ Likelihood)
				level of identification (how easy?)	prejudicial effect (how much damage?)	I	vulnerabilities of the supporting assets	capabilities of risk sources	L	
Disappearance of personal data	ED	Legitimacy of processing personal data	Personal data	1	2	3	3	2	5	
	Pobj	Legitimacy of processing personal data	Personal data	2	2	4	3	3	6	
Change in processing	ADNI	Safeguarding quality of personal data	Personal data	2	2	4	2	2	4	
Illegitimate access to personal data	IACP	Privacy by default	Personal data	2	2	4	1	2	3	

The risks can then be mapped:

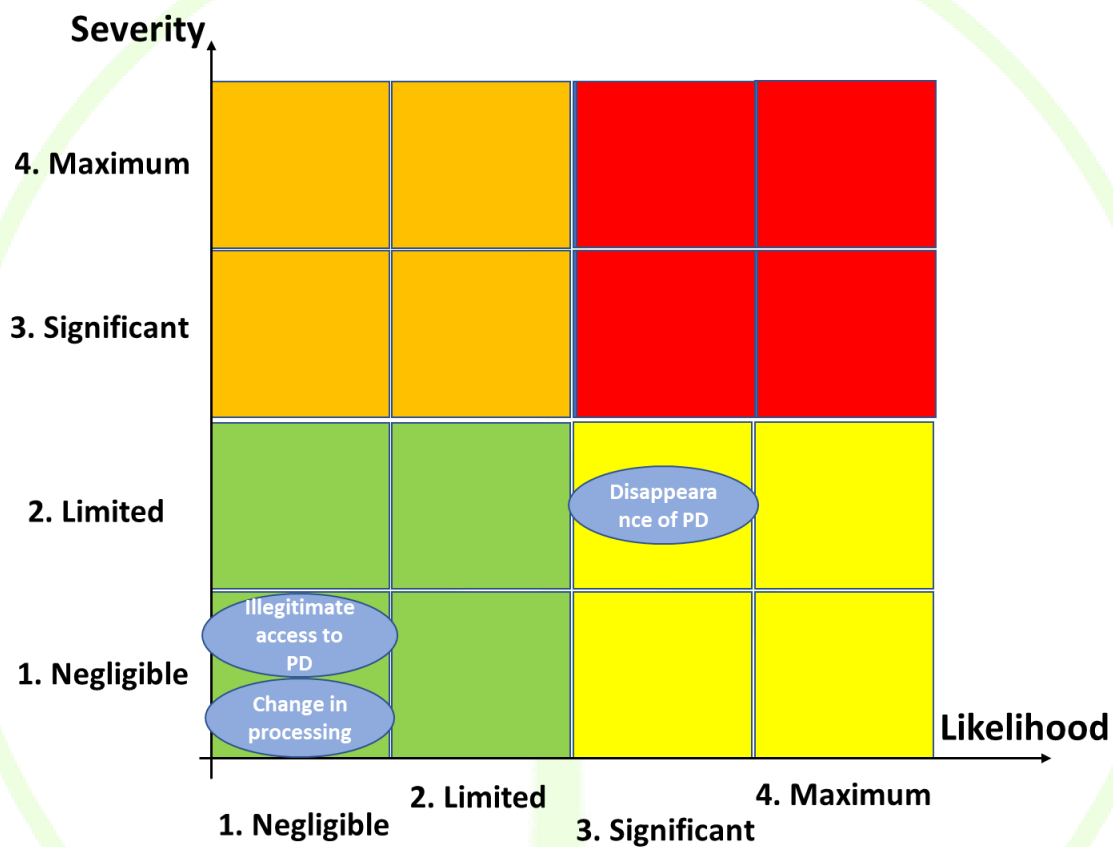


Figure 84 - Risk map for WiseCORP

#### 14.4.6.3.8 WiseHOME

Table 56 – Risk evaluation for WiseHOME

Feared events	Threat ID	Related Privacy targets	Affected assets	Impact (Severity)			Likelihood			Risk Level (Impact+ Likelihood)
				level of identification (how easy?)	prejudicial effect (how much damage?)	I	vulnerabilities of the supporting assets	capabilities of risk sources	L	
Disappearance of personal data	ED	Compliance with data retention requirements	Personal data	1	2	3	2	2	4	
	Pobj	Compliance with data retention requirements	Personal data	2	2	4	3	3	6	
Diverting of personal data to other users	DoS	Legitimacy of processing personal data	Personal data	2	3	5	2	3	5	
	IISC	Legitimacy of processing personal data	Personal data	1	2	3	3	3	6	
Unavailability of legal processes: they do not or no longer exist or work	AUS	Compliance with notification requirements	Processes	1	1	2	1	1	2	
	NL	Compliance with notification requirements	Processes	1	3	4	2	3	5	

Feared events	Threat ID	Related Privacy targets	Affected assets	Impact (Severity)			Likelihood			Risk Level (Impact+Likelihood)
				level of identification (how easy?)	prejudicial effect (how much damage?)	I	vulnerabilities of the supporting assets	capabilities of risk sources	L	
Change in processing	ADNI	Safeguarding quality of personal data	Personal data	2	2	4	2	2	4	

The risks can then be mapped:

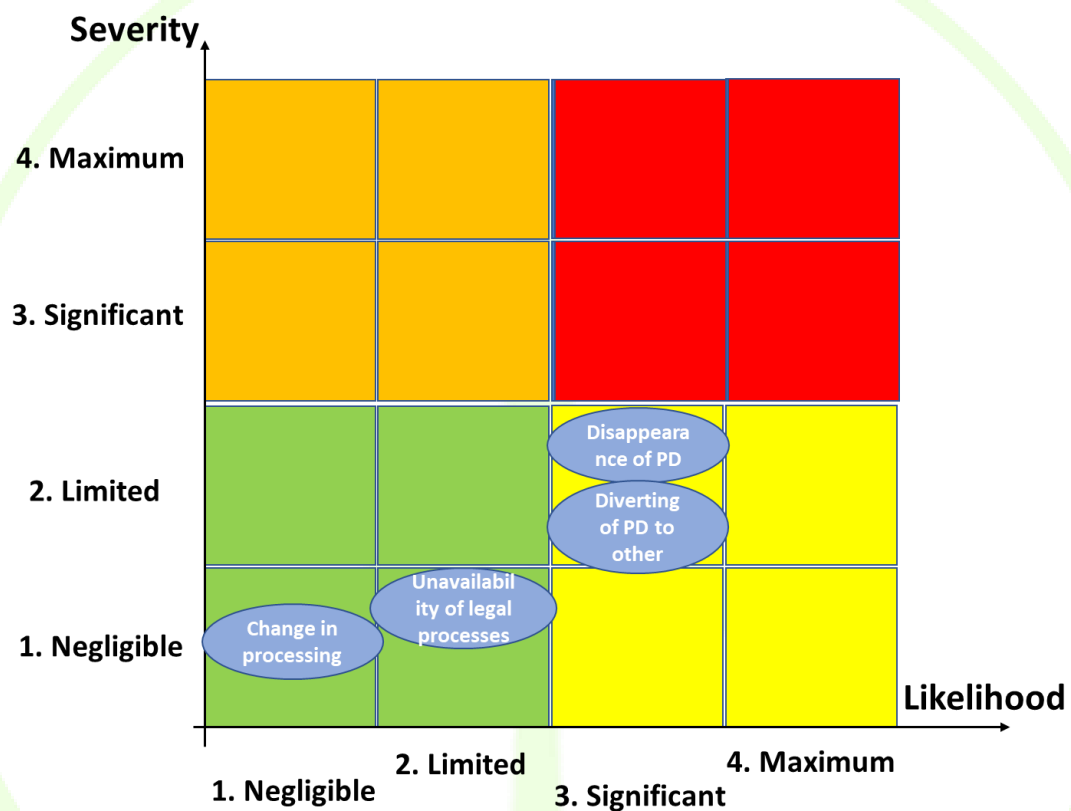


Figure 85 - Risk map for WiseHOME

#### 14.4.6.3.9 WG RESCO

Table 57 – Risk evaluation for WG RESCO

Feared events	Threat ID	Related Privacy targets	Affected assets	Impact (Severity)			Likelihood			Risk Level (Impact+ Likelihood)
				level of identification (how easy?)	prejudicial effect (how much damage?)	I	vulnerabilities of the supporting assets	capabilities of risk sources	L	
Illegitimate access to personal data	UDC	Legitimacy of processing personal data	Personal data	2	3	5	2	3	5	
Disappearance of personal data	ED	Compliance with data retention requirements	Personal data	1	2	3	3	2	5	
	Pobj	Compliance with data retention requirements	Personal data	2	2	4	2	3	5	
Diverting of personal data to other users	DoS	Legitimacy of processing personal data	Personal data	1	2	3	3	2	5	
	IISC	Legitimacy of processing personal data	Personal data	1	2	3	3	3	6	
Unavailability of legal processes	SA	Compliance with notification requirements	Processes	1	3	4	1	3	2	

The risks can then be mapped:

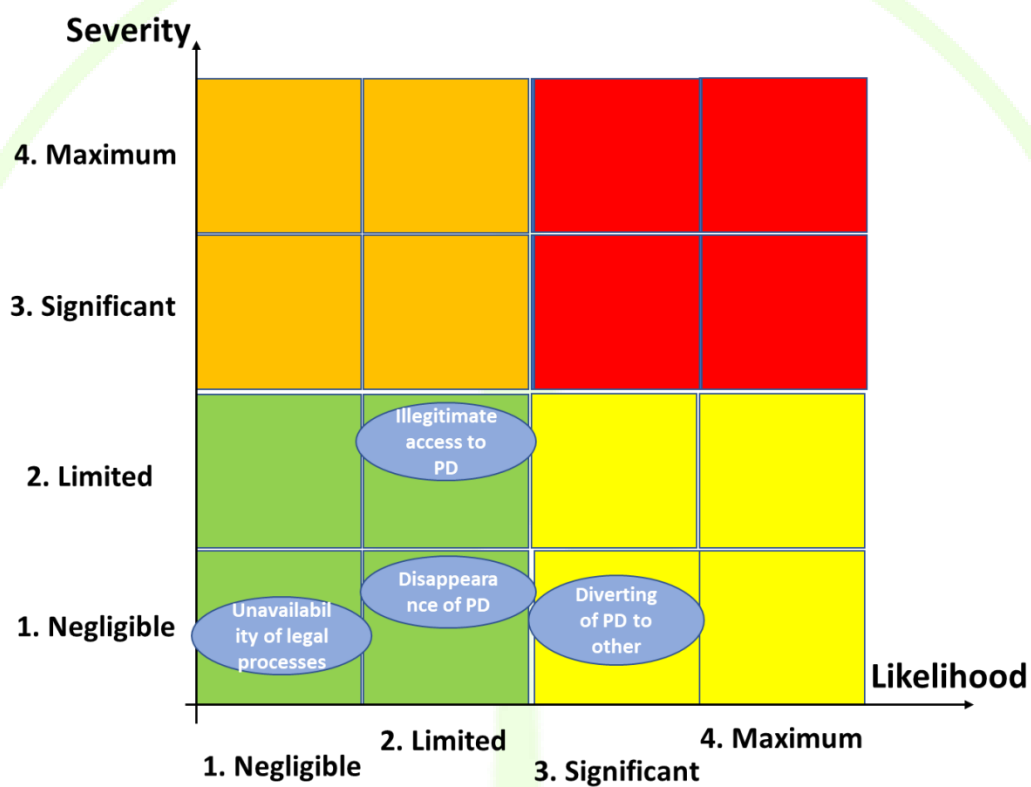


Figure 86 - Risk map for WG RESCO

The summary of above mentioned steps are in line with below diagram:

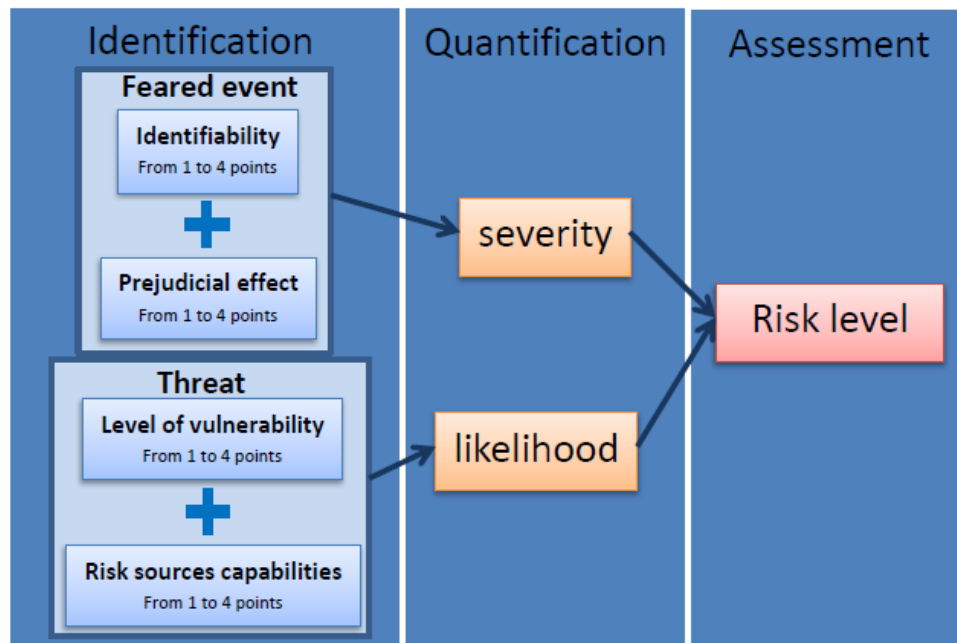


Figure 87 – Risk level identification diagram

#### **Results available after this step:**

A complete set of tables (one for each WG Tool) together with a mapping of the identified risks within the map, are provided. At this stage, the controls and mitigation measures are still not taken into account in the evaluation level of risks.

Risks are presented in order of priority. According to their respective levels, they could require additional (mitigation) measures as will be presented in the next step (step 6).

Where not already documented, these include details of the impacted part of the application and stakeholders which should have been listed in the description.

### **14.4.7 IDENTIFICATION AND RECOMMENDATION OF CONTROLS AND RESIDUAL RISKS;**

#### **14.4.7.1 ASSESSMENT OF IMPLEMENTED AND PLANNED CONTROLS**

At this stage, the aim was to consider the risks identified and assessed in the previous step and to present which controls are planned to be implemented (mitigation measures) in order to reduce the risk at lower and appropriate levels. Any risk found as unacceptable level, was appropriately mitigated by one or more controls considering their likelihood and impact.



The Expert Group 2 did establish a list of ‘Best Available Techniques’ in smart metering system environments which provided guidance to the data controller regarding which control would be the most efficient.

In 25 - APPENDIX H - PRIVACY & DATA PROTECTION LIST OF POSSIBLE CONTROLS, are presented the usual controls as provided. Specific controls were determined for WiseGRID under subchapter 14.4.7 - Identification and recommendation of controls and residual risks;

Best Available Techniques, refers to “the most effective and advanced stage” in the development of activities and their methods of operation, which indicate the practical suitability of particular techniques for providing in principle the basis for complying with the EU data protection framework. They are designed to prevent or mitigate risks on privacy, personal data and security.”

The controls (mitigation measures) adopted by the developer will cover the following dimensions:

- The infrastructure (communication network, Equipment Protection, hardening, etc.);
- The agents/personnel involved in the process (Individual access and control mechanism, etc.);
- The organization and procedure (Smart grid application governing practices, accountability measures, etc.);
- The technologies (system protection measures including Security Controls and IT based security methodology, etc.).

The DPIA report explains in detail how the selected (implemented or planned) controls related to specific risks, have results in acceptable risk levels. When the risk is shared with a third party, the developer explains which control this third party has implemented or planned to implement in order to address this risk in an acceptable way.

#### 14.4.7.2 RISK TREATMENT

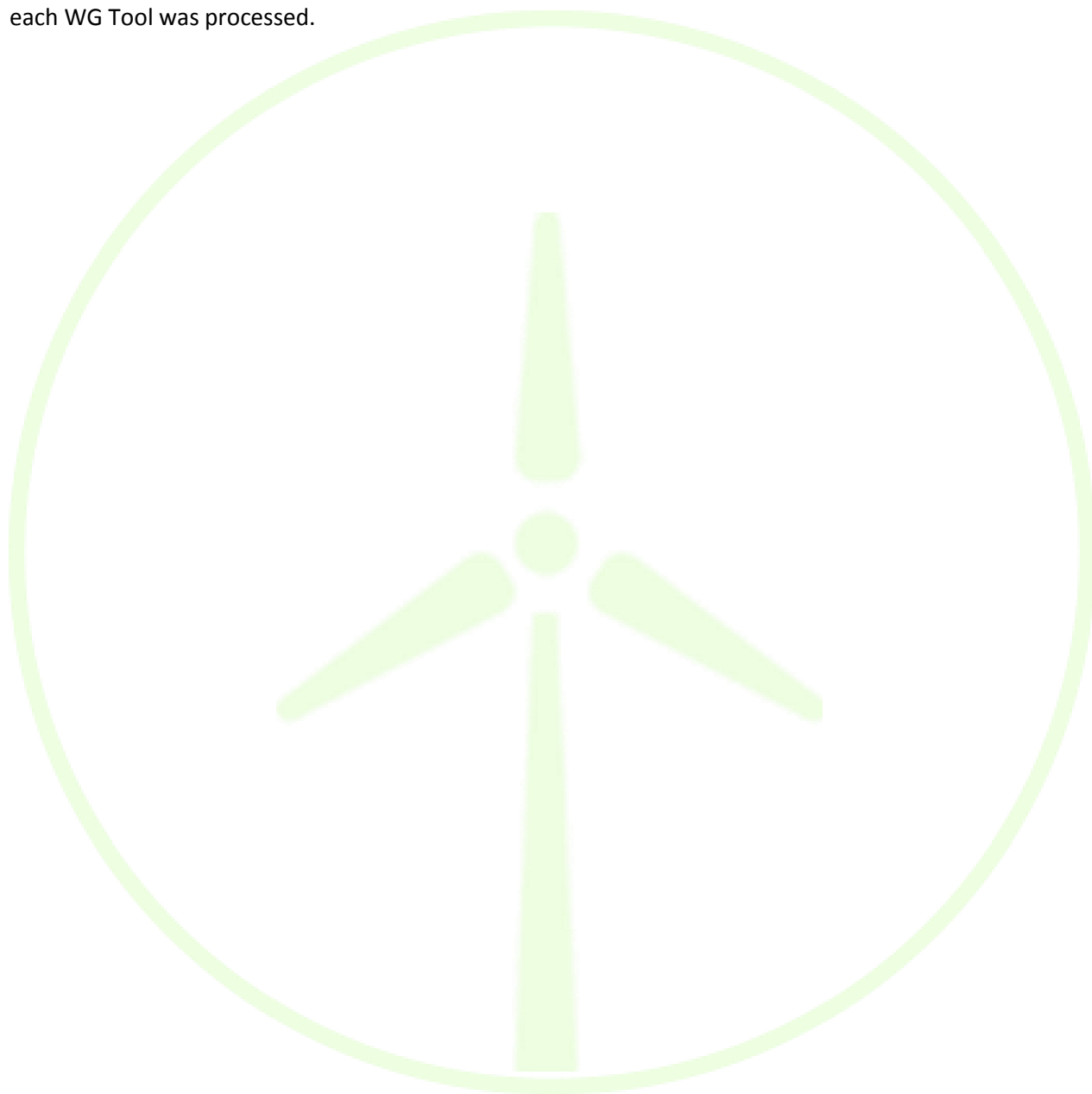
After identified and assessed the risks, the developer specified the way in which these risks were managed. The options that have been considered to manage those risks are as below:

- Risk Modification: The risk is managed by identifying and introducing additional (to those already implemented or planned and described in section 14.6.1) appropriate controls, thereby reducing the risk to acceptable levels;
- Risk Retention: The system owner accepts the risk as it is, if it meets the acceptance criteria, without any further action;
- Risk Avoidance: The system owner decides not to put the application in production;
- Risk Sharing: The risk is shared with a third party, which can manage the identified risk more effectively and thereby reduce the risk at acceptable levels.

In cases where risk level was below or similar to “Limited” level, the Risk was treated as Retention. For each WiseGRID Tool cases where events and threats were bringing risk level to a higher position than

“Limited”, various controls were defined for each such risk and “Risk Modification” was addressed. Further on there was no case for Risk Avoidance or Risk Sharing.

Under next subchapters tables with risk treatment and consequences of the control within risk level are presented. One table and associated map (Risk map for WG Tool with implemented/planned controls) for each WG Tool was processed.



#### 14.4.7.2.1 WiseGRID IOP

Table 58 – Risk treatment and residual risk for WG IOP

Feared events	Threat ID	Related Privacy targets	Controls planned or implemented	Risk level	Risk treatment (including implementation of privacy targets)	Residual risk
Change in processing	II	Legitimacy of processing personal data			Risk Retention	
Disappearance of personal data	ED	Compliance with data retention requirements			Risk Retention	
	Pobj	Compliance with data retention requirements			Risk Retention	
Diverting of personal data to other users	DoS	Legitimacy of processing personal data	Reducing hardware vulnerabilities		Risk Modification	
	IISC	Legitimacy of processing personal data	Anonymizing personal data		Risk Modification	
Illegitimate access to personal data	HL	Privacy by default	Reducing hardware vulnerabilities		Risk Modification	
	IACP	Privacy by default	Managing persons within the organization		Risk Modification	
Unavailability of legal processes	NL	Compliance with notification requirements			Risk Retention	
	SA	Compliance with notification requirements			Risk Retention	
Unwanted change in personal data	LQD	Safeguarding quality of personal data	Introduction automated controls on the data quality		Risk Modification	

Considered controls are:

- Reducing hardware vulnerabilities

Objective: to reduce the possibility to exploit hardware properties (servers, desktop computers, laptops, devices, communications relays, removable storage devices, etc.) to adversely affect personal data.

- Anonymizing personal data

Objective: to remove identifying characteristics from personal data.

- Reducing hardware vulnerabilities

Objective: to reduce the possibility to exploit hardware properties (servers, desktop computers, laptops, devices, communications relays, removable storage devices, etc.) to adversely affect personal data.

- Managing persons within the organization

Objective: to reduce the risks associated with persons within the organization (employees, seconded subcontractors, interns and visitors) who have legitimate access to personal data.

- Introduction automated controls on the data quality

Objective: to ensure that data quality is monitored and maintained on a regular basis.

The aim of this step is to obtain a list of planned and implemented controls for mitigating the identified risks and a new risk map with location of residual risks. This new risk map should have residual risks at a lower level compared to the first risk map with no controls.

The risks can then be mapped:

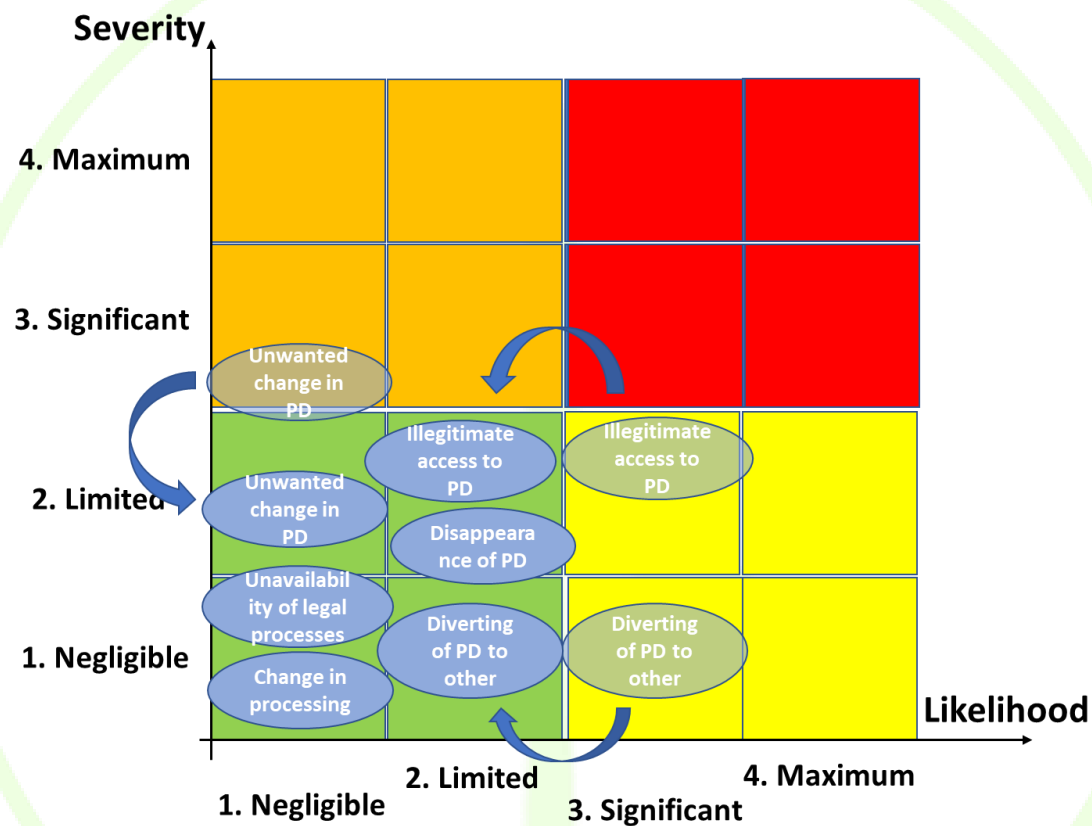


Figure 88 - Risk map for WG IOP with implemented/planned controls

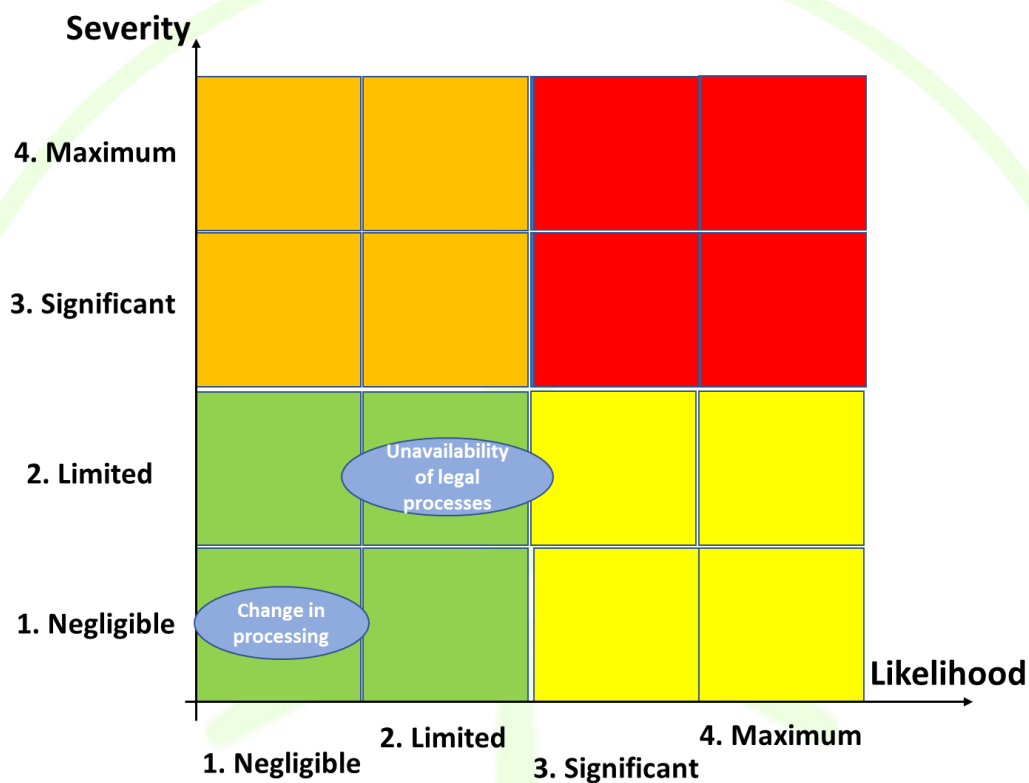
The results of the Risk treatment (Risk modification) based on applied controls for WG IOP, have brought the risk level within the “Limited” level or below.

#### 14.4.7.2.2 WG Cockpit

Table 59 – Risk treatment and residual risk for WG Cockpit

Feared events	Threat ID	Related Privacy targets	Controls planned or implemented	Risk level	Risk treatment (including implementation of privacy targets)	Residual risk
Change in processing	II	Legitimacy of processing personal data				
Disappearance of personal data	ED	Compliance with data retention requirements				
	Pobj	Compliance with data retention requirements				
Diverting of personal data to other users	DoS	Legitimacy of processing personal data				
	IISC	Legitimacy of processing personal data				
Unwanted change in personal data: they are altered or changed	MEP	Safeguarding quality of personal data				
	LQD	Safeguarding quality of personal data				
Unavailability of legal processes: they do not or no longer exist or work	SA	Compliance with notification requirements				

There is no need for additional controls as long as the risk is below acceptable level.



**Figure 89 - Risk map for WG Cockpit with implemented/planned controls**

The results of the Risk treatment (Risk modification) based on applied controls for WG Cockpit, have brought the risk level within the “Limited” level or below.

#### 14.4.7.2.3 WiseCOOP

Table 60 – Risk treatment and residual risk for WiseCOOP

Feared events	Threat ID	Related Privacy targets	Controls planned or implemented	Risk level	Risk treatment (including implementation of privacy targets)	Residual risk
Disappearance of personal data	ED	Compliance with data retention requirements			Risk Retention	
Diverting of personal data to other users	DoS	Legitimacy of processing personal data			Risk Retention	
	IISC	Legitimacy of processing personal data	Encrypting personal data Anonymizing personal data		Risk Modification	
Unwanted change in personal data	LQD	Safeguarding quality of personal data	Introduction automated controls on the data quality		Risk Modification	

- Encrypting personal data

Objective: to make personal data unintelligible to anyone without access authorization.

- Anonymizing personal data

Objective: to remove identifying characteristics from personal data.

- Introduction automated controls on the data quality

Objective: to ensure that data quality is monitored and maintained on a regular basis.



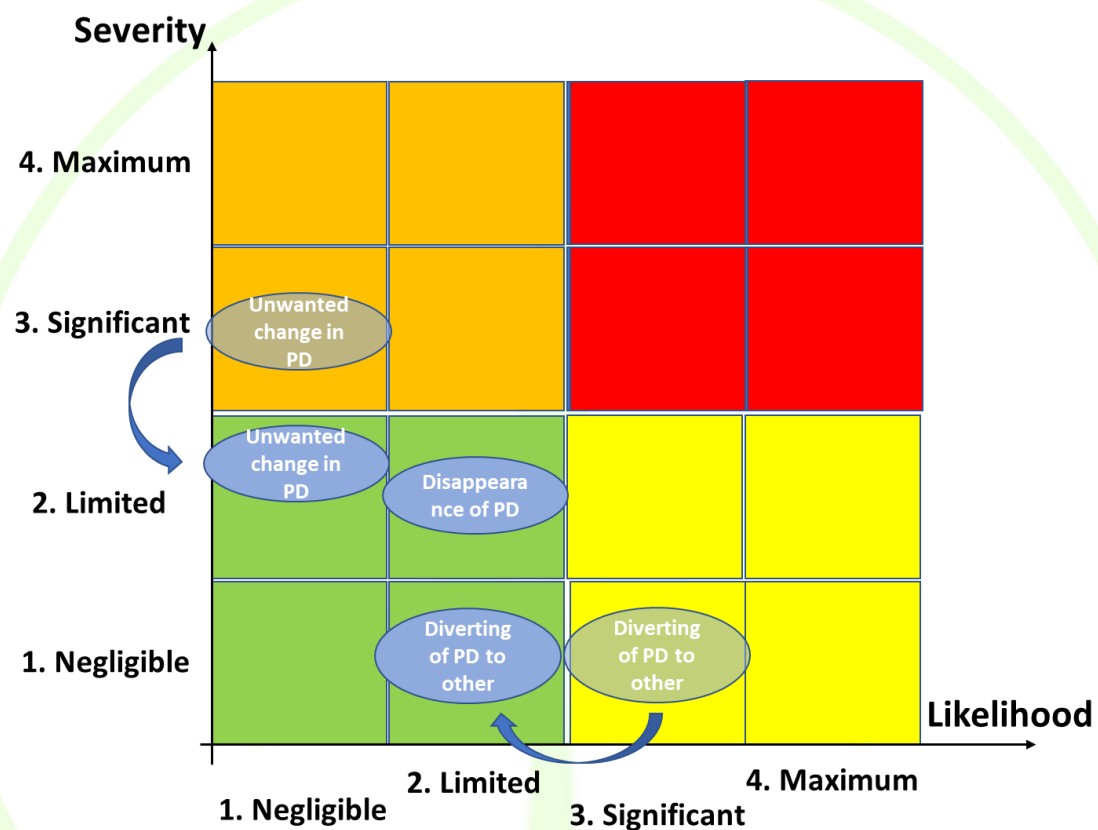


Figure 90 - Risk map for WG COOP with implemented/planned controls

The results of the Risk treatment (Risk modification) based on applied controls for WG COOP, have brought the risk level within the “Limited” level or below.

#### 14.4.7.2.4 WG STaaS

**Table 61 – Risk treatment and residual risk for WG STaaS**

Feared events	Threat ID	Related Privacy targets	Controls planned or implemented	Risk level	Risk treatment (including implementation of privacy targets)	Residual risk
Disappearance of personal data	ED	Compliance with data retention requirements	Reducing the vulnerabilities of computer communications networks		Risk Modification	
Diverting of personal data to other users	DoS	Legitimacy of processing personal data	Reducing hardware vulnerabilities		Risk Modification	
	CDEEA	Legitimacy of processing personal data	Limiting personal data transfer to countries that provide an adequate level of protection according to the article 25 of the Directive 95/46/EC		Risk Modification	

- Reducing the vulnerabilities of computer communications networks

Objective: to reduce the possibility to exploit communications networks properties (wired networks, Wi-Fi, radio waves, fibre optics, etc.) to adversely affect personal data.

- Reducing hardware vulnerabilities

Objective: to reduce the possibility to exploit hardware properties (servers, desktop computers, laptops, devices, communications relays, removable storage devices, etc.) to adversely affect personal data.

- Limiting personal data transfer to countries that provide an adequate level of protection according to the article 25 of the Directive 95/46/EC.

Objective: limiting the disclosure of personal data within states that do not provide an adequate level of protection according to the article 25 of the Directive 95/46/EC.

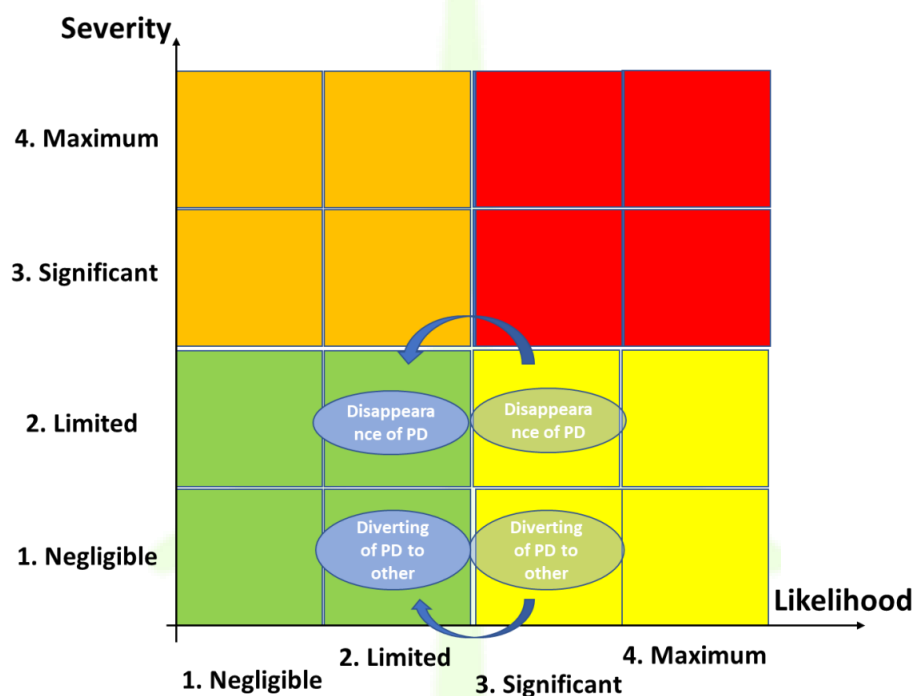


Figure 91 - Risk map for WG STaaS with implemented/planned controls

The results of the Risk treatment (Risk modification) based on applied controls for WG STaaS, have brought the risk level within the “Limited” level or below.

#### 14.4.7.2.5 WiseEVP

Table 62 – Risk treatment and residual risk for WiseEVP

Feared events	Threat ID	Related Privacy targets	Controls planned or implemented	Risk level	Risk treatment (including implementation of privacy targets)	Residual risk
Disappearance of personal data	ED	Compliance with data retention requirements			Risk Retention	
Diverting of personal data to other users	DoS	Legitimacy of processing personal data	Reducing hardware vulnerabilities		Risk Modification	
Unwanted change in personal data	ADNI	Safeguarding quality of personal data	Active measure to preclude the use of particular data-items in the making of particular decisions		Risk Modification	

- Reducing hardware vulnerabilities

Objective: to reduce the possibility to exploit hardware properties (servers, desktop computers, laptops, devices, communications relays, removable storage devices, etc.) to adversely affect personal data.

- Active measure to preclude the use of particular data-items in the making of particular decisions

Objective: to ensure that decisions are made based only on due data-items.

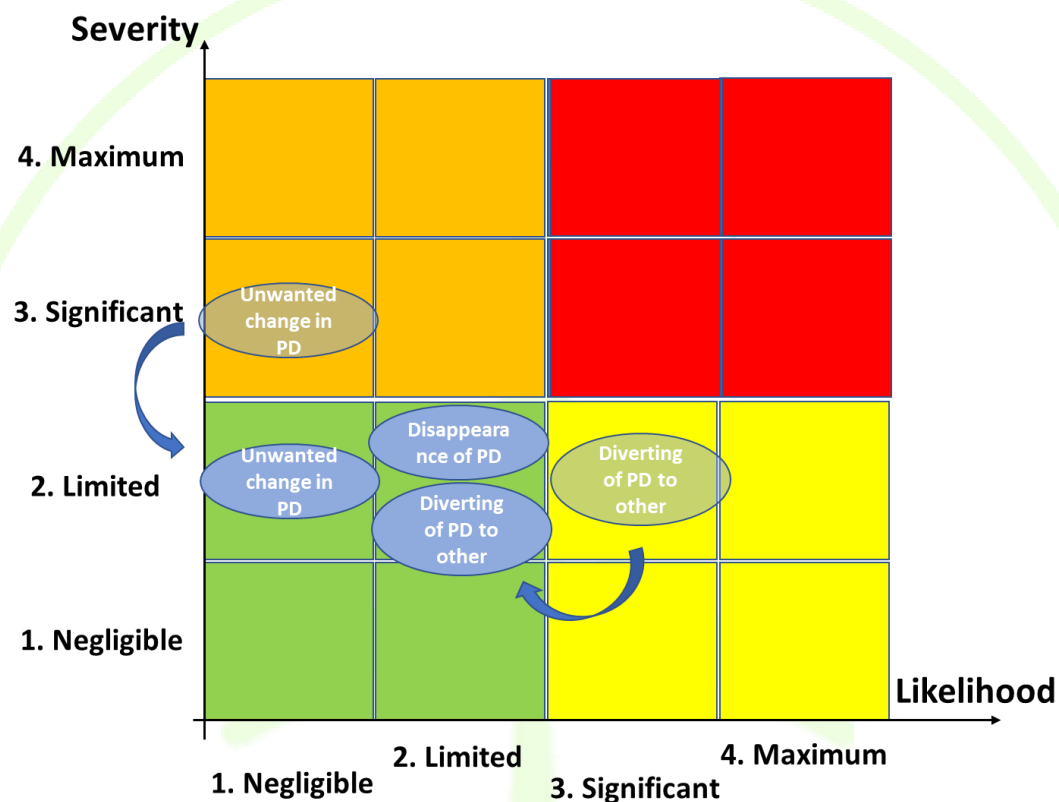


Figure 92 - Risk map for WiseEVP with implemented/planned controls

The results of the Risk treatment (Risk modification) based on applied controls for WG EVP, have brought the risk level within the “Limited” level or below.

#### 14.4.7.2.6 WG FastV2G

Table 63 – Risk treatment and residual risk for WG FastV2G

Feared events	Threat ID	Related Privacy targets	Controls planned or implemented	Risk level	Risk treatment (including implementation of privacy targets)	Residual risk
Change in processing	II	Legitimacy of processing personal data			Risk Retention	
Disappearance of personal data	ED	Compliance with data retention requirements			Risk Retention	
	Pobj	Compliance with data retention requirements			Risk Retention	
	HLPL	Privacy by design			Risk Retention	
Diverting of personal data to other users	DoS	Legitimacy of processing personal data	Reducing hardware vulnerabilities		Risk Modification	
	IISC	Legitimacy of processing personal data	Anonymizing personal data Encrypting personal data		Risk Modification	
Unwanted change in personal data	ADNI	Safeguarding quality of personal data	Active measure to preclude the use of particular data-items in the making of particular decisions		Risk Modification	
Illegitimate access to personal data	IACP	Privacy by default			Risk Retention	

- Reducing hardware vulnerabilities

Objective: to reduce the possibility to exploit hardware properties (servers, desktop computers, laptops, devices, communications relays, removable storage devices, etc.) to adversely affect personal data.

- Encrypting personal data

Objective: to make personal data unintelligible to anyone without access authorization.

- Anonymizing personal data

Objective: to remove identifying characteristics from personal data.

- Active measure to preclude the use of particular data-items in the making of particular decisions

Objective: to ensure that decisions are made based only on due data-items.

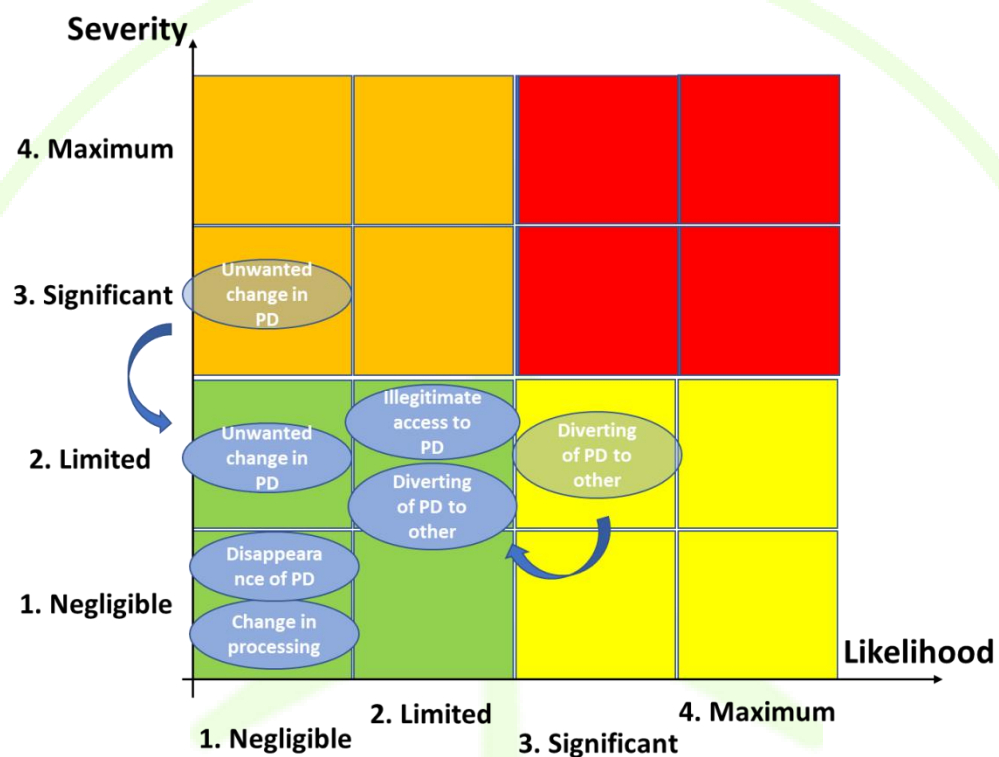


Figure 93 - Risk map for WG FastV2G with implemented/planned controls

The results of the Risk treatment (Risk modification) based on applied controls for WG FastV2G, have brought the risk level within the “Limited” level or below.



#### 14.4.7.2.7 WiseCORP

**Table 64 – Risk treatment and residual risk for WiseCORP**

Feared events	Threat ID	Related Privacy targets	Controls planned or implemented	Risk level	Risk treatment (including implementation of privacy targets)	Residual risk
Disappearance of personal data	ED	Legitimacy of processing personal data			Risk Retention	
	Pobj	Legitimacy of processing personal data	Make a privacy policy, code of conduct or certify the processing of the data to be more transparent.		Risk Modification	
Change in processing	ADNI	Safeguarding quality of personal data			Risk Retention	
Illegitimate access to personal data	IACP	Privacy by default			Risk Retention	

- Make a privacy policy, code of conduct or certify the processing of the data to be more transparent

Objective: to establish rights, responsibilities and boundaries in order to make data processing transparent to those involved.

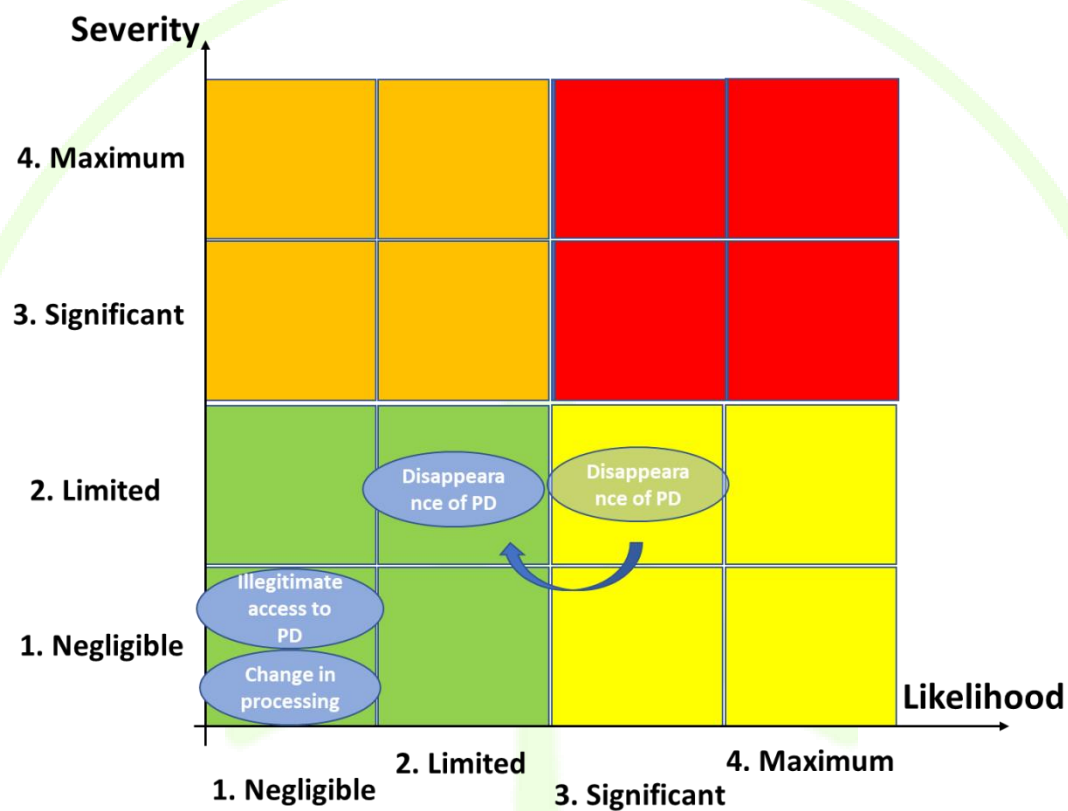


Figure 94 - Risk map for WiseCORP with implemented/planned controls

The results of the Risk treatment (Risk modification) based on applied controls for WiseCORP, have brought the risk level within the “Limited” level or below.

#### 14.4.7.2.8 WiseHOME

Table 65 – Risk treatment and residual risk for WiseHOME

Feared events	Threat ID	Related Privacy targets	Controls planned or implemented	Risk level	Risk treatment (including implementation of privacy targets)	Residual risk
Disappearance of personal data	ED	Compliance with data retention requirements			Risk Retention	
	Pobj	Compliance with data retention requirements	Make a privacy policy, code of conduct or certify the processing of the data to be more transparent		Risk Modification	
Diverting of personal data to other users	DoS	Legitimacy of processing personal data			Risk Retention	
	IISC	Legitimacy of processing personal data	Anonymizing personal data Encrypting personal data		Risk Modification	
Unavailability of legal processes: they do not or no longer exist or work	AUS	Compliance with notification requirements			Risk Retention	
	NL	Compliance with notification requirements			Risk Retention	
Change in processing	ADNI	Safeguarding quality of personal data			Risk Retention	

- Make a privacy policy, code of conduct or certify the processing of the data to be more transparent

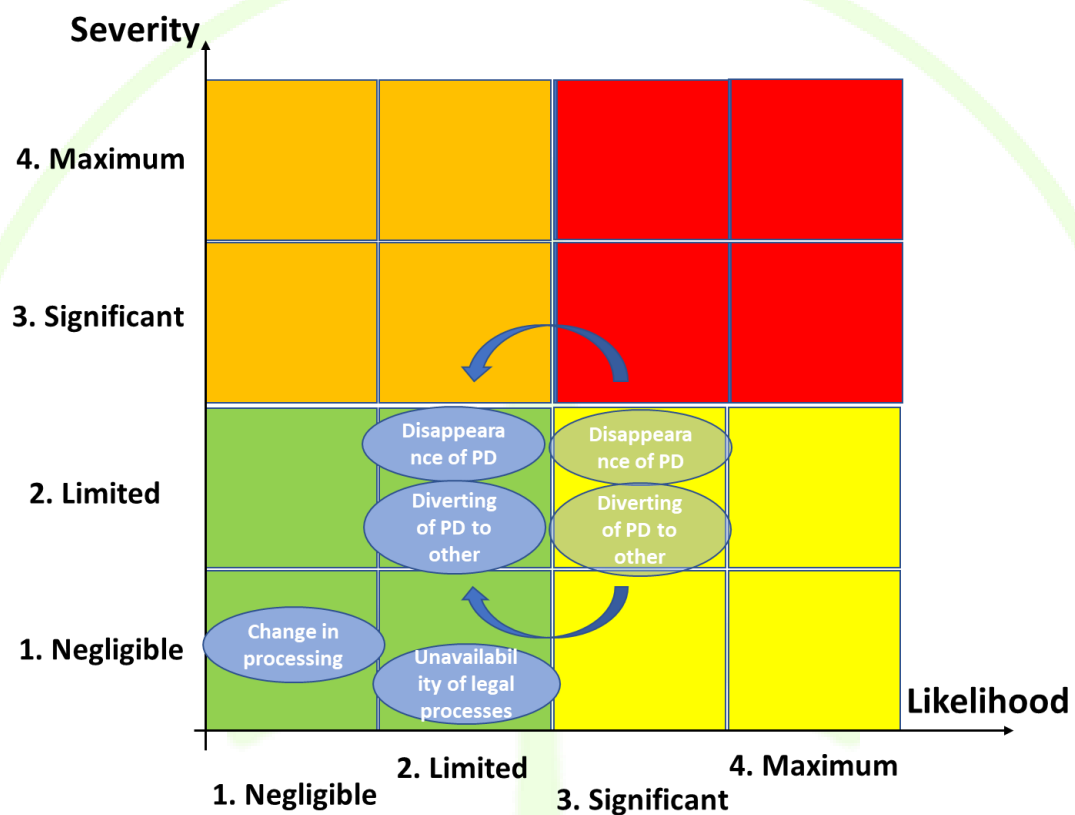
Objective: to establish rights, responsibilities and boundaries in order to make data processing transparent to those involved.

- Encrypting personal data

Objective: to make personal data unintelligible to anyone without access authorization.

- Anonymizing personal data

Objective: to remove identifying characteristics from personal data.



**Figure 95 - Risk map for WiseHOME with implemented/planned controls**

The results of the Risk treatment (Risk modification) based on applied controls for WiseHOME, have brought the risk level within the “Limited” level or below.

#### 14.4.7.2.9 WG RESCO

Table 66 – Risk treatment and residual risk for WG RESCO

Feared events	Threat ID	Related Privacy targets	Controls planned or implemented	Risk level	Risk treatment (including implementation of privacy targets)	Residual risk
Illegitimate access to personal data	UDC	Legitimacy of processing personal data			Risk Retention	
Disappearance of personal data	ED	Compliance with data retention requirements			Risk Retention	
	Pobj	Compliance with data retention requirements			Risk Retention	
Diverting of personal data to other users	DoS	Legitimacy of processing personal data	Reducing hardware vulnerabilities		Risk Modification	
	IISC	Legitimacy of processing personal data	Anonymizing personal data Encrypting personal data		Risk Modification	
Unavailability of legal processes	SA	Compliance with notification requirements			Risk Retention	

- Reducing hardware vulnerabilities

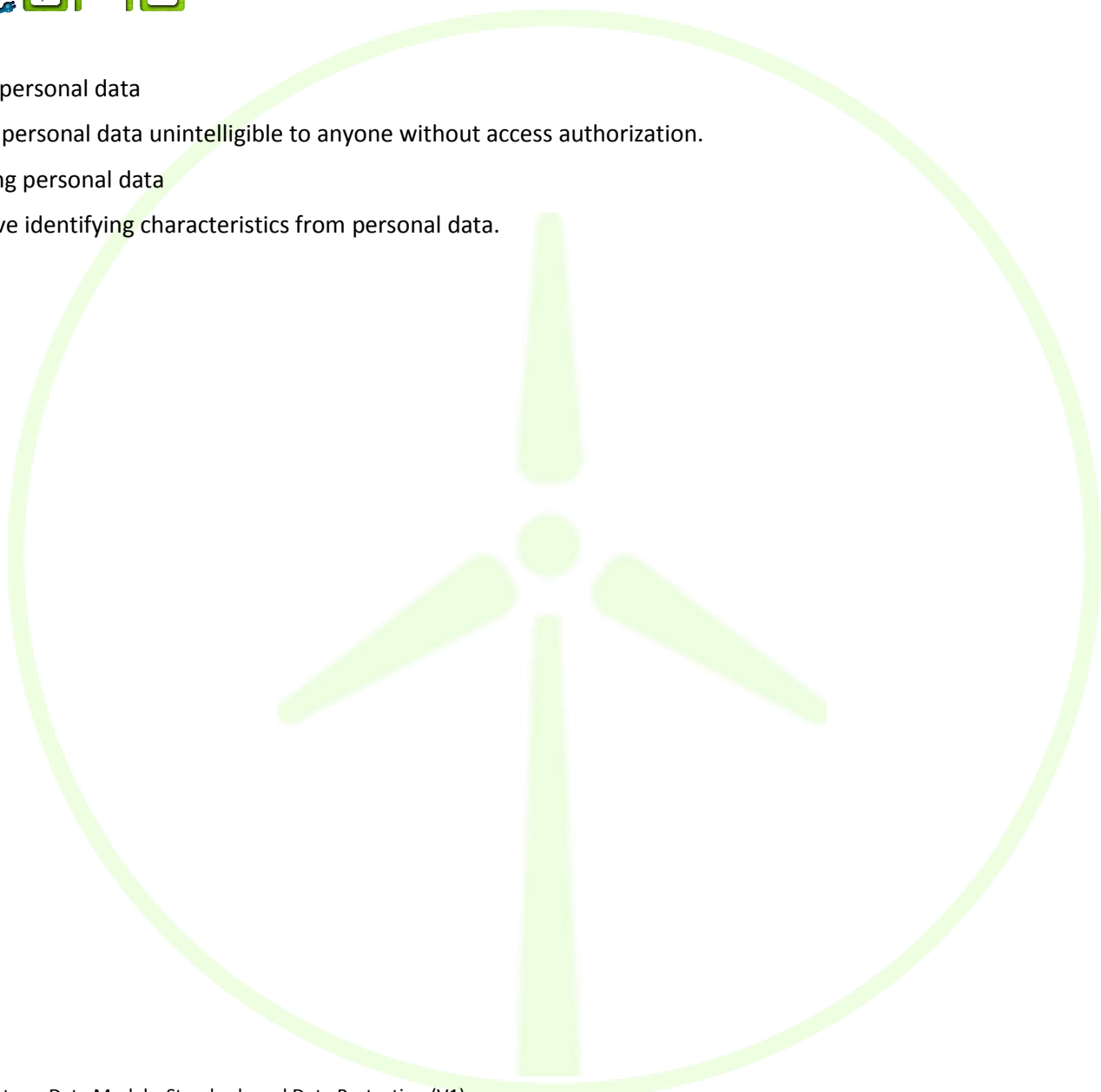
Objective: to reduce the possibility to exploit hardware properties (servers, desktop computers, laptops, devices, communications relays, removable storage devices, etc.) to adversely affect personal data.

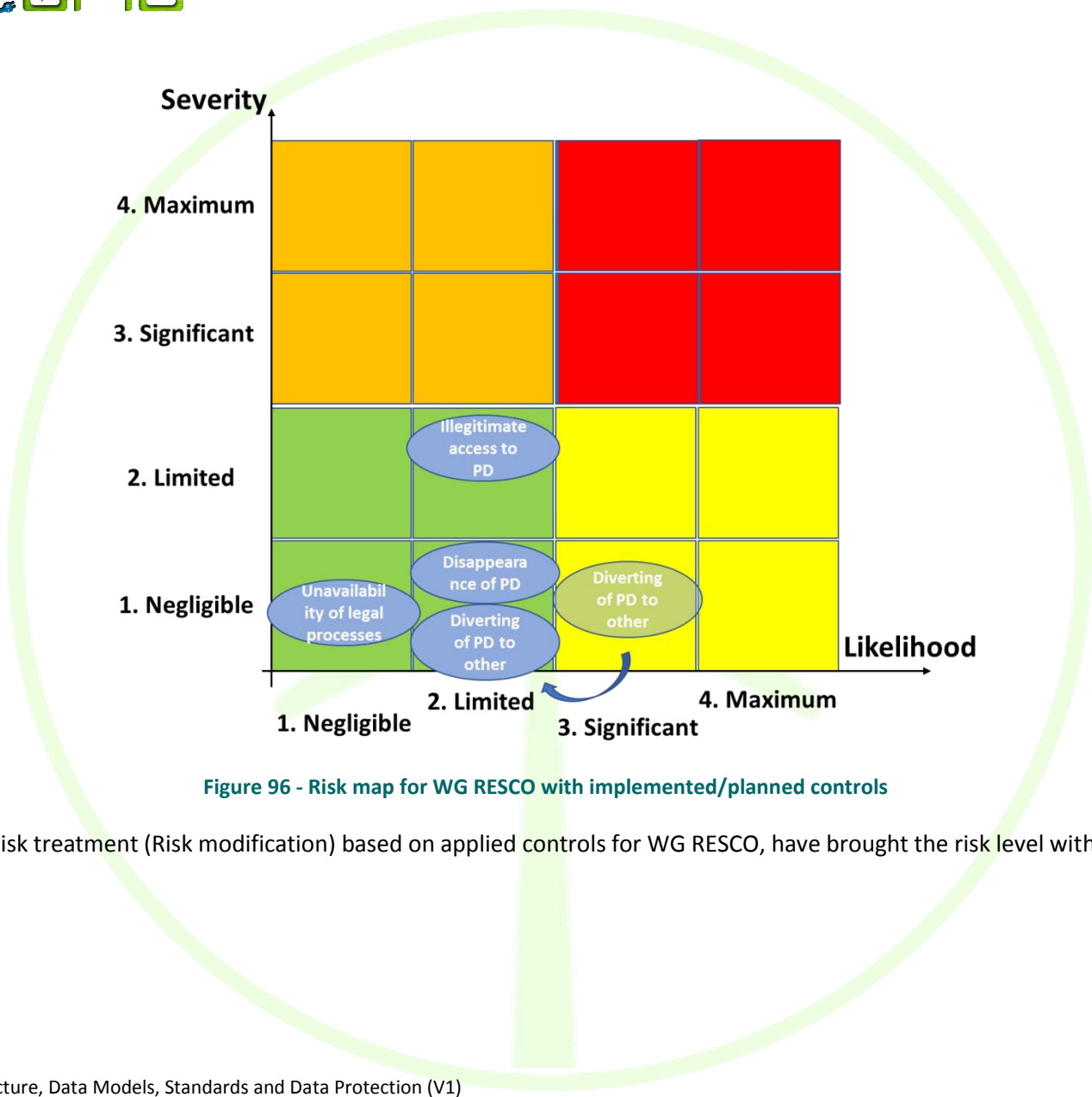
- Encrypting personal data

Objective: to make personal data unintelligible to anyone without access authorization.

- Anonymizing personal data

Objective: to remove identifying characteristics from personal data.





**Figure 96 - Risk map for WG RESCO with implemented/planned controls**

The results of the Risk treatment (Risk modification) based on applied controls for WG RESCO, have brought the risk level within the “Limited” level or below.



Within Risk Management process, the following considerations were in place:

- Appropriate justification for the selection of specific option(s) for treating the risk and proposed approach to ensure that the risk will be monitored to make sure acceptance is appropriate in light of the evolving external landscape (e.g. threats, vulnerabilities, legal requirements etc.).
- Consultation of the Data Protection Officer (DPO);
- Date: The decision for internal approval shall be subject of a further WiseGRID management board;
- Date of next review is scheduled within D3.1 (V2) deliverable, if no important changes (influencing the risk level) would occur meantime;

#### 14.4.7.3 RESIDUAL RISKS AND RISK ACCEPTANCE

According to ISO 27005, the residual risk is “the risk remaining after the risk treatment”. In this context, the developer identified the residual risks that remained after implementing controls as being at an acceptable level (Limited or Negligible).

Finally, based on this analysis, the proposal to accept those residual risks is considered. The proposal is based on results that there are no cases of risks that fall outside of the acceptable levels and that would be unacceptable.

It is pointed out that the right for the protection of personal data is a fundamental right, and the compliance with it is a high-level legal requirement. Independently of the outcome of this risk assessment, ***it is underlined that data protection and privacy targets (as listed in Table 46 – Description of privacy targets under section 14.4.6.1) need to be reached.***

#### 14.4.7.4 RESOLUTION

The resolution of the DPIA is based on the results of the risk management process that has been performed, as well as on the residual risks and the decision to accept risks or not.

The smart grid applications are considered by the developers (system owner) as satisfactory as the DPIA process has been completed with relevant risks identified and appropriately treated to ensure no unacceptable residual risks for the individuals remain, and in order to meet the requirements of compliance, with appropriate internal reviews and approvals.

The following resolution is considered at the end of current DPIA process for WiseGRID applications, still under design:

- ***The DPIA is positive:*** risks have been assessed and controls addressing those risks properly defined and tuned. Any residuals risks have been flagged and no further controls have been identified and / or certain risks have been accepted. The system implementation proceeds.
- ***This DPIA report shall be rechecked*** within deliverable D3.1 (V2) and further on when the system will be in production or whenever there would be changes in risk evaluation. Dates to be further defined.

The final resolution, that the DPIA is positive, is scheduled to be approved within WiseGRID management board (based on the results of the assessment performed, including and reflecting the societal stakes related to the development of the smart grid).

The DPIA presented in current report is just a first version and subject to internal approval. Moreover, in the next phase will be issued an attempted schedule with next steps to be carried out for the enhancement of the current DPIA (e.g. contact with national data privacy authorities, further analysis as the tools development progresses, integration of further feedback received.)

The updated version of the DPIA will be presented in the second version of D3.1 (V2) to be submitted in M18.

It is important to stress that shall be communicated to national data privacy authorities about the actions carried out within WiseGRID and also about the results of DPIA Report and further possible updates.

***It is also mentioned that DPIA will be under a continuous improvement process. It therefore requires monitoring changes over time (context, risk, measures...) and updates whenever a significant change occurs.***

#### **14.4.8 DOCUMENTATION AND DRAFTING OF THE DPIA REPORT, REVIEWING AND MAINTENANCE**

##### **14.4.8.1 DOCUMENTATION AND DRAFTING OF THE DPIA REPORT**

The performance of the DPIA as described above, was appropriately documented and its results presented in the final DPIA report. The DPIA report is structured around the phases of work described in this document, presenting the results of each phase to the reader and annexing all supporting documents or material used in the assessment.

The objective of the documentation is two-fold:

- (a) to facilitate the implementation of the process and
- (b) to produce a final report that could be submitted to the DPA if requested.

The signed DPIA Report is available to be given to the assigned CE's Data Protection Officer. This report is provided without prejudice to the obligations set forth in Directive 95/46/EC for data controllers, most notably the independent obligation to notify the competent authority as described in section IX of Directive 95/46/EC.

The DPIA report shall be distributed to stakeholders when appropriate.

##### **14.4.8.2 REVIEWING AND MAINTENANCE**

The purpose of this phase will be the undertaking arising from the conducted DPIA to be carried out in the implemented project.

The following tasks are considered:

- Reviewing the implementation of the mitigation and avoidance controls that were identified in the DPIA;
- Preparing a review report within each DPIA review;
- Presenting the privacy review report to the senior management and DPO where available;
- Rendering the privacy review report publicly available;
- Assessing whether there is a need for revising the DPIA after a certain amount of time or after a new stage within the project or program has been completed.

Each review shall be integrated within the organization's standard.

## 14.5 COLLECTION AND REVIEW OF NATIONAL REGULATIONS AND LEGISLATION (SURVEY)

### 14.5.1 SPECIFIC PRIVACY REQUIREMENTS IN BELGIUM

Belgium's regulatory framework for data protection and privacy is set out in the "Law on the protection of privacy in relation to the processing of personal data (*Wet tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens/Loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel*)" of 8 December 1992 and subsequently implemented by the Royal Decree of 13 February 2001 (*Koninklijk besluit ter uitvoering van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens/Arrêté royal portant exécution de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel*). The law has undergone a number of amendments and has commendably remained abreast with technological developments. The progressive approach taken by Belgian authorities have earned the country the accolade of data protection hub among some pundits [55]. The law provides for all the fundamental protections envisaged by the EU data protection directive, such as the as the registration of data controllers; prior informed consent for the collection and processing of personal data; as well as the data subject's right to access, request rectification and object to the processing of personal data. The Privacy Commission (*"Commissie voor de bescherming van de persoonlijke levenssfeer/Commission de la protection de la vie privée"*) is the national data protection authority and is responsible for ensuring compliance with the relevant laws.

In accordance with general data protection principles, the Belgian law imposes primary data protection responsibility on data controllers, which in the electricity context is the DSO. Consequently, controllers are required to notify the Privacy Commission prior to adopting any fully or partly automated systems for the processing of personal data. Article 1(3) of the law defines processing very broadly to include activities like the collection, recording, organization, storage, adaption, alteration, retrieval, consultation, use, disclosure, alignment, and deletion of personal data. It appears that by emphasizing "automation" in the law, the legislators intended to remove manual data processing activities from the remit of the law [56]. Therefore the duty to notify the Privacy Commission only arises when the controller employs computer systems in its processing activities. Further, Article 55 of Royal Decree of 13 February 2001, exempts data controllers from the notification requirement when processing is in furtherance of the administration of its clients and suppliers. In this vein, DSOs and energy retailers appear to be exempted from the notification requirement as far as billing information is concerned.

In addition to the data controller's notification responsibility, it must, in a bid to ensure fair and lawful processing of data ensure that it implements appropriate technical and organizational security measures to prevent accidental or unauthorized, access or loss of personal data. The law however does not specify any requirements for these measures. Data controllers are therefore at liberty to adopt such measures as are appropriate within the context of their processing activities. Further, there are no specific data retention periods prescribed by the law. However, pursuant to the data minimization principle, controllers must limit retention of personal data to periods for which processing of the data is necessary. The data controller has no obligation to notify the Privacy Commission of data breaches. However, a new Belgian Data Protection Act, which is currently being considered by the Belgian Chamber of Representatives, if passed into law, will make notification for data breaches mandatory.

Regarding the data subject's consent, Belgian law provides that the data subject's prior consent must be specific and freely given after they have been informed of the specific purpose of the processing activity. The information to be provided to the data subject must include information on the identity of the controller, the purposes of the processing, the existence of the right to object to the processing of personal data for direct marketing purposes, as well as the right to access and rectification, the recipients or categories of recipients of the personal data, and whether or not it is obligatory to respond to the data controller's request to submit personal data and any possible consequences of not responding.

The processing of personal data in breach of the applicable law constitutes a criminal offence under Articles 37 to 39 of the data protection law. The offences attract a penalty of imprisonment and/or fines of up to EUR 1,200,000. A person who suffers as a result of non-compliance with the laws could also bring a civil action for damages. Currently, the Privacy Commission seldom brings criminal action for non-compliance. It however investigates complaints of infringements and adopts appropriate measures [56].

The Belgian electricity market operates a uniform nationwide communication platform, the Belgian Utility Market Information Exchange (UMIX), through which DSOs use information such as working orders and forecasts supplied by the TSO to ensure the smooth operation of the network. The portal also allows suppliers to access the meter readings taken by DSOs for billing purposes [57]. This process calls into operation, the rules on third party processing. In this regard, article 16(1) of the data protection law requires that a contract exist between the controller and the third-party who processes the data. The contract must *inter alia* make provision for the necessary technical and organizational security measures, and establish the third party's responsibility towards the controller. The controller must however have informed the customer of the fact of sharing the data, and obtained the customer's consent. The Smart Grid Task Force has however noted that there is insufficient clarity on the control and certification of third-party processors, and called for greater scrutiny over third party processing [58].

The UMIK is undergoing a complete overhaul to cater for wide-scale roll-out of smart meters and the increase of DERs in the Belgian electricity system [59]. In this new system, the streams of personal data that would be processed would increase exponentially and therefore regulatory reform would be imperative to ensure that personal privacy is not compromised. It is also expected that the institution of DPIA will significantly reduce data and privacy risks [58].

#### 14.5.2 SPECIFIC PRIVACY REQUIREMENTS IN GREECE

There is no specific national legislation, exclusively designed for data access and security for smart grids in Greece. However, data protection is subsumable under the country's general data protection laws [60]. This law follows EU Directive 95/46/EC of the European Parliament and Council and protects individuals against the unlawful processing of personal data. There have also been various modifications of general data protection law to deal with situations arising from the collection and processing of data through ICT systems [61].

Greek data protection laws provide for the basic tenets of data protection, specifically, the registration of data controllers with the Hellenic Data Protection Authority (HDPA); prior informed written consent for the collection and processing of personal data; and security obligations on data controllers to ensure data security; the obligation to inform the data subject of breaches which compromise their personal data; as well as the data subject's right to access, request rectification and object to the processing of personal data. These general laws apply by extension to the electricity sector and ipso facto to all the players in a smart grid scenario.

The data protection obligation under the law are primarily imposed on the data controller who is required *inter alia* to register and notify the HDPA in writing of its intention to establish a system for processing personal data. The data controller is also required to adopt appropriate technical and organizational security measures to protect personal data from unauthorized access and processing. There is no obligation on the data controller to notify the HDPA of data breaches. However, the HDPA encourages voluntary notification. The penalty for non-compliance with these obligations could result in administrative, criminal or civil sanctions including: warnings, fines of up to EUR 150,000, revocation of licenses.

Within the context of smart grids, it is worth considering the definition of "personal data" under the Greek Data Protection law. The law defines personal data as information relating to the data subject, excluding data of a statistical nature from which the data subject can no longer be identified [62]. The Data Protection Authority has not issued guidelines for the definition of personal data however it appears from decisions of

the DPA that information which could, in combination with other information on a data subject lead to the identification of the data subject would be considered personal data. In this vein, the possibility that information collected through smart meters could be classified as personal data is high and might operate as an inhibition to the rapid deployment of smart grids.

It is also worth noting that Greek data protection law distinguishes between “personal data” and “sensitive data”. While the former may give rise to obligations in the smart grids, the latter, which is defined as information relating to the racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, social welfare and sexual life, criminal charges or convictions, are unlikely to give rise to data protection obligation in a smart grid context as the data likely to be collected and processed by these systems are unlikely to lead to access to, or processing of such categories.

Data retention remains an issue in Greece. Despite the invalidation of the Data Retention Directive by the European Court of Justice in Digital Rights Ireland [63], Greece has not amended Law 3918/2011, which transposed the Data Retention Directive. Consequently, the power to determine data retention periods is vested in HDPA. Given that the HDPA has not issued any guidelines on the retention of personal data collected through smart meters, it can be assumed that data collectors within a smart grid network have no specific obligation regarding the retention of such data. This notwithstanding, the general caveat of retaining such data beyond periods for which its processing is necessary would be deemed a violation of the rights of the data subject.

As far as data anonymization is concerned, Greek law does not define what categories of personal data must be anonymized. Indeed, the law does not define anonymization. However, the law states that “personal data in order to be lawfully processed must be...(d) kept in a form which permits identification of data subjects for no longer than the period required, according to the Authority, for the purposes for which data was collected or processed.”, the concept is adequately provided for. However, questions regarding what would be deemed sufficient anonymization remains uncertain. The general practice is to render data in coded formats, however there is insufficient guidance in Greece concerning the levels of codification which are regarded as acceptable [64]

There is no specific national legislation, exclusively designed for data access and security for smart grids in Greece. However, data protection is subsumable under the country’s general data protection laws. This law follows EU Directive 95/46/EC of the European Parliament and Council and protects individuals against the unlawful processing of personal data. There have also been various modifications of general data protection law to deal with situations arising from the collection and processing of data through ICT systems.

#### 14.5.3 SPECIFIC PRIVACY REQUIREMENTS IN ITALY

Italy’s data protection framework is set out in the Italian Personal Data Protection Code (Legislative Decree No. 196/2003). This comprehensive piece of legislation is of general application and therefore applies by extension to smart grids. It defines personal data very broadly, to include not just data relating to a natural person by which such person may be identified, but also data by which a person may be identified indirectly by reference to some other kind of information [60]. It provides for all the basic requirements for a robust data protection regime, as required by the 1995 Data Protection Directive, such as the registration of data controllers; prior informed consent for the collection and processing of personal data; and security obligations on data controllers to ensure data security; the obligation to inform the data subject of breaches which compromise their personal data; as well as the data subject’s right to access, request rectification and object to the processing of personal data.

The Italian Data Protection Authority (IDPA) (“Garante per la protezione dei dati personali”) is the national data protection authority and is responsible for ensuring compliance with the Data Protection Code. The Code seeks to protect natural persons from unlawful processing of information relating to them, that is, information by which they can be identified. Either directly or by reference to any other information.



Like other EU Member States, the Italian Code imposes the duty of ensuring lawful data processing on the data controller. The controller is therefore required to notify the IDPA when its processing activity involves (subject to stated exemptions) the processing of genetic and biometric data; geo-localization; and behavioral advertising. Notification must be made prior to the commencement of processing activities [65]. The data controller is also required to possess information systems and software which minimize the use of personal data, and when such data is to be processed, it must be done for the purpose and in the manner for which the written consent of the data subject has been obtained. There are no specific data retention periods. However, data must not be stored longer than it is necessary for processing.

With respect to maintaining security for data processing systems, the Italian Code is unique as it spells out minimum security measures that must be adopted by the data controller depending on whether the data processing is done electronically or manually. In the case of electronic processing, these security measures include: computerized authentication credentials management procedures for persons who have access to the processing system; regular update of specifications of the scope of processing; and procedures for safekeeping backup copies and restoring data and system availability. For manual processing, the Code requires, amongst others, procedures to keep certain records in restricted-access filing systems and mechanisms for regulating access; and the appointment of specific persons to be in charge of processing.

Notification to the IDPA for data breaches is only mandatory for providers of electronic communication services and controllers who process biometric data. However, where the data breach poses a threat to the data subject's privacy, the data subject must be notified of the breach. The law however provides an exception to the requirement of notification if the data that has been compromised had been anonymized or encrypted.

Enforcement of the Code is achieved through a system of administrative fines of up to EUR 2,448,000. In instances where individuals are found culpable in breaches of the Code, they may face criminal sanctions of up to three years imprisonment.

Within the Italian context, it can be said that primary data protection responsibility would fall on DSO's as they are responsible for metering and therefore the collection of personal data. Collection and processing is limited to load profiles of MV and LV with capacity exceeding 55kW. The supply contracts between retailers and the customers serves, amongst others to obtain consent for the collection and processing of personal data. However, the electricity data management model adopted in Italy is centralized; the data from smart meters is sent to the Integrated Information System (IIS), a central database operated by Acquirente Unico Spa [58]. DSOs then access customers' data from the IIS for the purpose of billing and the TSO also access the metering information available on the IIS purpose of undertaking its balancing responsibilities [58]. However given that consent is granted for the processing of data by the DSOs, it may be argued that the sharing of data with the TSO and perhaps Acquirente Unico Spa., to the extent that it cannot be described as a data processor acting on behalf of the DSO, is a violation of the customer's privacy rights. However, given the definition of personal data in the Italian Data Protection Code, it appears that the aggregated meter information shared with the TSO is not personal data and therefore does not fall within the remit of the law.

#### 14.5.4 SPECIFIC PRIVACY REQUIREMENTS IN SPAIN

The Data Protection Law 15/1999 of 13 December protects individuals with regard to the processing and the free movement of data. The Royal Decree 1720/2007 of 21 December develops the Data Protection Law 15/1999. Spain's data protection regime is one of the most severe in the whole of the EU. This is so as penalty fines are among the heftiest (up to EUR 600.000 per infringement) [66]. Furthermore, the national data protection authority, the Spanish Data Protection Agency, is well known for its strict enforcement of data protection rules [67].

The Data Protection Law 15/1999 requires data controllers to draft an internal security policy clarifying the technical and organizational measures to be implemented by its staff. The nature of these measures will be

based on the security level (low, medium and high). In turn, the security level is ascertained pursuant to the sensitivity of the data being processed or the nature of the entity in question. By data controller, the Data Protection Law 15/1999 understands any individual or legal person who controls and is responsible for the storage and use of personal data on a computer or in structured manual files. The data processor is the entity that processes the data on behalf of the data controller as a result of their relationship. Were the processing of personal data to be outsourced, so that the processing is exclusively carried out by the data processor, the data controller may be entitled to delegate the obligation to outline an internal security policy to the data processor. The Data Protection Law 15/1999 charts the measures that must be implemented under each security level [68].

Data controllers must register with the Spanish Data Protection Agency (“Agencia Española de Protección de Datos”). This registration is free of charge. The applicant will have to fill in a form available on the website of the Spanish Data Protection Agency before engaging in the processing of personal data. The notification of data files entails no costs either. The Data Protection General Registry will approve notifications provided that they meet the necessary requirements. Additionally, a data protection officer must be appointed if the security level is medium or high according to the Data Protection Law 15/1999 [69]. The Spanish Data Protection Agency commends itself for the compliance with the prescriptions of the Data Protection Law 15/1999 in terms of registration. Indeed, the Data Protection Agency has observed an upswing in the number of registrations, especially from medium-sized companies as well as independent professionals [70]. The data controller must also adopt the technical and organisational measures necessary to ensure the security of the personal data. There are no specific data retention periods mandated by the law. Nevertheless, personal data shall be erased when they have ceased to be necessary or relevant for the purpose for which they were obtained or recorded. There is no requirement to notify data security breaches under The Data Protection Law 15/1999 of 13 December. Nevertheless, acknowledging guilt for a specific breach will be taken into consideration by the Spanish Data Protection Agency when imposing penalties. Notifying data subjects can also reduce civil liability.

The Royal Decree 216/2014 of 28 March is the relevant legal source that frames the obligations in terms of consumption information to be submitted by DSOs to consumers. For end users that already have a smart meter installed, the Royal Decree 216/2014 requires DSOs to publish hourly consumption data. Moreover, DSOs provide a website that permits their customers to consult and download their hourly consumption data (after billing). Interestingly, DSOs also offer the possibility for consumers to download their consumption profile made available to the energy supplier for billing purposes in comma separated values (CSV) and Excel flat-files. Data stemming from smart meters are stored in the DSOs’ metering managing system. DSOs submit data to energy suppliers through secure File Transfer Protocol (FTP). Energy suppliers can only access the data pertaining to their customers. Energy suppliers may solely access the consumption profiles of other customers than their own if they have been granted consent [71]. In conclusion, smart metering data is the property of the DSOs but distributors are required to submit these data to end users for consultation and to energy suppliers for billing purposes [72].

Another legal basis worth noting is the Royal Decree 1074/2015 of 27 November. The Royal Decree 1074/2015 amends some aspects related to the data to be stored in the Supply Points Information System or “Sistema de Información de Puntos de Suministro” (SIPS) which is regulated by Article 7 of the Royal Decree 1435/2002 setting the basic conditions for acquisition of energy contracts and access to low voltage networks. The SIPS is a database managed by the DSOs. Only the NRA, the CNMC, and energy suppliers are entitled to access this database. The SIPS includes information, which is complete and regularly updated, related to the supply points connected to the networks and transport networks of the areas that each particular DSO is responsible for. The purpose of the SIPS is to trigger greater competence in the reduced market of electricity supply. The SIPS does so by facilitating the necessary consumption data to prompt the emergence of new energy suppliers whilst safeguarding consumer privacy [73]. The amendment introduced by the Royal Decree 1074/2015 excludes from the SIPS data corresponding to consumer hourly load curves. This is so as consumption data, collected by DSOs through smart meters, are treated as personal data which

calls for the necessary protection. In that vein, energy suppliers are precluded from having access to any information, other than that of their own customers, which can lead to the direct identification of the supply point incumbent (such as supply point location, household address, forename and surname, for instance) [73].





## 15 STANDARDS AND INTEROPERABLE DATA MODELS

### 15.1 GENERAL CONSIDERATIONS

This section summarizes the main outputs of T3.3 Standards and interoperable data models. T3.3 includes the following sub-tasks:

1. Identification of the main interfaces between components and actors to be developed in the scope of WiseGRID project.
2. For each interface, assess the available standards and data models according to CEN-CENELEC.
3. For each interface, assess the available new data models based on ontologies.
4. Gather the applicability of the standards and data models identified to the WiseGRID project (collaboration of WPs and task leaders).
5. For each interface, assess the most appropriate standards and best suitable data models.

### 15.2 WISEGRID PRODUCTS AND INTERFACES

The main objective of this section is the identification of the main interfaces between WiseGRID products and external agents and resources as a preliminary stage of the standards and data model assessment. To reach this objective a simplified WiseGRID architecture was included first. Then the external actors of each product were identified and described. The next step was mapping all the WiseGRID products with the IEC Smart Grid Standards Map to provide a clear definition of each of them. Finally the main interfaces of the WiseGRID were identified and represented in diagrams showing the differences between the communications among WiseGRID products, the communications between WiseGRID products and external actors and the communication between these products and the external resources.

#### 15.2.1 WISEGRID SIMPLIFIED ARCHITECTURE

The foreseen communications architecture among the different products of this Project is defined in a summarized way in the diagram down below.

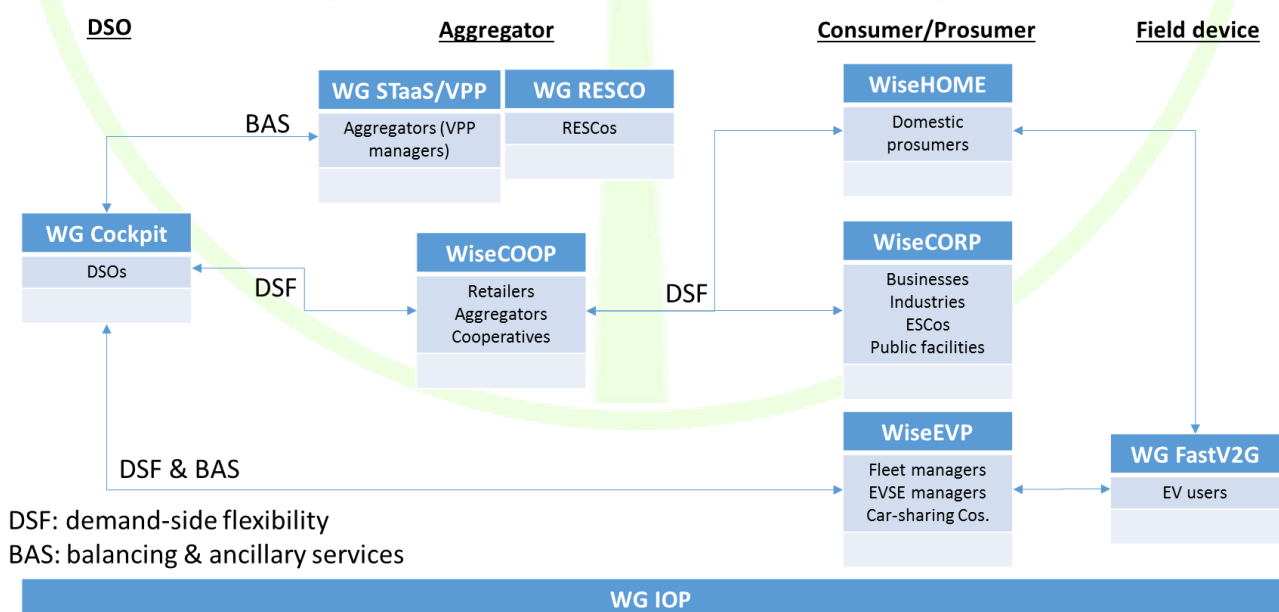


Figure 97 – WiseGRID simplified architecture schema

### 15.2.2 WISEGRID EXTERNAL ACTORS DESCRIPTION

The external actors who are involved in WiseGRID are defined as follows.

- **Aggregator.** This is an organization that accumulates flexibility from Prosumers and sells it to the Suppliers, the DSO or the TSO.
- **AMI (Advanced Metering Infrastructure).** Consists in a set of systems that monitor, collect and analyze electricity consumption/production and have two-way communication capabilities.
- **Balance Responsible Party.** This actor can be described like a party that has a contract providing financial security and identifying balance<sup>7</sup> responsibility with the Market Operator entitling the party to operate in the market.
- **Battery Operator.** This organization is an entity responsible for operating a set of Storage Units connected to the electricity grid.
- **Building Management System.** This is a system actor that consists in an automated system which monitors and controls the equipment of a building (ventilation, HVAC, lighting, electricity infrastructure, control system, etc.).
- **CHP (Combined Heat and Power).** This device is a system that generates electricity and useful thermal energy from a single source of energy at the same time.
- **Consumer.** A consumer is an entity connected to the grid that consumes energy, i.e. a Prosumer without any production capabilities.
- **Distributed Energy Resource.** This can be defined like any type of generation units, storage units and load flexibility resources connected to the distribution network.
- **DMS (Distribution Management System).** Is a system that monitors, controls and analyses in real-time or near real-time the electricity distribution system.
- **DSO (Distribution System Operator).** This actor is part of the organization and is the responsible entity for: the distribution network planning and development; the safe and secure operation and management of distribution system; for data management associated with the use of the distribution system; for procurement of flexibility services.
- **Electronic Meter.** This actor consists in a physical device able to count consumption or production of different energy resources, containing one or more data registers, electronic means of nonvolatile recording of consumption, production data.
- **Energy Management System.** This is a system that monitor, controls and optimizes the operation of the energy system under supervision.
- **ERP (Enterprise Resource Planning).** This is a system that offers integrated management and automation of business processes. Is also used to refer to the Customer Relationship Management (CRM) system.
- **ESCO (Energy Service Company).** This organization is in charge of offering auxiliary energy-related services to Prosumers.

---

<sup>7</sup>The meaning of the Word “balance” in this context signifies that the quantity contracted to provide or to consume must be equal to the quantity really provided or consumed.

- **EV** (Electric Vehicle). Which is a vehicle that uses stored electricity as a source of energy.
- **EV Fleet Manager**. This actor is an organization that operates and controls and EV fleet.
- **EVSE** (Electric Vehicle Supply Equipment). This set of devices consists in the infrastructure external to the EV that provides connection to a power source for charging the EV.
- **EVSE Operator**. This entity is responsible for managing and operating the EV charging infrastructure.
- **Facility Manager**. This organization is an entity responsible for the management of one or more buildings or other facilities in general.
- **Forecast Provider**. This actor is an organization that provides, upon demand, forecast regarding certain variables (e.g. electricity demand, RES production, weather conditions, etc.).
- **Gas Distribution Company**. This is the organization responsible for the distribution of natural gas to final customers.
- **GIS**. This is the acronym of "Geographical Information System".
- **Load Controller**. This is a device that communicates with on-site electricity loads and has capabilities of sending control signals for increasing/decreasing the electricity demand.
- **Market Operator**. This entity has the function to match the unique power exchange of trades for the actual delivery of energy that receives the bids from the Balance Responsible Parties that have a contract to bid. Determines the market energy price taking into account the technical constraints form the Transmission System Operator.
- **P2G Unit** (Power to Gas Unit). This is a device that converts electrical power to a gas fuel.
- **PDC** (Phasor Data Concentrator). This device receives and time-synchronizes phasor data from multiple phasor measurement units (PMUs) to produce a real-time, time-aligned output data stream.
- **Producer**. This is an entity connected to the grid that injects electricity to the grid.
- **Prosumer**. This entity consumes and produces energy. There is no distinction between residential and users, small and medium-sized enterprises or industrial users.
- **Public Authority**. Governmental organization that administrates the public life on the level of a municipality.
- **RES Unit** (Renewable Energy Source Unit). This device is a type of Producer that transforms energy from renewable energy sources (e.g. sun, wind, etc.) to electricity and injects it to the grid.
- **RESCO**. This is a type of ESCO that delivers energy to Consumers from renewable energy sources (Not to be confused with WG RESCO).
- **SCADA**. This word is the acronym of "*Supervisory Control And Data Acquisition*".

### 15.2.3 WISEGRID PRODUCTS DESCRIPTION

The aim of this deliverable document is to define a suitable set of standards for each component that is going to be developed within this project. To achieve this purpose, it has been made use of a map of standards related to all different fields of the smart grids. This map is available on IEC website [74] and has the appearance that is shown in the picture down below.

The next subsections define each component to be developed during WiseGRID project, together with an image of the standards map, which indicates the suitable smart grids fields for each component.

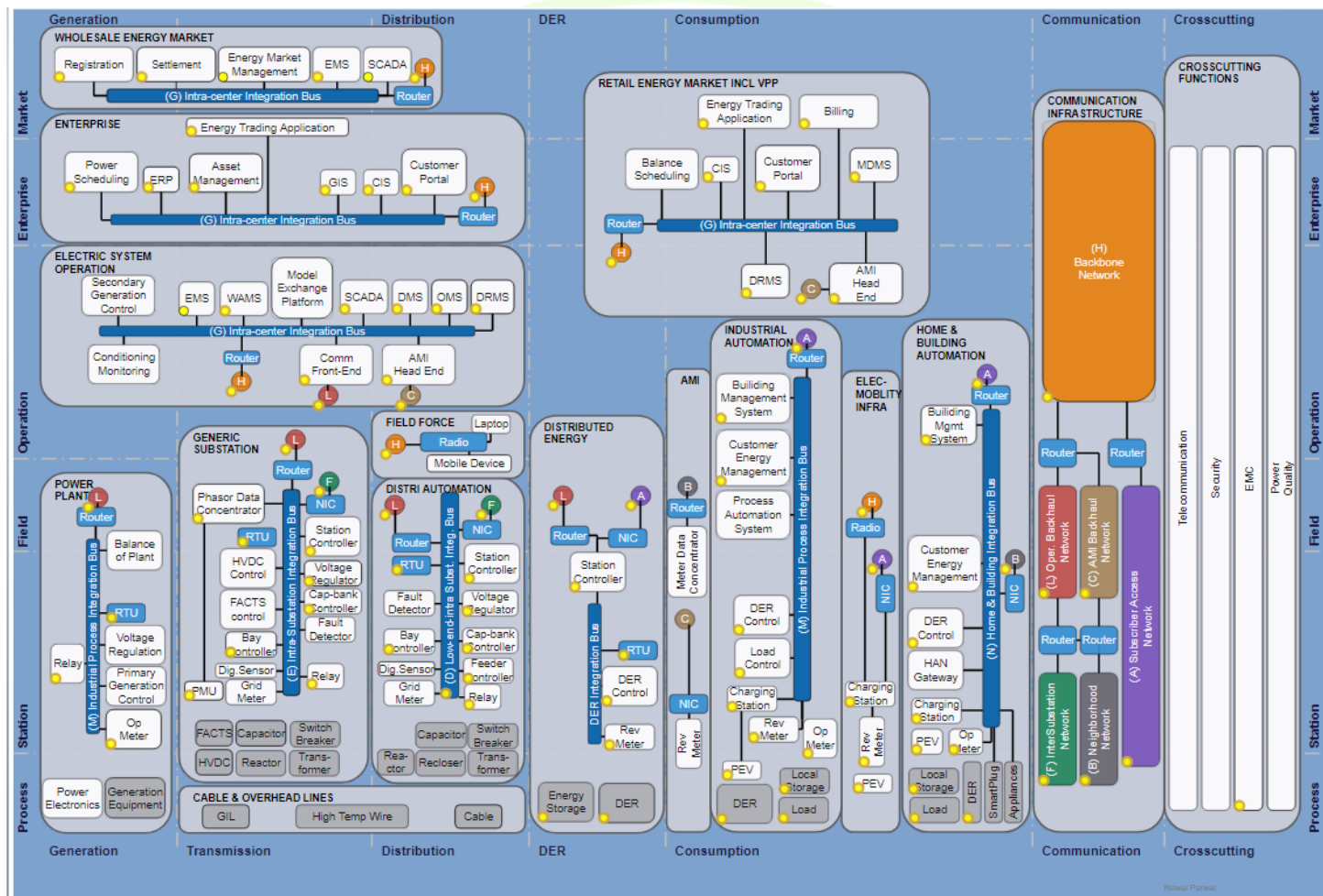


Figure 98 - Smart Grids Standards Map [75].

### 15.2.3.1 WISEGRID IOP

The WiseGRID IOP or Inter Operable Platform will be an ICT platform based on interoperable interfaces which will hold all the communication among the WiseGRID tools. Hence the main objective of the platform is the management of the massive data coming from the distributed energy infrastructure deployed. As the WiseGRID IOP will be giving support to the communications of all the other systems, this tools IOP has been mapped to the IEC standards maps covering all the zones (process, field, station, operation, enterprise and market). Regarding the domains, the WiseGRID IOP is focused in communication and it includes all the components included in the “communication infrastructure” functional cluster by the IEC.

The most suitable smart grid fields for this component are labelled in the image down below.

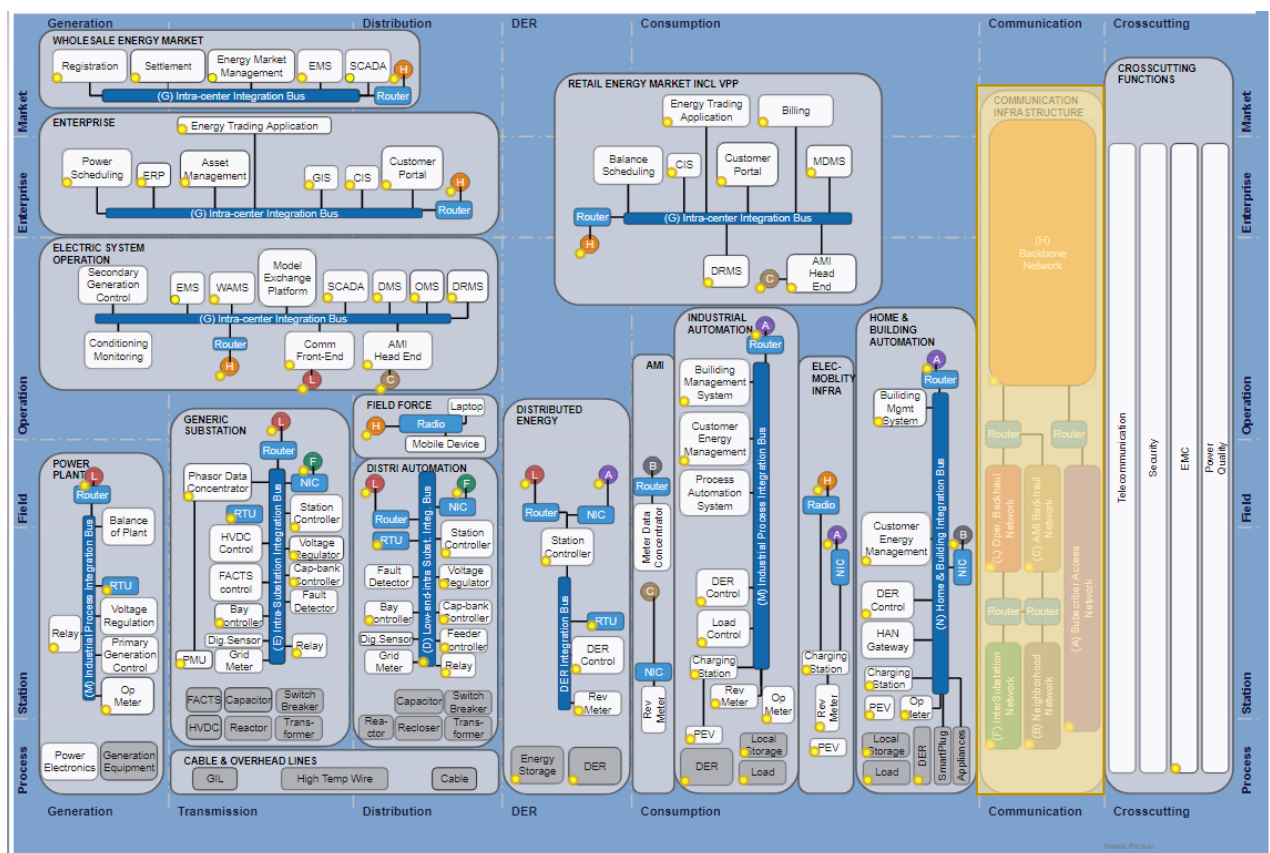


Figure 99 - Standards map for WG IOP.

### 15.2.3.2 WISEGRID COCKPIT

The WiseGRID Cockpit is the solution for DSOs proposed by the project in order to control, manage and monitor a medium voltage (MV) and low voltage (LV) distribution network. This tool has been mapped to the IEC standards map covering all the components included in the “enterprise” and “electric system operation” functional clusters. This means that the WiseGRID Cockpit will cover all the traditional functionalities included in a management software for DSOs in enterprise and operation zones: power scheduling, asset management, customer management, SCADA, AMI management, etc. In addition, the WiseGRID Cockpit has been also mapped to the “generic substation” and “AMI” functional cluster because in the scope of the project this tool will include advanced functionalities to detect faults, self-protect and self-configure the network in a robust way making use of the information coming from the advanced metering infrastructure



(or AMI) and also other components able to provide information and receive orders from the WiseGRID Cockpit.

The most suitable smart grid fields for this component are labelled in the image down below.

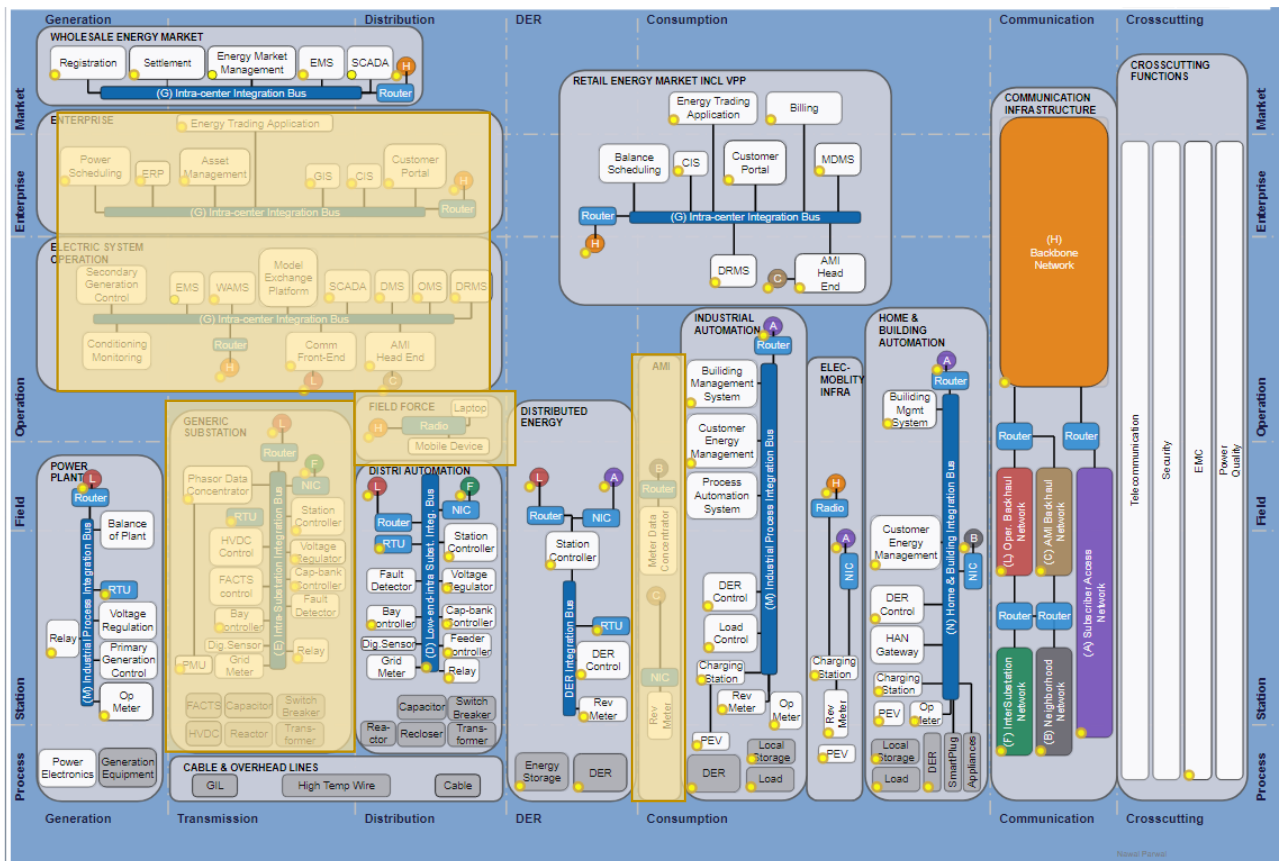


Figure 100 - Standards map for WG Cockpit.

The covered areas include:

- Enterprise and Operation zones of the distribution domain: since most features to be implemented within WiseGRID Cockpit have the objective of efficiently assisting DSOs in their daily operations, including monitoring of the grid, advanced control policies, asset management, field force management...
- AMI: one of the most valuable inputs of WiseGRID Cockpit to enable a good observability of the low voltage grid includes the integration of data provided by smart meters.
- Generic substation: advanced control policies of the WiseGRID Cockpit, such as self-healing mechanisms, will interact with elements at substation level.

### 15.2.3.3 WISECORP

The WiseCORP is addressed to businesses, industries, ESCOs and public facilities consumers and prosumers as the main tool for the energy management of their building or other kind of facility allowing the integration of distributed energy resources or (DER), trying to ease the participation of the consumers and reducing their energy bill. Based on this description, the WiseCORP tool has been mapped to the “industrial automation” and “home and building automation” functional clusters including all the components proposed by the IEC: energy management, DER and storage integration, smart appliances, etc.

The most suitable smart grid fields for this component are labelled in the image down below.

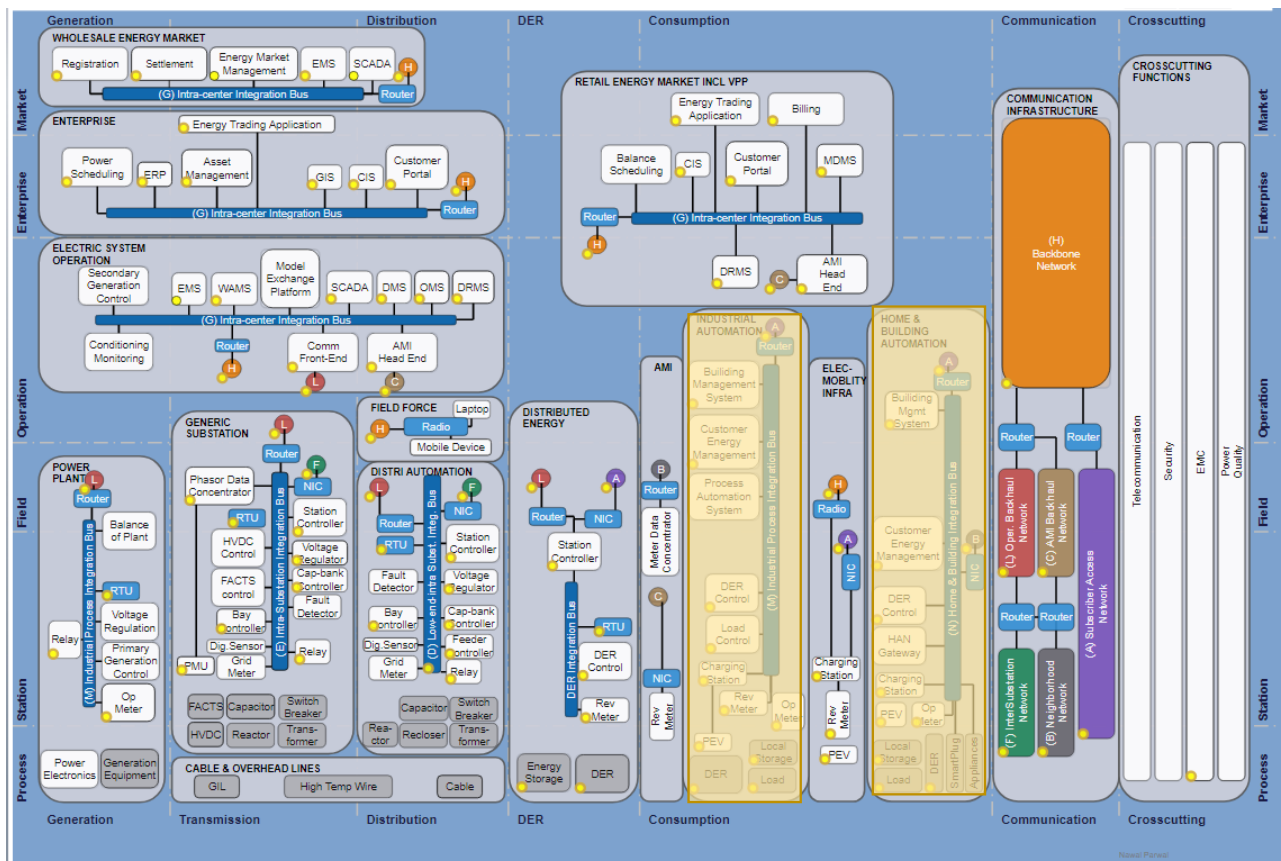


Figure 101 – Standards map for WiseCORP.

The covered areas include:

- Industrial automation: core features of the WiseCORP deal with monitoring and optimizing usage of demand assets under the controlled facilities, which include industrial process-related assets, renewable production, HVAC, lighting...
- Home and building automation: in a similar way, core features of the WiseCORP deal with monitoring and optimizing usage of demand assets under the controlled facilities, including smart appliances.

#### 15.2.3.4 WISECOOP

The WiseCOOP is addressed to energy retailers, aggregators, local communities and cooperatives of consumers and prosumer and any other kind of intermediary companies. This tool will provide support to these actors to achieve better energy deals in the energy market. Based on this definition, the WiseCOOP has been mapped to the “retail energy market including VPP” functional cluster of the IEC standards map including all the components: energy trading, customer management, balance scheduling, etc.

The most suitable smart grid fields for this component are labelled in the image down below.



- Retail energy market, including VPP: core functionality of the WiseCOOP is enabling advanced analysis and active management of the aggregator/retailer over a portfolio of prosumers (tertiary and domestic). Therefore, areas considering retail energy market and demand response mechanisms shall be included.

### 15.2.3.5 WISEHOME

The WiseHOME is addressed to individual domestic consumer and prosumers as the main tool for their household's energy management in order to become active energy players by the integration of renewable energy, storage and demand side management options. This tool has been mapped to the "home and building automation" functional cluster including all the components proposed by the IEC standards map: building management system, customer energy management, DER control, etc.

The most suitable smart grid fields for this component are labelled in the image down below.



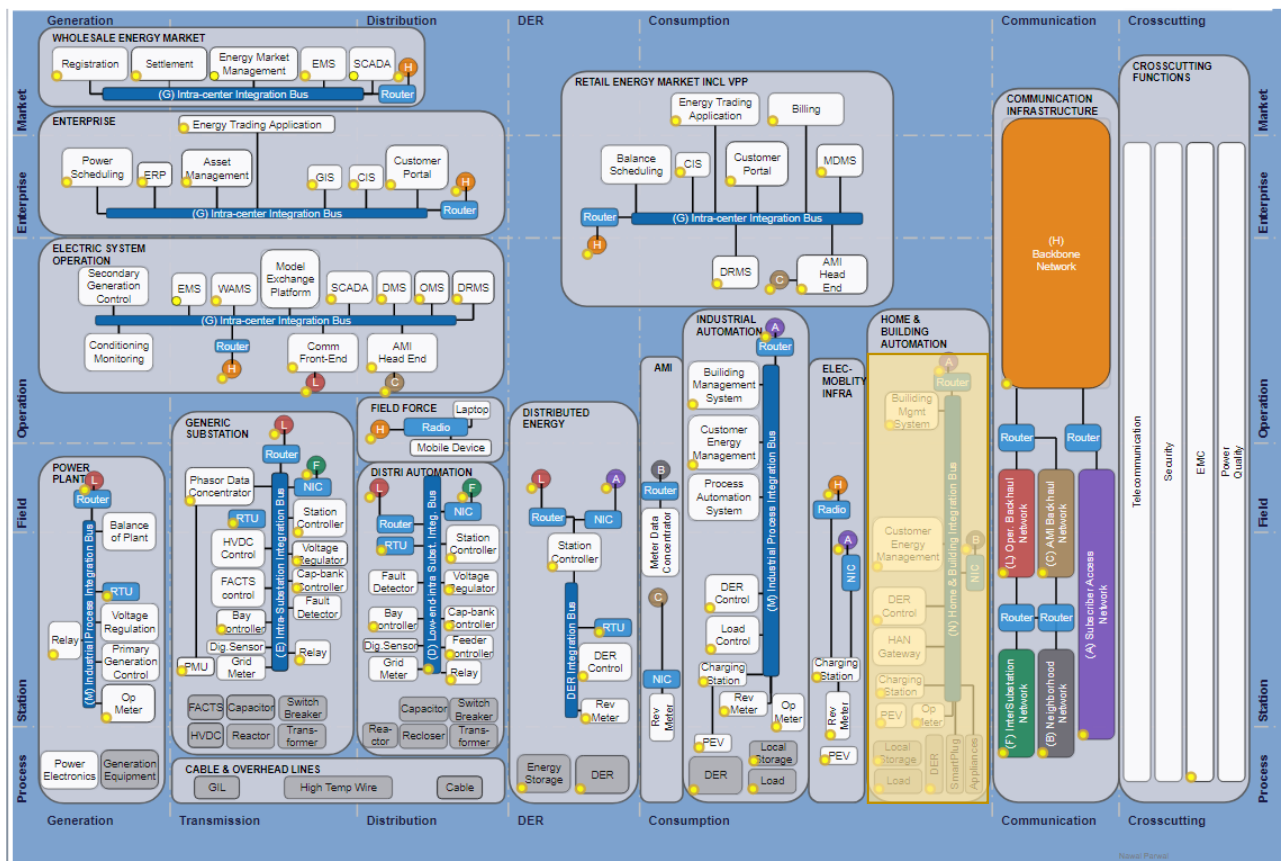


Figure 103 - Standards map for WiseHOME.

### 15.2.3.6 WISEEVP

The WiseEVP or Electric Vehicle Platform is the tool addressed for the e-vehicles fleet managers and the charging infrastructure managers. This tool will allow the asset management of vehicles and charging stations, but also the management of the charging sessions in order to receive orders from the grid actors (such as DSOs). These orders will flexibly the EV demand to avoid network congestion and enhance the integration of renewable energy in the scope of a flexibility market. In the IEC standards maps there was not a specific functional cluster for this kind of tool. For this reason, the WiseEVP has been mapped to different functionalities or components in different functional cluster. In the consumption domain, the charging stations and the electric vehicles have been selected. In the operation zone and enterprise zone also some functionalities have been selected such as asset management or demand response management system.



- Specific areas under enterprise and operation zones (asset management, EMS, demand response, monitoring, customer portal): despite the fact that the standards map represents those for generation, transmission and distribution domains, those features are also present in a system for fleet and charging point management.
- Demand response area under consumption domain, since WiseEVP will be in position of offering services to the DSO for modulating the demand.
- Electromobility infrastructure: core of the functionality of WiseEVP, includes all standards related to charging station infrastructure monitoring.

The WG FastV2G is a bidirectional charging station able to make fast charging but also with the main capability of controlling the charging sessions (modulating the power consumed for charging and discharging) based on the instruction received from the WiseEVP. This component has been mapped to the “electromobility infrastructure” functional cluster but also to the “distributed energy” functional cluster as with the vehicle to grid (V2G) capability the WG FastV2G can be managed as a storage system. Also some functionalities of the “home and building automation” functional cluster have been selected because this kind of controllable charging station might also be installed in a household (without the fast charging option).

259

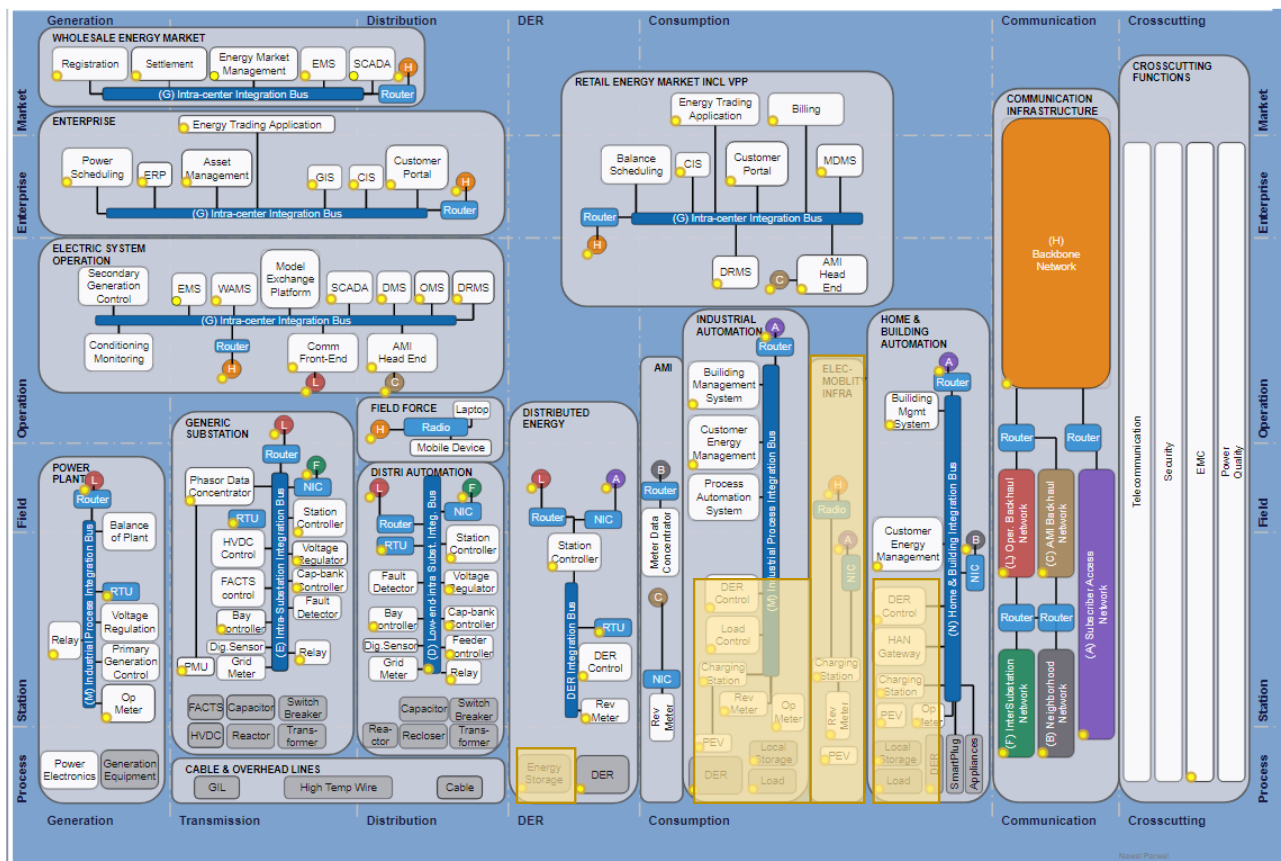


Figure 105 - Standards map for WG FastV2G.

### 15.2.3.8 WG STAAS/VPP

The WG STAAS/VPP or WiseGRID Storage AS A Service and Virtual Power Plant is the tool addressed to households or corporations in order to manage as a VPP the generation, storage and consumption resources available in their facilities and offer to the market (through a third party which operates the service) their unused storage or generation capacity. This tool has been mapped to several components related to distributed energy resources and storage in different functional clusters, such as “distributed energy”, “industrial automation” and “home and building automation”. In order to consider the market interaction of this tool, it has been also mapped to the “retail energy market” functional cluster proposed by the IEC standards maps.

The most suitable smart grids fields for this component are labelled in the image down below.

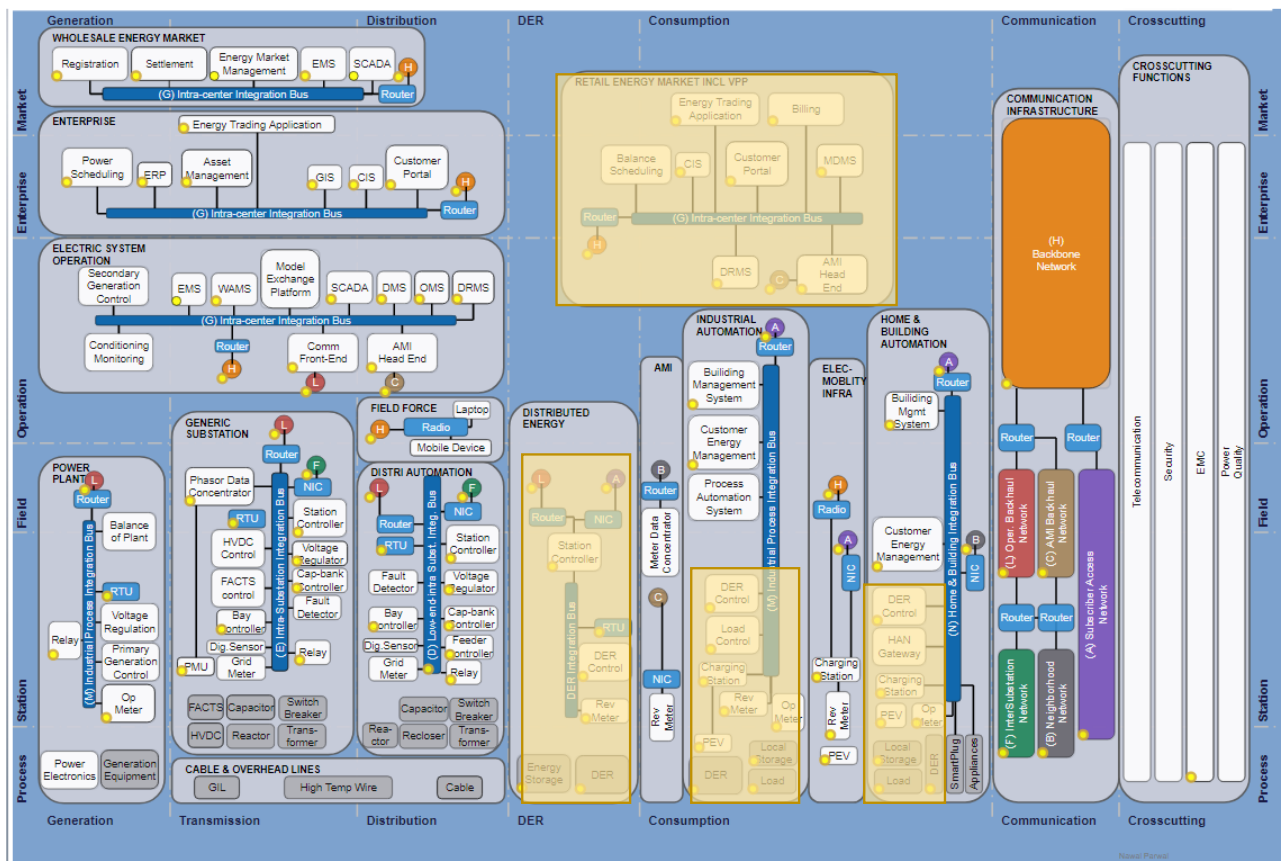


Figure 106 - Standards map for WG STas/VPP.

### 15.2.3.9 WG RESCO

The WG RESCO is addressed to RESCOs or renewable energy service companies to provide renewable energy (mainly PV, wind power or micro hydro) to the end consumers even if do not own and maintain the generation equipment. The renewable installation will be owned, serviced and operated by the RESCO itself. In the IEC standards maps there was not a specific functional cluster for this kind of tool. For this reason, the WG RESCO has been mapped to different functionalities or components in different functional cluster. Specifically it has been mapped to the DER control inside the “distributed energy”, “industrial automation” and “home and building automation” functional clusters. In order to consider the market interaction of this tool, it has been also mapped to some functionalities inside the “retail energy market” functional cluster proposed by the IEC standards maps.

The most suitable smart grids fields for this component are labelled in the image down below.

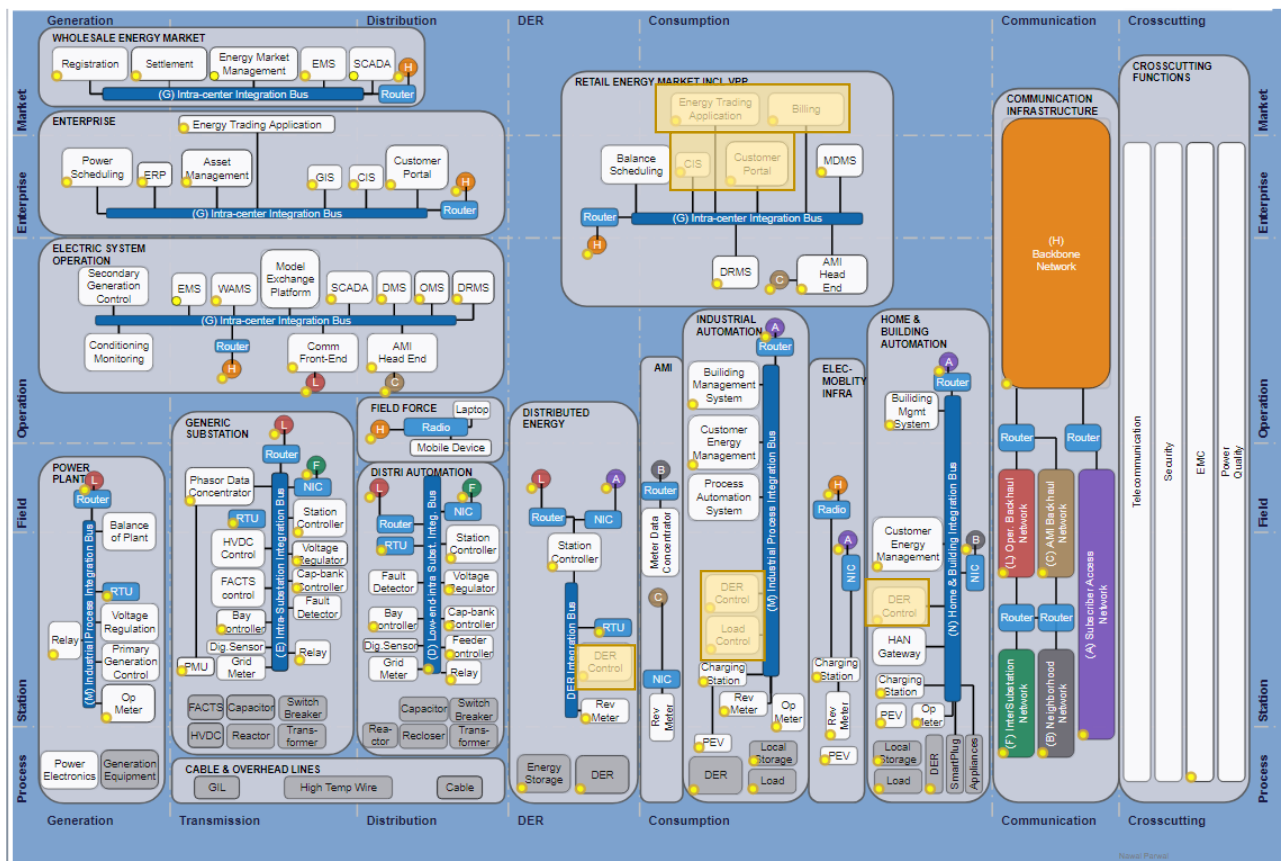


Figure 107 - Standards map for WG RESCO.

## 15.2.4 WISEGRID INTERFACES

In this section of the present deliverable document, it is going to be defined all the communication interfaces among all the different WiseGRID components. These interfaces have been defined thanks to the collaboration of all the WiseGRID consortium partners, who are in charge of each component development as work package leader. In the next sub-sections the different communication interfaces are defined in a graphical way with diagrams. In all the images the WiseGRID components are in blue, WiseGRID actors are in green, and WiseGRID resources or components to be managed or integrated are in grey.

### 15.2.4.1 WG IOP

The communication interface schema for WG IOP, structured by the consortium is:

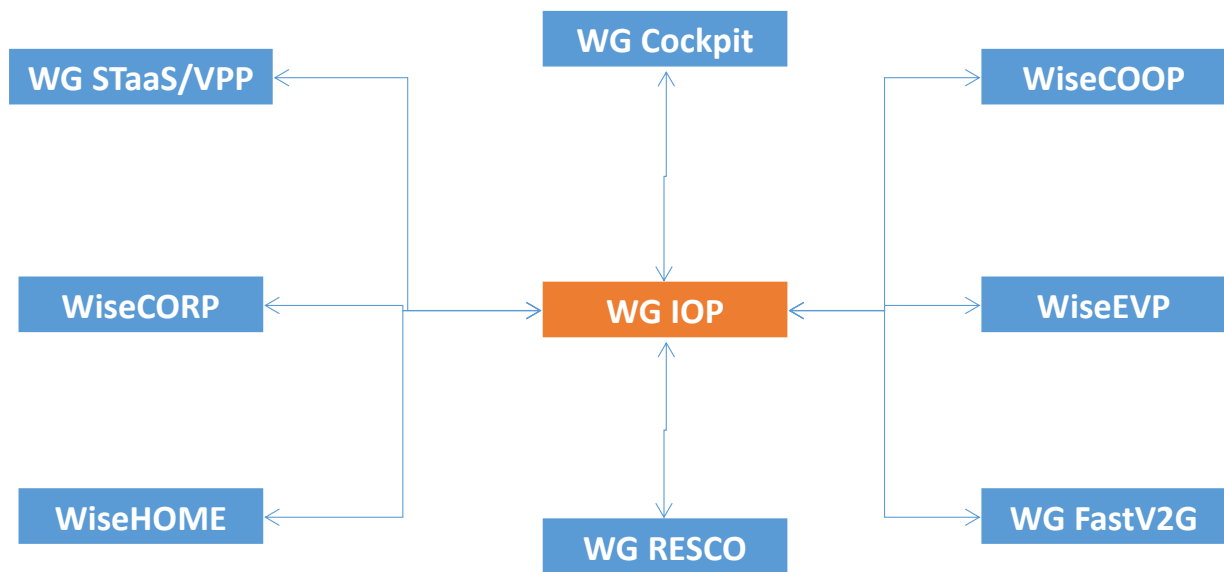


Figure 108 - Communication interfaces of WG IOP.

#### 15.2.4.2 WG COCKPIT

For the case of WG Cockpit the structured communication interface architecture is:

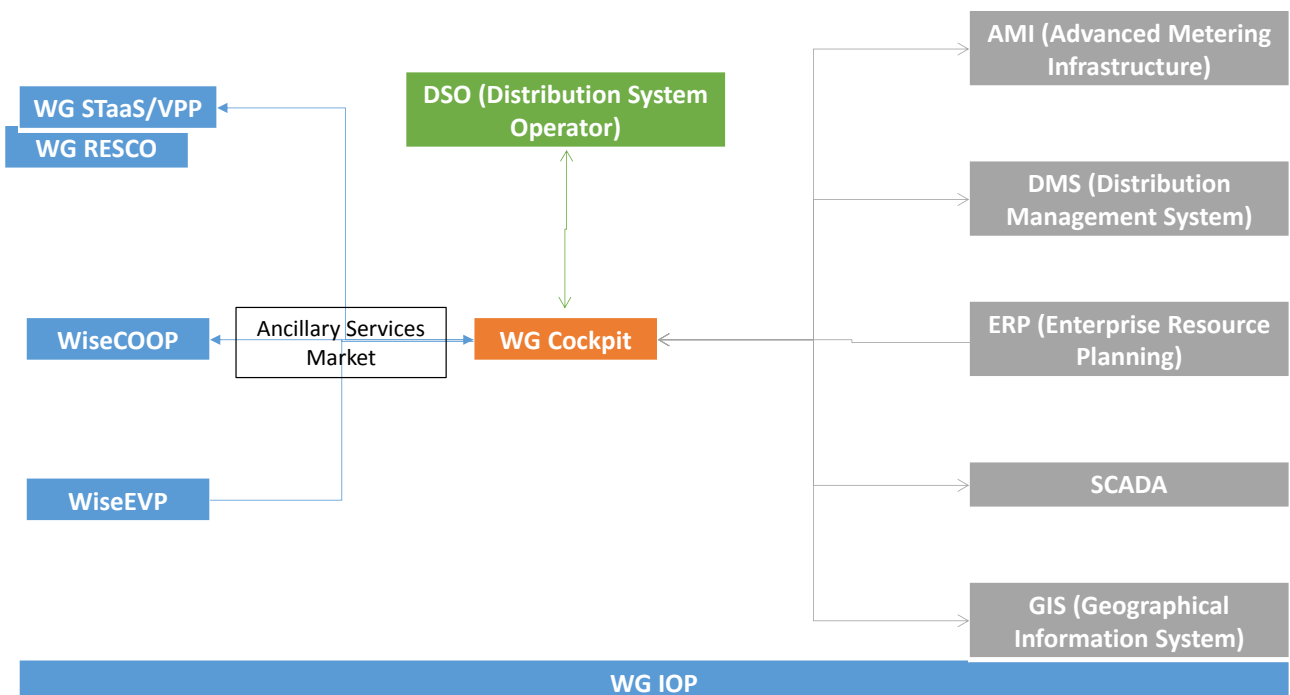


Figure 109 - Communication interfaces of WG Cockpit.

The main actor interacting with the WiseGRID Cockpit is the DSO, since it is the target of the application. WiseGRID Cockpit will integrate several existing systems of the DSO in order to provide a holistic

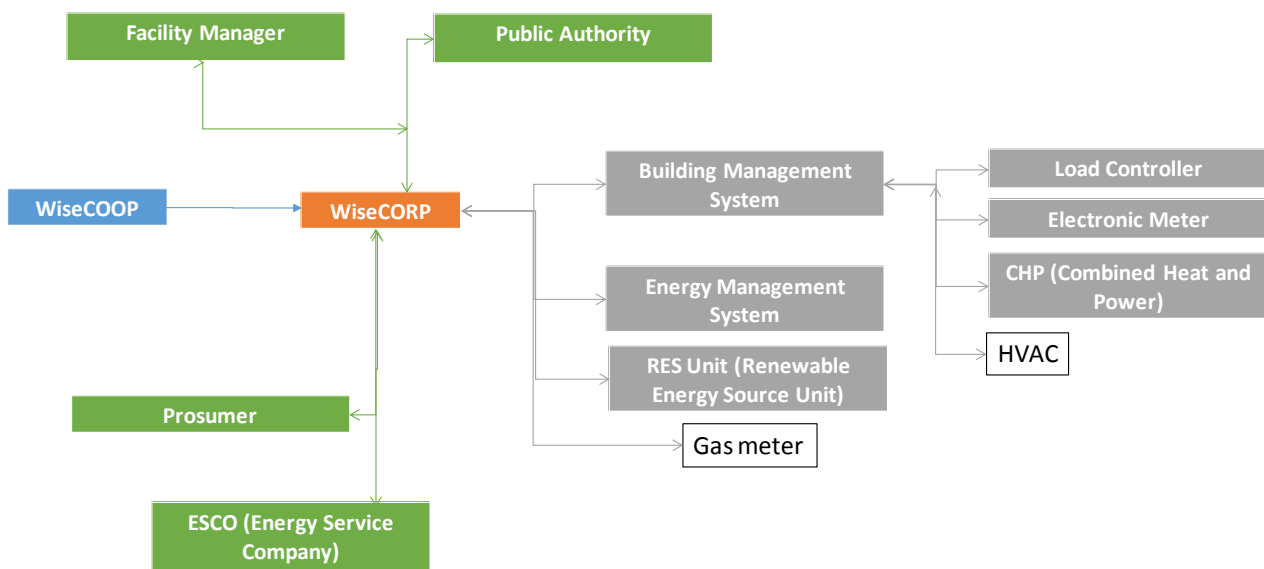


representation of the status of the grid and enable different analysis of the information. Those systems include AMI – for retrieval of energy metering -, existing DMS, ERP – for integration with the maintenance processes of the DSO -, SCADA – for retrieving data from DSO substations and from different sensors deployed in the grid -, and GIS – in order to provide a comprehensive georeferenced visualization of the different data and results of the analysis.

WG Cockpit will also allow the DSO to request ancillary services to other applications of the WiseGRID ecosystem (WG StaaS/VPP, WG RESCO, WiseCOOP and WiseEVP are in position of providing support to the DSO), all of those orchestrated by a common Ancillary Services Market module.

### 15.2.4.3 WISECORP

For the case of WiseCORP, the structured communication interfaces are:



**Figure 110 - Communication interfaces of WiseCORP.**

The main actors interacting with the WiseCORP are actors responsible of facility management, therefore including owners of those facilities, public authorities, ESCOs...

Under the umbrella of monitoring and control of WiseCORP, several field devices appear: controllable loads, CFP, HVAC, RES units... In summary, any devices capable of providing information about its energy demand/production, as well as any devices that may be controlled to achieve modulation of the demand. It is likely that those elements communicate through a common Building Management System, which will be also considered for integration with the WiseCORP application.

The main interaction with another tool of the WiseGRID ecosystem will happen with the WiseCOOP, since demand and production of buildings under control of the WiseCORP are subject to be aggregated and cooperate together with a common objective, orchestrated by the WiseCOOP.

#### 15.2.4.4 WISECOOP

For WiseCOOP, the structured communication interfaces are:

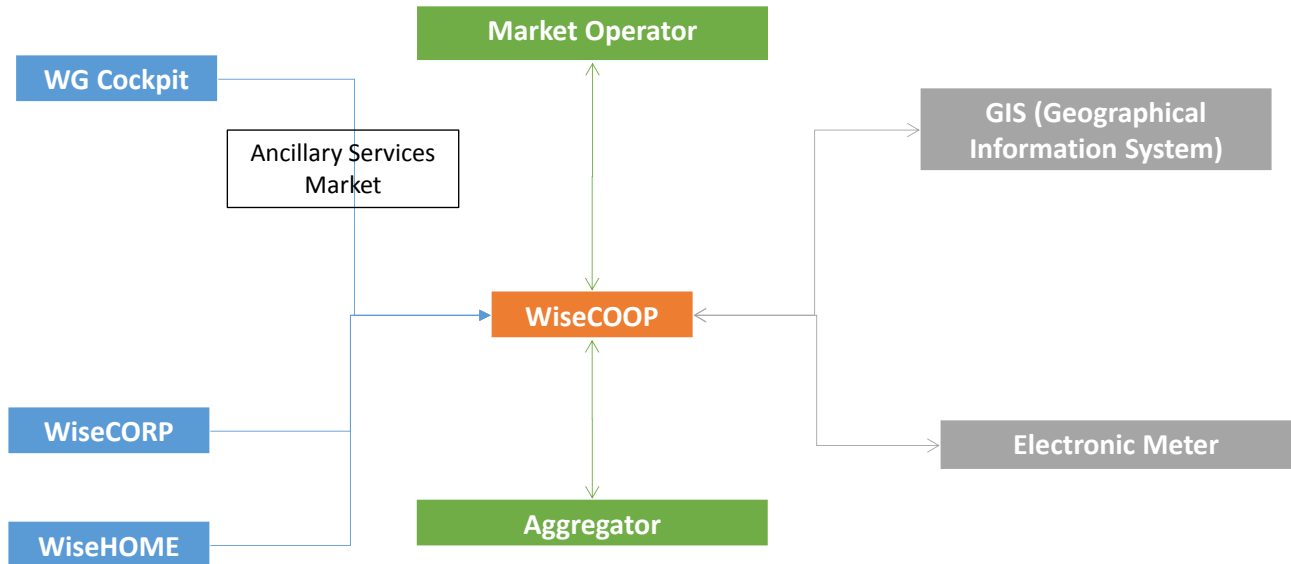


Figure 111 - Communication interfaces of WiseCOOP.

The main actors interacting with the WiseCOOP are aggregators – the main targeted actor of the tool – and the market operator – since the tool shall facilitate the operation of the aggregator in their role of retailers.

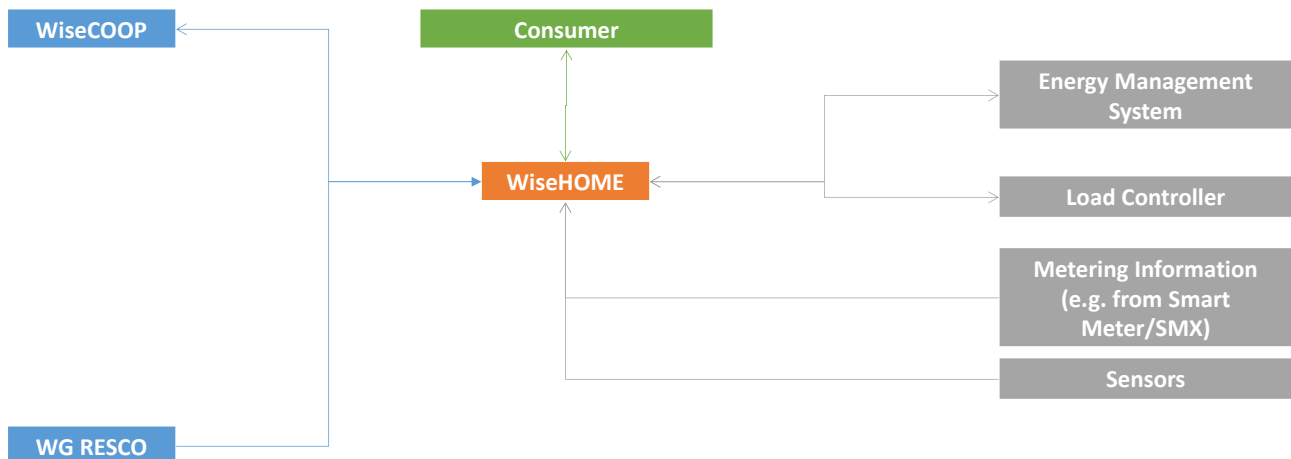
Main information handled by WiseCOOP includes the energy demand and production of the members of the portfolio managed by the aggregator, provided by smart meters. In addition, geolocation of this information is deemed necessary, since the geographical distribution of the demand and the production needs to be handled to properly manage the portfolio.

The main interactions with applications of the WiseGRID ecosystem are two-wise. On one hand, integration with WiseCORP and WiseHOME, since those will be the applications used by end-users, and will display advises coming from the aggregator and information about the on-going demand response campaigns. On the other hand, ancillary services (demand modulation) may be offered to the DSO – WiseGRID Cockpit – by actively participating in the Ancillary Services Market.

#### 15.2.4.5 WISEHOME

For the case of WiseHOME the structured communications scheme is:



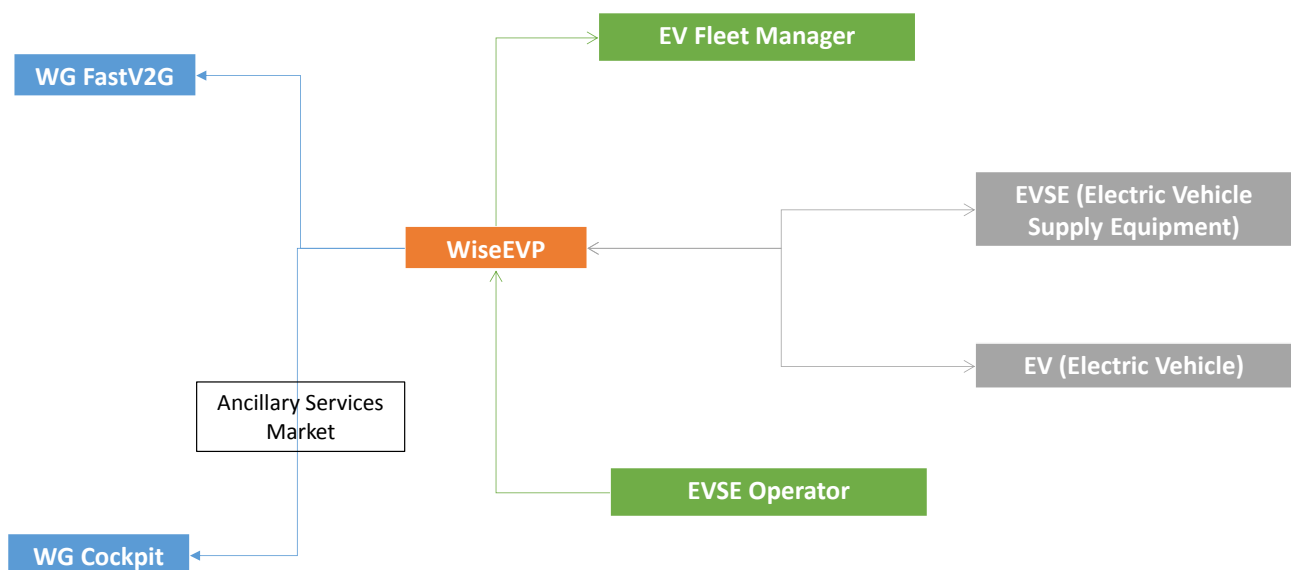


**Figure 112 - Communication interfaces of WiseHOME.**

The WiseHOME tool will be able to help the small, residential prosumer to become an actor in energy market helping him to connect with aggregators in WiseCoop and WG RESCO.

#### 15.2.4.6 WISEEVP

The structured communication architecture for WiseEVP is:



**Figure 113 - Communication interfaces of WiseEVP.**

The main actors interacting with the WiseEVP are EVSE operators and EV Fleet managers, the main targeted actors of the tool.

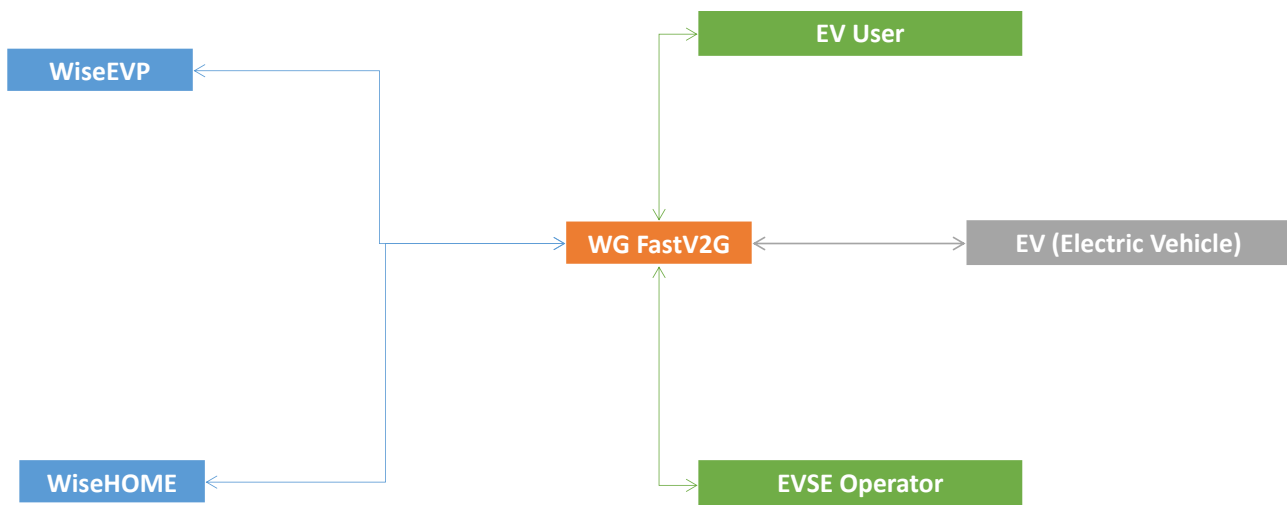
Main information handled by WiseEVP is directly provided by the controlled charging points – all information about the charging session schedules – and the electric vehicles – including current status of the battery, and possibly the geolocation of the vehicles.

The main interactions of WiseEVP with other applications of the WiseGRID ecosystem include:

- Interactions with WiseGRID FastV2G, which will be one of the charging stations integrated and demonstrated in the project
- Interactions with the WiseGRID Cockpit by actively participating in the ancillary services market in order to offer the available flexibility of the fleet to support the DSO dealing with congestion problems.

#### 15.2.4.7 WG FASTV2G

For the case of WG FastV2G, the structured communication interfaces are:



**Figure 114 - Communication interfaces of WG STaaS/VPP.**

#### 15.2.4.8 WG STAAS/VPP

In the case of WG STaaS/VPP, the structured communication interfaces are:

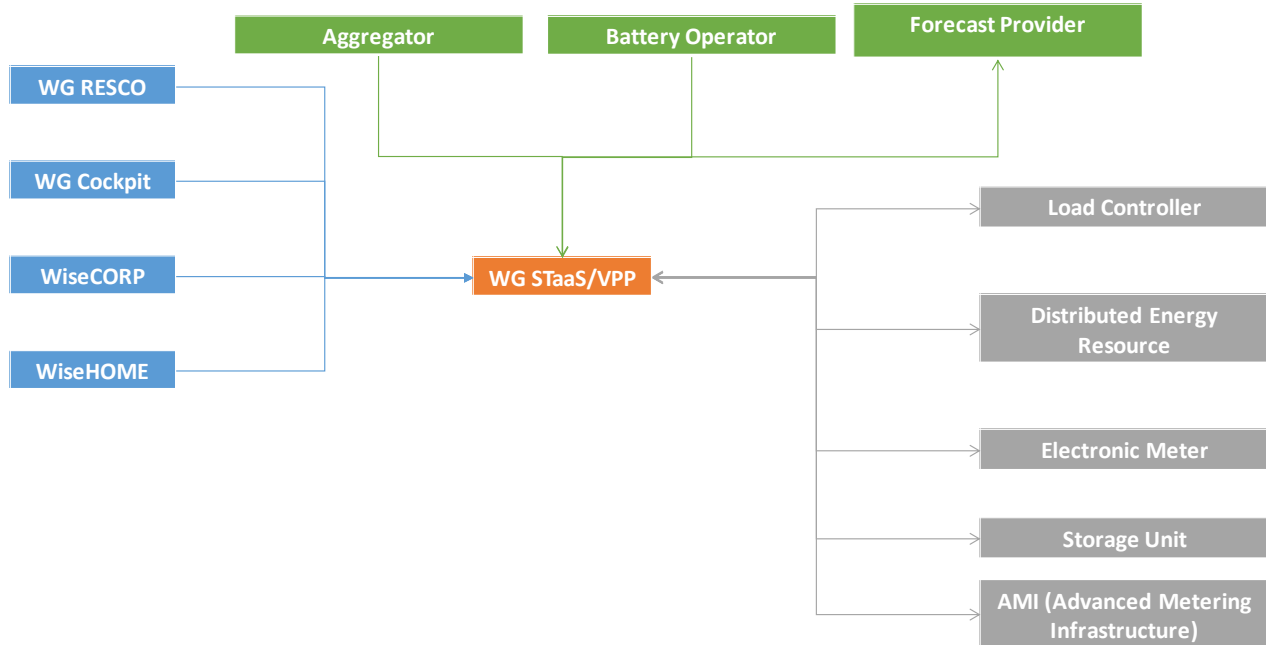


Figure 115 - Communication interfaces of WG STaaS/VPP.

#### 15.2.4.9 WG RESCO

Finally, for WG RESCO, the structured communication interfaces are:

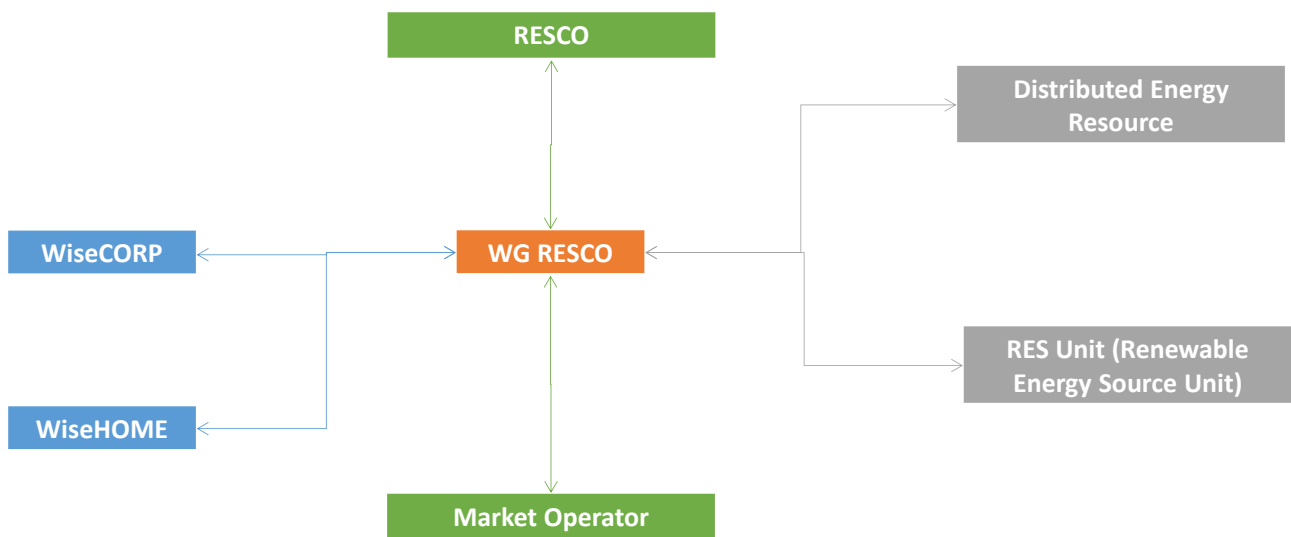


Figure 116 - Communication interfaces of WG RESCO.

## 15.3 STANDARDS AND DATA MODELS STATE OF THE ART

### 15.3.1 AVAILABLE STANDARDS FOR WISEGRID

This section of the document has the objective of identifying all the standards related to each product of the WiseGRID Project. In order to approach this classification in an easy way, it is going to match each product with the high level fields which are related to, and within the Appendix J “List of standards related to Smart Grids fields” listed all the suitable standards for each field.

#### 15.3.1.1 WG IOP

**Table 67 – Smart Grid fields associated to WG IOP.**

High level field	Subfields
Communication Automation	Backbone Network, OPER Backhaul Network, AMI Backhaul Network, Subscriber Access Network, Inter-Substation Network, Neighbourhood Network

#### 15.3.1.2 WG COCKPIT RELATED FIELDS

**Table 68 -Smart Grid fields associated to WG Cockpit.**

High level field	Subfields
AMI	Meter Data Concentrator, Revenue Meter, Network Interface Controller
Electric System Operation	Secondary Generation Control, EMS, WAMS, Model Exchange Platform, SCADA,DMS, OMS, DRMS, AMI Head End, Communication Front-End, Conditioning Monitoring
Enterprise	Power Scheduling, ERP, Asset Management, Energy Trading Application, GIS, CIS, Customer Portal
Field Force	Mobile Device, Laptop
Generic Substation	Phasor Data Concentrator, HVDC Control, FACTS Control, Bay Controller, Digital Sensor, PMU, Grid Meter, FACTS, HVDC, Capacitor, Reactor, Switch Breaker, Transformer, Station Controller, Voltage-Regulator, Cap-bank Controller, Fault Detector, Relay, Network Interface Controller.

## WISECORP RELATED FIELDS

**Table 69 -Smart Grid fields associated to Wise CORP.**

High level field	Subfields
Home and Building Automation	Building Management System, Customer Energy Management, DER Control, HAN Gateway, Charging Station, PEV, Operation Meter, Local Storage, Load, DER Smart Plug, Appliances, Network Interface Controller.
Industrial Automation	Building Management System, Customer Energy Management, Process Automation System, DER Control, Load Control, Charging Station Revenue Meter, PEV, Operation Meter, DER, Local Storage, Load

### 15.3.1.3 WISECOOP RELATED FIELDS

**Table 70 -Smart Grid fields associated to Wise COOP.**

High level field	Subfields
Retail Energy Market including VPP	Balance Scheduling, CIS, Energy Trading Application, Customer Portal, Billing, MDMS, AMI Head End, DRMS

### 15.3.1.4 WISEHOME RELATED FIELDS

**Table 71 -Smart Grid fields associated to Wise HOME.**

High level field	Subfields
Home and Building Automation	Building Management System, Customer Energy Management, DER Control, HAN Gateway, Charging Station, PEV, Operation Meter, Local Storage, Load, DER, Smart Plug, Appliances, Network Interface Controller.

### 15.3.1.5 WISEEVP RELATED FIELDS

**Table 72–Smart Grid fields associated to Wise EVP.**

High level field	Subfields
Electric System Operation	Conditioning Monitoring, EMS, WAMS, DRMS
Electromobility Infrastructure	PEV, Revenue Meter, Charging Station
Enterprise	Asset Management, CIS, Customer Portal
Retail Energy Market including VPP	DRMS

### 15.3.1.6 WG FASTV2G RELATED FIELDS

**Table 73–Smart Grid fields associated to WG FastV2G.**

High level field	Subfields
Electromobility Infrastructure	Charging Station, Revenue Meter, PEV
Home and Building Automation	DER Control, HAN Gateway, Charging Station, PEV, Operation Meter, Local Storage, Load, DER

Industrial Automation	DER Control, Load Control, Charging Station, Revenue Meter, Operation Meter, PEV, DER, Local Storage, Load
-----------------------	--

### 15.3.1.7 WG STAAS/VPP RELATED FIELDS

Table 74 -Smart Grid fields associated to WG STaaS/VPP.

High level field	Subfields
Distributed Energy	Station Controller, RTU, DER Control, Revenue Meter, Energy Storage, DER
Home and Building Distribution	DER Control, HAN Gateway, Charging Station, PEV, Operation Meter, Local Storage, Load, DER
Industrial Automation	DER Control, Load Control, Charging Station, Revenue Meter, PEV, Operation Meter, DER, Local Storage, Load
Retail Energy Market including VPP	Balance Scheduling, CIS, Energy Trading Application, Billing, Customer Portal, MDMS, DRMS, AIM Head End

### 15.3.1.8 WG RESCO RELATED FIELDS

Table 75 -Smart Grid fields associated to WG RESCO.

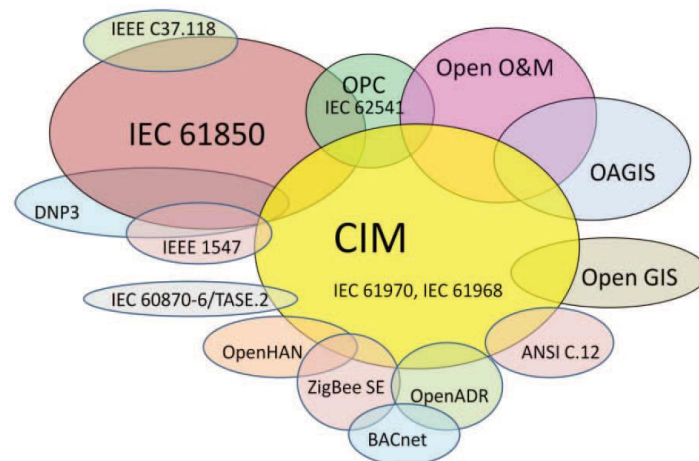
High level field	Subfields
Distributed Energy	DER Control
Home and Building Distribution	DER Control
Industrial Automation	DER Control, Load Control
Retail Energy Market including VPP	CIS, Energy Trading Application, Customer Portal, Billing

## 15.3.2 AVAILABLE DATA MODELS FOR WISEGRID

This section has the objective of putting in common the main standards which are applied in everything related to the field of Smart Grids.

Nowadays, in the field of Smart Grids, there are two main standards which are applied in different levels. Those two standards are IEC 6180 and CIM model (Common Information Model). As has said, each standard work in different levels, IEC 61850 defines protocols and data models which allow interoperability in substation among all its devices, and CIM model is an ontologic model which allows exchanging information of the electric grid among different software applications.

The next figure tries to explain the relationships among the different standards applied in the Smart Grids. As it is possible to aware the main two standards are CIM and IEC 61850 standards.



**Figure 117 - Relationship among applied standards in Smart Grids.**

Trying to define in detail the IEC 61850 standard, this could be defined as an international adopted standard for the communication in electric substations. Initially this standard was defined in order to communicate the control, measure and protection devices of an automatized electric substation. But finally, this standard not only covers communications, but also the necessary aspects of designing, maintaining and operating an electric substation in the fields that concerns to control and protection. In consequence, due to this standard, the control of electric substations is independent of the vendor that manufactures the installed devices in the electric substation.

With the aim of achieving interoperability, this standard defines a data model, which is an oriented object data model. This data model allows the substation to be divided in basic functions thanks to the definition of logic nodes, and thanks to this making the associated data bases simpler.

The defined data models of this standard can be matched with different protocols. The current protocols matched in this standard are GOOSE (Generic Object Oriented Substation Event), MMS (Manufacturing Message Specification), SMV (Sampled Measured Values) and Web Services.

With the definition of IEC 61850 it was introduced the usage of WAN and LAN and TCP/IP networks in electric substations. With this introduction the response time has been improved, and at the same time, communication infrastructure has become simpler and scalable.

Moreover, CIM model, has a different task. This standard was developed by the electric power industry, and afterward has been officially adopted by the International Electrotechnical Commission (IEC). Initially this model was planned with the objective of developing a common power system network model, in order to have a common basis to exchange information. Nowadays this standard has been adopted by the main part of vendors, in order to allow exchange of information among different devices, and it has been extended to cover tasks related to electric power industry, such as asset tracking, customer billing and work scheduling.

CIM model core is mainly composed by the standards IEC 61970-301 and IEC 61968-11. IEC 61970-301 describes the components of a power system at an electrical level and relationships between each component, and IEC 61968-11 defines semantics of other aspects of power system software data exchange such as work scheduling or customer billing. Due to CIM model is an ontologic model, it must deal with exchanges of information with all type of systems such as GIS (Geographical Information Systems), CSS (Customer Support System) or ERP (Enterprise-Resource Planning). With this purpose CIM covers 53 UML packages (Unified Modeling Language), having approximately 820 classes with more than 8500 attributes. In addition it exists different serializations, such as XML and XML schema for build its own EAI messages based on the CIM and to use Pre-defined messages built by IEC. In the case of modeling graphs of power grids CIM model is provided of RDF serializations and RDF schemas. All these serializations it has been developed CIM OWL (Web Ontology Model) serializations.



Thanks to the expanded use of CIM model, this is considered as one of the biggest standardized domain ontologies in combination with IEC 61850.

The current efforts of standardization work groups are oriented to harmonize the two main ontologies applied in the fields of Smart Grids, but this issue is going to be dealt as part of the next section.

### 15.3.3 AVAILABLE NEW DATA MODELS BASED ON ONTOLOGIES FOR WISEGRID

If it is tried to focus on the current efforts on harmonizing standards and data models related to the field of Smart Grids, it is possible to find several initiatives which tries to unify the main standards which are used nowadays. One of the main initiatives is the one which is trying to harmonize CIM model and standard IEC 61850, and it is leaded by the Technical Committee number 57 of the International Electrotechnical Commission. This initiative emerges as a consequence of the common usage of both standards in the power electric industry. In a first stage, both standards were defined to be applied separately, but the evolution of the power grids has made both standards expand and it has been reached a point in which CIM model and IEC 61850 standard are overlapping. Due to this overlap it is necessary to harmonize both standards. Despite the different nature of both standards, but because their overlap, it is necessary to adapt both of them to each other.

The current works are focusing on unifying data mappings for data exchanges, and thus trying to achieve as result a harmonized model. The harmonized model for connectivity has its base on a unification approach. This model is structured in a model level (this level defines classes) and an object level (this level presents instances of classes). Once reached this point, in which the harmonization principles are defined, it is necessary to extend them. With this purpose it must be identified all the data flow scenarios and fill the lack of entities of each standard to be completed with the other standard. In this process must be merged all the semantic object of each standard in order to be aware which are not in each standard and those which are duplicated.

The transformation described above it is performed by the use of QVT (Query/View/Transformation), which is the standard for model transformation by OMG (Object Modelling Group). This standard can support the transformation, both for IEC 61850 and CIM model, to the harmonized model.

The harmonizing connectivity of CIM model and IEC 61850 standard is the starting point to harmonize completely both standards.

Another alternative and clear example of ontologic data model is OpenADR (Open Automated Demand Response). This initiative lead by North American research labs and companies was crated, as they claim, “to accelerate the development, adoption and compliance of OpenADR standards throughout the energy industry” and “provide common language”. With this aim OpenADR tries to provide non-proprietary standardized interfaces for electric services companies to communicate demand response and distributed energy resources to their users, making use of existing information and communications technologies, such as internet. The aim of this open model is to make electric grids smarter, enabling a two-ways communication among the different agents of the electric market and its users, guaranteeing interoperability in the electric grids. The next figure shows a schema of this standard communication architecture.

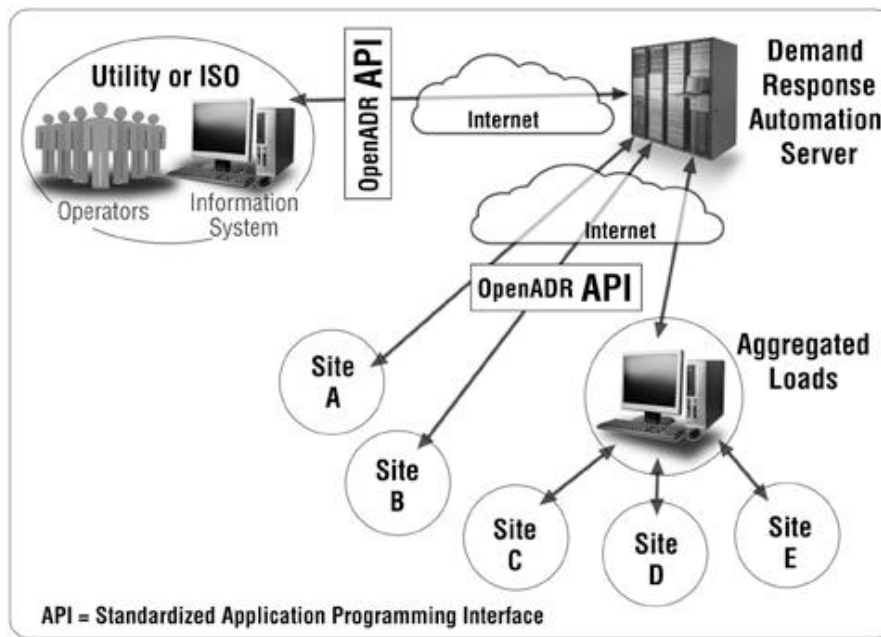


Figure 118 - OpenADR communication architecture schema [76].

OpenADR, making use of Web Service schemas is able to transmit information in push and pull data exchange. To accomplish this it is required a server that allocates all the data transmission mechanisms and clients that select the most suitable mechanism. After evaluating the available data transmission technologies, such as Simple Object Access Protocol (SOAP), Representational State Transfer (REST), Hyper Text Transfer Protocol (HTTP), eXtensible Messaging and Presence Protocol (XMPP); REST-styled simple HTTP has been the chosen protocol to implement OpenADR.

OpenADR adapts to standard the achievement of research, providing insights for interoperability systems.

## 16 CONCLUSIONS AND NEXT STEPS

### Architecture

In this deliverable the modelling using a systematic approach of both the PUCs and the WiseGRID tools was carried. The modelling was based on the SGAM framework and underlying methodology, which consists the state-of-the-art approach for modelling the architecture of UCs for Smart Grid projects.

In parallel with this deliverable (D3.1) the deliverables related to the WiseGRID tools are also under preparation with the involvement of the various partners that are responsible for each tool. Although this deliverable laid the foundations concerning the architecture, as well as aspects related to standards, data models, privacy, and data protection, refinements in all aforementioned areas will be carried out in the subsequent deliverables dedicated to each one of the WiseGRID tools. These refinements will be taken into account and all the necessary modifications will be considered and included in the second version of this deliverable, namely D3.2.

As in the preparation of this deliverable an agile approach was followed, a similar iterative approach will be used when consolidating the information from the deliverables related to the various tools to the updated version of this deliverable that is due to month 18 of the WiseGRID project.

### Privacy and Data Protection

As conclusions from the “Privacy and Data Protection” process within this deliverable, we can consider at this moment:

- A DPIA process was performed as concluded necessary in line with Regulation EU 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC - shortly: General Data Protection Regulation, and appropriate template developed by “Expert Group 2: Regulatory Recommendations for Privacy, Data Protection and Cyber-Security in the Smart Grid Environment”.
- The smart grid applications are considered satisfactory as the DPIA process has been completed with relevant risks identified and appropriately managed ensuring there are no unacceptable residual risks remaining for the individuals.
- The following resolution is considered at the end of current DPIA process for WiseGRID applications, still under design:
  - **The DPIA is positive:** risks have been assessed and controls addressing those risks properly defined and tuned. Any residuals risks have been flagged and there are no further controls still necessary. There are not anymore more unacceptable risks. The systems implementation can proceed.
  - **This DPIA report shall be rechecked** within deliverable D3.1 (V2) and further on when the system will be in production or whenever there would be changes in risk evaluation.

Next steps within “Privacy and Data Protection activity” would be to continue the application of above mentioned regulation and therefore:

- Organize the internal approval of the DPIA within WiseGRID management board;
- Presenting the privacy review report to the DPO;
- Rendering the privacy review report publicly available;

- Communicate to national data privacy authorities about the actions carried out within WiseGRID and also about the results of DPIA Report and further possible updates;
- Reviewing the implementation of the mitigation and avoidance controls that were identified in the DPIA;
- Update the DPIA Report within the next deliverable D3.1 (V2);
- Monitoring changes over time (context, risk, measures...) and update (review) whenever a significant change occurs and preparing a review report within each DPIA review;
- Assessing whether there is a need for revising the DPIA after a certain amount of time or after a new stage within the project or program has been completed.

### *Standards and Interoperable Data Models*

This deliverable includes the main results of the activities carried out in the scope of task 1.3 “Standards and interoperable data models” of the WiseGRID project. The main objective of this task was to value the necessary interfaces between actors of components and recommend the appropriate set of standards or new data models based on ontologies.

Regarding the identification of the main WiseGRID interfaces, the main outputs of task 1.3 are:

- Simplified architecture to work in the definition of WiseGRID standards (section 15.2).
- Mapping all the WiseGRID products with the IEC Smart Grid Standards Map (section 15.2.3).
- WiseGRID products representation in diagrams showing the differences between the communications among WiseGRID products, the communications between WiseGRID products and external actors and the communication between these products and external resources that will be managed or integrated in WiseGRID solution (section 15.2.4).

Regarding the data standards and data models assessment, the main outputs of task 1.3 are:

- State of the art of available standards for WiseGRID products based on the IEC mapping (section 15.3.1).
- State of the art of available data models for WiseGRID products, focused on most extended: IEC 61850 and CIM model (section 16.2).
- Review of the new data models based on ontologies that might be applied to WiseGRID products (section 15.3.3).

Most of the WiseGRID partners have been involved in the development of task 1.3, specifically the partners with expertise in standardization and the partners in charge of developing a WiseGRID product. The WiseGRID consortium face to face meetings that took place in Kythnos (June 2017) and Crevillent (September 2017) have been vital to identify the interfaces and map the WiseGRID tools to the IEC Smart Grids Standards Map. The output of these workshops has been the base of the contents included in this deliverable regarding task 1.3

The main objective of task 1.3 “Standards and interoperable data models” of the WiseGRID project was to value the necessary interfaces between actors of components and recommend the appropriate set of standards or new data models based on ontologies. This first release of the “WiseGRID architecture, data models, standards and data protection (D3.1) includes the identification of the WiseGRID interfaces and also the state of the art of the available standards and data models.

In the second release of this document (D3.2), once the design of the WiseGRID tools is almost finished, the respective sections will be extended to study the applicability of data models and standards to WiseGRID.

Based on the state of the art included on this release, for each WiseGRID tool, the most appropriate standards and data models will be selected.

## 17 REFERENCES AND ACRONYMS

### 17.1 REFERENCES

- [1] CEN-CENELEC-ETSI, Smart Grid Coordination Group, "Smart Grid Reference Architecture," 2012.
- [2] C. Neureiter, "Introduction to the "SGAM Toolbox"," 2014.
- [3] CEN-CENELEC-ETSI, Smart Grid Coordination Group, "D3.1 Smart grids reference architecture and data models v1," 2016.
- [4] "Toward a commodity enterprise middleware," [Online]. Available: [http://www.acm.org/acmqueue/digital/Queuevol5no4\\_May2007.pdf](http://www.acm.org/acmqueue/digital/Queuevol5no4_May2007.pdf).
- [5] "ISO/IEC 20922:2016 Information technology - Message Queuing Telemetry Transport (MQTT) v3.1.1," [Online]. Available: <https://www.iso.org/standard/69466.html>.
- [6] D. P. a. C.-S. i. t. S. G. E. Expert Group 2: Regulatory Recommendations for Privacy, "Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems," Brussels, 2014.
- [7] Expert Group 2: Regulatory Recommendations for Privacy, Data Protection and Cyber-Security in the Smart Grid Environment, "Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems," 2014.
- [8] European Commission, "Directive Directive 95/46/EC on the Protection of Individuals with regard to the processing of personal data and on the free movement of such data," 1995.
- [9] European Parliament, "Charter of fundamental rights of the European Union," 2000.
- [10] E. Commission, "2012/148/EU: Commission Recommendations of 9 March 2012 on preparations for the roll-out of smart metering systems," Brussels, 2012.
- [11] E. Commission, "2014/724/EU: Commission Recommendation of 10 October 2014 on Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems," 10 October 2014. [Online]. Available: [http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:JOL\\_2014\\_300\\_R\\_0013&qid=1413790118102&from=EN](http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:JOL_2014_300_R_0013&qid=1413790118102&from=EN). [Accessed 27 June 2017].
- [12] European Commission, "Recital 14, 2014/724/EU: Commission Recommendation of 10 October 2014 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems," Brussels, 2014.
- [13] European Commission, "EU General Data Protection Regulation, Article 1 (1)," Brussels, 2016.
- [14] European Commission, "General Data Protection Regulation, Article 1 (2) and (3)," Brussels, 2016.
- [15] European Convention of Human Rights, "Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols no. 11 and no. 14," Rome, 1950.
- [16] Council of Europe, "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS no. 108," 1981.
- [17] European Union Agency for Fundamental Rights, "Handbook on European Data Protection Law," 2014.

]

[18 Council of Europe, "Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding Supervisory Authorities and Transborder Data Flows, CETS 181," 2001.

[19 European Convention on Human Rights, "Charter of Europe, CETS No. 005," 1950.  
]

[20 European Union, "Treaty on the Function of the European Union, Article 16 (2)," 2012.  
]

[21 European Commission, "General Data Protection Regulation, Recital 4," 2016.  
]

[22 European Commission, "General Data Protection Regulation, Article 4 (10)," 2016.  
]

[23 European Union, "Charter of Fundamental Rights of the European Union, OJ 2012 C 326," 2012.  
]

[24 European Commission, "Data Protection Directive, OJ 1995 L 281, p. 31," 1995.  
]

[25 European Commission, "Directive 2012/27/EU on energy efficiency," 2012.  
]

[26 European Commission, "General Data Protection Regulation, Article 6 (1)," 2016.  
]

[27 European Commission, "General Data Protection Regulation, Article 4 (11)," 2016.  
]

[28 European Commission, "General Data Protection Regulation, Article 7," 2016.  
]

[29 European Commission , "General Data Protection Regulation, Article 25," 2016.  
]

[30 European Commission , "General Data Protection Regulation, Article 25 (1)," 2016.  
]

[31 European commission, "General Data Protection Regulation, Article 17 (1)," 2016.  
]

[32 European Commission, "General Data Protection Regulation, Article 26," 2016.  
]

[33 European commission, "Directive 95/46/EC," 1995.  
]

[34 European Commission, "General Data Protection Regulation, Article 5 (2)," 2016.  
]

[35 European Commission, "General Data Protection Regulation, Article 26 (1)," 2016.  
]

[36 European Commission, "General Data Protection Regulation, Article 28 (2)," 2016.

]

[37 European Commission, "General Data Protection Regulation, Article 25 (2)," 2016.

]

[38 European Commission, "General Data Protection Regulation, Article 28," 2016.

]

[39 European Commission, "General Data Protection Regulation, Article 29," 2016.

]

[40 European Commission, "General Data Protection Regulation, Recital 13," 2016.

]

[41 European Commission, "General Data Protection Regulation, Article 6 (9)," 2016.

]

[42 European Commission, "General Data Protection Regulation, Article 39," 2016.

]

[43 European Commission, "General Data Protection Regulation, Article 3 (2) and (3)," 2016.

]

[44 European Commission, "General Data Protection Regulation, Recital 22-24," 2016.

]

[45 European Commission, "Article 1 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects," 2000.

]

[46 European Commission, "General Data Protection Regulation, Article 2 (3)," 2016.

]

[47 European Commission, "General Data Protection Regulation, Article 51 (1)," 2016.

]

[48 European Commission, "General Data Protection Regulation, Article 53 (1) and (2)," 2016.

]

[49 European Commission, "General Data Protection Regulation, Article 68," 2016.

]

[50 European Commission, "General Data Protection Regulation, Article 83," 2016.

]

[51 European Commission, "General Data Protection Regulation, Article 33 (1)," 2016.

]

[52 European Commission, "General Data Protection Regulation, Article 33 (2)," 2016.

]

[53 European Commission, "General Data Protection Regulation, Article 34 (1) and (2)," 2016.

]

[54 Smart Grid Task Force 2012-14, Expert Group 2: Regulatory Recommendations for Privacy, Data Protection and Cyber-Security in the Smart Grid Environment, "Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems, Chapters 2 and 3," 2014.

]

[55 S. D. Smedt, "Belgium - The New Data Protection Hub?," *European Data Protection Law Review*, vol. 3,



] pp. 213 - 218, 2015.

[56 T. D'hulst, "Data Protection in Belgium: overview," Practical Law - Thomson Reuters, 1 July 2016. [Online]. Available: [https://uk.practicallaw.thomsonreuters.com/2-502-2977?\\_lrTS=20170610192313070&transitionType=Default&contextData=\(sc.Default\)](https://uk.practicallaw.thomsonreuters.com/2-502-2977?_lrTS=20170610192313070&transitionType=Default&contextData=(sc.Default)). [Accessed 12 September 2017].

[57 Council of European Energy Regulators (CEER), "CEER Benchmarking Report on Meter Data Management Case Studies," CEER, Brussels, 2012.

[58 Smart Grids Task Force, "My Energy Data (Report by Expert Group on Smart Grid Deployment (EG1))," 2016.

[59 SIA Partners, "Atrias and MIG6.0: Towards a new energy market model in Belgium," SIA PARTners, 1 July 2016. [Online]. Available: <http://energy.sia-partners.com/20160701/atrias-and-mig60-towards-new-energy-market-model-belgium>. [Accessed 12 September 2017].

[60 Data Protection Act 2472/1997 and its amendment for electronic telecommunications, Law 3471/2006.. ]

[61 Law 2472/1997, including modifications from the more recent Law 4139/2013: protection of the individuals from processing of personal data; Law 3471/2006, including modifications from the Laws 3783/2009, 3917/2011 and 4070/2012: protection of personal da.

[62 Karageorgiou & Associates Law Firm, "Linklaters LLP," [Online]. Available: <https://clientsites.linklaters.com/Clients/dataprotected/Pages/Greece.aspx>.

[63 Joined Cases C-293/12 and 594/12, Digital Rights Ireland and Seitlinger and Others. ]

[64 T. Garanis-Papadatos and D. Boukis, "Research Ethics Committees in Greece," in *Research Ethics Committees, Data Protection and Medical Research in European Countries*, D. Beyleveld, D. Townend and J. Wright, Eds., New York, Routledge, 2016.

[65 R. Panetta and A. D'Ottavio, "Data protection in Italy: overview," Thomson Reuters, 1 12 2015. [Online]. Available: [https://uk.practicallaw.thomsonreuters.com/9-502-4794?transitionType=Default&contextData=\(sc.Default\)](https://uk.practicallaw.thomsonreuters.com/9-502-4794?transitionType=Default&contextData=(sc.Default)). [Accessed 3 October 2017].

[66 Article 45, paragraph 3 Data Protection Law 15/1999. ]

[67 Hogan Lovells, "Data protection compliance in Spain. Mission impossible?," Hogan Lovells, 2015. ]

[68 R. Azim-Khan, "New Spanish Regulation Tightens Up Data Protection Requirement," *Privacy and Data Security Law Journal*, 2008.

[69 Linklaters, "Data Protected. Spain. General. Data Protection Laws," Linklaters, [Online]. Available: <https://clientsites.linklaters.com/Clients/dataprotected/Pages/Spain.aspx>. [Accessed 16 June 2017].

[70 Spanish Data Protection Agency, "Spanish Data Protection Agency," Spanish Data Protection Agency, Madrid.

[71 European Smart Grid Task Force, "My Energy Data," Smart Grids Task Force Ad hoc group of the Expert Group 1 - Standards and Interoperability, 2016.

[72 J. Leiva, "Smart metering trends, implications and necessities: A policy review," *Renewable and*

] *Sustainable Energy Reviews*, vol. 55, 2016.

[73 EnerConsultoría. Derecho de la energía, "contadores inteligentes y protección de datos,"

] EnerConsultoría. Derecho de la energía, 8 December 2015. [Online]. Available: <http://www.enerconsultoria.es/BlogLeyesEnergia.aspx?id=36002236&post=Contadoresinteligentesyprotecciondedatos>. [Accessed 15 June 2017].

[74 International Electrotechnical Commission, "Smart Grid Standards Map," [Online].

]

[75 IEC, "<http://www.iec.ch/smartgrid/mappingtool/>," [Online].

]

[76 O. Alliance, "[www.openadr.org](http://www.openadr.org)," [Online].

]

[77 SmartGrids, "SmartGrids," [Online]. Available: [www.smartgrids.eu](http://www.smartgrids.eu). [Accessed 2009 03 15].

]

[78 NOBEL Consortium, "D8.1 Dissemination Master Plan," Valencia, Spain, 2010.

]

[79 NOBEL Consortium, *NOBEL Annex I*, Valencia: EC, 2009.

]

[80 EC, "Annex II General Conditions," v5, Brussels, 2009.

]

[81 [Online]. Available: [http://www.sparxsystems.com.au/resources/mdg\\_tech/](http://www.sparxsystems.com.au/resources/mdg_tech/).

]

[82 M. O. d. M. A. E. D. R. Á. Juan Carlos Nieves, "Harmonization of Semantic Data Models of Electric Data Standards," no. 12289578, 2011.

[83 D.-K. K. Byunghun Lee, "Harmonization IEC61850 and CIM for connectivity of substation automation," vol. 50, 2017.

[84 G. G. a. R. Bienert, "Smart Grids Standards and Systems Interoperability: A Precedent with OpenADR," no. LBNL-5273E, 2011.

[85 D. P. a. C.-S. i. t. S. G. E. Expert Group 2: Regulatory Recommendations for Privacy, "Data Protection Impact Assessment Template for Smart Grid and Smart Metering," Brussels, 2014.

[86 [Online]. Available: <http://smartgridstandardsmap.com/>.

]

[87 "D3.1 Smart grids reference architecture and data models v1," 2016.

]

[88 "CEN-CENELEC-ETSI Smart Grid Coordination Group Smart Grid Reference Architecture," 2012.

]

## 17.2 ACRONYMS

Table 76 - List of Acronyms

Acronyms List	
AMI	Advanced Metering Infrastructure
BA	Business Actor
BC	Business Case
BF	Business Function
BG	Business Goal
BMS	Building Management System
BP	Business Process
BRP	Balance Responsible Party
BS	Business Service
CEN-CENELEC	Comité Européen de Normalisation - Comité Européen de Normalisation Electrotechnique
CIM	Common Information Model
CIS	Customer Information System
CM	Conceptual Model
CSS	Customer Support System
DER	Distributed Energy Resource
DER	Distributed Energy Resources
DLMS/COSEM	Device Language Message Specification
DMS	Distribution Management System
DRMS	Demand Response Management System
EAI	Enterprise Application Integration
ECM	European Conceptual Model
EMS	Energy Management System
ERP	Enterprise Resource Planning
ESCO	Energy Service Company
EV	Electric Vehicle
EVP	Electric Vehicle Platform
EVSE	Electric Vehicle Supply Equipment
GIS	Geographical Information Systems
GOOSE	Generic Object Oriented Substation Event
HEM	Harmonized Electricity Market
HLUC	High Level Use Case
HTTP	Hyper Text Transfer Protocol
HVAC	High Voltage Alternating Current

## Acronyms List

ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
JSON	JavaScript Object Notation
JWG	Joint Working Group
LAN	Local Area Network
MDMS	Meter Data Management System
MG	Micro Grid
MMS	Manufacturing Message Specification
OCPP	Open Charge Point Protocol
OMG	Object Modelling Group
OMS	Outage Management System
OPC-UA	OPC Unified Architecture
OWL	Web Ontology Model
PEV	Plug-in Electric Vehicle
PUC	Primary Use Case
QVT	Query/View/Transformation standard
RA	Reference Architecture
RDF	Resource Description Framework
RESCO	Renewable Energy Service Company
REST	Representational State Transfer
RM	Role Model
RTU	Remote Terminal Unit
SAP	System Analysis Phase
SCADA	Supervisory Control And Data Acquisition
SG	Smart Grid
SGAM	Smart Grids Architecture Model
SMV	Sampled Measured Values
SOAP	Simple Object Access Protocol
SUC	Secondary Use Case
TCP/IP	Transmission Control Protocol / Internet Protocol
UC	Use Case
UML	Unified Modelling Language
USEF	Universal Smart Energy Framework
VPP	Virtual Power Plant
WAMS	Wide Area Monitoring System

#### Acronyms List

WAN	Wide Area Network
XML	Extensible Markup Language
XML	eXtensible Markup Language
XMPP	Extensible Messaging and Presence Protocol

## **18 APPENDIX A - ARCHITECTURE**

### **HL-UC 1: DISTRIBUTED RES INTEGRATION IN THE GRID**

## 18.1 HL-UC 1\_PUC\_1: NETWORK MONITORING

### 18.1.1 PRIMARY USE CASE DESCRIPTION

This PUC addresses the observability of the electricity distribution network in presence of RES. It has four main components. The first one deals with measurements acquisition (Voltage [U], Active Power [P], Reactive Power [Q] from nodes, P, Q from RES production connected to the nodes and P, Q from network sections or specific lines). The second one deals with the forecast of RES production, consumption and of total power flow in critical sections, based on the data already collected. The third component is looking to provide the DSO with the necessary mechanisms in order to calculate Key Performance Indicators (KPIs) to assess the correct operation of the grid. The fourth component is dealing with the big amount of data -field measurements, mainly- obtained from the Advance Metering Infrastructure (AMI) deployed in the grid during the scope of the project.

### 18.1.2 SECONDARY USE CASE DESCRIPTION

This PUC invokes several SUCs dealing with data collection and analysis.

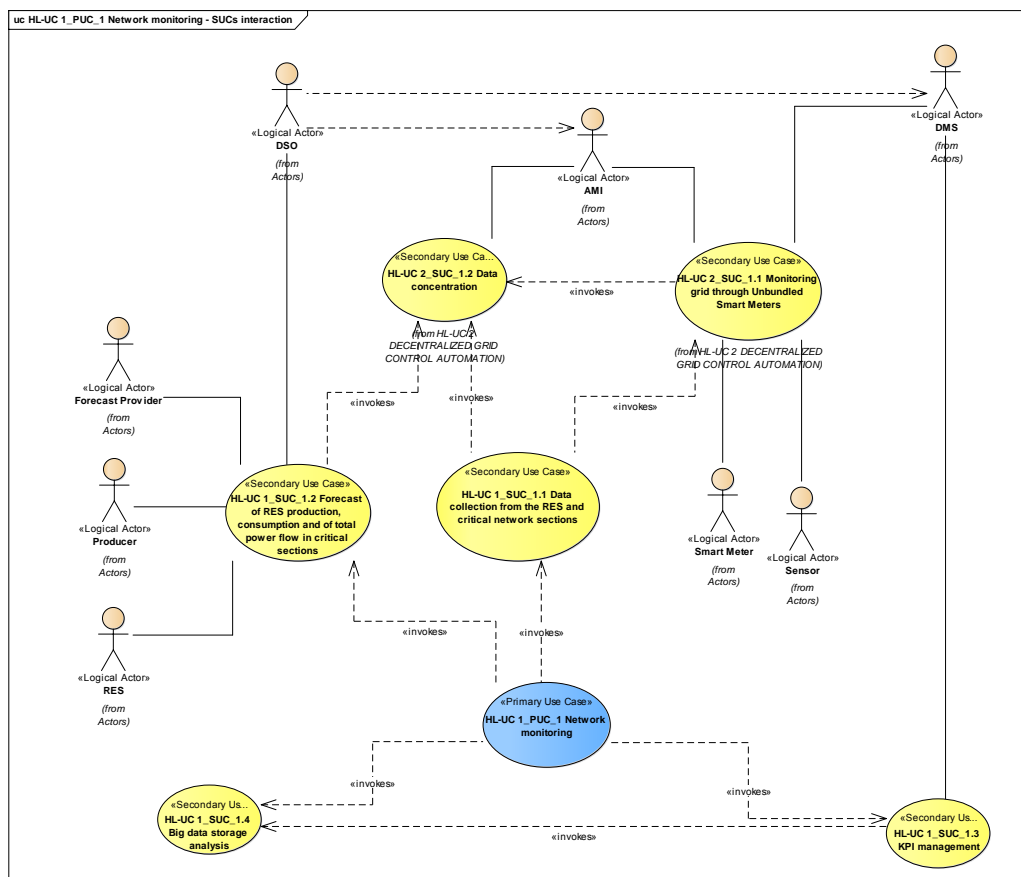


Figure 119 - SUCs Interactions Diagram

**Table 77 - Table of list of participating SUCs**

SUC Name	Description	Relation	PUC/SUC
HL-UC 1_SUC_1.1	Data collection from the RES and critical network sections	invokes	HL-UC 2_SUC_1.1 Monitoring grid through Unbundled Smart Meters HL-UC 2_SUC_1.2 Data concentration
HL-UC 1_SUC_1.2	Forecast of RES production, consumption and total power flow in critical sections	invokes	HL-UC 2_SUC_1.2 Data concentration
HL-UC 1_SUC_1.3	KPI Management	invokes	HL-UC 1_SUC_1.4 Big data storage analysis
HL-UC 1_SUC_1.4	Big data storage analysis		



The use case covers the whole chain of the *distribution* SGAM domain, since it includes operations related to collection of data (field, station and operation zones) and analysis (enterprise zone)



290

**Table 78 - List of Actors Involved**

Actor Name	Actor Type
AMI	System
DMS	System
DSO	Organization
Forecast provider	Organization
Sensor	Device
Smart meter	Device
RES	Device
Producer	Person

#### 18.1.4 SGAM COMPONENT LAYER

The main involved components identified are those elements used by the DSO related with the acquisition of the grid data. The main WiseGRID applications implementing this use case will be the WG IOP (as communication-enabling module) and the WiseGRID Cockpit (application for the DSO).

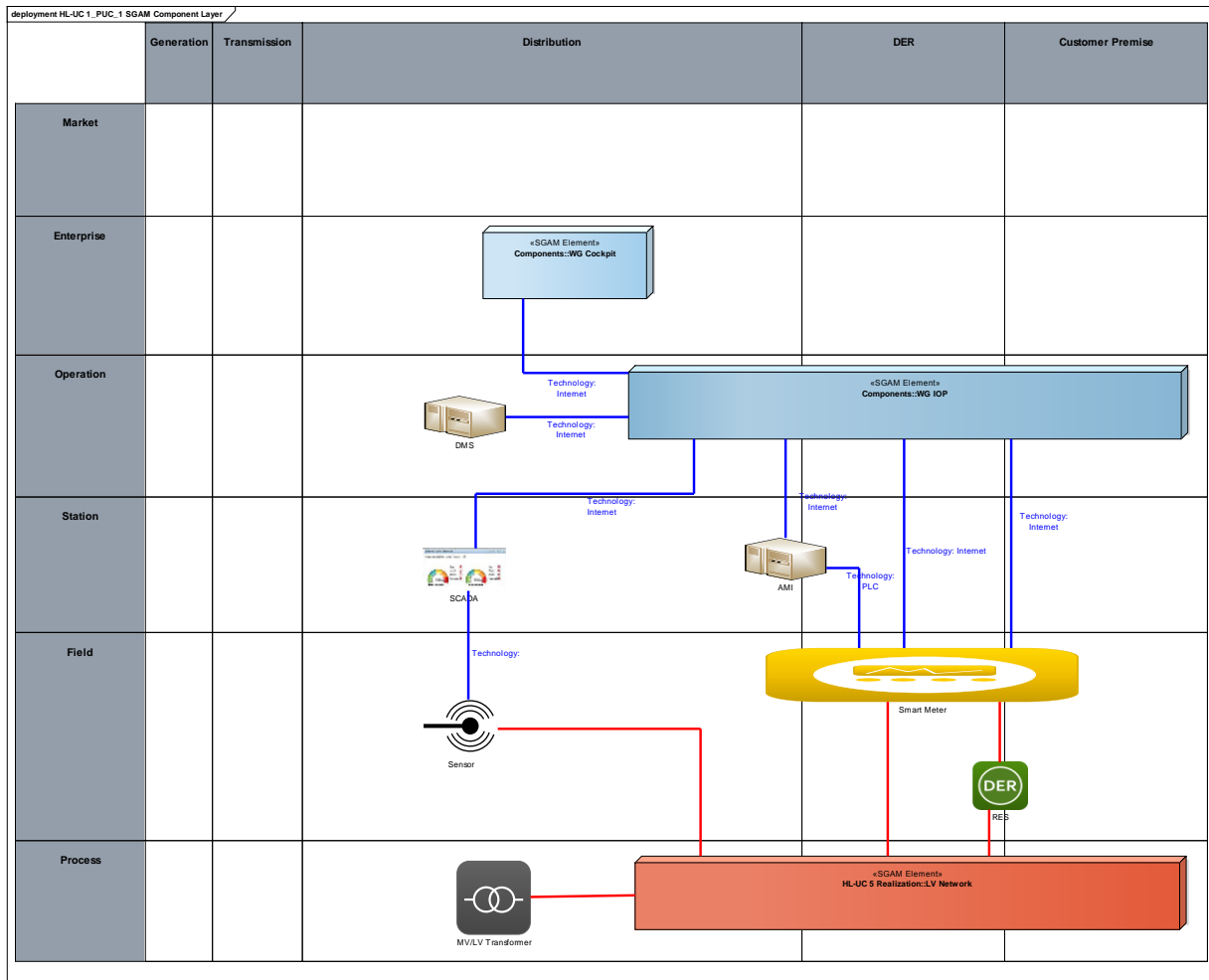


Figure 121 - SGAM Component Layer

**Table 79 - List of Components Participating in the Primary Use Case**

Component	Component Type
DMS	SGAM Element
AMI	SGAM Element
SCADA	SW Application
WG IOP	SGAM Element
WG Cockpit	SGAM Element
Smart meter	Smart meter
RES	SGAM Element
MV/LV Transformer	Transformer
LV Network	SGAM Element

### 18.1.5 SGAM COMMUNICATION LAYER

Communications identified can be divided in two different groups:

- Communication of already deployed field devices and control systems: include a variety of industrial and smart grid protocols
- Communications with WiseGRID components: include the protocols considered to be enabled by the WG IOP

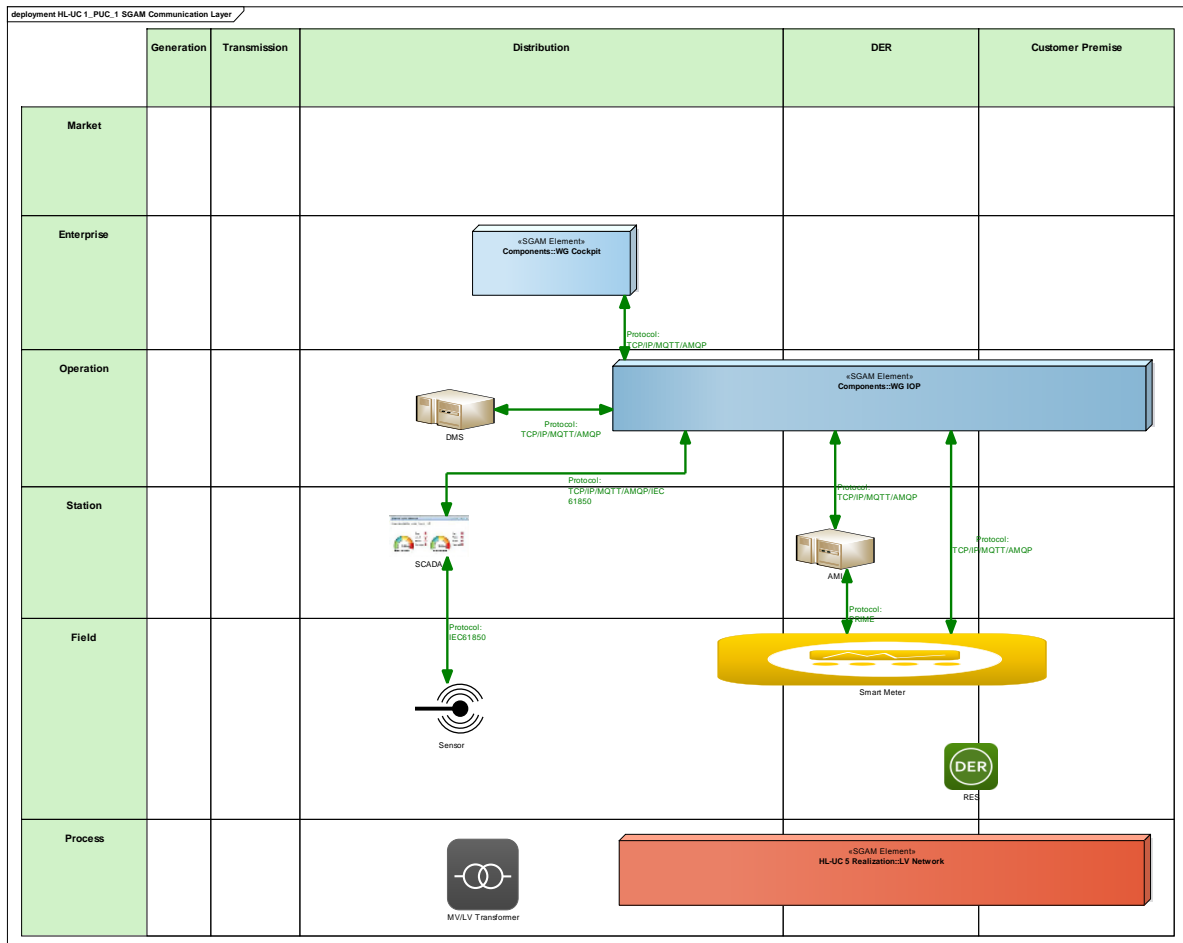


Figure 122 - SGAM Communication Layer

Table 80 - List of Communication Technologies Involved

Communication Technology	Description
TCP/IP	Group of protocols enabling communication between devices in a network up to the transport layer
MQTT	ISO standard (ISO/IEC PRF 20922) publish-subscribe-based lightweight messaging protocol for use on top of the TCP/IP protocol
AMQP	Open standard application layer protocol for message-oriented middleware, featuring message orientation, queuing, routing (including point-to-point and publish-and-subscribe), reliability and security

Communication Technology	Description
IEC61850	Standard for vendor-agnostic engineering of the configuration of Intelligent Electronic Devices for electrical substation automation systems
PRIME	Specification for narrow band powerline communication

Main information items handled within this PUC include energy metering data from different sections of the grid - MV grid, LV usage points, production units...



The identified canonical data models include those models related to energy metering.

<b>Data Models</b>
DLMS/COSEM
CIM

## STANDARDS AND INFORMATION OBJECT MAPPING

The identified data standards include those related to energy metering.

**Table 82 - List of Data Standards**

Data Standards
DLMS/COSEM
CIM

**Table 83 - List of Information Objects**

Information Objects	Data Model
Energy metering	DLMS/COSEM - CIM



### 18.1.7 ACTIVITY DIAGRAM

The activity diagram represents how the DSO retrieves the data from the actors producing it in order to process KPIs.

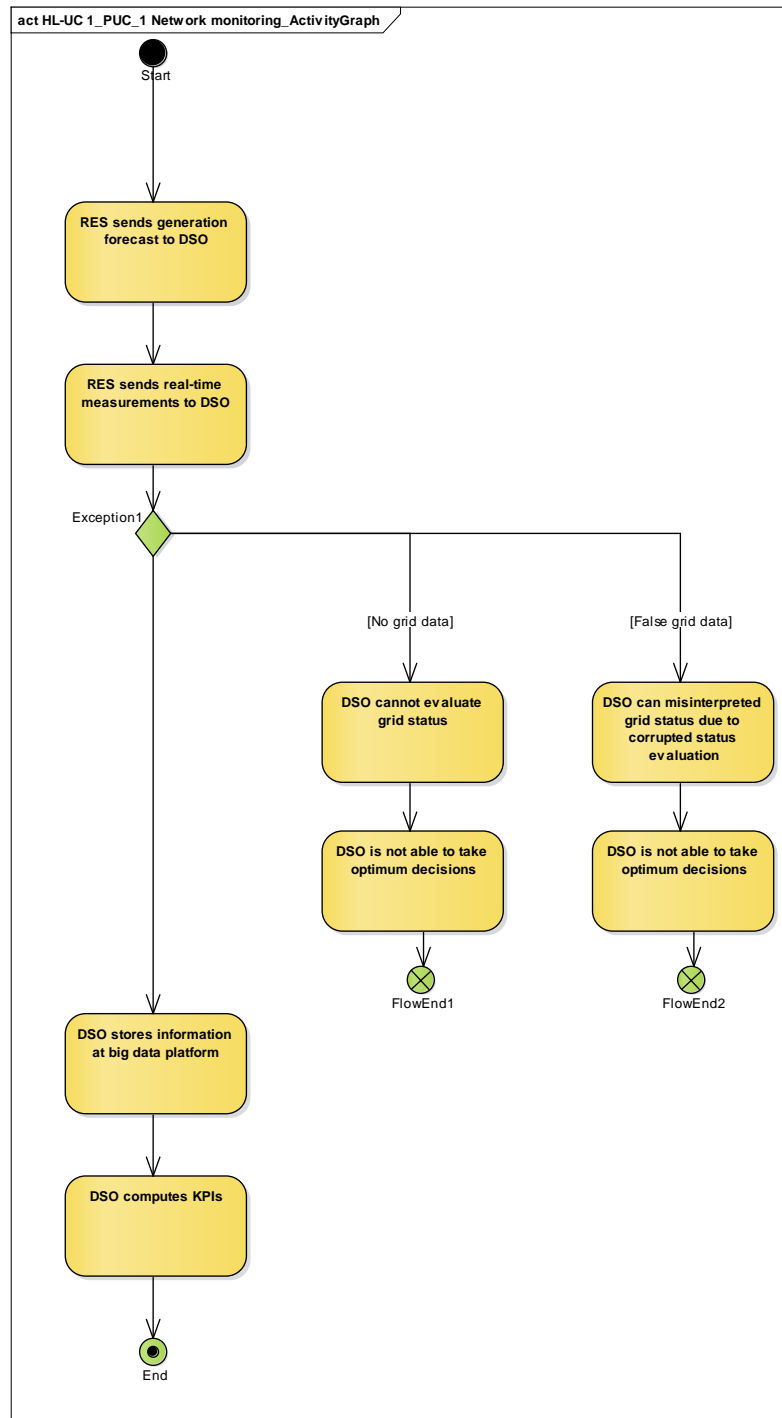


Figure 124 - Primary Use Case Activity Diagram

## 18.1.8 SEQUENCE DIAGRAM

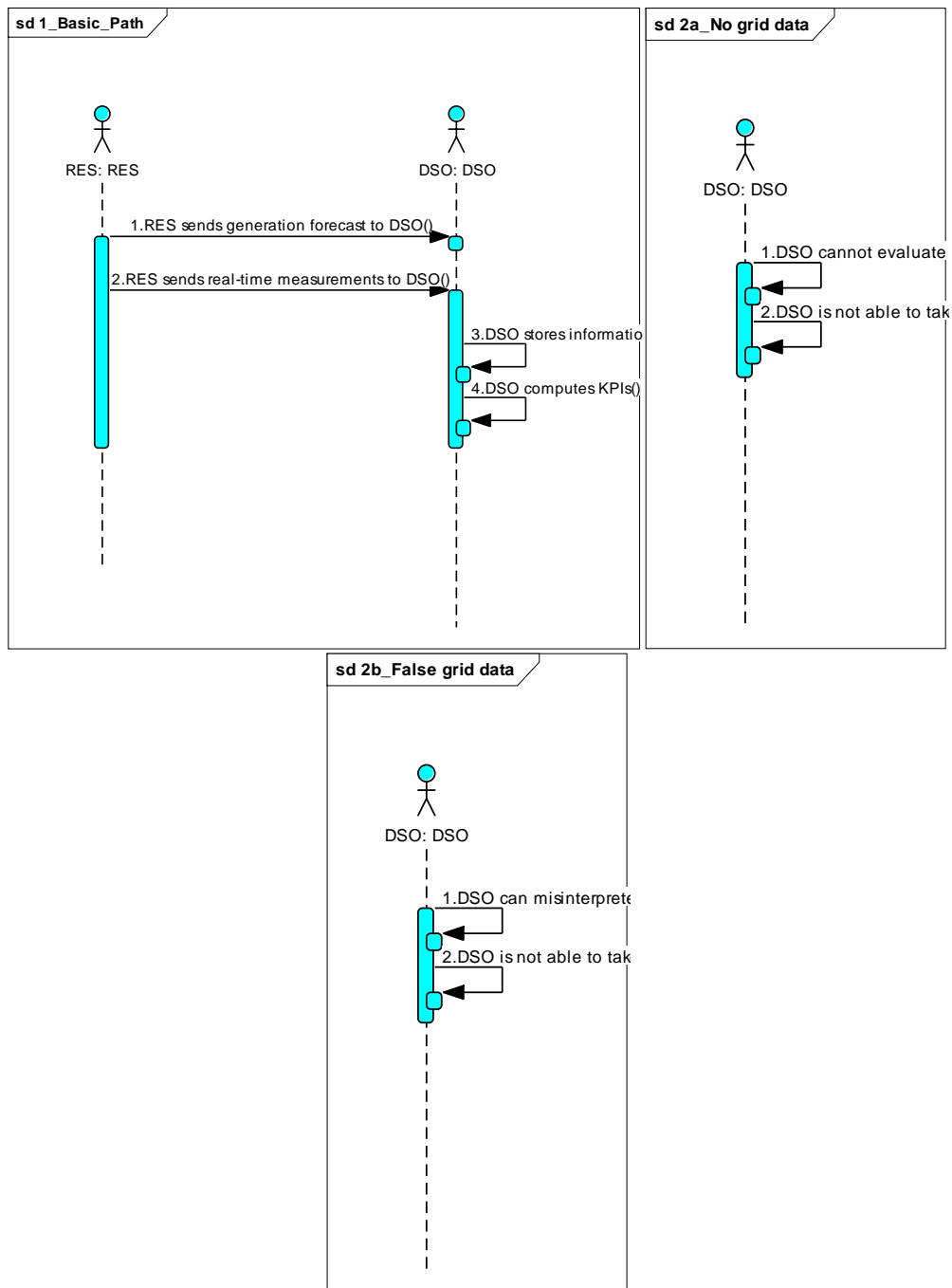


Figure 125 - Primary Use Case Sequence Diagram

## 18.2 HL-UC 1\_PUC\_2: CONTROL STRATEGIES FOR REDUCING RES CURTAILMENT

### 18.2.1 PRIMARY USE CASE DESCRIPTION

This PUC focuses on optimizing the general strategy of reducing or avoiding RES curtailment by using the relevant inputs from secondary use-cases, which have different technics in order to achieve the afore-mentioned goal. For this, all HL-UC 1\_SUC\_2.1 to HL-UC 1\_SUC\_2.4, are used as candidates for the optimization.

The main purpose is to find various solutions for solving the grid congestions by various means: stimulate local consumption, storage, use of V2G or other means, thus making a stable energy ecosystem which does not stress the grid and the system stability.

### 18.2.2 SECONDARY USE CASE INTERACTIONS

This PUC invokes several SUCs that describe different strategies that can be used to reduce RES curtailment

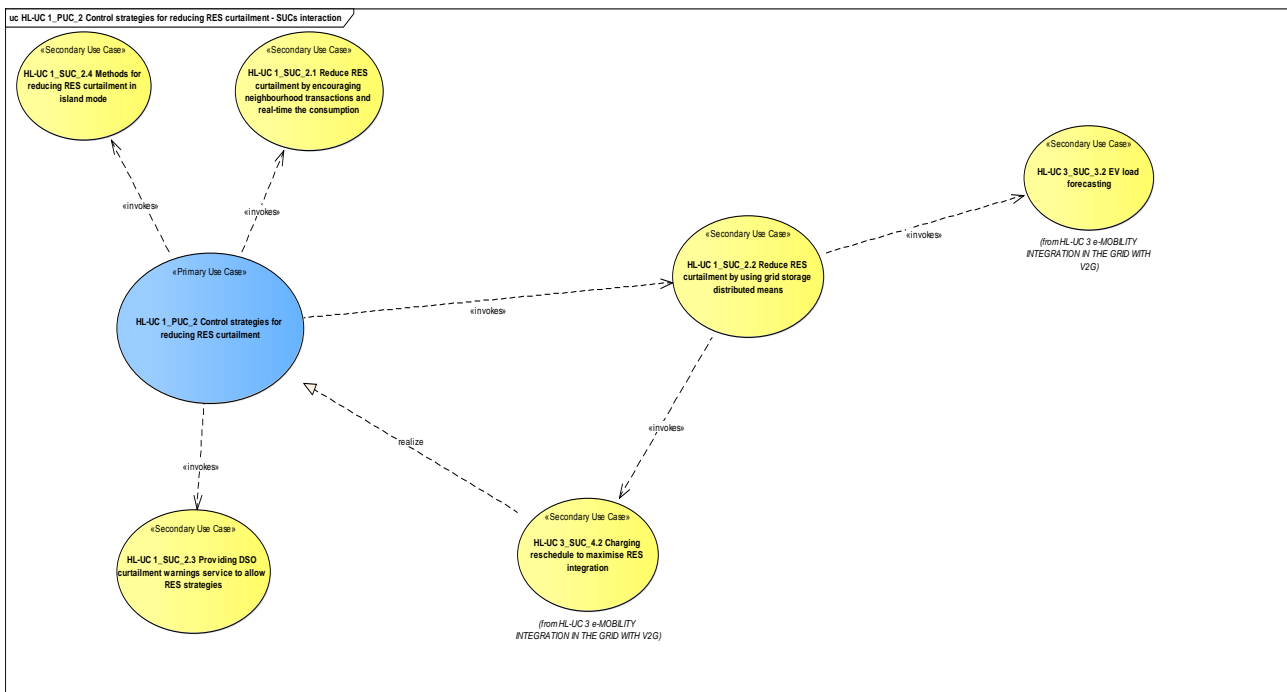


Figure 126 - SUCs Interactions Diagram

Table 84 - Table of list of participating SUCs

SUC Name	Description	Relation	PUC/SUC
HL-UC 1_SUC_2.1	Reduce RES curtailment by encouraging neighbourhood transactions and real-time consumption		
HL-UC 1_SUC_2.2	Reduce RES curtailment by using grid storage distributed means	invokes	HL-UC 2_SUC_3.2 EV load forecasting HL-UC 3_SUC_4.2 Charging reschedule to maximise RES integration

SUC Name	Description	Relation	PUC/SUC
HL-UC 1_SUC_2.3	Providing DSO curtailment warnings service to allow RES strategies		
HL-UC 1_SUX_2.4	Methods for reducing RES curtailment in island mode		

### 18.2.3 SGAM FUNCTION LAYER

This PUC mainly covers the operation zone of the distribution, RES and customer premise domains, since actors from all those domains are involved and capable of supporting the RES curtailment avoidance.

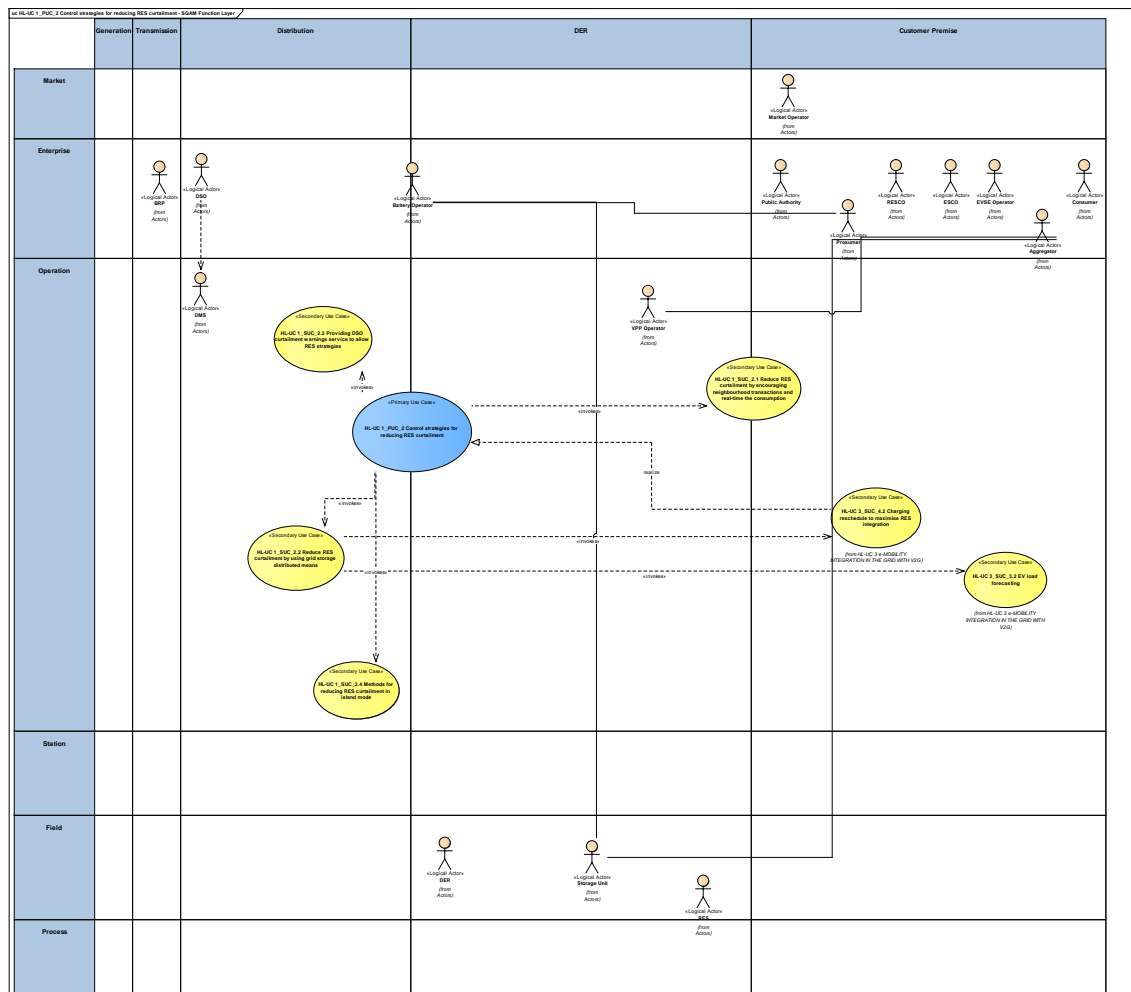


Figure 127 - SGAM Function Layer

**Table 85 - List of Actors Involved**

Actor Name	Actor Type
VPP Operator	Organization
BRP	Organization
Storage Unit	Device
Consumer	Person
Battery operator	Organization
Prosumer	Person
DSO	Organization
ESCO	Organization
RESCO	Organization
RES	Device
EV Fleet Manager	Organization
EVSE Operator	Organization
Forecast provider	Organization

#### 18.2.4 SGAM COMPONENT LAYER

As presented in the previous section, RES curtailment needs to be addressed by a broad set of actors, targeted by different WiseGRID applications - WG Cockpit, WG StaaS/VPP, WiseCOOP and WiseEVP. The architecture includes a central orchestration module - the Ancillary Services Market - in order to coordinate these collaborations.

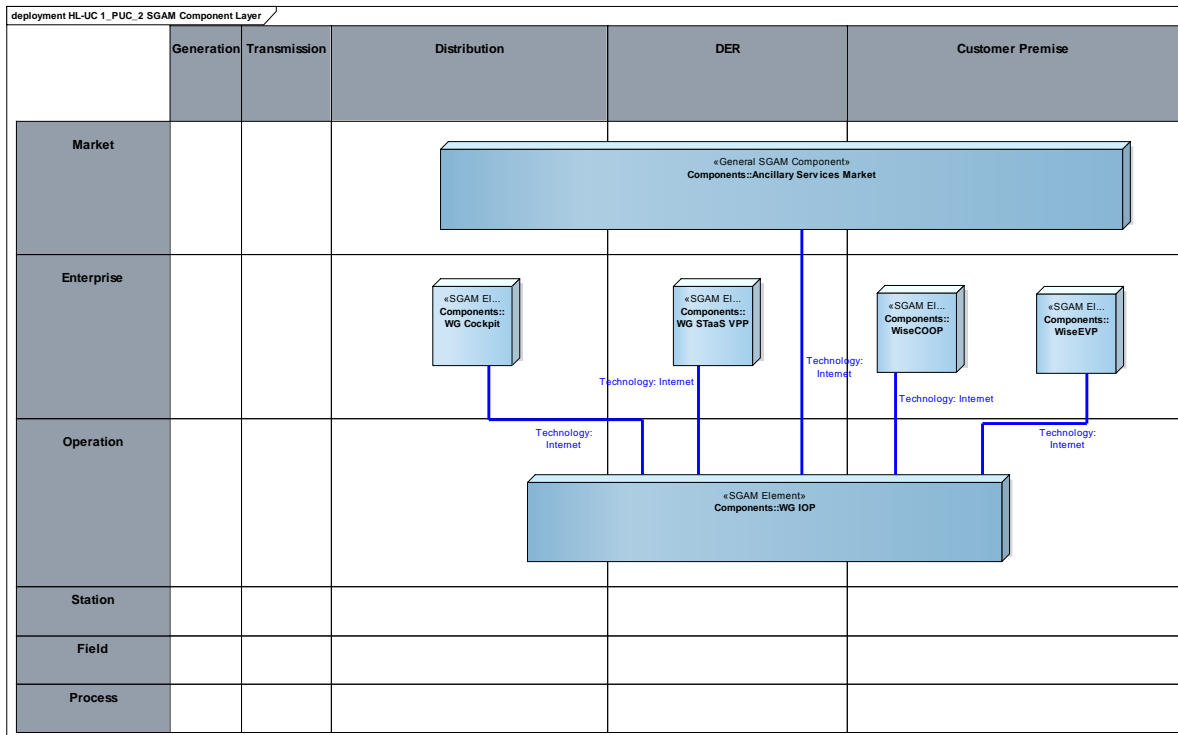


Figure 128 - SGAM Component Layer

Table 86 - List of Components Participating in the Primary Use Case

Component	Component Type
WG IOP	SGAM Element
WG Cockpit	SGAM Element
WG StaaS/VPP	SGAM Element
WiseCOOP	SGAM Element
WiseEVP	SGAM Element
Ancillary Services Market	General SGAM Component

### 18.2.5 SGAM COMMUNICATION LAYER

All communications considered in this PUC are enabled by the WG IOP.

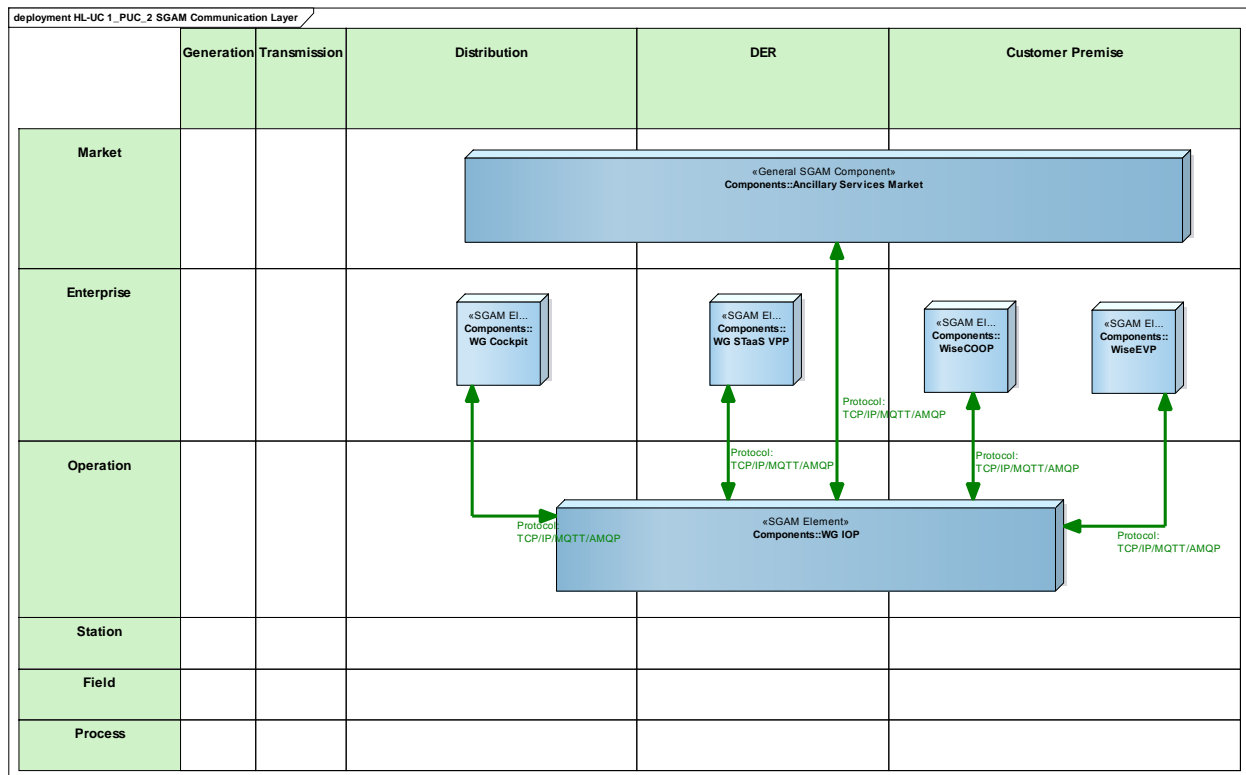


Figure 129 - SGAM Communication Layer

Table 87 - List of Communication Technologies Involved

Communication Technology	Description
TCP/IP	Group of protocols enabling communication between devices in a network up to the transport layer
MQTT	ISO standard (ISO/IEC PRF 20922) publish-subscribe-based lightweight messaging protocol for use on top of the TCP/IP protocol
AMQP	Open standard application layer protocol for message-oriented middleware, featuring message orientation, queuing, routing (including point-to-point and publish-and-subscribe), reliability and security

## 18.2.6 SGAM INFORMATION LAYER

Main information items handled within this PUC include the demand flexibility offered by the different applications, which is the main commodity exchanged to deal with modulation of the demand and avoidance of RES curtailment.

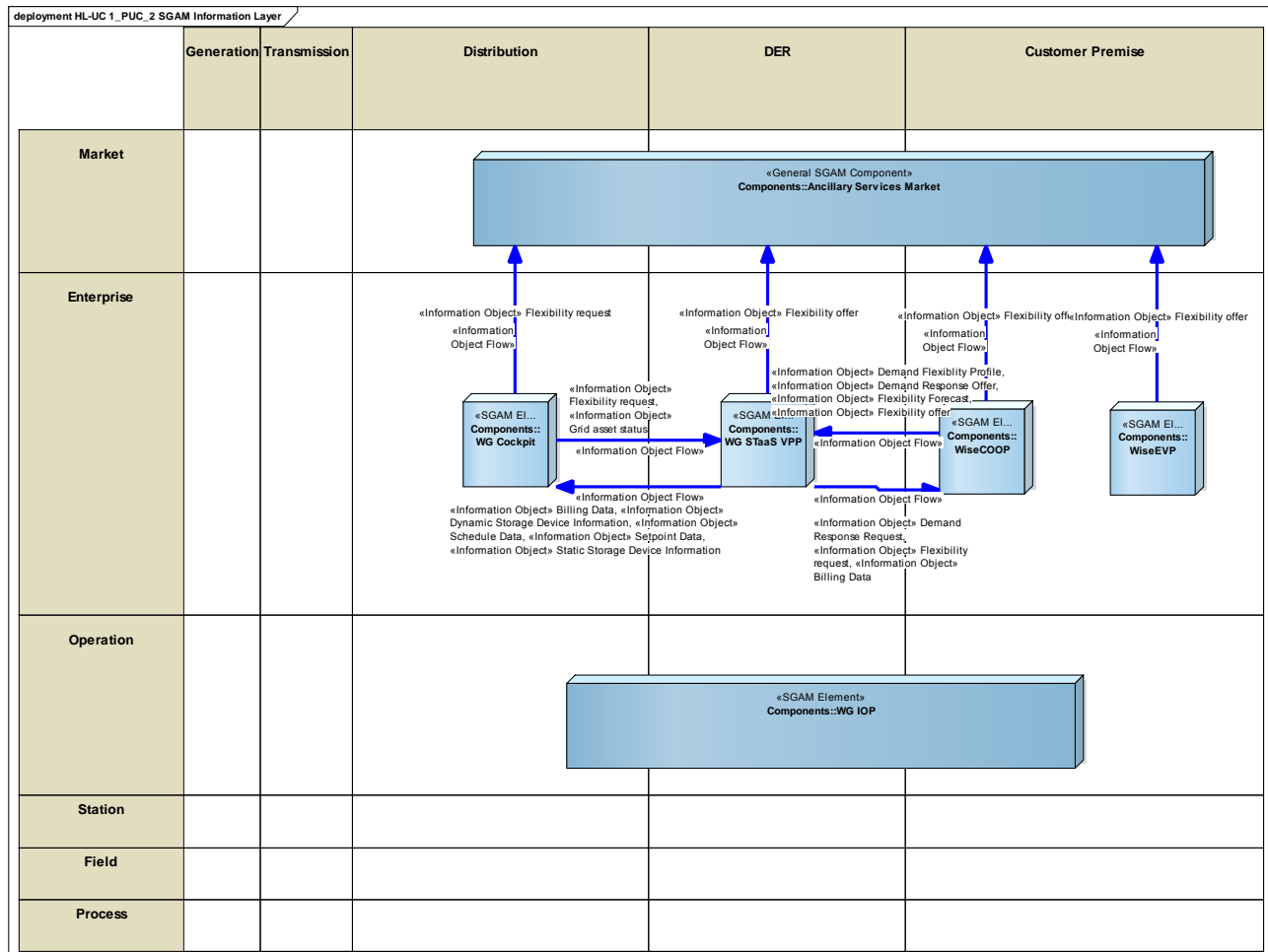


Figure 130 - SGAM Information Layer



## CANONICAL DATA MODEL

The identified canonical data models include those models related to definition of demand flexibility.

**Table 88 - List of Data Models**

Data Models
Flexibility data model (USEF)

## STANDARDS AND INFORMATION OBJECT MAPPING

The identified standards include those related to definition of demand flexibility and demand response signaling.

**Table 89 - List of Data Standards**

Data Standards
Flexibility data model (USEF)

**Table 90 - List of Information Objects**

Information Objects	Data Model
Demand flexibility profile	Flexibility data model (USEF)
DR Signal	Flexibility data model (USEF)
Demand Response request	Flexibility data model (USEF)
Flexibility offer	Flexibility data model (USEF)
Flexibility request	Flexibility data model (USEF)

### 18.2.7 ACTIVITY DIAGRAM

The activity diagram shows the different actions triggered by the DSO to different actors in order to apply the different strategies for preventing RES curtailment.

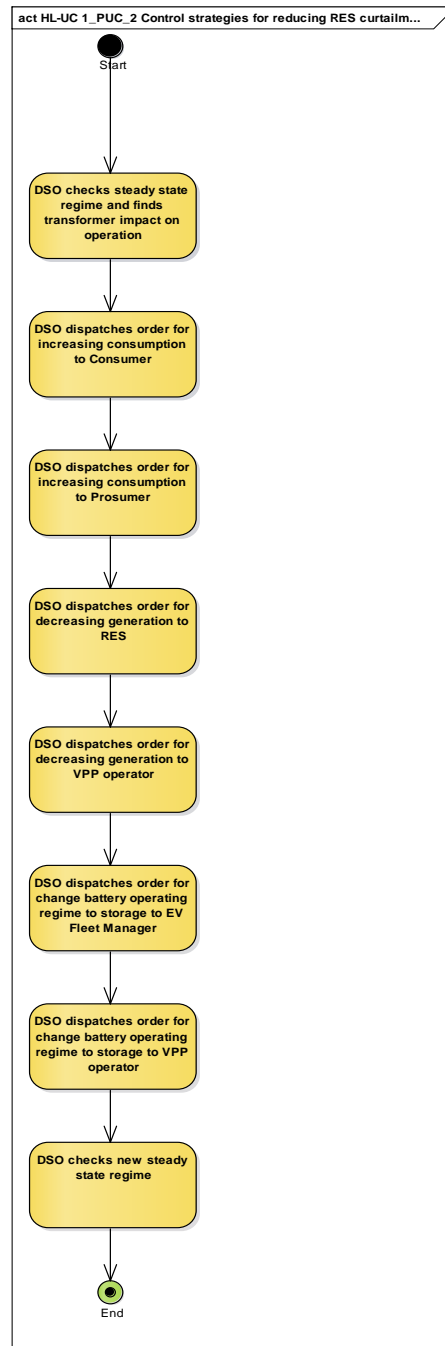


Figure 131 - Primary Use Case Activity Diagram

## 18.2.8 SEQUENCE DIAGRAM

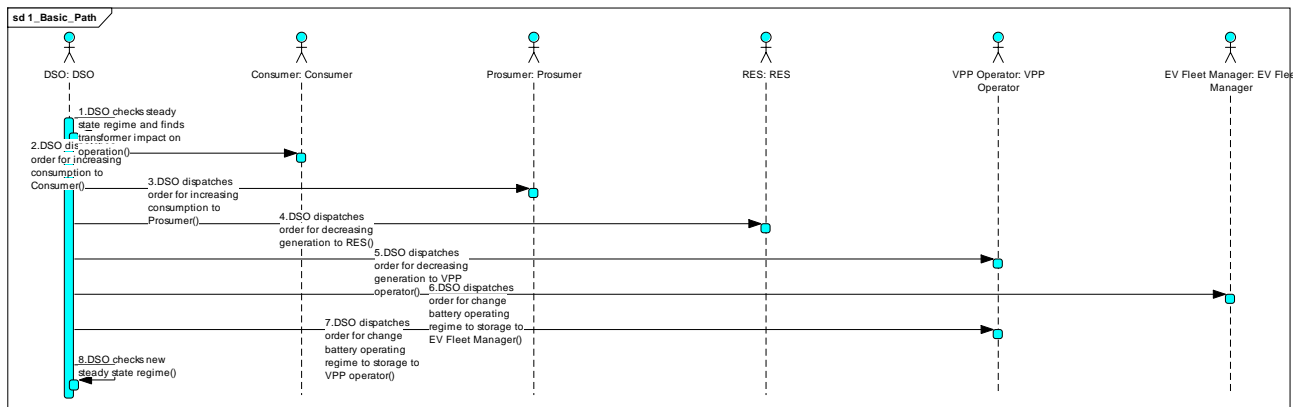


Figure 132 - Primary Use Case Sequence Diagram

## 18.3 HL-UC 1\_PUC\_3: VOLTAGE SUPPORT AND CONGESTION MANAGEMENT

### 18.3.1 PRIMARY USE CASE DESCRIPTION

In this PUC global and local methods are demonstrated, aiming to keep the voltage level in accepted boundaries. Network losses are reduced and possible network congestions should be signaled. These important activities must be performed diligently, through centralized and decentralized voltage control solutions

### 18.3.2 SECONDARY USE CASE INTERACTIONS

The interaction of the Secondary Use Cases for this Primary Use Case are depicted below.

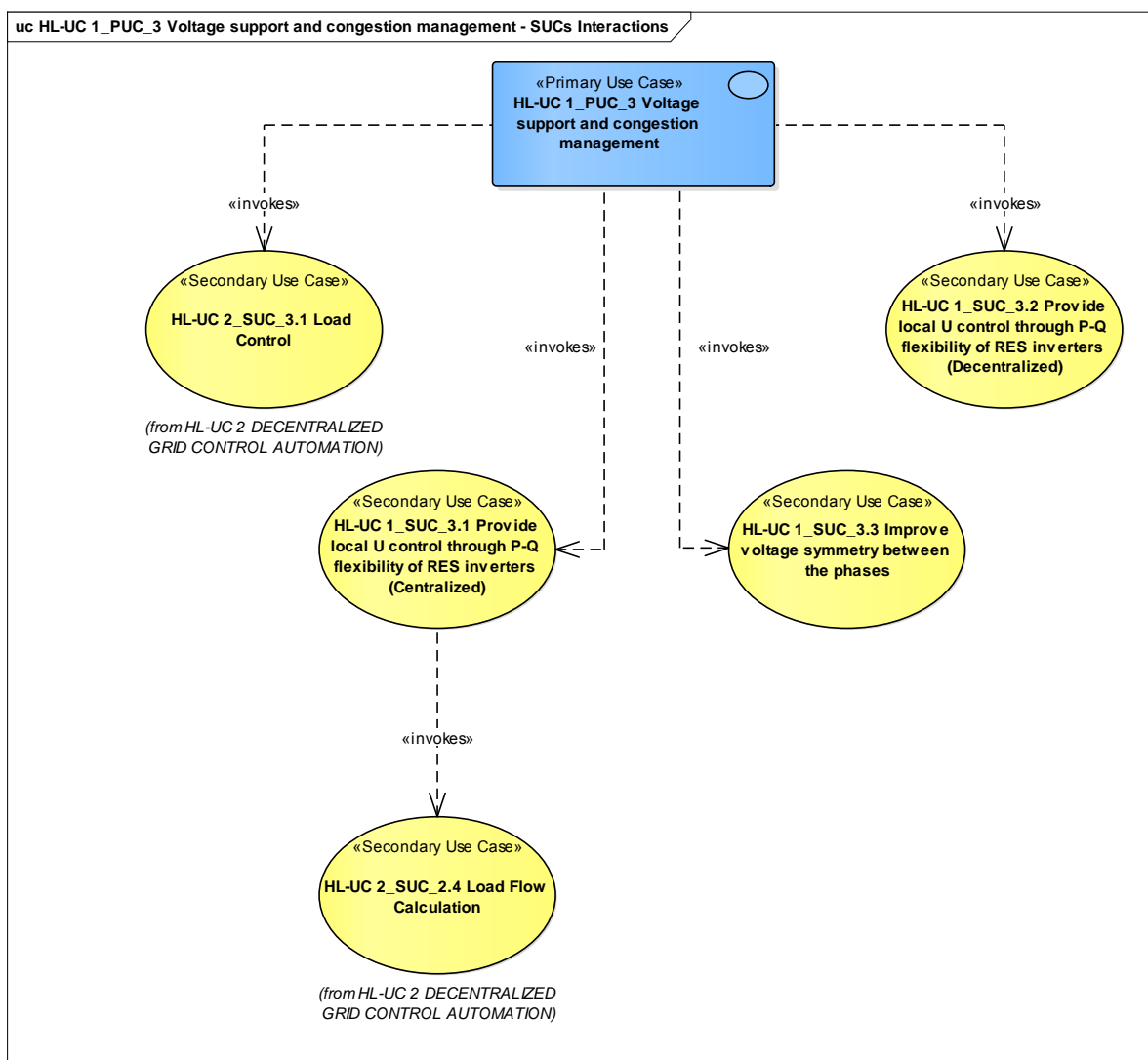


Figure 133 - SUCs Interactions Diagram

**Table 91 - Table of list of participating SUCs**

SUC Name	Description	Relation	PUC/SUC
HL-UC 1_SUC_3.1	This SUC will provide a local U control through flexibility of RES inverters (centralized voltage control coordinated by a Dispatch centre)	invokes	HL-UC 2_SUC_2.4 Load Flow Calculation
HL-UC 1_SUC_3.2	SUC demonstrates the possibility of improving the voltage level by using local loops of automation for the available RES units in the area (decentralized voltage control)		
HL-UC 1_SUC_3.3	SUC aims to improve voltage level quality and loss reduction by controlling reactive power in on each phase and modulating active power between phases.		
HL-UC 2_SUC3.1	SUC deals with the management and operation of conventional loads (DSO periodical monitoring)		

### 18.3.3 SGAM FUNCTION LAYER

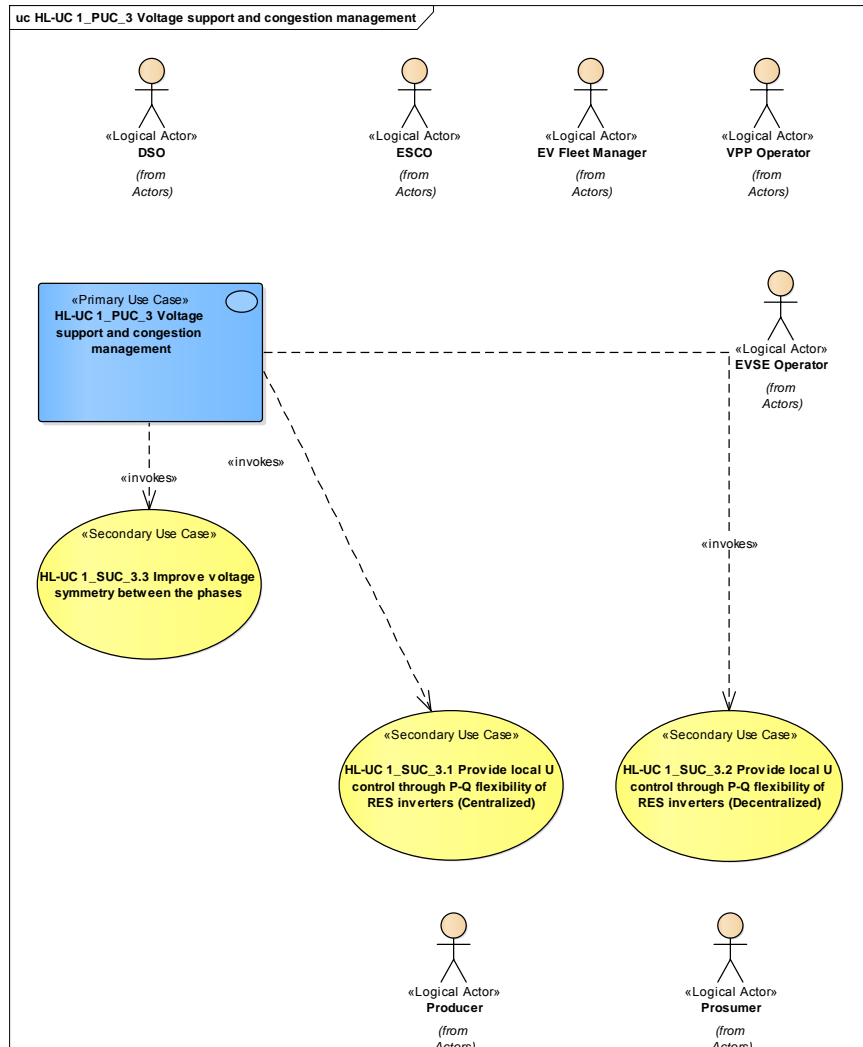


Figure 134 - SGAM Function Layer

Table 92 - List of Actors Involved

Actor Name	Actor Type
DSO	Organization
ESCO	Organization
EV Fleet Manager	Organization
VPP Operator	Organization
EVSE Operator	Organization
Producer	Person
Prosumer	Person

### 18.3.4 SGAM COMPONENT LAYER

The SGAM component layer for the Primary Use Case is shown below.

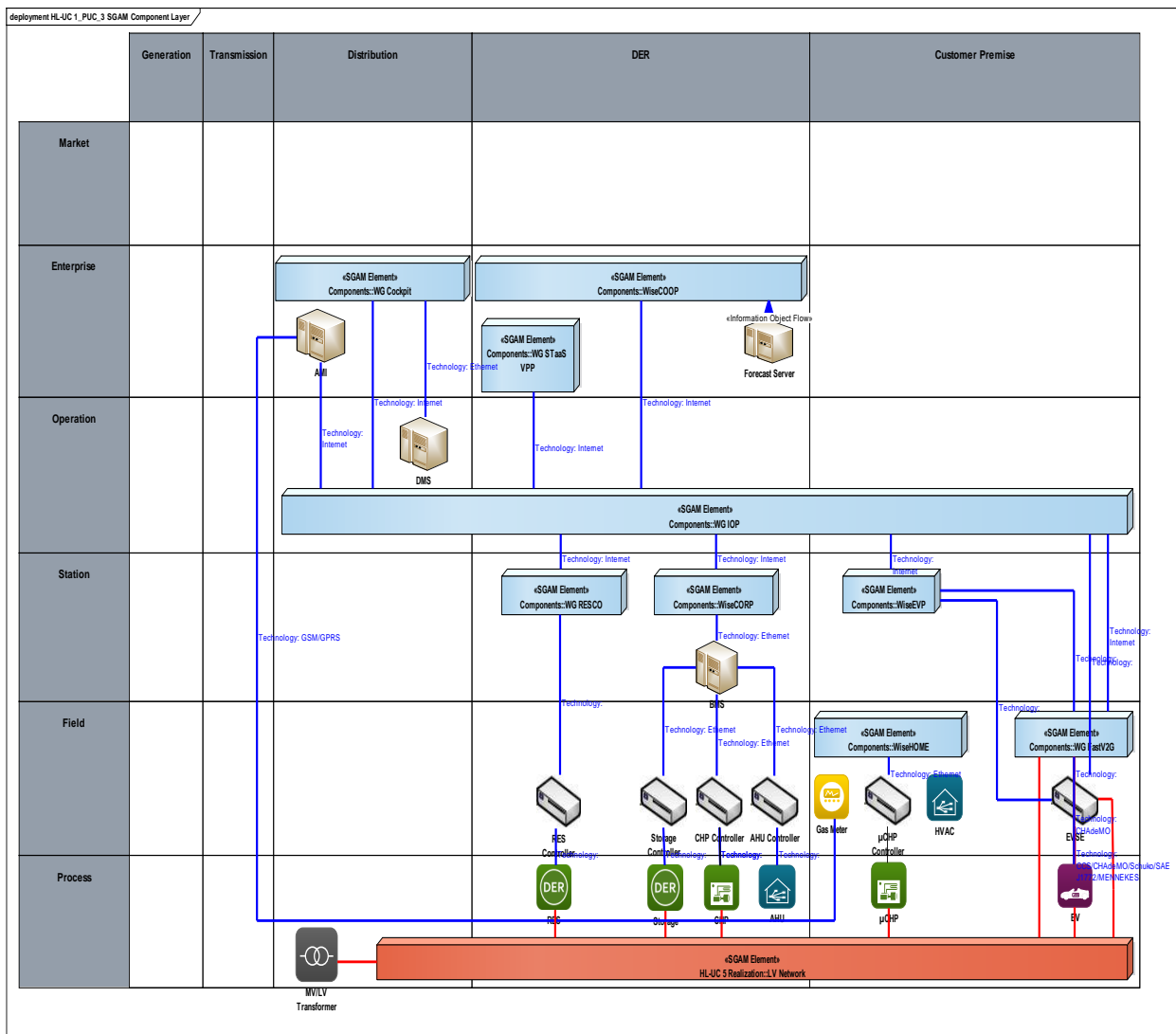


Figure 135 - SGAM Component Layer

Table 93 - List of Components Participating in the Primary Use Case

Component	Component Type
WG IOP	SGAM Element
WG Cockpit	SGAM Element
WG STaaS/VPP	SGAM Element
WiseCOOP	SGAM Element
WG RESCO	SGAM Element
WiseCORP	SGAM Element
WiseEVP	SGAM Element
WiseHOME	SGAM Element
WG FastV2G	SGAM Element

### 18.3.5 SGAM COMMUNICATION LAYER

The SGAM communication layer for the Primary Use Case is shown below.

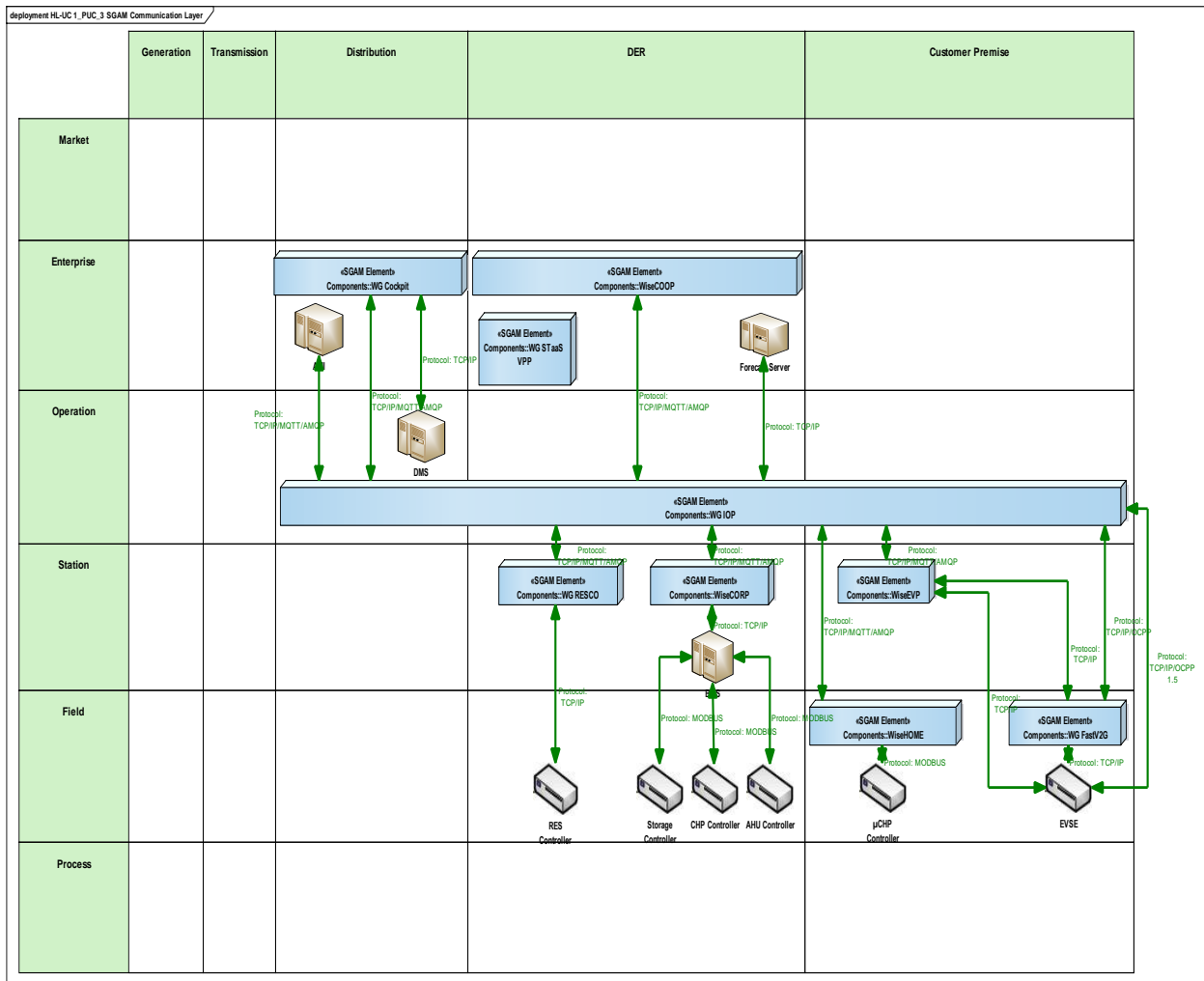


Figure 136 - SGAM Communication Layer

Table 94 - List of Communication Technologies Involved

Communication Technology	Description
TCP/IP	Group of protocols enabling communication between devices in a network up to the transport layer
MQTT	ISO standard (ISO/IEC PRF 20922) publish-subscribe-based lightweight messaging protocol for use on top of the TCP/IP protocol
AMQP	Open standard application layer protocol for message-oriented middleware, featuring message orientation, queuing, routing (including point-to-point and publish-and-subscribe), reliability and security
OCPP	Application protocol for communication between EV charging stations and a central management system
OCPP1.5	The Open Charge Point Protocol is an open standard which describes a method enabling electrical vehicles to communicate with a central system.



Communication Technology	Description
MODBUS	Serial communications protocol originally published for use with programmable logic controllers (PLCs). Simple and robust, it has become a de facto standard communication protocol and is now a commonly available means of connecting industrial electronic devices



## CANONICAL DATA MODEL

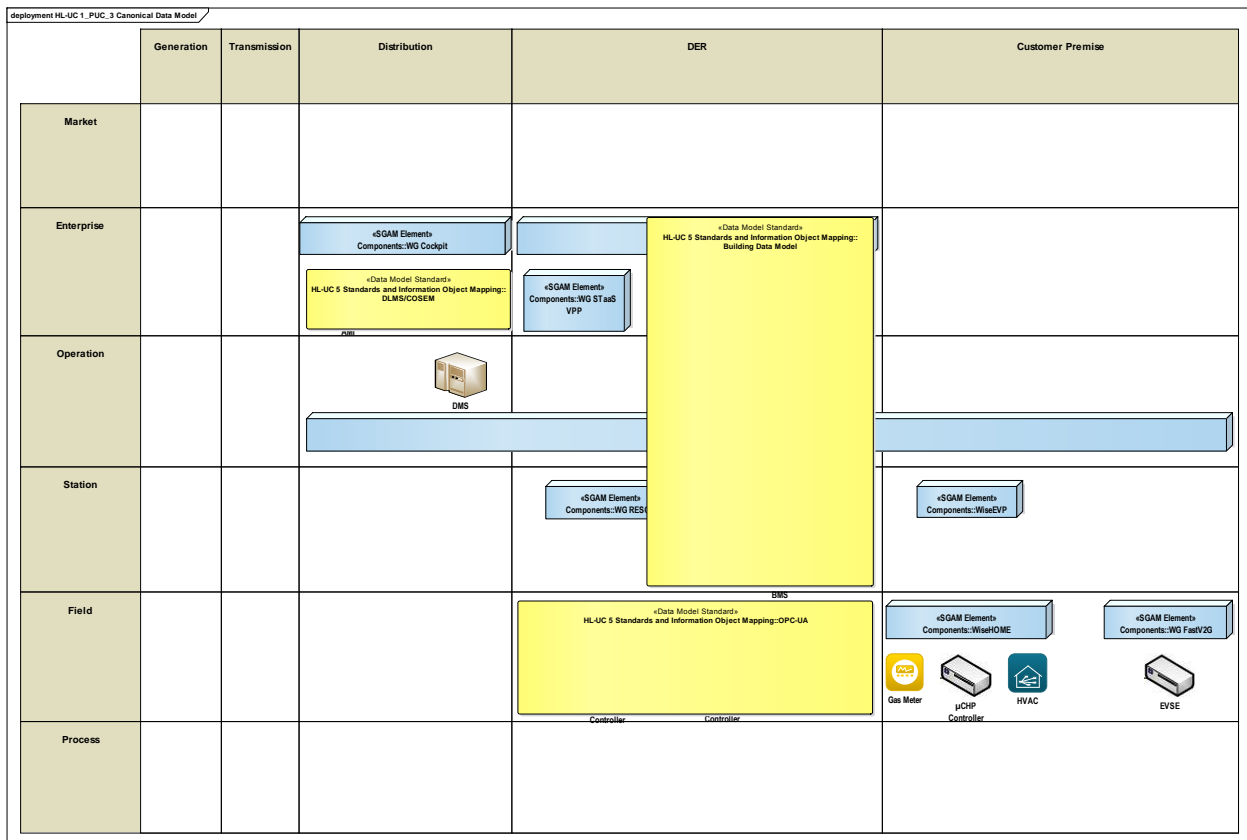


Figure 138 - Canonical Data Model diagram

Table 95 - List of Data Models

Data Models
Building Data Model
DLMS/COSEM
OPC-UA

## STANDARDS AND INFORMATION OBJECT MAPPING

The standards and information object mappings associated with the Primary Use Case are shown below.

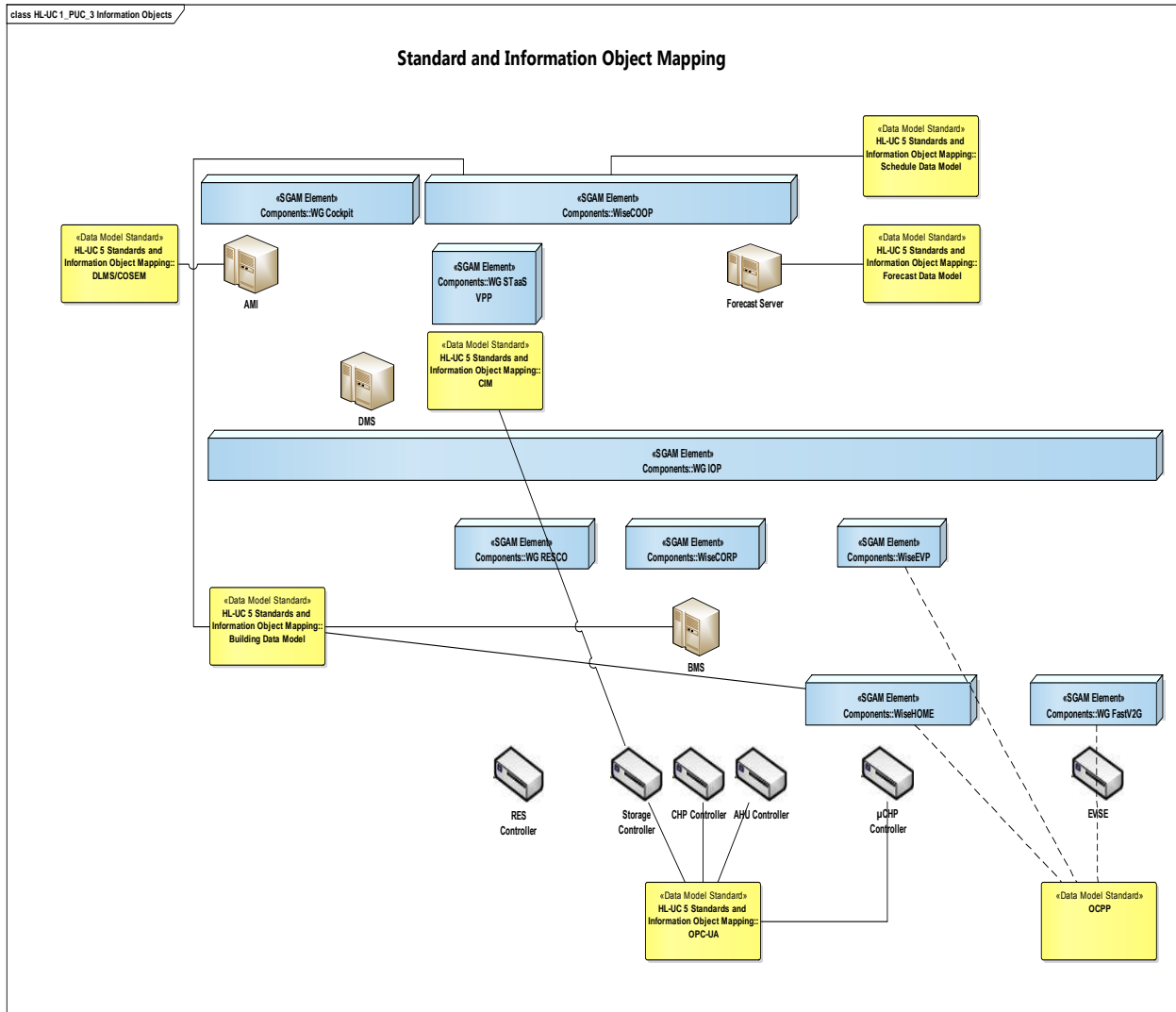


Figure 139 - Standard and information object mapping diagram

Data Standards
DLMS/COSEM
Schedule Data Model
Forecast Data Model
CIM
Building Data Model
OPC-UA
OCPP

**Table 96 - List of Information Objects**

### 18.3.7 ACTIVITY DIAGRAM

The activity diagram for the Primary Use Case is shown below.

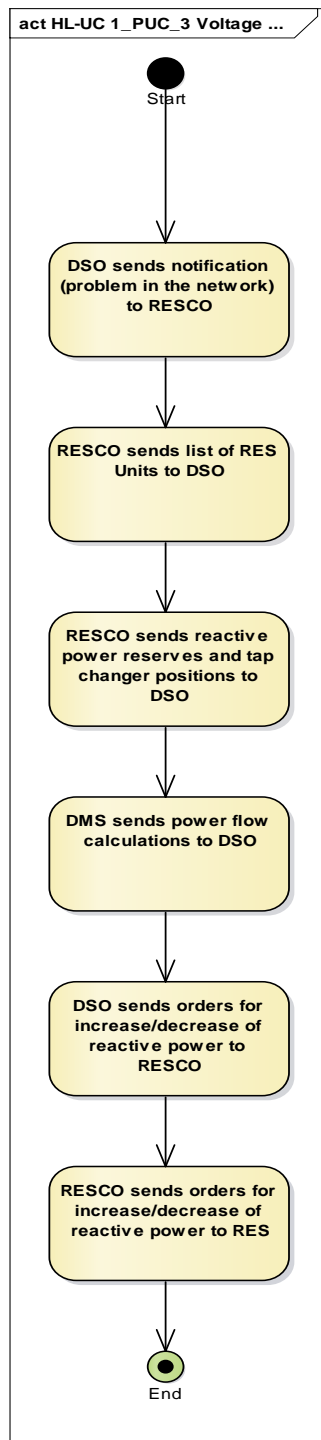


Figure 140 - Primary Use Case Activity Diagram

### 18.3.8 SEQUENCE DIAGRAM

The sequence diagram for the Primary Use Case is shown below.

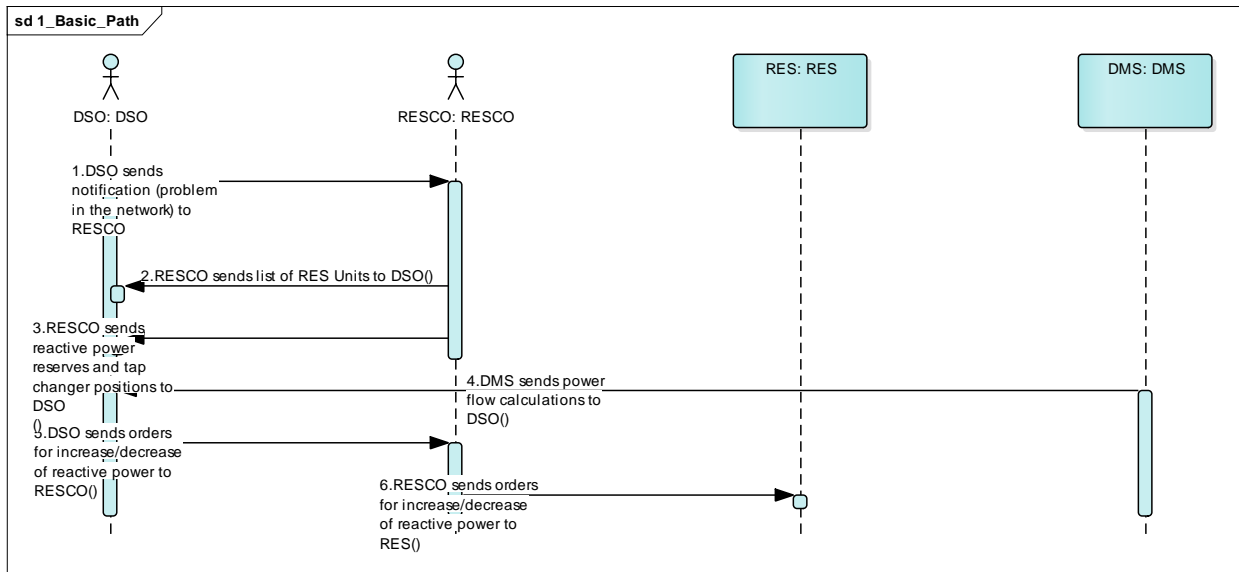


Figure 141 - Primary Use Case Sequence Diagram

## 18.4 HL-UC 1\_PUC\_4: GRID PLANNING ANALYSIS

### 18.4.1 PRIMARY USE CASE DESCRIPTION

The objective of this PUC is to provide to DSOs tools for the grid planning activities. Indicative examples of possible topics that need to be addressed are the following:

- Where is storage needed?
- What type of storage is needed?
- Where should public EVSEs be more convenient installed?

### 18.4.2 SECONDARY USE CASE INTERACTIONS

This PUC considers two different SUCs describing the simulation of EV-related and RES and storage-related scenarios. No further interaction with other SUCs has been identified.



Figure 142 - SUCs Interactions Diagram



Table 97 - Table of list of participating SUCs

SUC Name	Description	Relation	PUC/SUC
HL-UC 1_SUC_4.1	EV charge points planning analysis		
HL-UC 1_SUC_4.2	Grid storage planning analysis		

### 18.4.3 SGAM FUNCTION LAYER

Since the PUC describes planning functionalities to be used by DSOs, all use cases fall into the enterprise zone of the distribution domain.

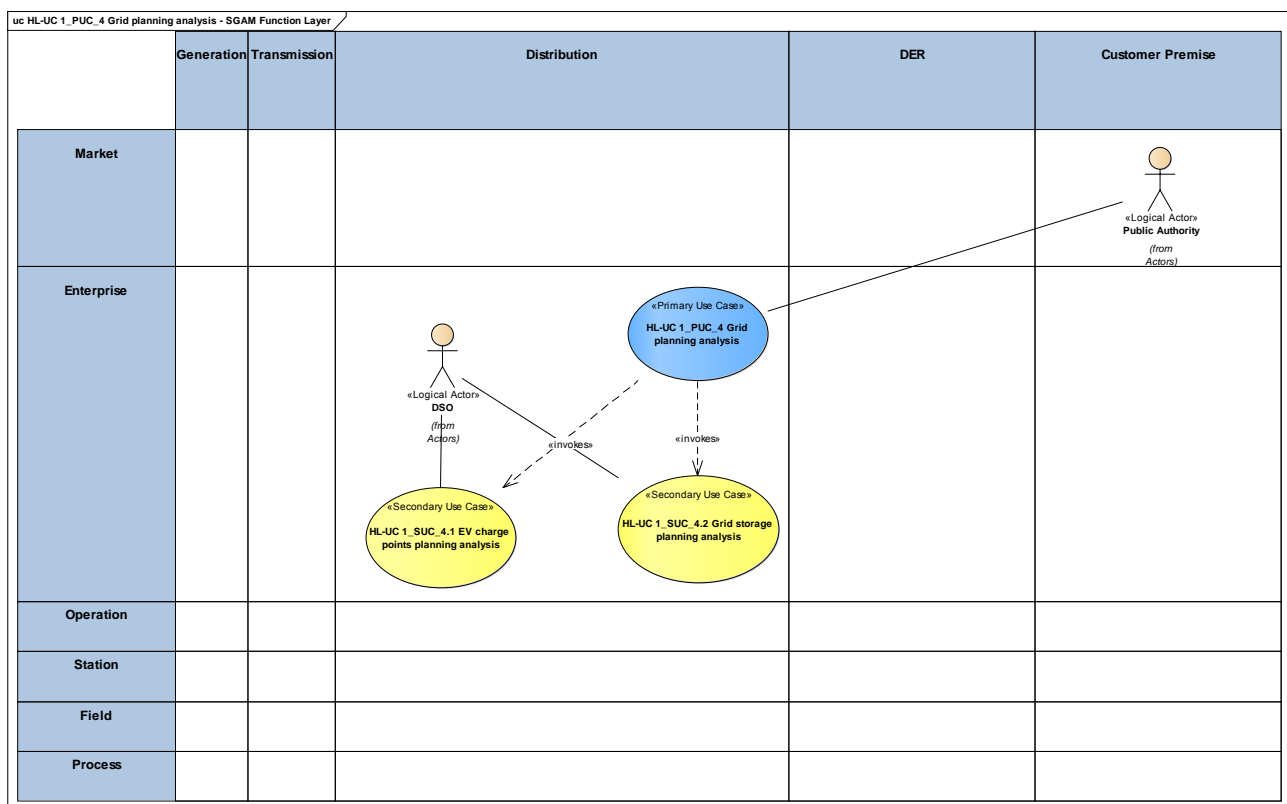


Figure 143 - SGAM Function Layer

Table 98 - List of Actors Involved

Actor Name	Actor Type
Public authority	Organization
DSO	Organization

#### 18.4.4 SGAM COMPONENT LAYER

The features described within this PUC will be implemented as part of the WG Cockpit. This application will mainly use information coming from the SCADA and GIS systems, retrieved via the WG IOP.

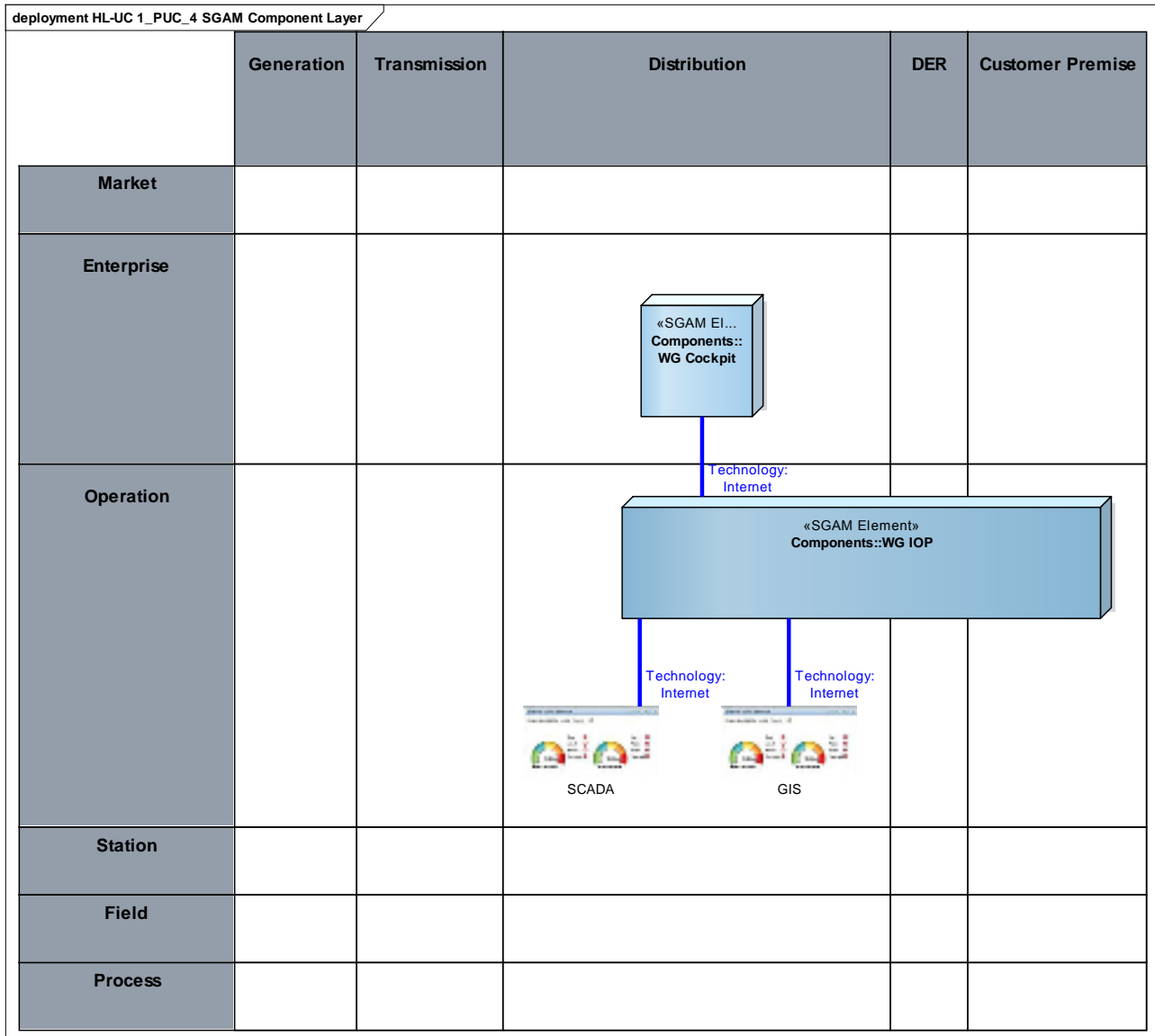


Figure 144 - SGAM Component Layer

Table 99 - List of Components Participating in the Primary Use Case

Component	Component Type
WG Cockpit	SGAM Element
WG IOP	SGAM element
SCADA	SW Application
GIS	SW Application

#### 18.4.5 SGAM COMMUNICATION LAYER

Data from SCADA and GIS will be retrieved by the corresponding adaptors and published to the WG IOP, which will redirect it to the WG Cockpit. Analysis and visualization of results will happen within the WG Cockpit application.

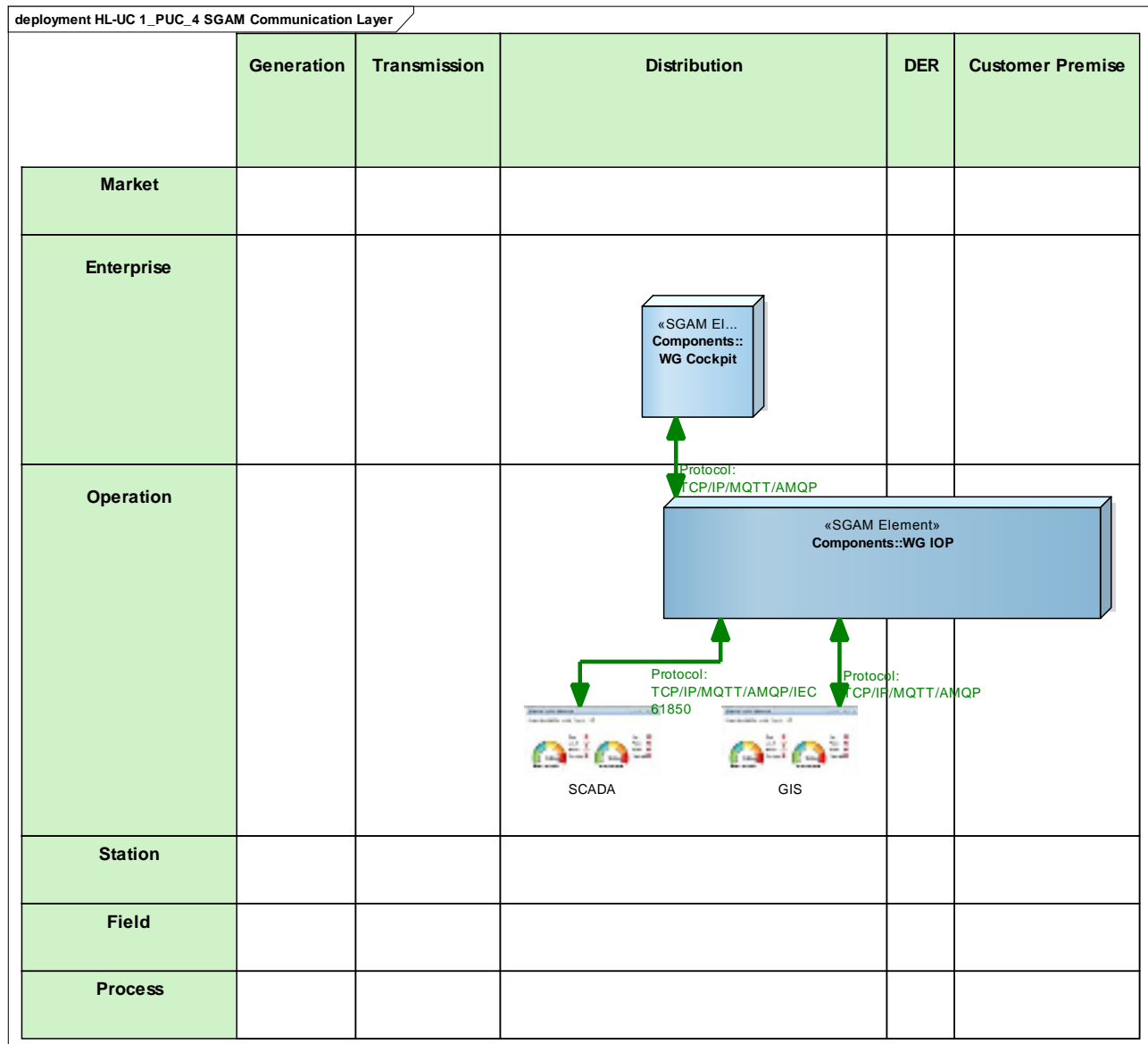


Figure 145 - SGAM Communication Layer

Table 100 - List of Communication Technologies Involved

Communication Technology	Description
TCP/IP	Group of protocols enabling communication between devices in a network up to the transport layer

Communication Technology	Description
MQTT	ISO standard (ISO/IEC PRF 20922) publish-subscribe-based lightweight messaging protocol for use on top of the TCP/IP protocol
AMQP	Open standard application layer protocol for message-oriented middleware, featuring message orientation, queuing, routing (including point-to-point and publish-and-subscribe), reliability and security
IEC61850	Standard for vendor-agnostic engineering of the configuration of Intelligent Electronic Devices for electrical substation automation systems

### 18.4.6 SGAM INFORMATION LAYER

Main information needed by the WG Cockpit in order to perform the simulations for grid planning assistance includes historical energy readings, topology of the grid and asset geolocation (for proper visualization of the results).

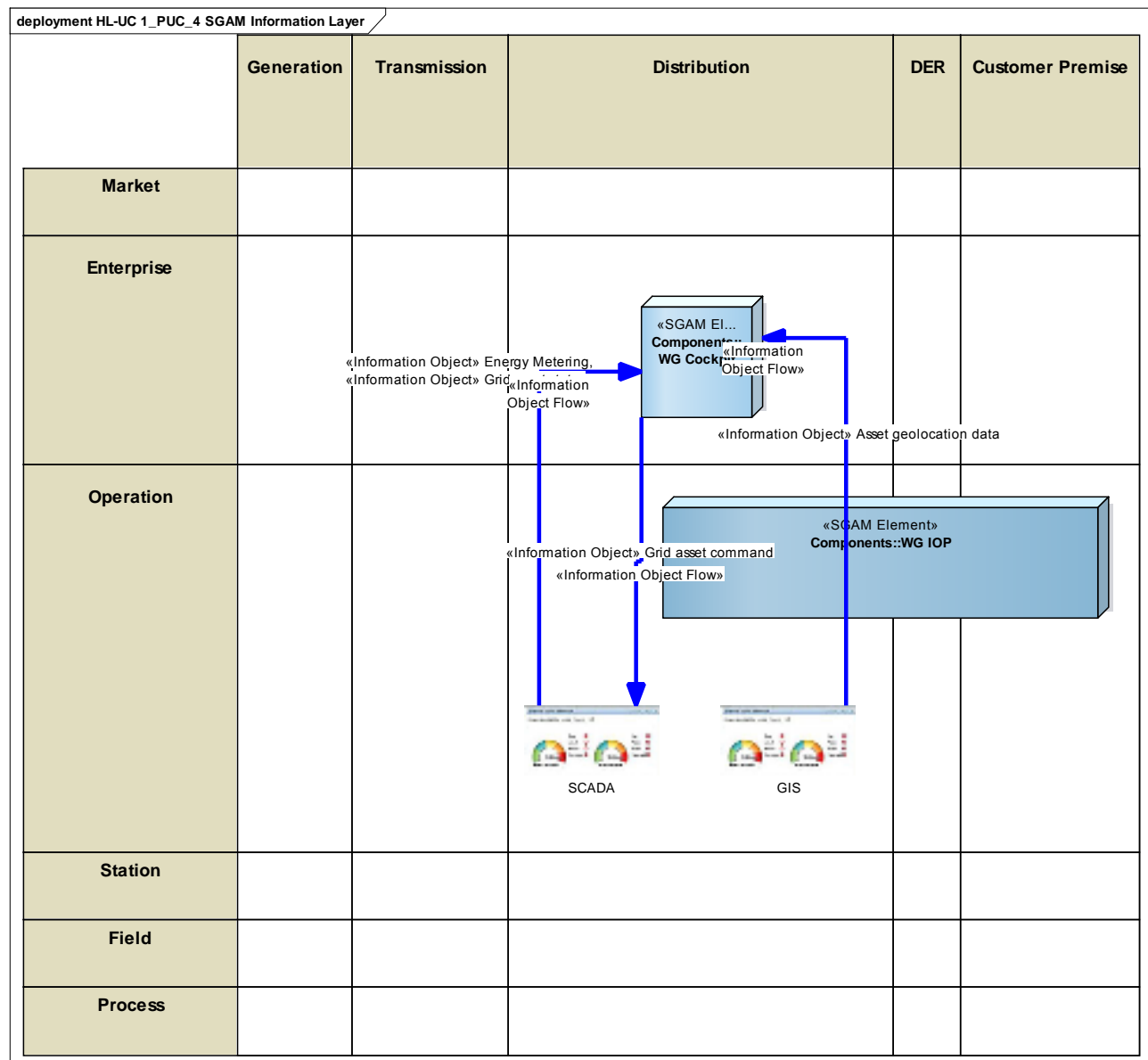


Figure 146 - SGAM Information Layer

## CANONICAL DATA MODEL

The identified canonical data models include those models related to energy metering.

Data Models
DLMS/COSEM
CIM

Table 101 - List of Data Models

## STANDARDS AND INFORMATION OBJECT MAPPING

The identified data standards include those related to energy metering.

Table 102 - List of Data Standards

Data Standards
DLMS/COSEM
CIM

Table 103 - List of Information Objects

Information Objects	Data Model
Energy readings	DLMS/COSEM CIM
Grid topology	CIM

### 18.4.7 ACTIVITY DIAGRAM

The activity diagram describes the storyline of the DSO grid planning activities.

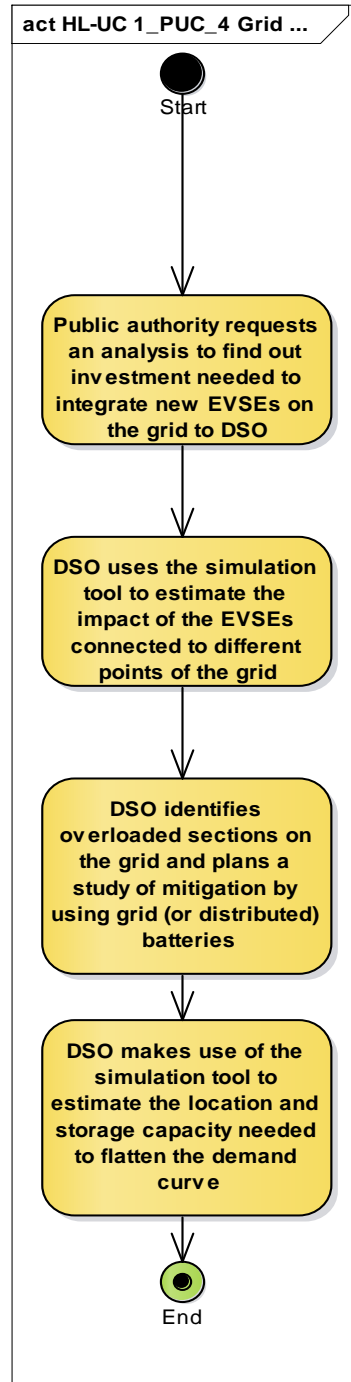


Figure 147 - Primary Use Case Activity Diagram

## 18.4.8 SEQUENCE DIAGRAM

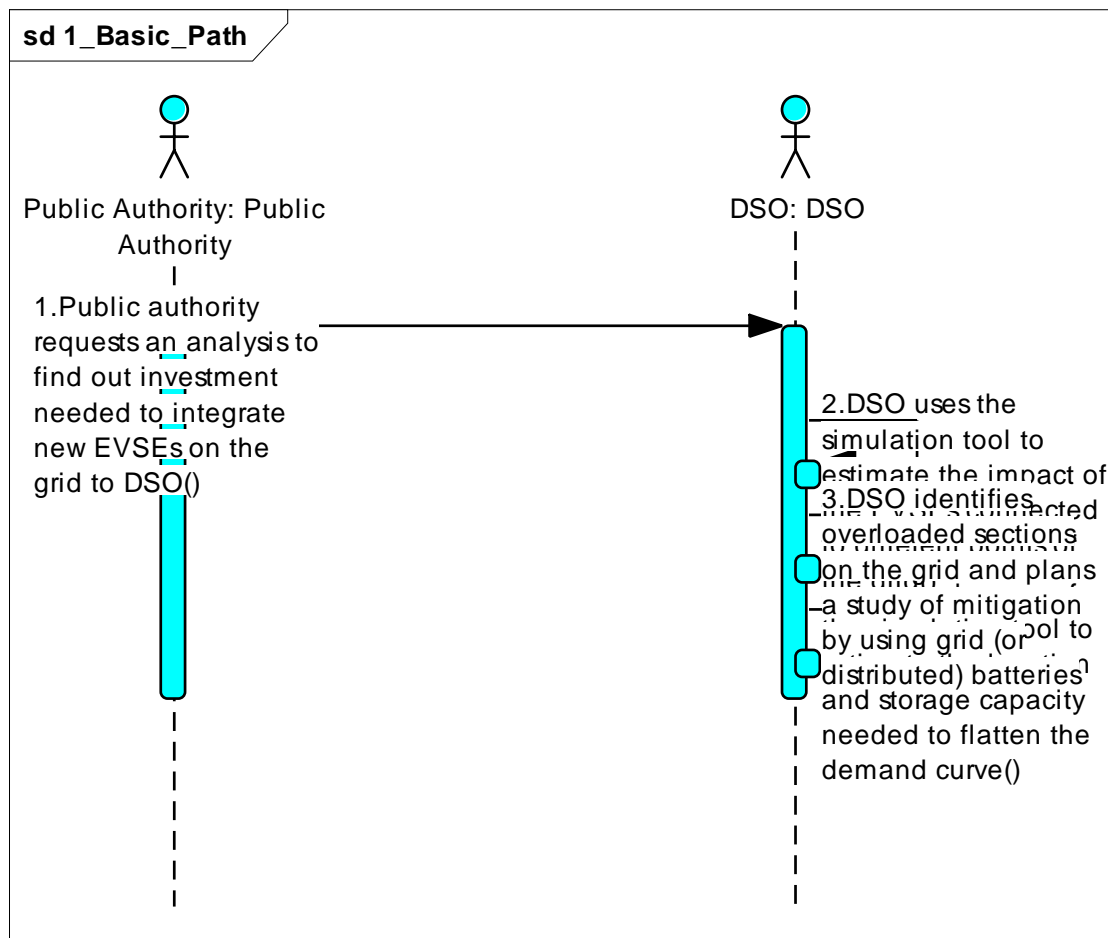


Figure 148 - Primary Use Case Sequence Diagram



## 18.5 HL-UC 1\_PUC\_5: PROMOTE RES VIA RESCO COMPANIES

### 18.5.1 PRIMARY USE CASE DESCRIPTION

According to the description already provided in the D2.1, the objective of this PUC is to support the operations of RESCO companies, namely:

- create an inventory of their assets,
- monitor and control all parameters related to their assets

Measuring the economic impact for RESCO companies and their customers, RESCO companies will enable the provision of energy from RES to its consumers, where the serviced household/business does not own (operate and maintain) the RES generation equipment. Customers of RESCO will be able to self-consume energy produced by RES units, while RESCO will be able to bring on market the energy surplus. These companies will encourage the adoption of distributed generation through RES.

## 18.5.2 SECONDARY USE CASE INTERACTIONS

In the figure below is showed the interactions among the primary and secondary use cases as well as with the involved actors.

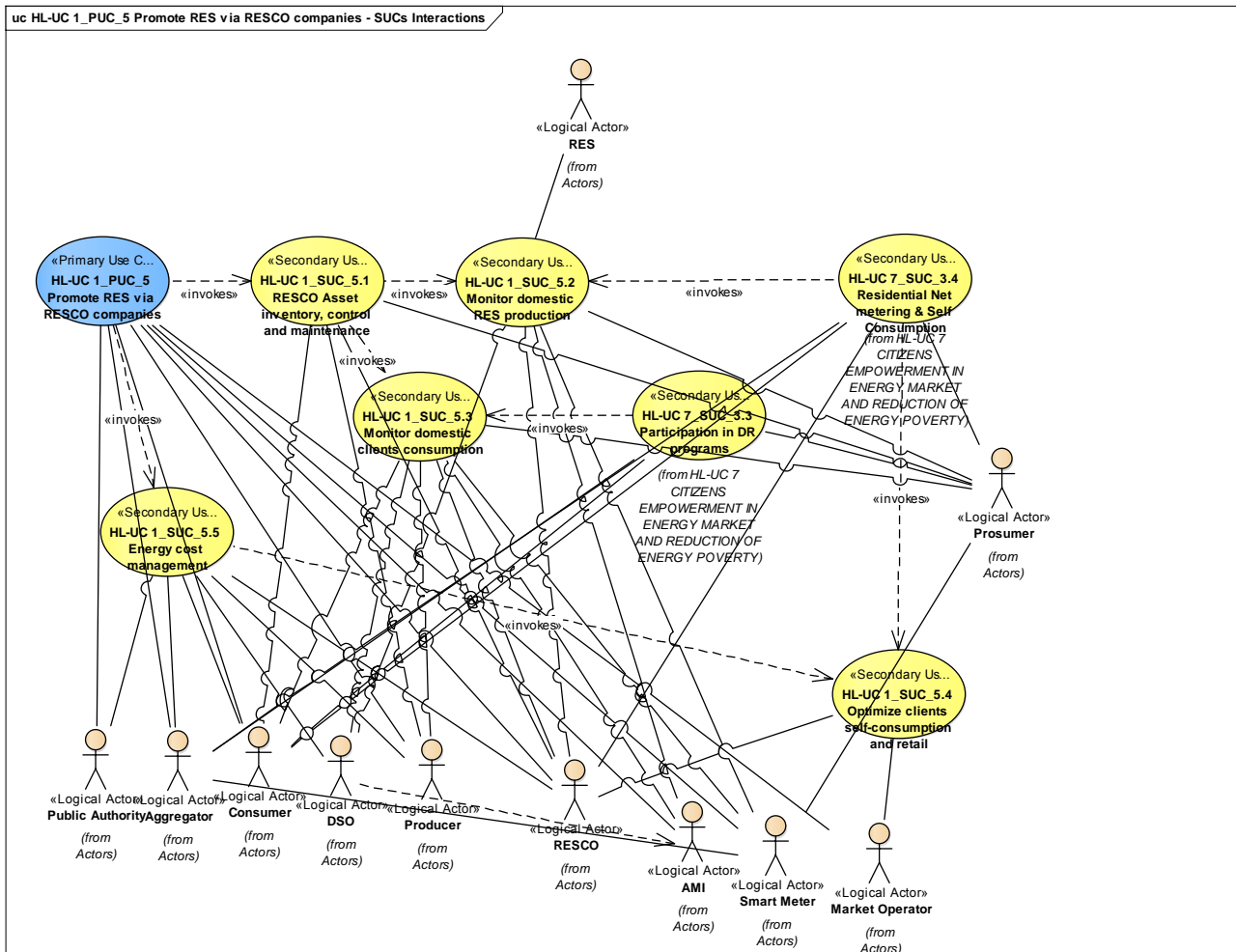


Figure 149 - SUCs Interactions Diagram

In the table below a brief description for each SUC involved in the considered PUC, as well as their relations.

Table 104 - Table of list of participating SUCs

SUC Name	Description	Relation	PUC/SUC
HL-UC 1_SUC_5.1_RES CO asset inventory, control and maintenance	<p>The objective of this SUC is to support the operations of RESCO companies: make an inventory of their assets, monitor and control all parameters related to their assets, measure the economic impact for them and their customer RESCO companies. These companies will encourage the adoption of distributed RES.</p> <p>The application will be developed to administrate all distributed RES installations from the residential area. The purpose of this is related to installation part (investment) and also the operation and maintenance of the distributed</p>	Invoke	<p>HL-UC 1_PUC_5_Promote RES via RESCO companies</p> <p>HL-UC 1_SUC_5.2_Monitor domestic RES production</p>

SUC Name	Description	Relation	PUC/SUC
	facilities.		
HL-UC 1_SUC_5.2_Monitor domestic RES production	<p>This SUC will be focused on the determination of the domestic RES production capacity in relation to the limits for domestic RES usage within different grid parts.</p> <p>The algorithm will evaluate grid facilities, load profiles, weather conditions and most suitable RES technologies to be used.</p> <p>In the prosumer situation (consumption, RES and storage behind the meter), control of maximum grid injection will be considered as main automation, avoiding the need of RES curtailment.</p>	Invoke	<p>HL-UC 1_SUC_5.1_RESCO asset inventory, control and maintenance</p> <p>HL-UC 7_SUC_3.4_Residential net metering &amp; self-consumption</p>
HL-UC 1_SUC_5.3_Monitor domestic clients consumption	<p>This SUC will focus on determining the most relevant load profile (LP) of the residential consumption for the specific area. The procedure will evaluate both “generation possibilities” and “consumption most probable” based on specific season, day-night cycle, weather conditions and patterns, etc.</p> <p>The application will also record specific load profiles for domestic consumption and will build a data base to be considered for further estimations (forecasting and profiling).</p> <p>Considering 4 seasons and working/weekend days, as well as RES availability, a number of <math>4 \times 2 \times 2 = 16</math> specific load profiles should be considered, at 15 minutes LP resolution. Average LPs over seasons, day types and solarisation type (sunny/cloudy) shall be produced, as non-high private data to be used in RESCO profiling.</p>	Invoke	<p>HL-UC 1_SUC_5.1_RESCO asset inventory, control and maintenance</p> <p>HL-UC 7_SUC_3.3_Participation in DR programs</p>
HL-UC 1_SUC_5.4_Manage energy selling	<p>This SUC defines how the RESCO can forecast the energy surplus that will be available from its assets in short-term (day-ahead). This surplus is calculated considering also forecasted production (based on data coming from HL-UC 1_SUC_7.2) and forecasted demand (based on data coming from HL-UC 1_SUC_7.3) of its customers.</p>	Invoke	<p>HL-UC 7_SUC_3.4_Residential net metering &amp; self-consumption</p> <p>HL-UC 1_SUC_5.5_Energy cost</p>
HL-UC 1_SUC_5.5_Energy cost management	<p>The objective of this SUC is to provide KPIs and data to RESCO companies to check the investment they do when installing the assets (e.g. the cost associated to installing a PV on the rooftop of a customer), estimating the costs of maintenance, and monitor the profit of the produced energy.</p> <p>This will be connected to findings from HL-UC_1_SUC_5.4.</p> <p>KPIs: kWh/m<sup>2</sup>, kWh/occupancy, kWh/production unit, kWh/ shift, kWh/€ invested (depending on application).</p>	Invoke	<p>HL-UC 1_PUC_5_Promote RES via RESCO companies</p> <p>HL-UC 1_SUC_5.4_Manage energy selling</p>
HL-UC 7_SUC_3.3_Participation in DR programs	<p>One of the main objectives in the deregulated energy market environment is to promote DR mechanisms and tools allowing even residential Consumers to actively participate in the market for retail energy and ancillary</p>	Invoke	HL-UC 1_SUC_5.3_Monitor domestic clients consumption

SUC Name	Description	Relation	PUC/SUC
	<p>services. This is actually the main objective of this SUC, to develop and integrate advanced mechanisms for DR that will enable final clients/Prosumers (household), individually or by means of third-party actors (retailers, Aggregators, etc.), to actively participate in the energy markets.</p> <p>The residential user should be able to participate in different types of DR programmes providing their potential for demand flexibility:</p> <p>a) Explicit DR: either by consenting to direct load control schemes by the Aggregator (if remotely controllable loads and the necessary communication path are available in the home) or through manual intervention on the loads upon DR signals from the Aggregator (intervention can be facilitated by the app in case the respective loads are remotely controllable through the web);</p> <p>b) Implicit DR: by actively participating in dynamic electricity pricing schemes.</p> <p>The WiseHOME app will also provide alerts, notifications, advices and tips to make the DR signals understandable to citizens and enable them to respond in the most appropriate and beneficial manner.</p> <p>The enrolment of residential clients in DR programmes should be facilitated in a smooth and non-intrusive way, ensuring the minimum of disturbance to end-clients. Moreover, collaborative DR strategies will be explored that amplify and improve the expected reliability of the DR response to a signal.</p>		
HL-UC 7_SUC_3.4_Residential net metering & self-consumption	<p>The main objective of this SUC is to allow the end-users of the application (residential clients) to participate in net metering &amp; self-consumption concepts, promoting that way the idea of green, carbon-free living.</p> <p>Nowadays, the mass penetration of PV rooftop in residences gives the opportunity to Prosumers to exploit the demand flexibility of residential equipment/loads in order to reduce the carbon footprint and/or energy costs. Availability of electricity storage can amplify the potential impact of self-consumption/net metering toward energy cost reduction. The purpose of this SUC is to offer the client the necessary tools in order to optimise the demand profile of the home in order to match some generation profile (local generation or cooperative owned).</p> <p>The WiseHOME app will facilitate net metering/self-consumption practices by informing the Consumer about RESCO strategies, green energy generation surplus (from the cooperative or their own installation), etc. and enabling him/her to adjust his/her consumption accordingly.</p> <p>The idea of net metering &amp; self-consumption has been proven beneficial for large Consumers, and is now considered as a very interested case scenario also for small</p>	Invoke	HL-UC 1_SUC_5.4_Manage energy selling

SUC Name	Description	Relation	PUC/SUC
	Prosumers.		

### 18.5.3 SGAM FUNCTION LAYER

In the figure below the actor and SUCs involved in the HL 1 PUC 5 are positioned on the SGAM Layer.

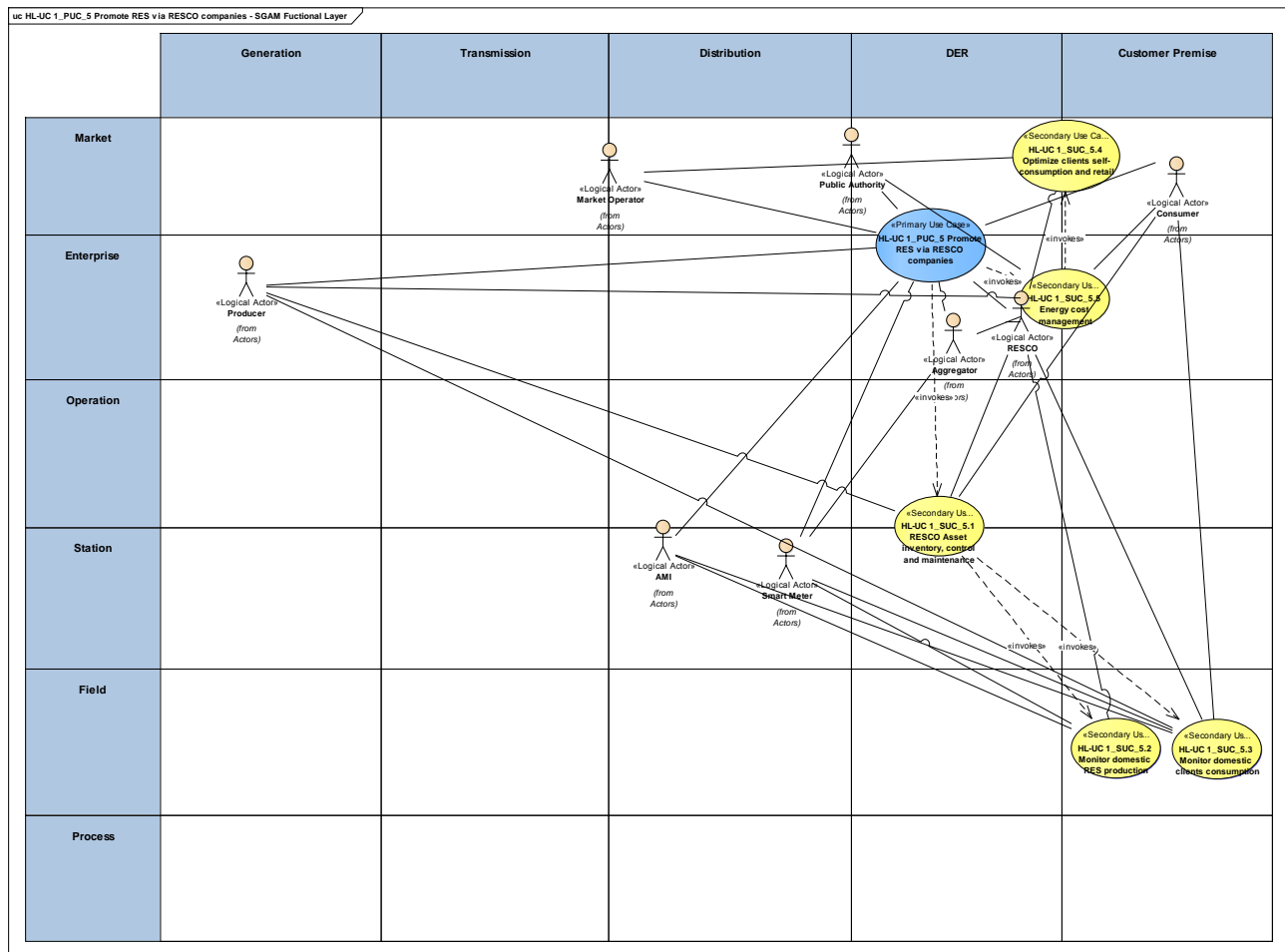


Figure 150 - SGAM Function Layer

The table shows the actors involved in the HL UC 1 PUC 5

Table 105 - List of Actors Involved

Actor Name	Actor Type
Market Operator	Logical Actor
Producer	Logical Actor
Public Authority	Logical Actor
Aggregator	Logical Actor
Consumer	Logical Actor
RESCO	Logical Actor
AMI	Logical Actor
Smart Meter	Logical Actor

#### 18.5.4 SGAM COMPONENT LAYER

The figure below show the components involved in the HL UC1 PUC 5 and how they are positioned on the SGAM layer.

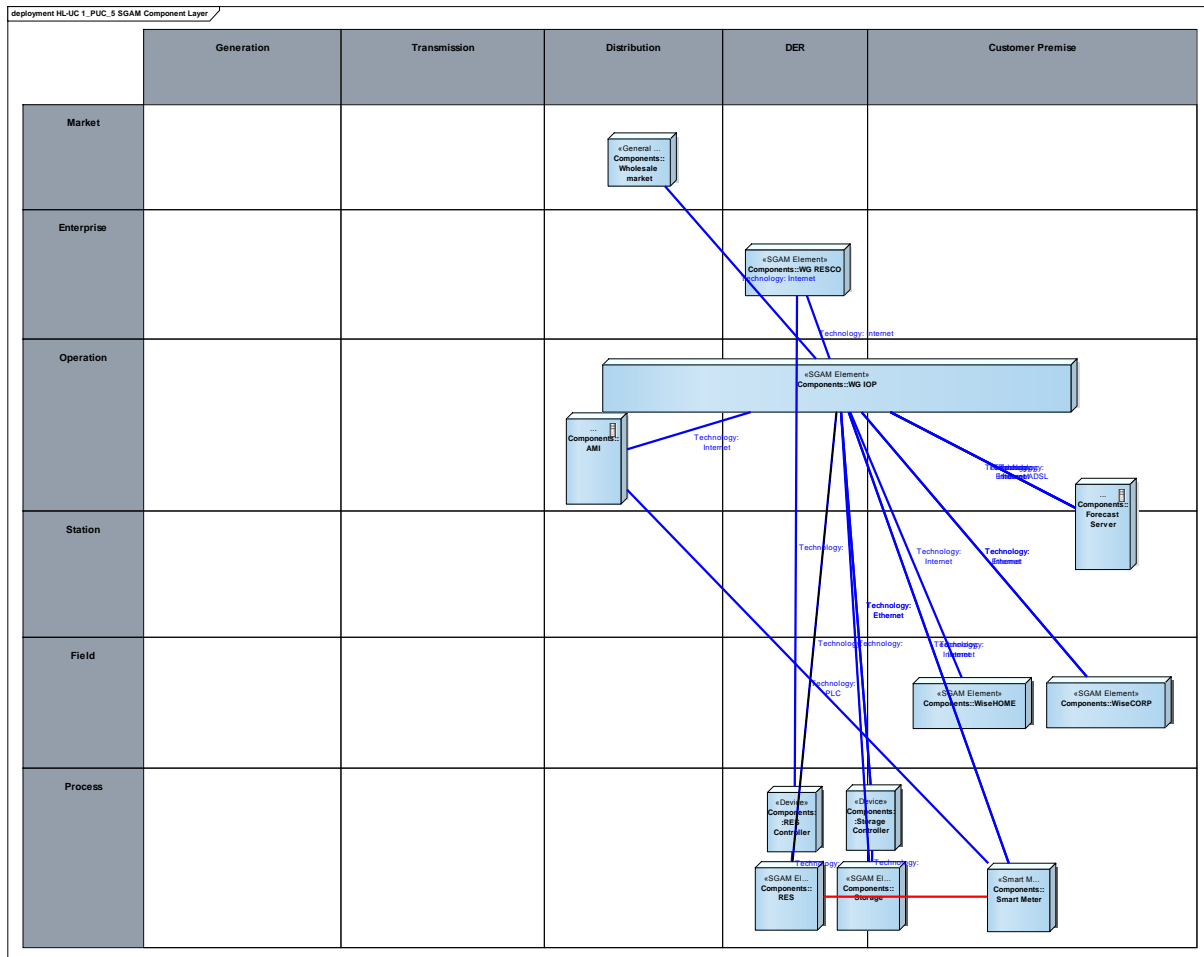


Figure 151 - SGAM Component Layer

The table below shows the components involved in the PUC.

Table 106 - List of Components Participating in the Primary Use Case

Component	Component Type
WG RESCO	SGAM element
WG IOP	SGAM element
Wholesale market	General Component
Forecast Server	Component
AMI	Component
Smart meter	Smart meter component
RES	Component
Storage	Component
RES Controller	Device

Component	Component Type
Storage Controller	Device
WiseHOME	SGAM element
WiseCORP	SGAM element



### 18.5.5 SGAM COMMUNICATION LAYER

In the following figure the SGAM communication layer is shown.

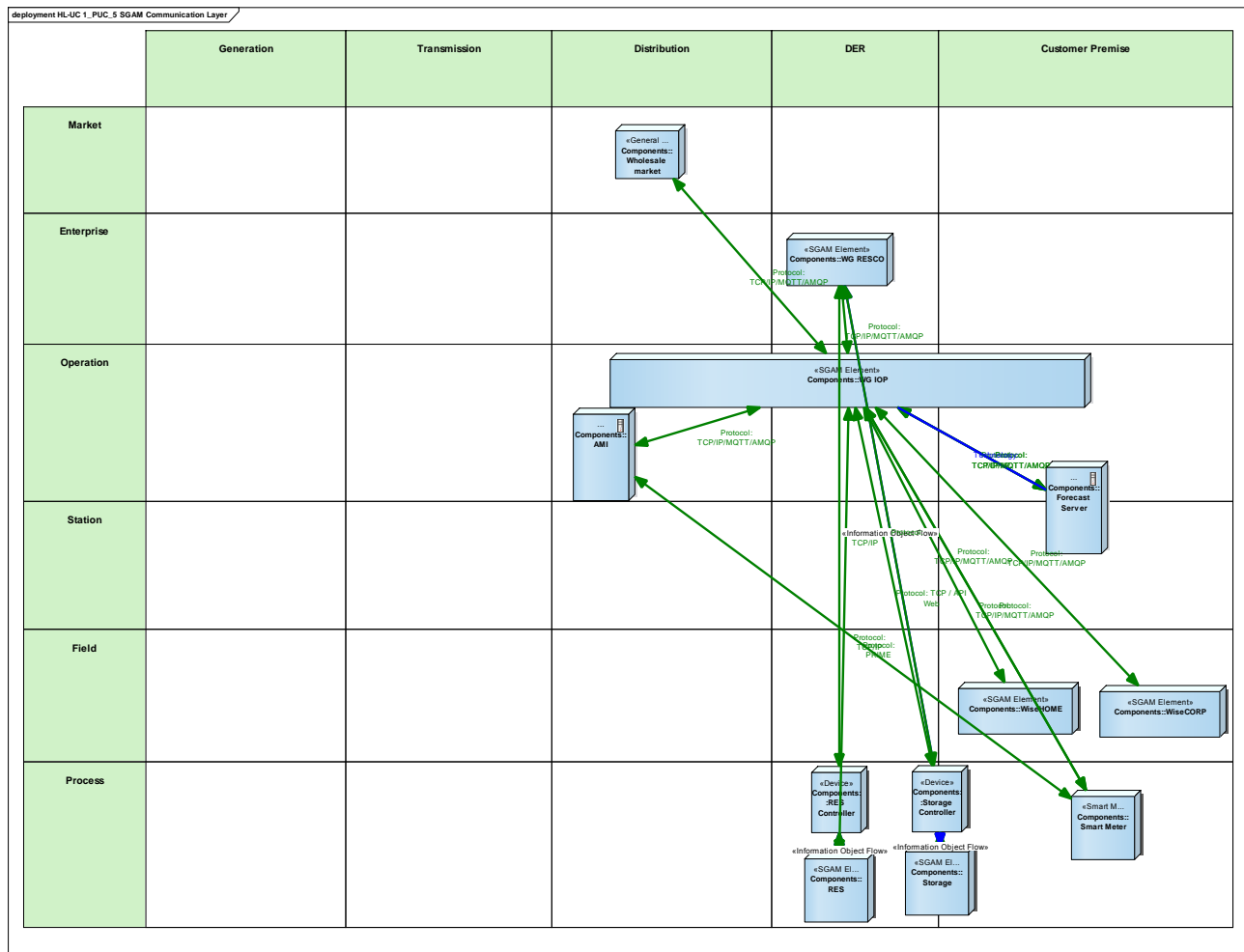


Figure 152 - SGAM Communication Layer

The table below list the main communication technologies and their brief description.

Table 107 - List of Communication Technologies Involved

Communication Technology	Description
TPC/IP	Transmission Control Protocol/Internet Protocol is a Communications protocol for computer networks, the main protocol used on the Internet. It follows specific rules to get data from one network device to another assuring that data will not be lost in transmission
MQTT	It is an internet protocol. It is a machine-to-machine "Internet of Things" connectivity protocol. It was designed as a lightweight publish/subscribe messaging transport. It is useful for connections with remote locations where a small code footprint is required and/or network bandwidth is at a premium.
AMQP	The Advanced Message Queuing Protocol (AMQP) is an open standard application layer protocol for message-oriented middleware. It is a binary, application layer protocol, designed to efficiently support a wide variety of messaging applications and communication patterns.

Communication Technology	Description
PRIME	PRIME is an acronym for "PowerLine Intelligent Metering Evolution". It is a worldwide PLC standard for Advanced Metering, Grid Control and Asset Monitoring applications.

### 18.5.6 SGAM INFORMATION LAYER

The figure below shows the information layer.

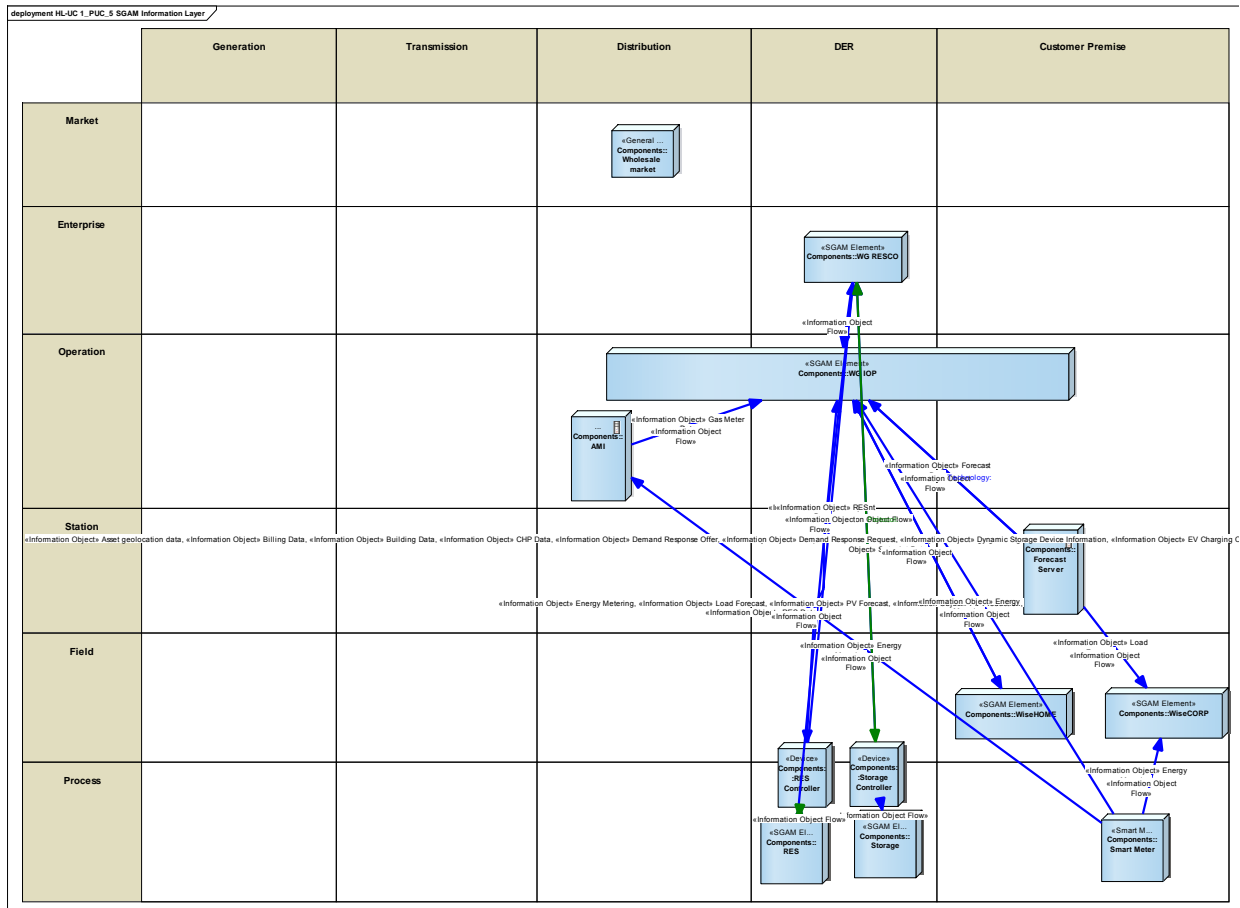


Figure 153 - SGAM Information Layer

## CANONICAL DATA MODEL

Here below some identified canonical data models.

**Table 108 - List of Data Models**

Data Models
Flexibility Data Model (USEF)
GRID Topology
OCPP

## STANDARDS AND INFORMATION OBJECT MAPPING

Here below some identified data standards.

**Table 109 - List of Data Standards**

Data Standards
Flexibility Data Model (USEF)
GRID Topology
OCPP

### 18.5.7 ACTIVITY DIAGRAM

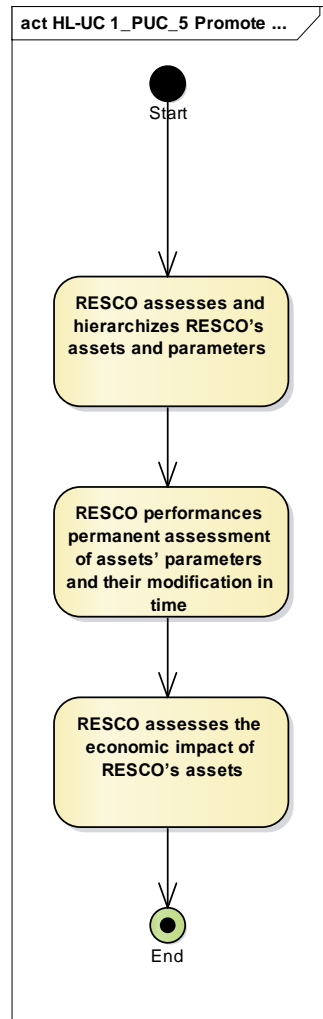


Figure 154 - Primary Use Case Activity Diagram

## 18.5.8 SEQUENCE DIAGRAM

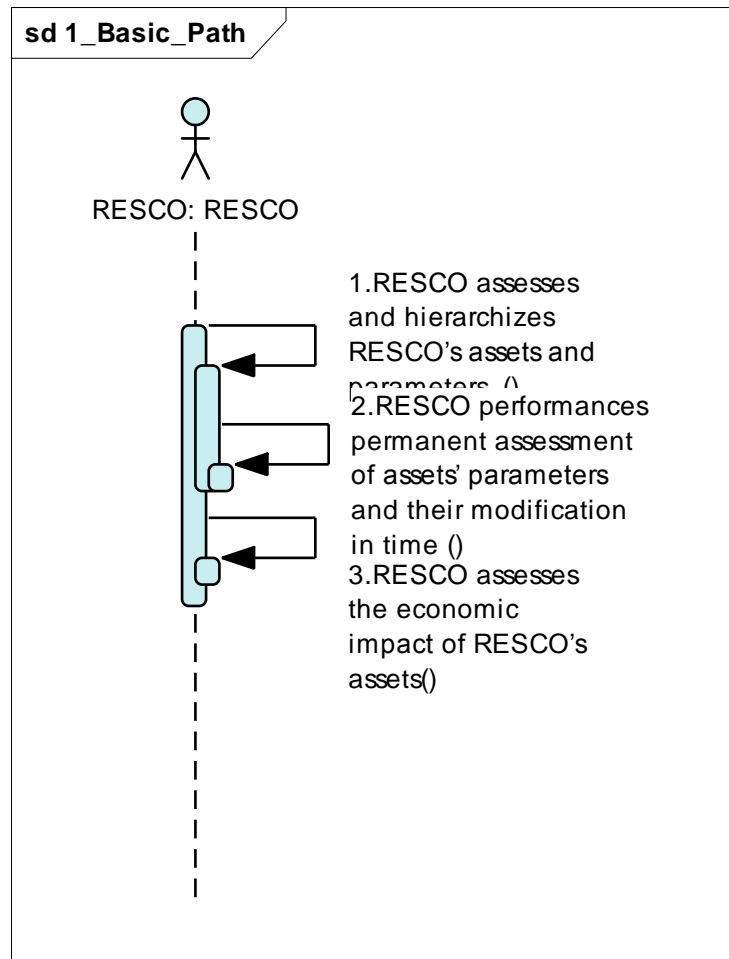


Figure 155 - Primary Use Case Sequence Diagram

## **19 APPENDIX B - ARCHITECTURE**

### **HL-UC 2: DECENTRALIZED GRID CONTROL AUTOMATION**

## 19.1 HL-UC 2\_PUC\_1: DISTRIBUTION NETWORK REAL-TIME MONITORING

### 19.1.1 PRIMARY USE CASE DESCRIPTION

The smart grid environment requires the upgrade of tools for monitoring at all levels of the grid. These components will provide the data necessary for monitoring the grid.

This PUC aims to validate new smart grid technologies and business models and provide two-way communication between

- on the one hand, distributed generation, storage, demand assets, and
- on the other hand, the existing grid operator (dispatch center).

The measurement techniques may include various device types including smart meters (HL-UC 2\_SUC\_1.1), remote terminal units (RTUs), and phasor measurement units (PMUs).

Measurements are captured, stored (HL-UC 2\_SUC\_1.2), and analyzed (HL-UC 2\_SUC\_1.3) in order to determine in every moment the status of the grid. Thanks to these analyses, faults can be detected (HL-UC 2\_SUC\_1.4), thus assuring the correct functioning of the system. Additional tasks for the maintenance of the elements in the grid are considered as well (HL-UC 2\_SUC\_1.5).

### 19.1.2 SECONDARY USE CASE INTERACTIONS

This PUC invokes several different SUCs dealing with monitoring of different parameters of the grid (power quality, faults, asset status) and using different technologies available (AMI, unbundled smart meters)

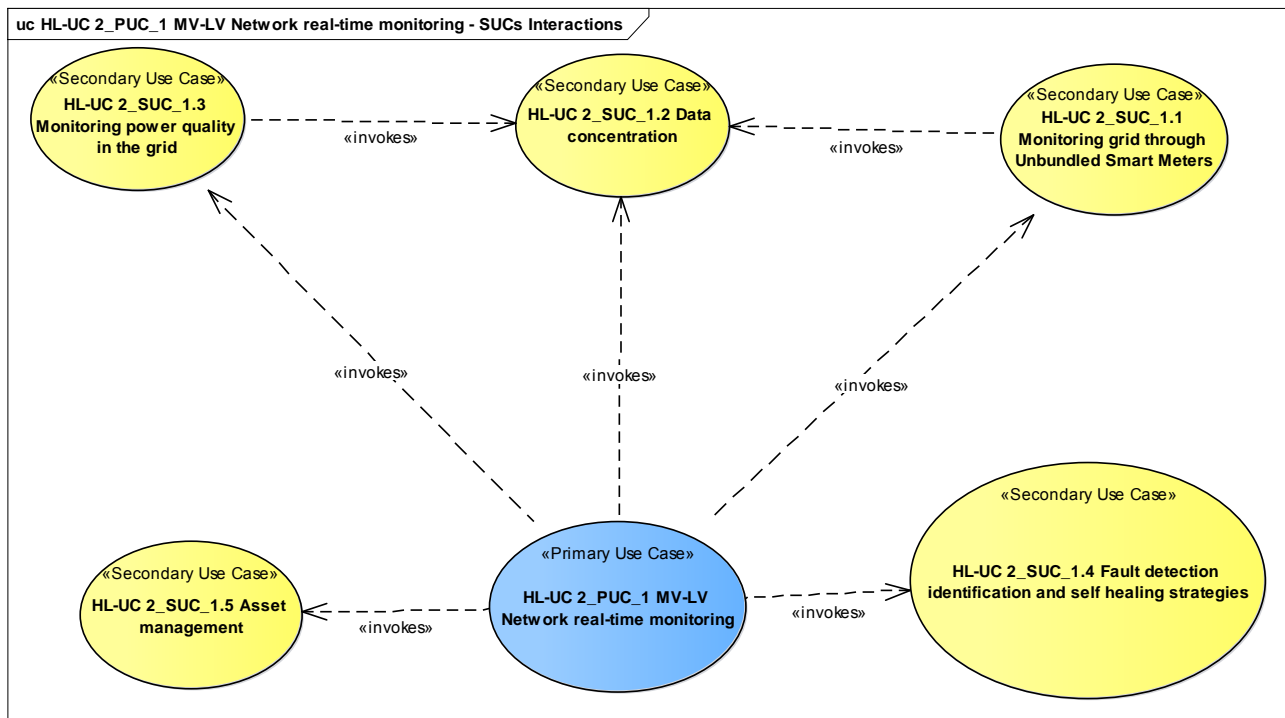


Figure 156 - SUCs Interactions Diagram

Table 110 - Table of list of participating SUCs

SUC Name	Description	Relation	PUC/SUC
HL-UC 2_SUC_1.1	Monitoring grid through Unbundled Smart Meters	invokes	HL-UC 2_SUC_1.2 Data concentration
HL-UC 2_SUC_1.2	Data concentration		
HL-UC 2_SUC_1.3	Monitoring power quality in the grid	invokes	HL-UC 2_SUC_1.2 Data concentration
HL-UC 2_SUC_1.4	Fault detection identification and self-healing strategies		
HL-UC 2_SUC_1.5	Asset management		



### 19.1.3 SGAM FUNCTION LAYER

This PUC covers several domains and zones of the SGAM matrix, namely:

- Distribution domain
  - Enterprise zone: asset management
  - Station zone: use cases related to monitoring the grid and commanding upon detection of problems
- DER and customer premises domain
  - Field zone: use case related to retrieving information from USMs

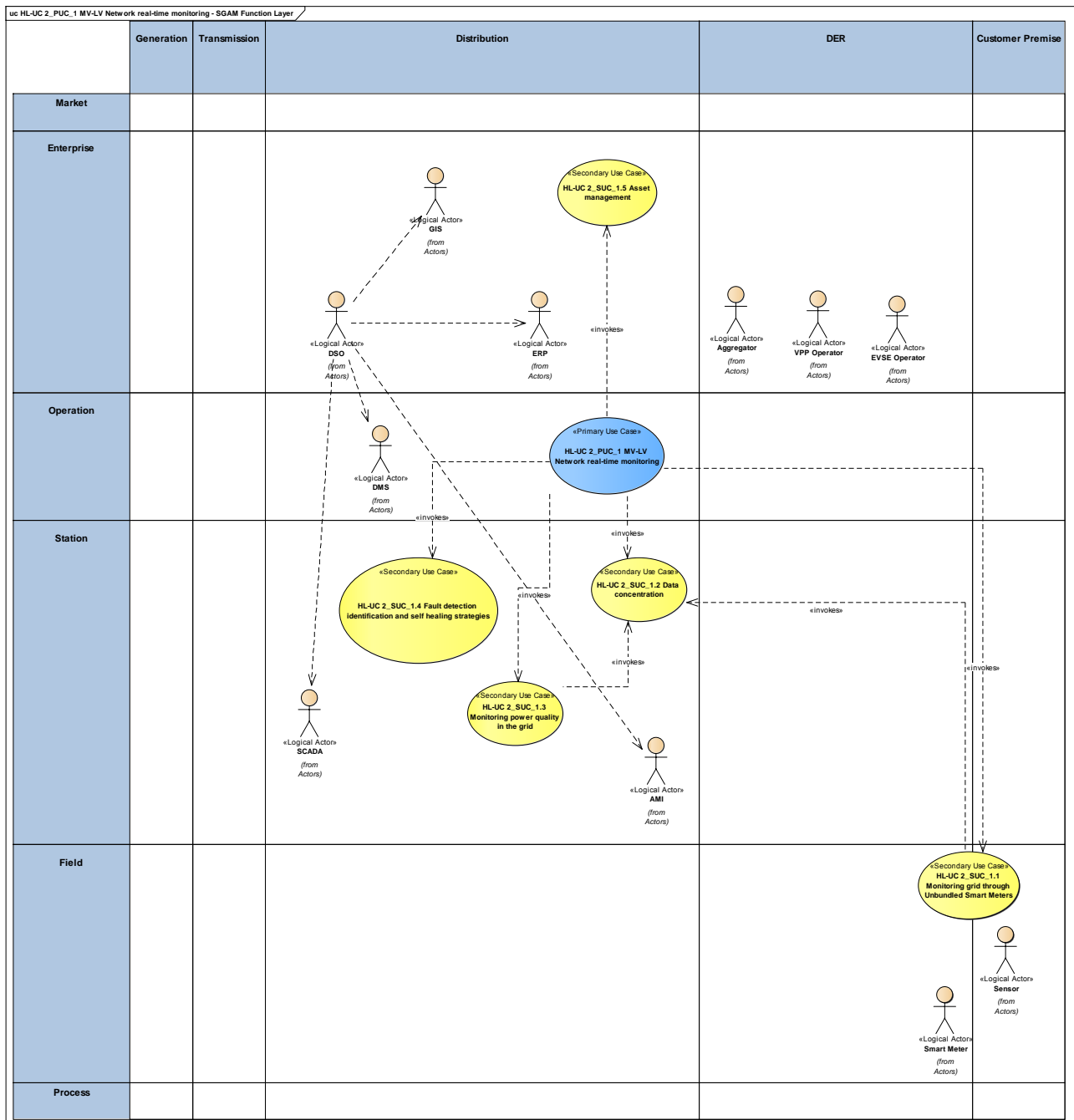


Figure 157 - SGAM Function Layer

Table 111 - List of Actors Involved

Actor Name	Actor Type
DSO	Organization
SCADA	Device
AMI	System
ERP	System
GIS	System

Actor Name	Actor Type
DMS	System
Sensor	Device
EVSE Operator	Organization
Smart meter	Device
Aggregator	Organization
VPP Operator	Organization

#### 19.1.4 SGAM COMPONENT LAYER

Main components involved are those system under the premises of the DSO and the WG Cockpit, covering different zones of the distribution domain. Other WiseGRID products (WiseEVP, WiseCOOP and WG StaaS/VPP) are included as well since they may support the DSO to solve some problems of the grid, as considered in this PUC.

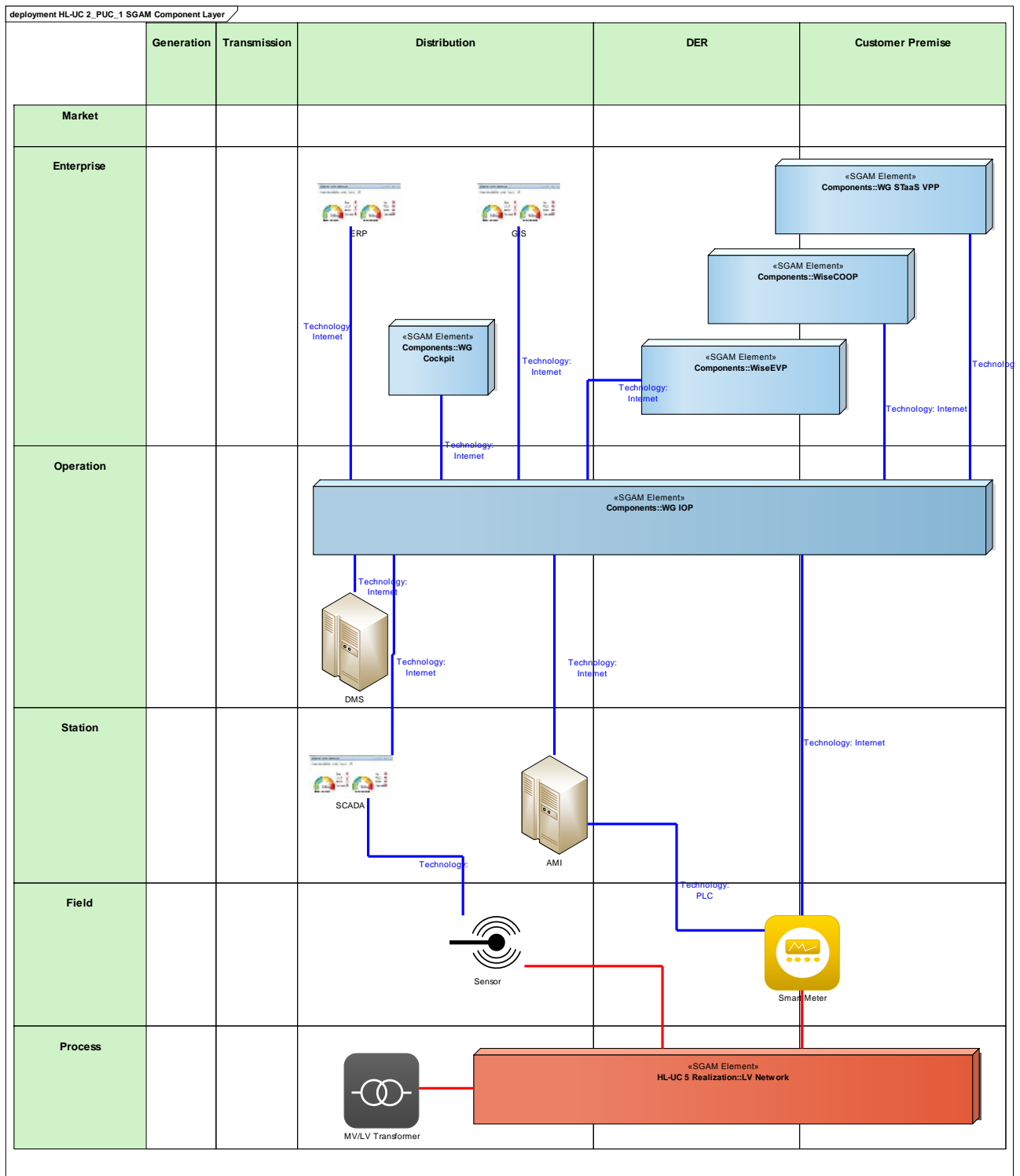










Figure 158 - SGAM Component Layer

**Table 112 - List of Components Participating in the Primary Use Case**

Component	Component Type
ERP	SW application
GIS	SW application
WG Cockpit	SGAM Element
WG StaaS/VPP	SGAM Element
WiseCOOP	SGAM Element
WiseEVP	SGAM Element
WG IOP	SGAM Element
DMS	SGAM Element
SCADA	SW Application
AMI	SGAM Element
Smart meter	Smart meter
Sensor	Sensor
LV network	SGAM Element
MV/LV Transformer	Transformer

Communications identified can be divided in two different groups:

- | Deployment HL-UC 2_PUC_1 SGAM Communication Layer |            |              |   |     |                  |
|---|------------|--------------|---|-----|------------------|
|   | Generation | Transmission | Distribution  | DER | Customer Premise |
| Market  |            |              |   |     |                  |
| Enterprise  |            |              |  ERP  GIS<br>«SGAM Element»<br>Components:WG Cockpit<br>«SGAM Element»<br>Components:WiseCOOP<br>«SGAM Element»<br>Components:WiseEVP<br>«SGAM Element»<br>Components:WG SaaS VPP |     |                  |
| Operation   |            |              |  DMS<br>«SGAM Element»<br>Components:WG IOP  |     |                  |
| Station   |            |              |  SCADA<br> AMI   |     |                  |
| Field   |            |              |  Sensor<br> Smart Meter   |     |                  |
| Process   |            |              |  MVLV Transformer<br>«SGAM Element»<br>HL-UC 5 Realization:LV Network  |     |                  |

### Figure 159 - SGAM Communication Layer

**Table 113 - List of Communication Technologies Involved**

Communication Technology	Description
TCP/IP	Group of protocols enabling communication between devices in a network up to the transport layer
MQTT	ISO standard (ISO/IEC PRF 20922) publish-subscribe-based lightweight messaging protocol for use on top of the TCP/IP protocol
AMQP	Open standard application layer protocol for message-oriented middleware, featuring message orientation, queuing, routing (including point-to-point and publish-and-subscribe), reliability and security
IEC61850	Standard for vendor-agnostic engineering of the configuration of Intelligent Electronic Devices for electrical substation automation systems
PRIME	Specification for narrow band powerline communication



## 19.1.6 SGAM INFORMATION LAYER

Main information identified to be handled in this PUC can be divided into two groups:

- Energy metering: retrieved from different devices and systems, provides a vision of the status of the grid and the quality of the energy supplied
- Flexibility requests: commodity exchanged between the DSO and third parties providing support to solve certain problems, such as congestion

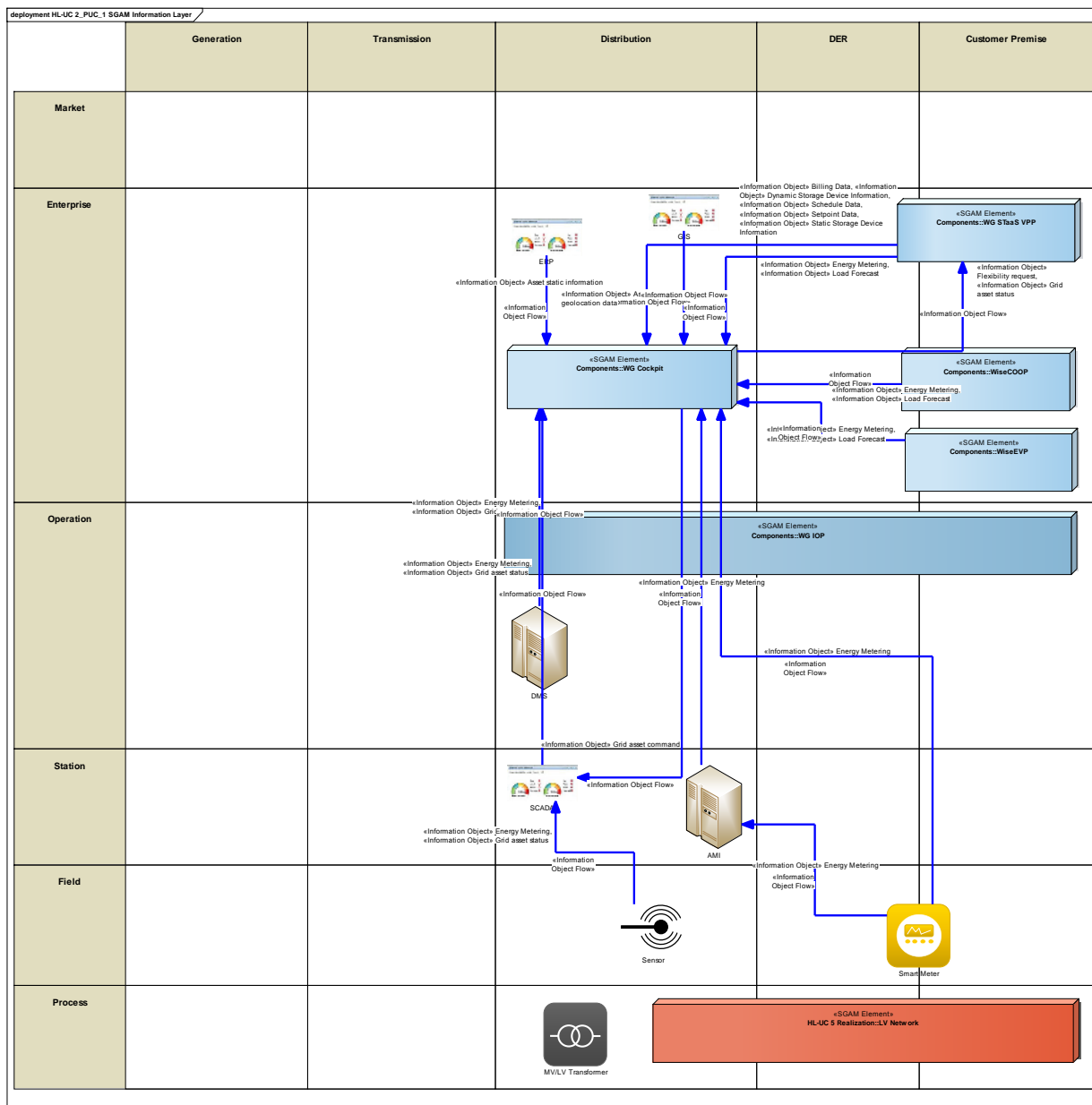


Figure 160 - SGAM Information Layer

## CANONICAL DATA MODEL

The identified canonical data models include those models related to energy metering and modelling of the grid and its assets.

**Table 114 - List of Data Models**

Data Models
Asset inventory
Grid topology
Energy metering

## STANDARDS AND INFORMATION OBJECT MAPPING

The identified data standards include those related to energy metering and modelling of the grid and its assets.

**Table 115 - List of Data Standards**

Data Standards
CIM
DLMS/COSEM

**Table 116 - List of Information Objects**

Information Objects	Data Model
Asset inventory	CIM
Grid topology	CIM
Energy metering	DLMS/COSEM CIM

### 19.1.7 ACTIVITY DIAGRAM

The following diagram depicts the steps needed to provide DSO a good overview of the status of the grid, the quality of the supply and proper mechanisms for problem detection.

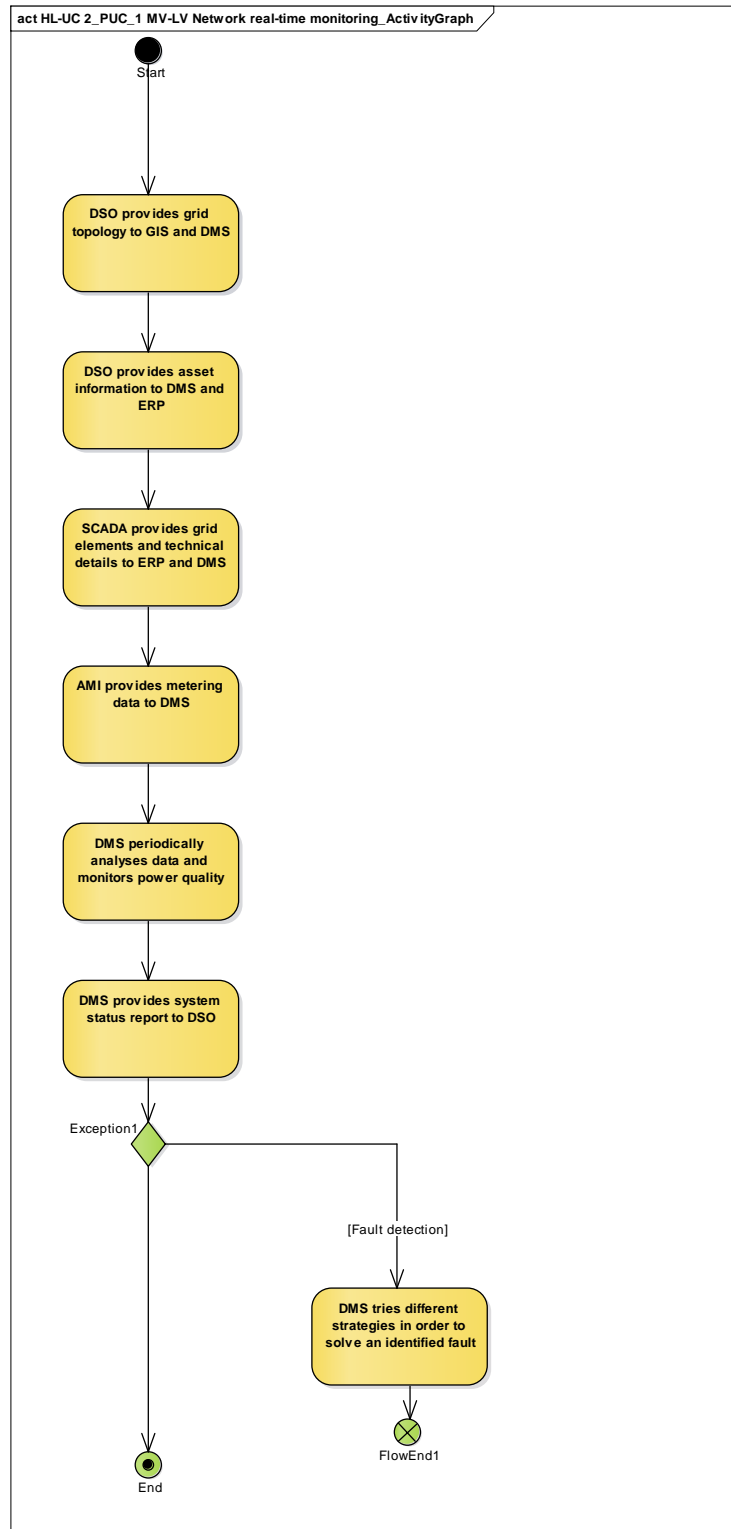


Figure 161 - Primary Use Case Activity Diagram

## 19.1.8 SEQUENCE DIAGRAM

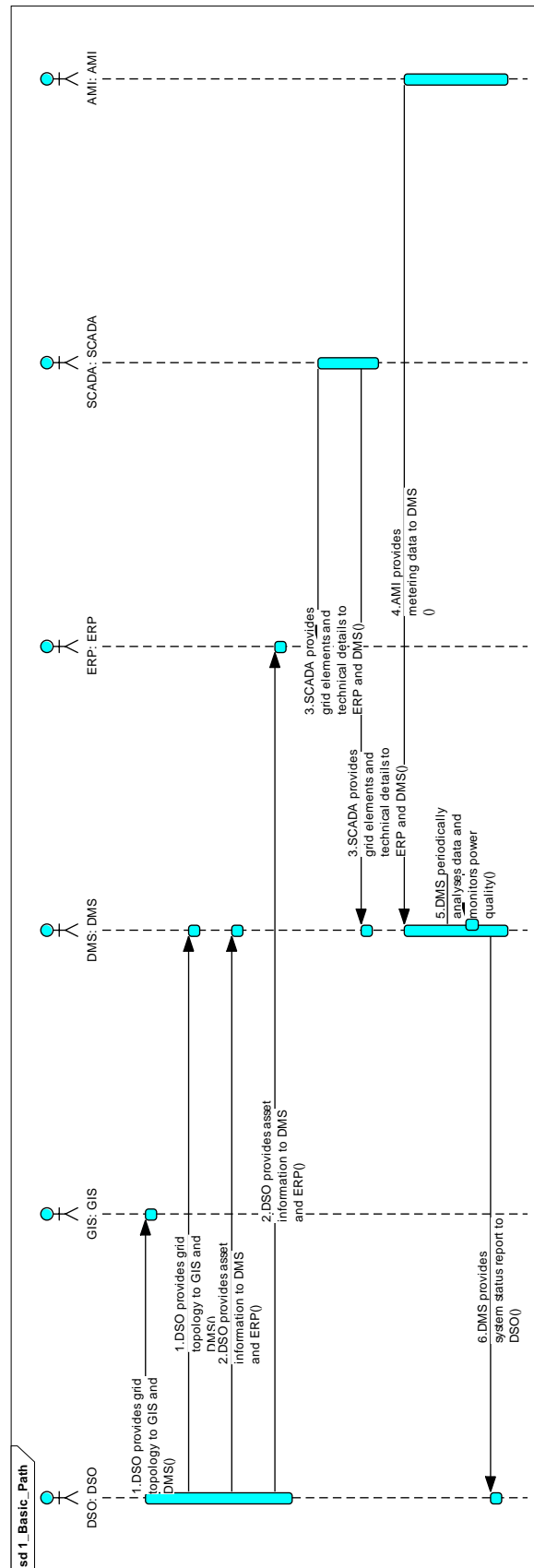


Figure 162 - Primary Use Case Sequence Diagram

## 19.2 HL-UC 2\_PUC\_2: REAL-TIME DISTRIBUTION SYSTEM AWARENESS

### 19.2.1 PRIMARY USE CASE DESCRIPTION

It is important to be capable of identifying the operating conditions of an electrical grid at every time-step. This can be achieved if the status of the grid is known. Additionally, it is important to monitor the grid status as regularly as possible (namely, as close as possible to “real-time”); therefore, it is crucial to reach high refresh rates of system awareness.

The grid operation may be characterized by the following states: normal, emergency and restorative, since its operation conditions change due to sudden and unexpected events. If the state changes to emergency, then it is necessary to take suitable corrective measures and bring the state back to normal. The measurements are acquired in suitable concentration structures, such as SCADA, AMI, and PDC (HL-UC 2\_SUC\_1.2).

Once the topological data are known (HL-UC 2\_SUC\_2.2) and the network is found to be fully observable (HL-UC 2\_SUC\_2.3), the measurements, together with other data, are processed by the state estimator (HL-UC 2\_SUC\_2.5) which aims at filtering/removing the measurement noise and compute a system state that is as close as possible to the true one. It is possible to use the load flow analysis tool to verify the state estimation calculation or make a comparison (HL-UC 2\_SUC\_2.4). If bad data is detected (HL-UC 2\_SUC\_2.6), then the state estimation process has to be re-executed, otherwise the state estimation result is wrong.

The estimated state is passed on to the Energy management system (EMS) and Distribution Management Systems (DMS) applications (HL-UC 2\_PUC\_3), which are related to the real-time grid control and operation.

### 19.2.2 SECONDARY USE CASE INTERACTIONS

This PUC includes different SUCs that operate on data retrieved by the DSO in order to provide a meaningful overview of the status of the grid, including bad data identification, observability analyses and load/production forecasting.

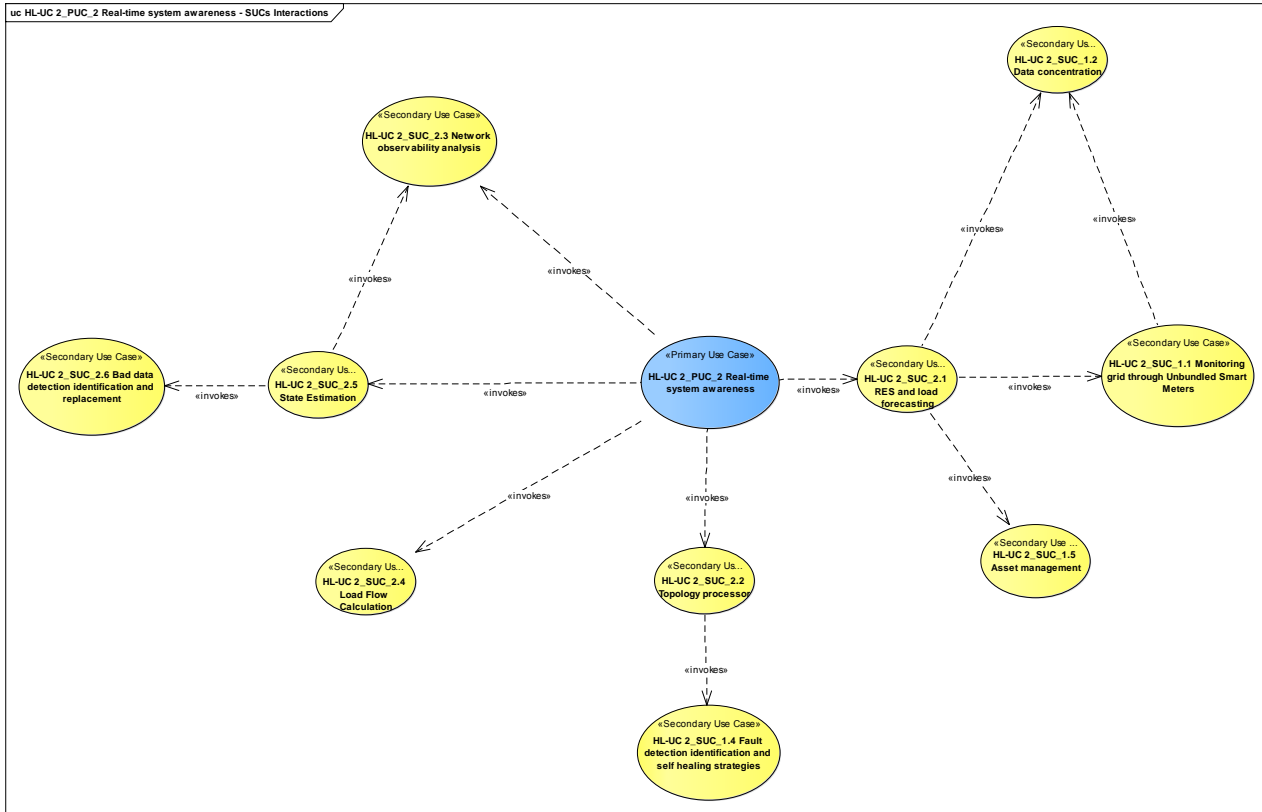


Figure 163 - SUCs Interactions Diagram

Table 117 - Table of list of participating SUCs

SUC Name	Description	Relation	PUC/SUC
HL-UC 2_SUC_2.1	RES and load forecasting	invokes	HL-UC 2_SUC_1.1 Monitoring grid through Unbundled Smart Meters HL-UC 2_SUC_1.2 Data concentration HL-UC 2_SUC_1.5 Asset management
HL-UC 2_SUC_2.2	Topology processor	invokes	HL-UC 2_SUC_1.4 Fault detection identification and self-healing strategies
HL-UC 2_SUC_2.3	Network observability analysis		
HL-UC 2_SUC_2.4	Load flow calculation		
HL-UC 2_SUC_2.5	State estimation	invokes	HL-UC 2_SUC_2.3 Network observability analysis HL-UC 2_SUC_2.6 Bad data detection, identification and replacement
HL-UC 2_SUC_2.6	Bad data detection, identification and replacement		

### 19.2.3 SGAM FUNCTION LAYER

Most SUCs of this PUC fall under the distribution domain - since the objective of the PUC is providing DSOs with an optimal overview of the status of the grid-, and under the operation zone - since this PUC mainly implies data analysis.

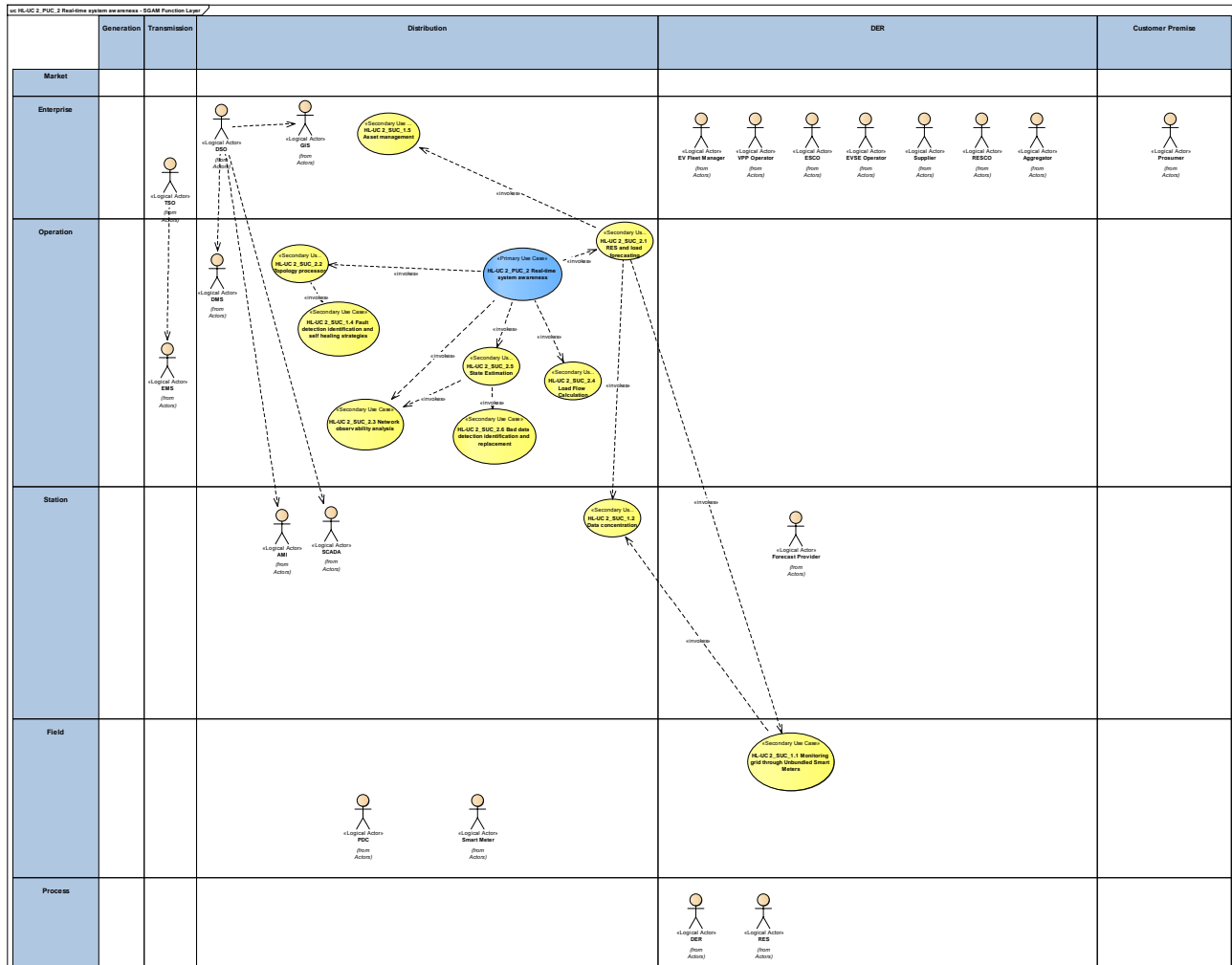


Figure 164 - SGAM Function Layer

The related actors are those in position of either providing information or getting benefit from the availability of a proper grid monitoring function that ensures the quality of the supply.

Table 118 - List of Actors Involved

Actor Name	Actor Type
Supplier	Organization
RESCO	Organization
ESCO	Organization
VPP Operator	Organization
RES	Device

Actor Name	Actor Type
EVSE operator	Organization
Aggregator	Organization
TSO	Organization
EMS	System
DSO	Organization
GIS	System
PDC	Device
SCADA	Device
AMI	System
DMS	System
DER	System
Prosumer	Person
Smart meter	Device
EV Fleet Manager	Organization



### 19.2.4 SGAM COMPONENT LAYER

The main component involved in this PUC is the WG Cockpit, which will depend in several components under the distribution domain to retrieve all necessary data to perform the required analysis. Other tools of the WiseGRID ecosystem are indicated as well, since they are in position of providing further information, such as demand or production forecasts, that may contribute to the correct management of the grid.

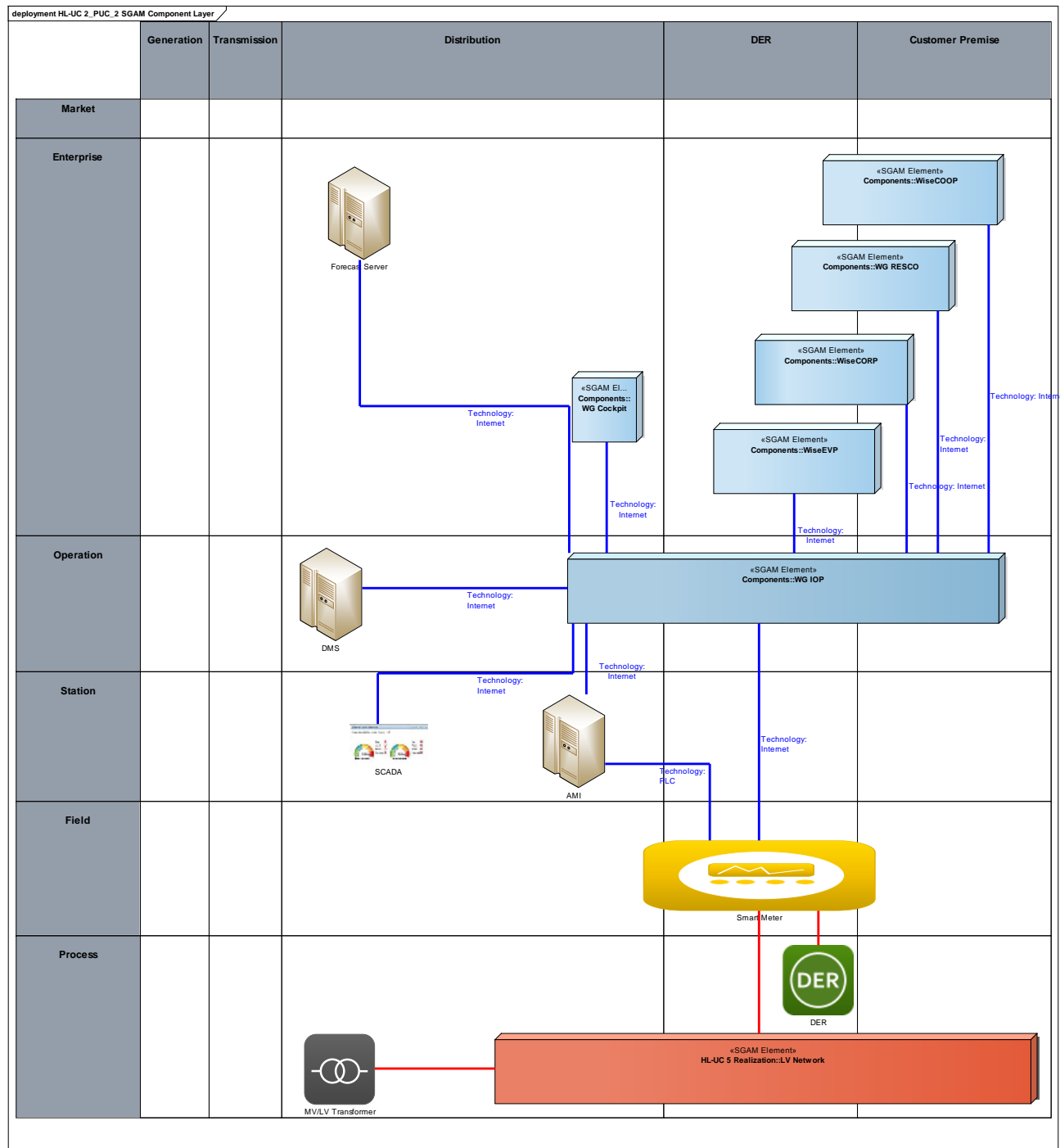


Figure 165 - SGAM Component Layer

**Table 119 - List of Components Participating in the Primary Use Case**

Component	Component Type
Forecast server	SGAM Element
WiseCOOP	SGAM Element
WG RESCO	SGAM Element
WiseCORP	SGAM Element
WiseEVP	SGAM Element
WG Cockpit	SGAM Element
WG IOP	SGAM Element
DMS	SGAM Element
SCADA	SW Application
AMI	SGAM Element
Smart meter	Smart meter
DER	DER
LV Network	SGAM Element
MV/LV Transformer	Transformer

### 19.2.5 SGAM COMMUNICATION LAYER

Communications identified can be divided in two different groups:

- Communication of already deployed field devices and control systems: include a variety of industrial and smart grid protocols
- Communications with WiseGRID components: include the protocols considered to be enabled by the WG IOP

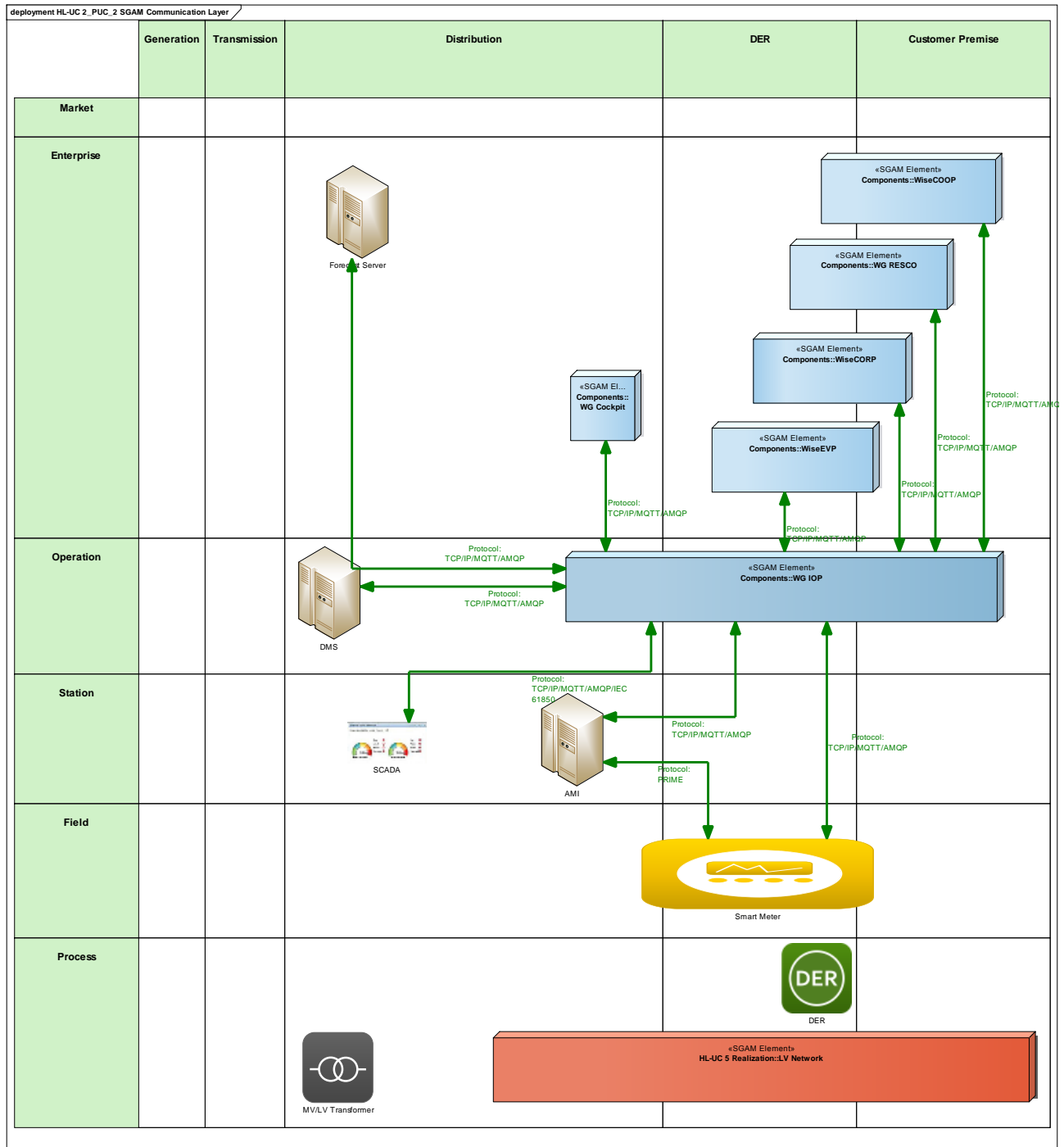


Figure 166 - SGAM Communication Layer

**Table 120 - List of Communication Technologies Involved**

Communication Technology	Description
TCP/IP	Group of protocols enabling communication between devices in a network up to the transport layer
MQTT	ISO standard (ISO/IEC PRF 20922) publish-subscribe-based lightweight messaging protocol for use on top of the TCP/IP protocol
AMQP	Open standard application layer protocol for message-oriented middleware, featuring message orientation, queuing, routing (including point-to-point and publish-and-subscribe), reliability and security
PRIME	Standard for vendor-agnostic engineering of the configuration of Intelligent Electronic Devices for electrical substation automation systems
IEC61850	Specification for narrow band powerline communication

### 19.2.6 SGAM INFORMATION LAYER

The main information items handled in this PUC are related to energy and electrical measurements that are either retrieved from field devices, either calculated - power flow and state estimation - or forecasted, thus allowing a proper vision of the grid status and quality of the supply both in real-time and in the near future.

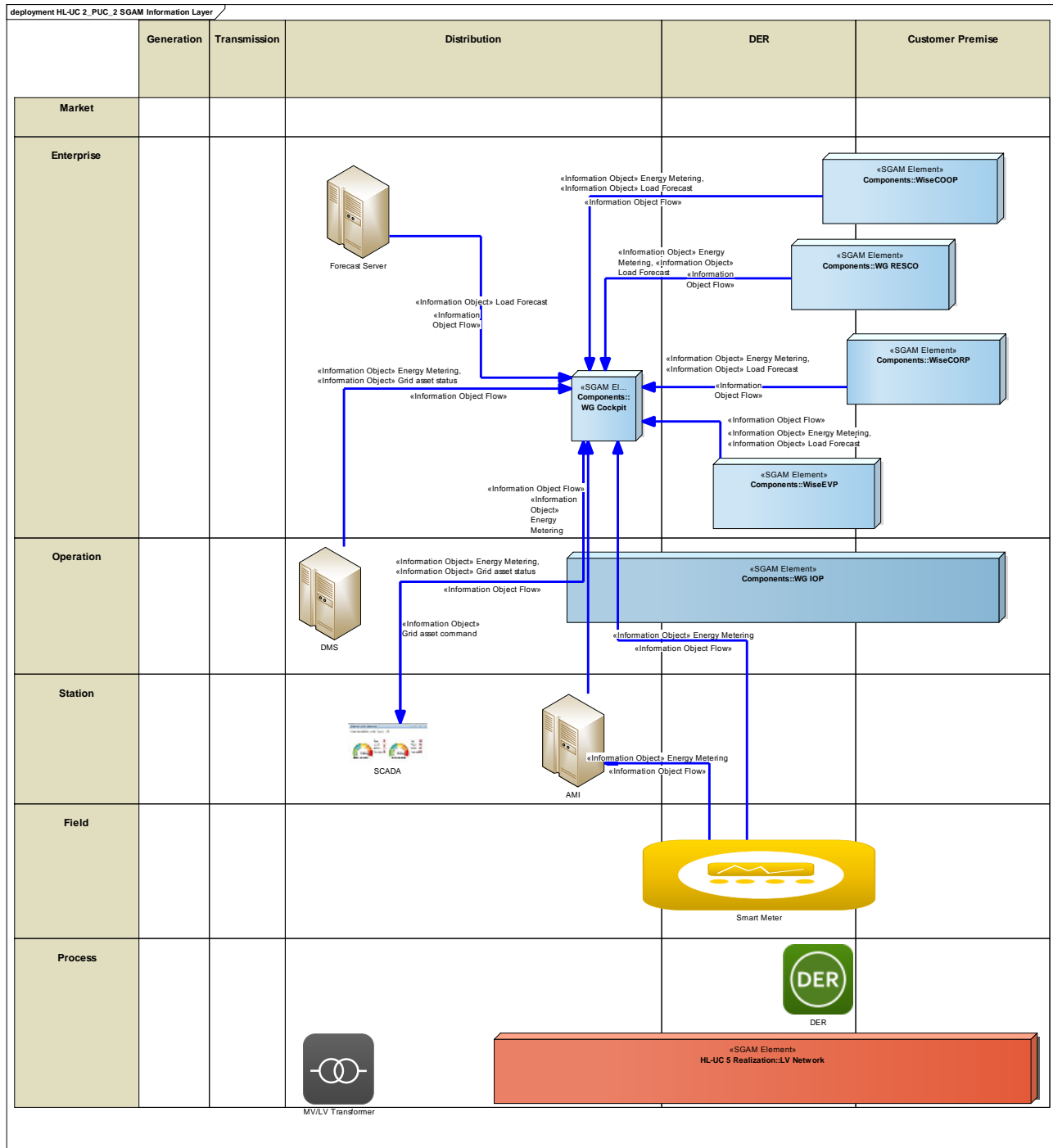


Figure 167 - SGAM Information Layer

## CANONICAL DATA MODEL

As pointed out in the previous diagram, data models for energy metering, electrical measurements and forecasted projections are needed.

**Table 121 - List of Data Models**

Data Models
DLMS/COSEM
CIM
Forecast data model

## STANDARDS AND INFORMATION OBJECT MAPPING

The following standards have been identified for energy metering and electrical measurements.

**Table 122 - List of Data Standards**

Data Standards
DLMS/COSEM
CIM

**Table 123 - List of Information Objects**

Information Objects	Data Model
Energy metering	DLMS/COSEM CIM
Demand/production forecasts	CIM

### 19.2.7 ACTIVITY DIAGRAM

The following diagrams depicts the necessary steps to transform field data into information providing a proper overview of the status of the grid.

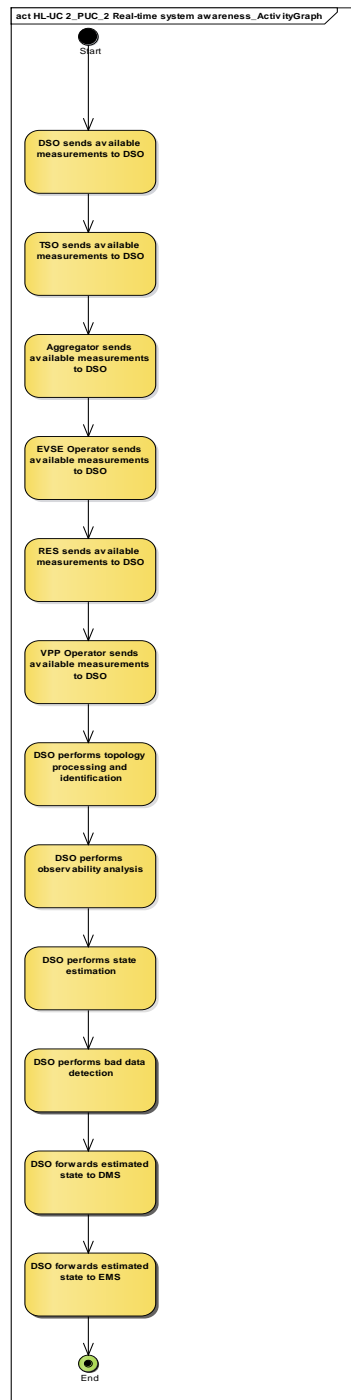


Figure 168 - Primary Use Case Activity Diagram

## 19.2.8 SEQUENCE DIAGRAM

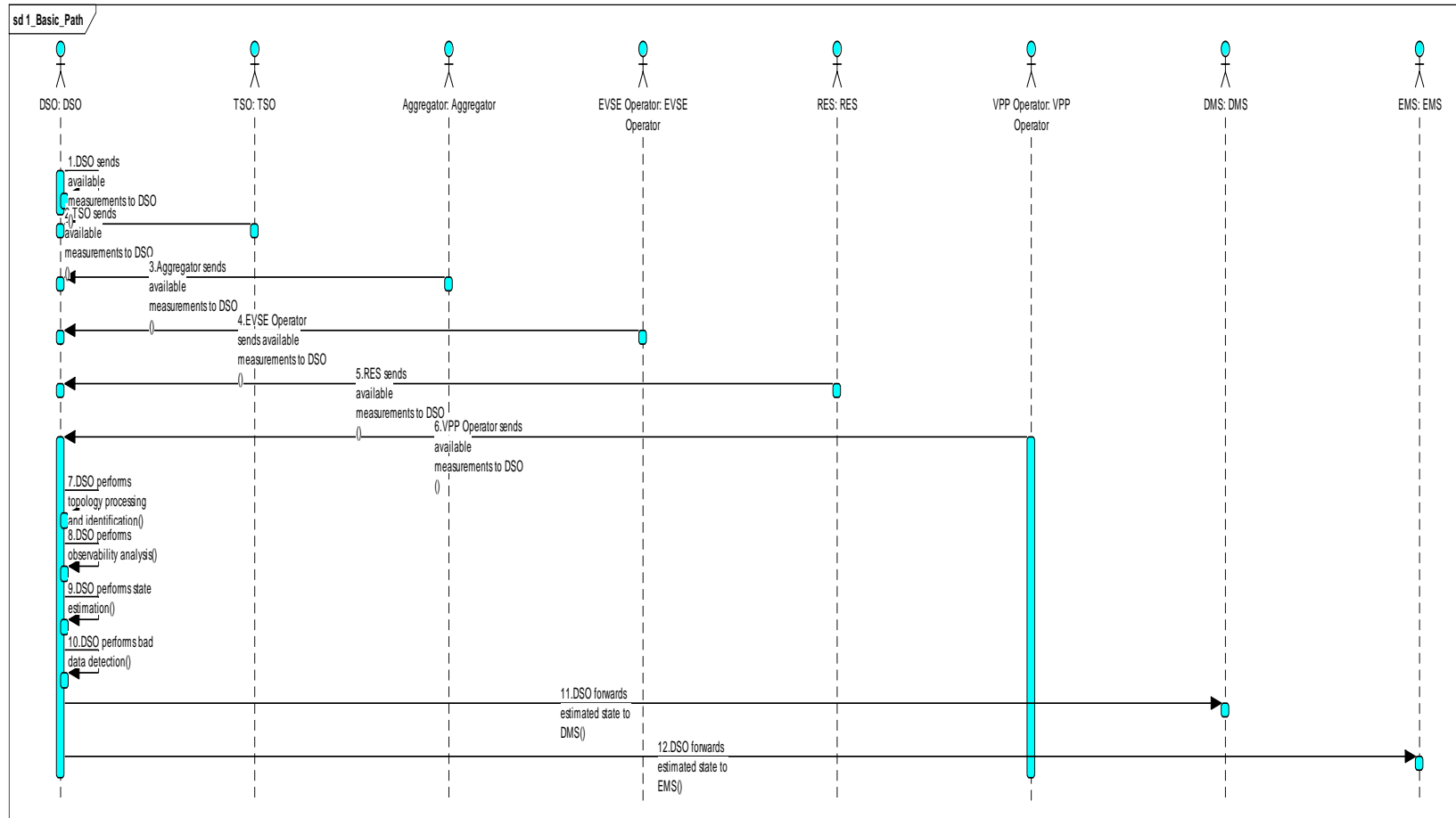


Figure 169 - Primary Use Case Sequence Diagram



## 19.3 HL-UC 2\_PUC\_3: GRID CONTROL

### 19.3.1 PRIMARY USE CASE DESCRIPTION

The main goal of the Distribution System Operator (DSO) is to ensure the network operation and management in a reliable and economic manner under normal and abnormal conditions. Furthermore, being part of the electricity system, the distribution grid and its resources can contribute to the smooth operation of the entire system. Thus, application of grid control -especially under abnormal situations- is motivated either by the inherent needs of the distribution grid operated by the DSO or by the extraneous needs of the transmission system operated by the Transmission System Operator (TSO).

Accomplishing these goals requires continuous monitoring of the prevailing conditions in the MV/LV distribution network (HL-UC 2\_PUC\_1) and identification of the operating state of the distribution network (HL-UC 2\_PUC\_2). Combining this information, the DSO determines the necessary preventive actions in case the distribution grid state is identified as insecure (inherent needs) or in case the TSO has sent a request for specific actions or a notification regarding the current state of the transmission system (HL-UC 2\_PUC\_3). These actions include a combination of control actions performed by the DSO over available loads of conventional type in a direct way (HL-UC 2\_SUC\_3.1) or indirectly through an intermediary (HL-UC 2\_SUC\_3.2, HL-UC 2\_SUC\_3.6, HL-UC 1\_SUC\_4.2, HL-UC 7\_SUC\_2.7, HL-UC 7\_SUC\_2.8), adjustments in the network topology (HL-UC 2\_SUC\_3.4), islanding of the local grid (HL-UC 2\_SUC\_3.5) -if deemed necessary- with control over RES units (HL-UC 1\_PUC\_3), electric vehicles (HL-UC 3\_SUC\_4.1), VPPs (HL-UC 6\_SUC\_3.2) and buildings (HL-UC 5\_SUC\_4.2).

The decision-making process for solving the distribution grid operation problems and/or for contributing to the smooth operation of the transmission system is facilitated through the use of optimization methods (HL-UC 2\_SUC\_3.3) and can refer either to the day-ahead scheduling or the real-time operation of the grid, while the objective of the optimization might be different depending on the circumstances.

### 19.3.2 SECONDARY USE CASE INTERACTIONS

The following diagram shows all SUCs considered under this Grid Control PUC, which contemplates not only actions that fall inside the scope of action of the DSO, but also activation of certain ancillary services provided by third parties.

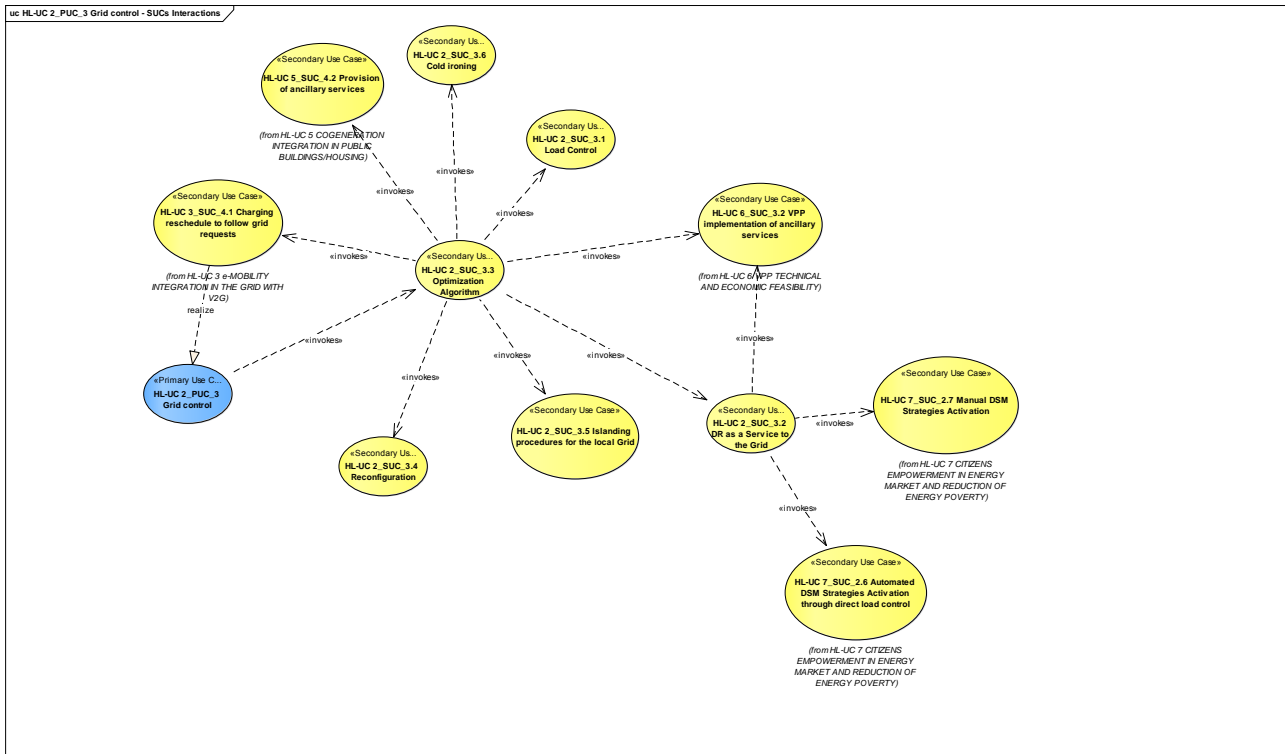


Figure 170 - SUCs Interactions Diagram

**Table 124 - Table of list of participating SUCs**

SUC Name	Description	Relation	PUC/SUC
HL-UC 2_SUC_3.1	Load control		
HL-UC 2_SUC_3.2	DR as a service to the grid	invokes	HL-UC 7_SUC_2.6 Automated DSM strategies activation through direct load control HL-UC 7_SUC_2.7 Manual DSM strategies activation
HL-UC 2_SUC_3.3	Optimization algorithm	invokes	HL-UC 2_SUC_3.1 Load control HL-UC 2_SUC_3.2 DR as a service to the grid HL-UC 2_SUC_3.4 Reconfiguration HL-UC 2_SUC_3.5 Islanding procedures for the local grid HL-UC 2_SUC_3.6 Cold ironing HL-UC 3_SUC_4.1 Charging reschedule to follow grid requests HL-UC 5_SUC_4.2 Provision of ancillary services HL-UC 6_SUC_3.2 VPP implementation of ancillary services
UC 2_SUC_3.4	Reconfiguration		
HL-UC 2_SUC_3.5	Islanding procedures for the local grid		
HL-UC 2_SUC_3.6	Cold ironing		

### 19.3.3 SGAM FUNCTION LAYER

This PUC mainly covers the operation zone of the distribution, DER and customer premise domains. This is motivated by the variety of actors and elements that may collaborate with the DSO to solve problems detected in the grid.

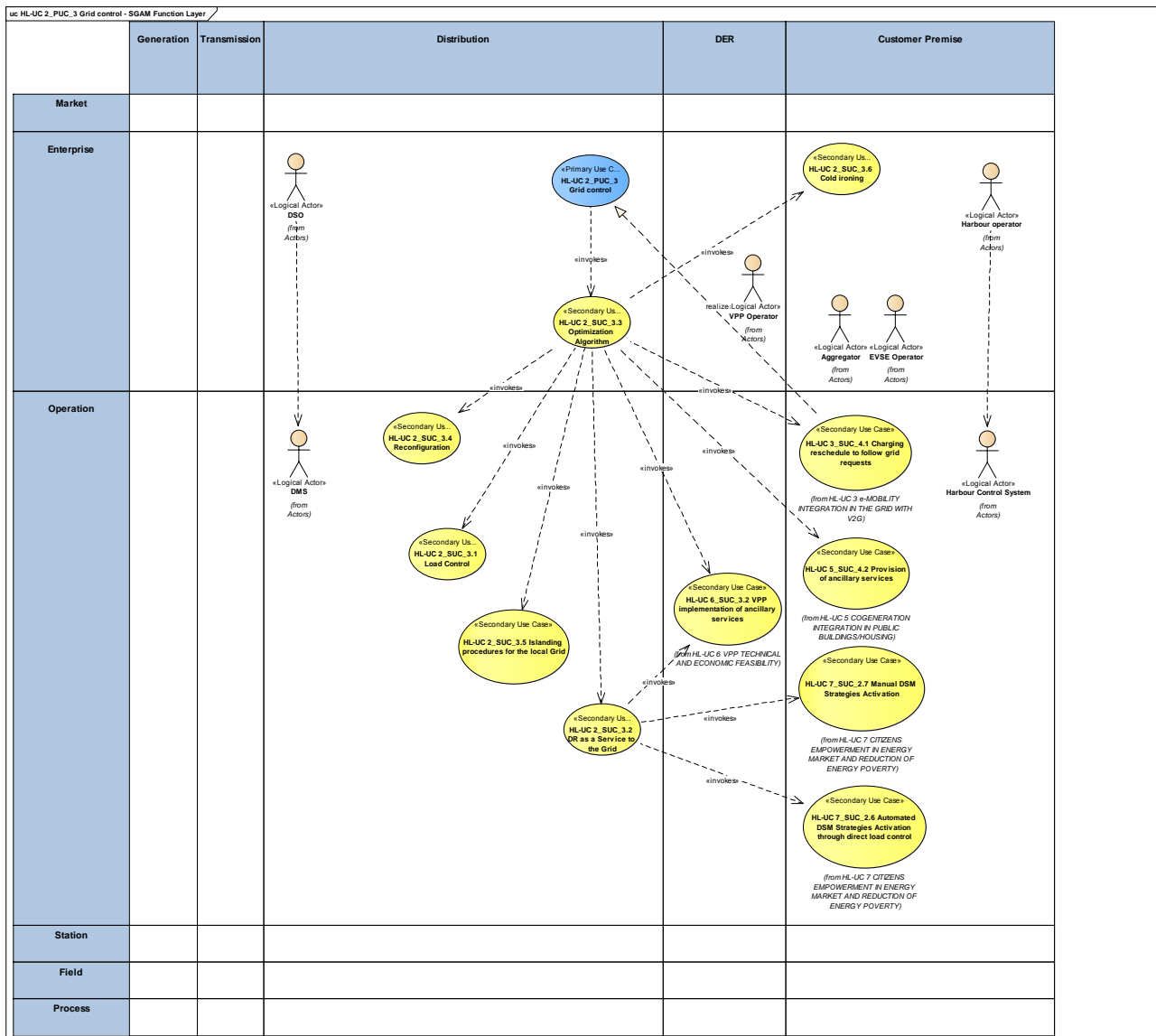


Figure 171 - SGAM Function Layer

**Table 125 - List of Actors Involved**

Actor Name	Actor Type
DSO	Organization
DMS	System
TSO	Organization
EVSE operator	Organization
RES	Device
RESCO	Organization
EVSE	Device
Harbour Control System	System
Harbour operator	Organization
EV	Device
Supplier	Organization
ESCO	Organization
VPP Operator	Organization
Aggregator	Organization
Prosumer	Person

### 19.3.4 SGAM COMPONENT LAYER

The core component of this PUC is the WG Cockpit, which is in charge of triggering actions upon the detection of a problem in the grid. Those actions may be directed to:

- Control assets under scope of action of the DSO by commanding the SCADA
- Requesting support to third party actors in the ancillary services market. The main WiseGRID applications in position to deliver this support are the WG StaaS/VPP and the WiseEVP

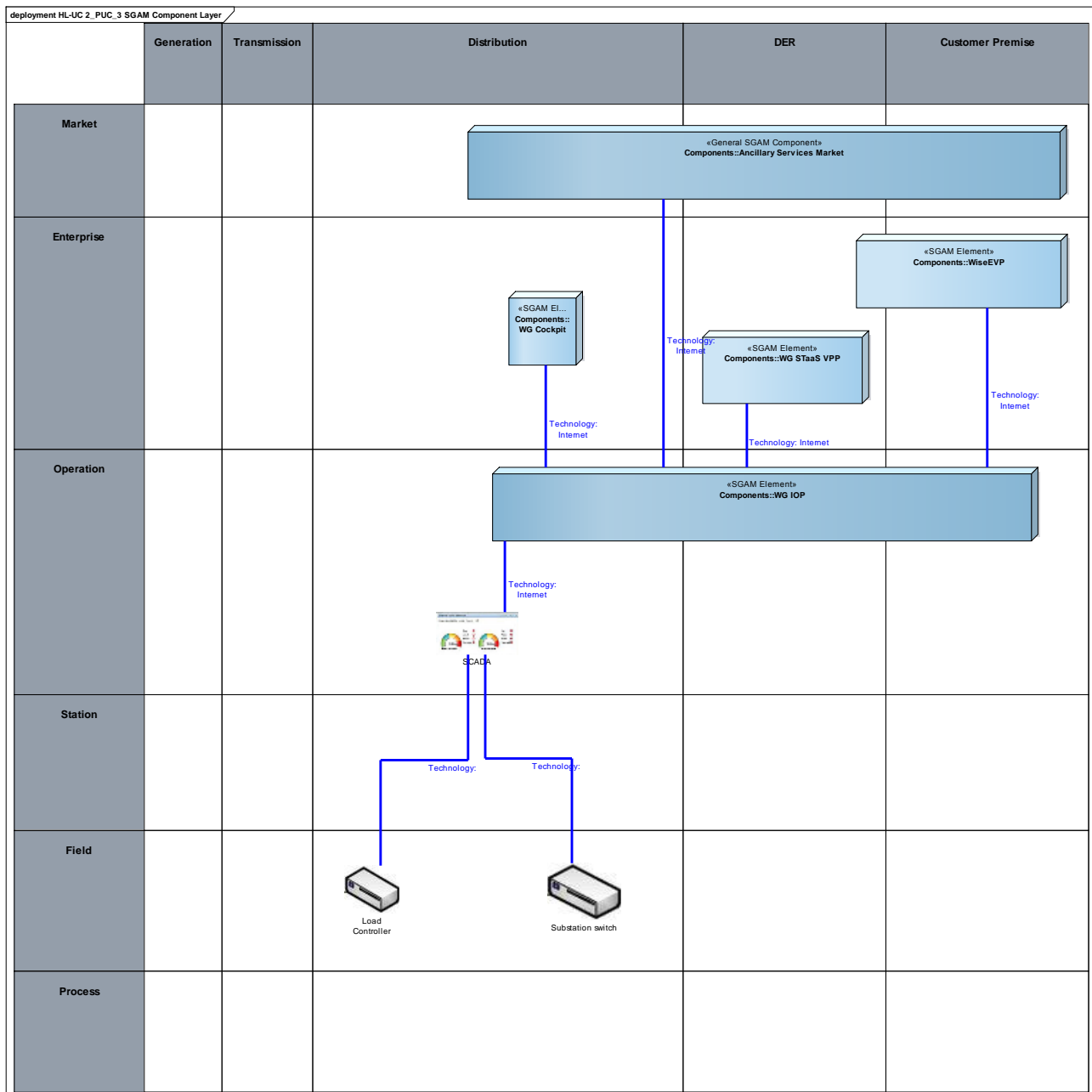


Figure 172 - SGAM Component Layer

**Table 126 - List of Components Participating in the Primary Use Case**

Component	Component Type
Ancillary Services Market	General SGAM Component
WG Cockpit	SGAM Element
WG StaaS/VPP	SGAM Element
WiseEVP	SGAM Element
WG IOP	SGAM Element
SCADA	SW Application
Load controller	Device
Substation switch	Device

### 19.3.5 SGAM COMMUNICATION LAYER

Communications identified can be divided in two different groups:

- Communication of already deployed field devices and control systems: include a variety of industrial and smart grid protocols
- Communications with WiseGRID components: include the protocols considered to be enabled by the WG IOP

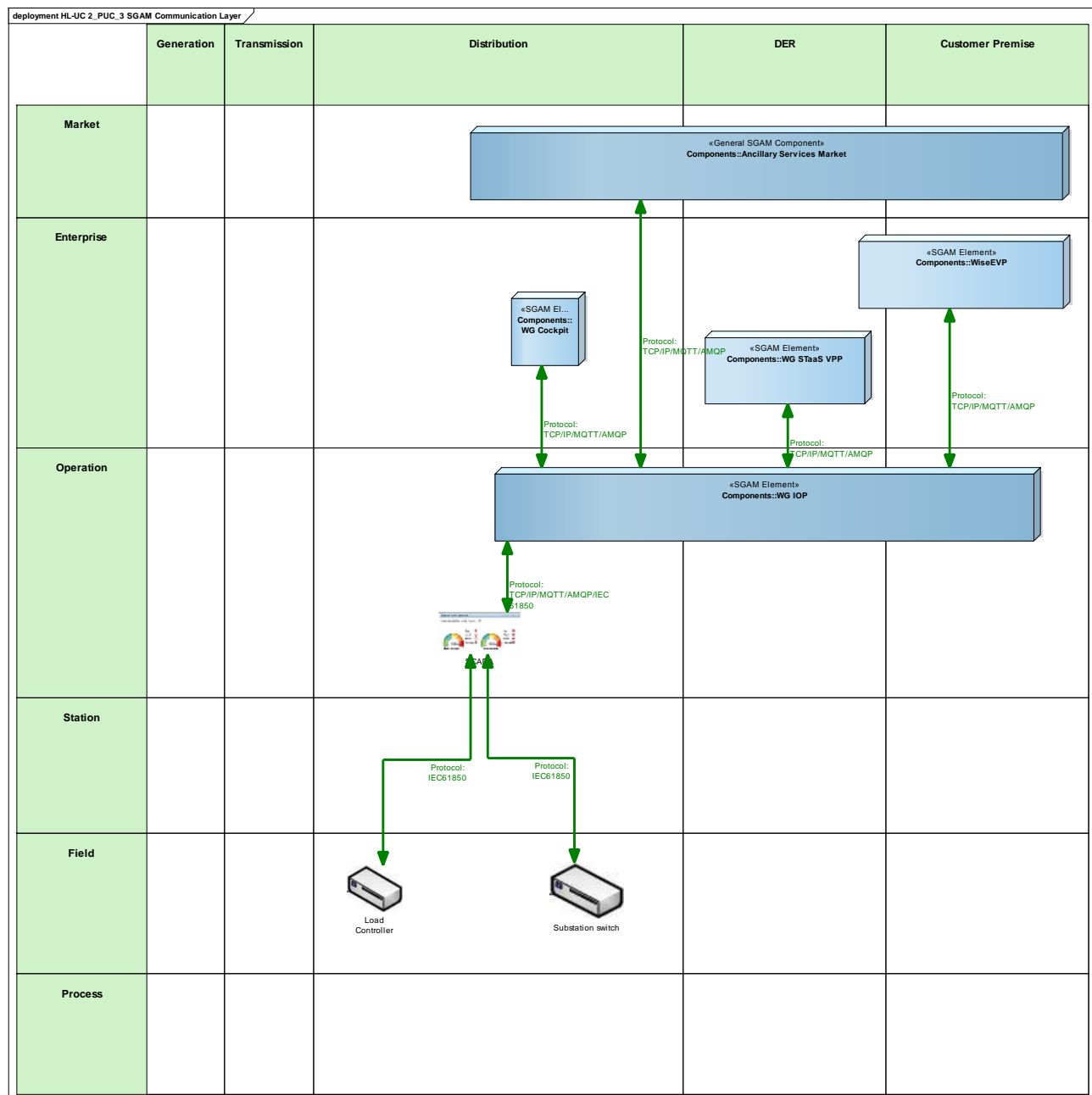


Figure 173 - SGAM Communication Layer



**Table 127 - List of Communication Technologies Involved**

Communication Technology	Description
TCP/IP	Group of protocols enabling communication between devices in a network up to the transport layer
MQTT	ISO standard (ISO/IEC PRF 20922) publish-subscribe-based lightweight messaging protocol for use on top of the TCP/IP protocol
AMQP	Open standard application layer protocol for message-oriented middleware, featuring message orientation, queuing, routing (including point-to-point and publish-and-subscribe), reliability and security
IEC61850	Standard for vendor-agnostic engineering of the configuration of Intelligent Electronic Devices for electrical substation automation systems

### 19.3.6 SGAM INFORMATION LAYER

Main information items handled within this PUC include commands to elements under control of the DSO - through the SCADA - and flexibility requests to third party actors.

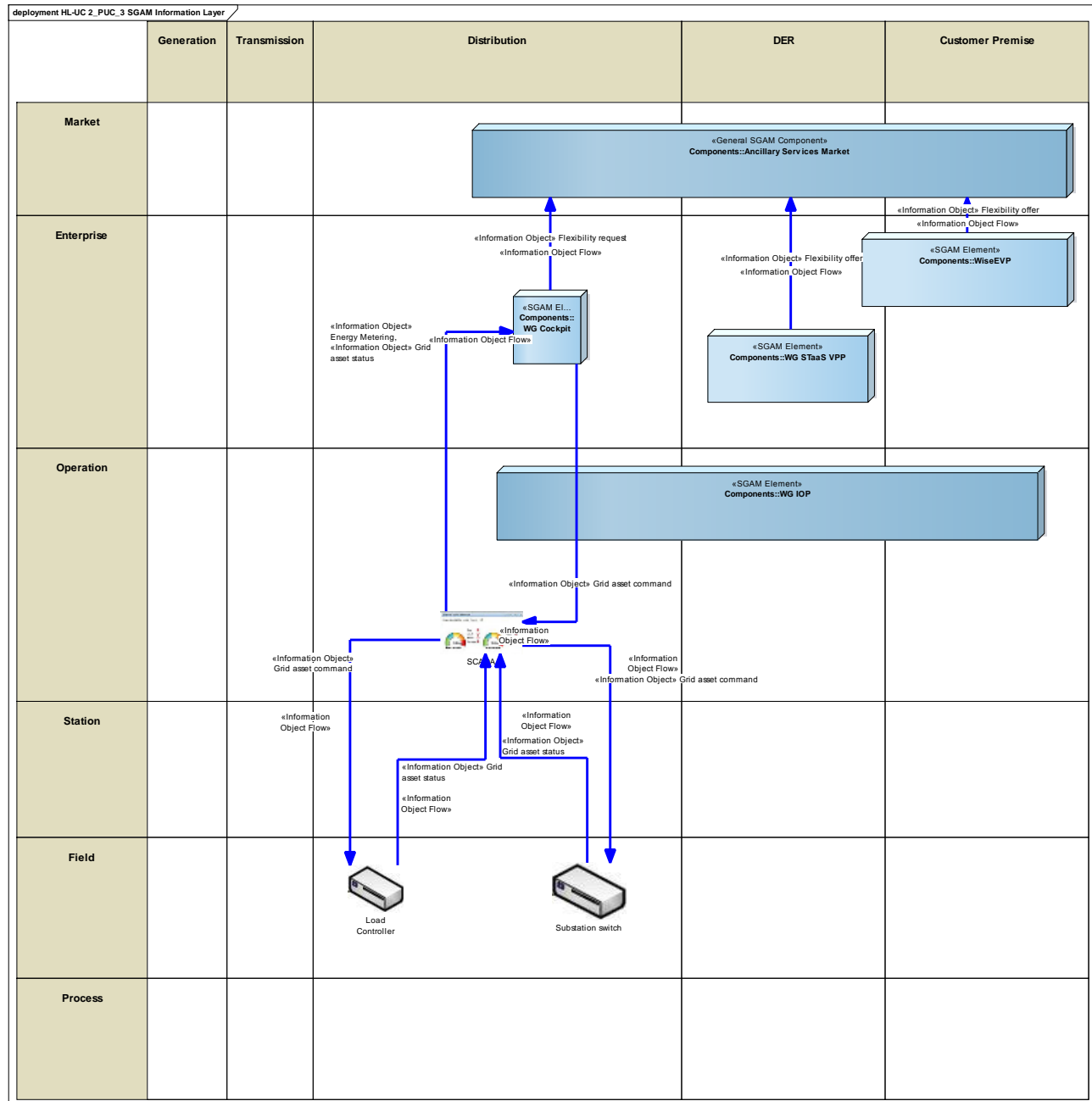


Figure 174 - SGAM Information Layer

## CANONICAL DATA MODEL

The following data models identified under this PUC for managing flexibility request, energy metering and SCADA commands.

**Table 128 - List of Data Models**

Data Models
Flexibility Data Model (USEF)
DLMS/COSEM
IEC61850

## STANDARDS AND INFORMATION OBJECT MAPPING

The following data models identified under this PUC for managing flexibility request, energy metering and SCADA commands.

**Table 129 - List of Data Standards**

Data Standards
Flexibility Data Model (USEF)
DLMS/COSEM
IEC61850

**Table 130 - List of Information Objects**

Information Objects	Data Model
DR Signal	Flexibility Data Model (USEF)
Demand Flexibility profile	Flexibility Data Model (USEF)
Demand Response request	Flexibility Data Model (USEF)
Energy metering	DLMS/COSEM
Setpoint data	IEC61850

### 19.3.7 ACTIVITY DIAGRAM

The following activity diagram depicts how the DSO shall interact with the grid elements and third party actors in order to deal with problems detected in the grid.

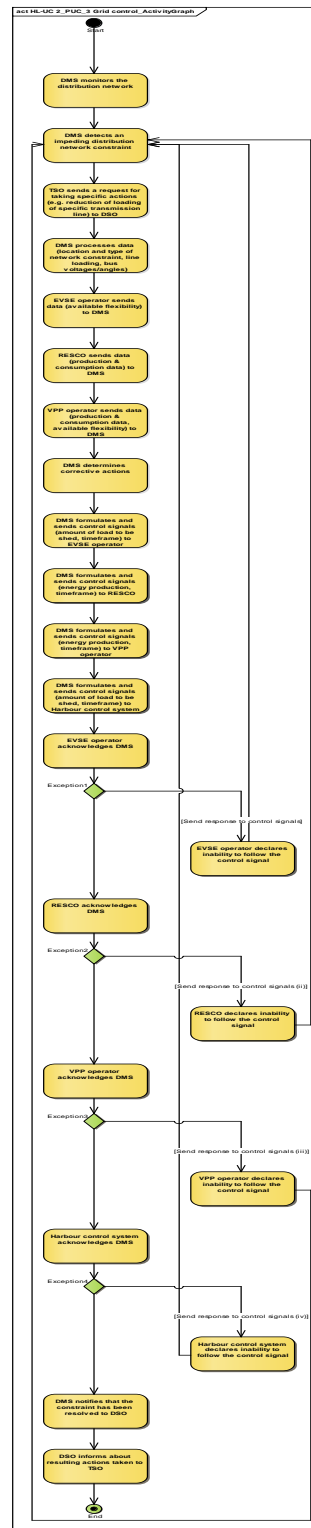


Figure 175 - Primary Use Case Activity Diagram

### 19.3.8 SEQUENCE DIAGRAM

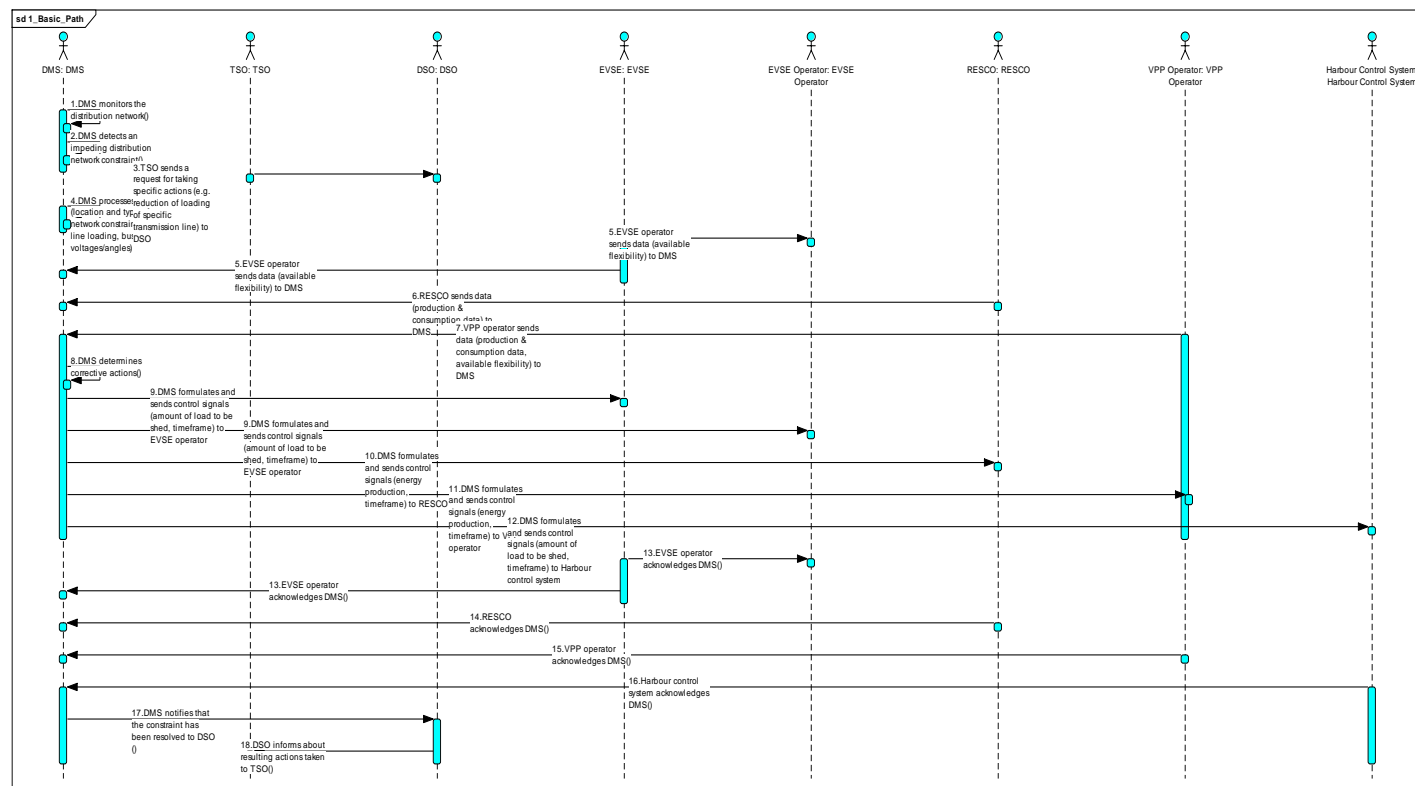


Figure 176 - Primary Use Case Sequence Diagram

## **20 APPENDIX C - ARCHITECTURE**

### **HL-UC 3: E-MOBILITY INTEGRATION IN THE GRID WITH V2G**

## 20.1 HL-UC 3\_PUC\_1: EVSE AND EV FLEET MONITORING

### 20.1.1 PRIMARY USE CASE DESCRIPTION

This PUC describes the data collection process from the EVSEs and the EVs. This PUC contains two SUCs:

#### DATA COLLECTION FROM EVSE:

This secondary use case describes the data gathering from each EVSE to the WiseEVP and the WG IOP. The gathered data will be mainly the energy parameters that are provided by a smart meter per socket (power, current, etc.) and also EVSE status information (available, reserved, charging, unavailable, faulted etc.).

#### DATA COLLECTION FROM EVS:

This secondary use case describes the data gathering from the EVs to the WiseEVP/WiseHOME and the WG IOP.

### 20.1.2 SECONDARY USE CASE INTERACTIONS

This PUC invokes two SUCs to retrieve data from EVSEs and EVs

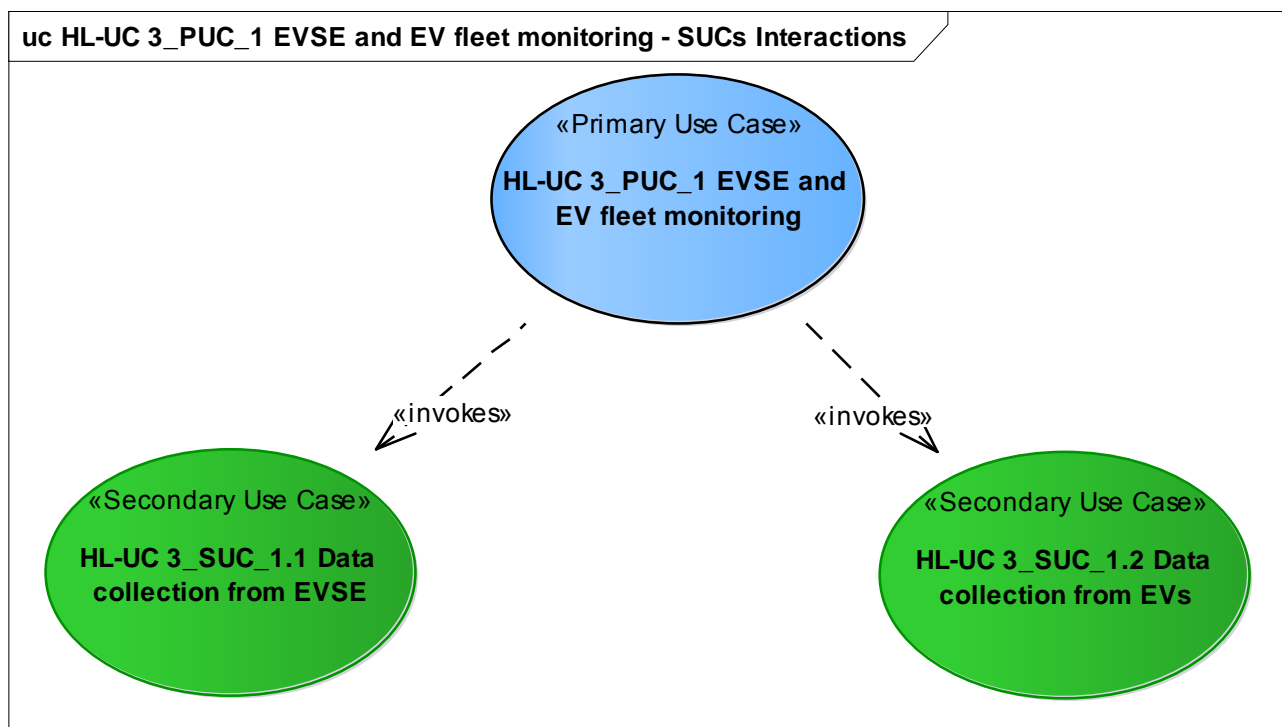


Figure 177 - SUCs Interactions Diagram

Table 131 - Table of list of participating SUCs

SUC Name	Description	Relation	PUC/SUC
HL-UC 3_SUC_1.1	Data collection from EVSE		
HL-UC 3_SUC_1.2	Data collection from EVs		

### 20.1.3 SGAM FUNCTION LAYER

Both SUCs under this PUC are located in the *station* zone - since they deal with collection of data from field devices - of the *DER* domain - since those field devices are basically electric vehicles batteries and the required charging infrastructure, which can be seen as distributed storage.

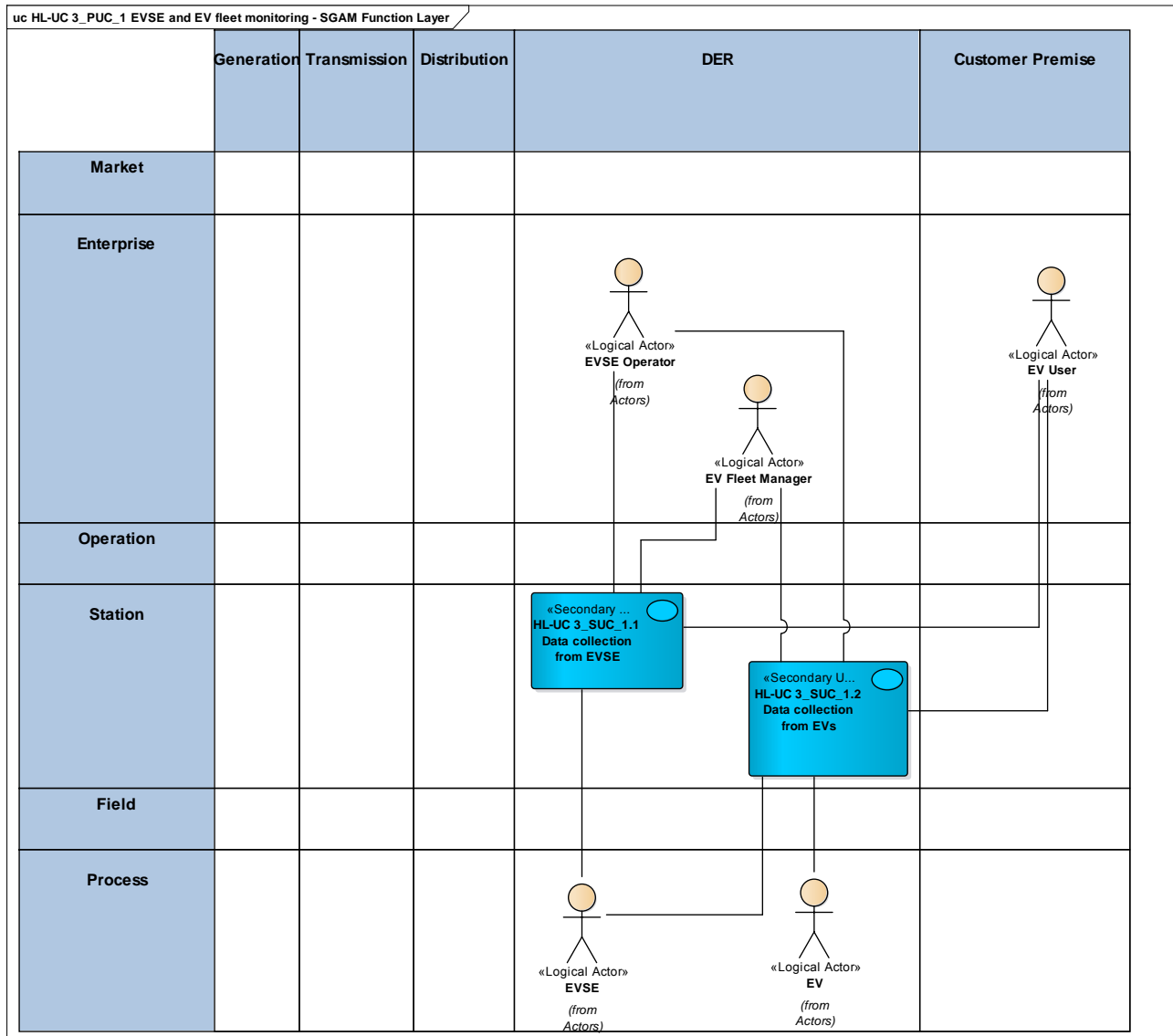


Figure 178 - SGAM Function Layer

Table 132 - List of Actors Involved

Actor Name	Actor Type
EV	Device
EVSE	Device
EVSE Operator	Organization
EV Fleet Manager	Organization
EV User	Person



#### 20.1.4 SGAM COMPONENT LAYER

Core component of this PUC is the WiseEVP application, in charge of managing fleets of electric vehicles and the required charging infrastructure. WiseHOME is also considered, since we envisage the integration of domestic charging point monitoring and operation within the project as well. Those applications will interact with EVSEs of the pilot sites and with the FastV2G charging station developed as part of the project as well.

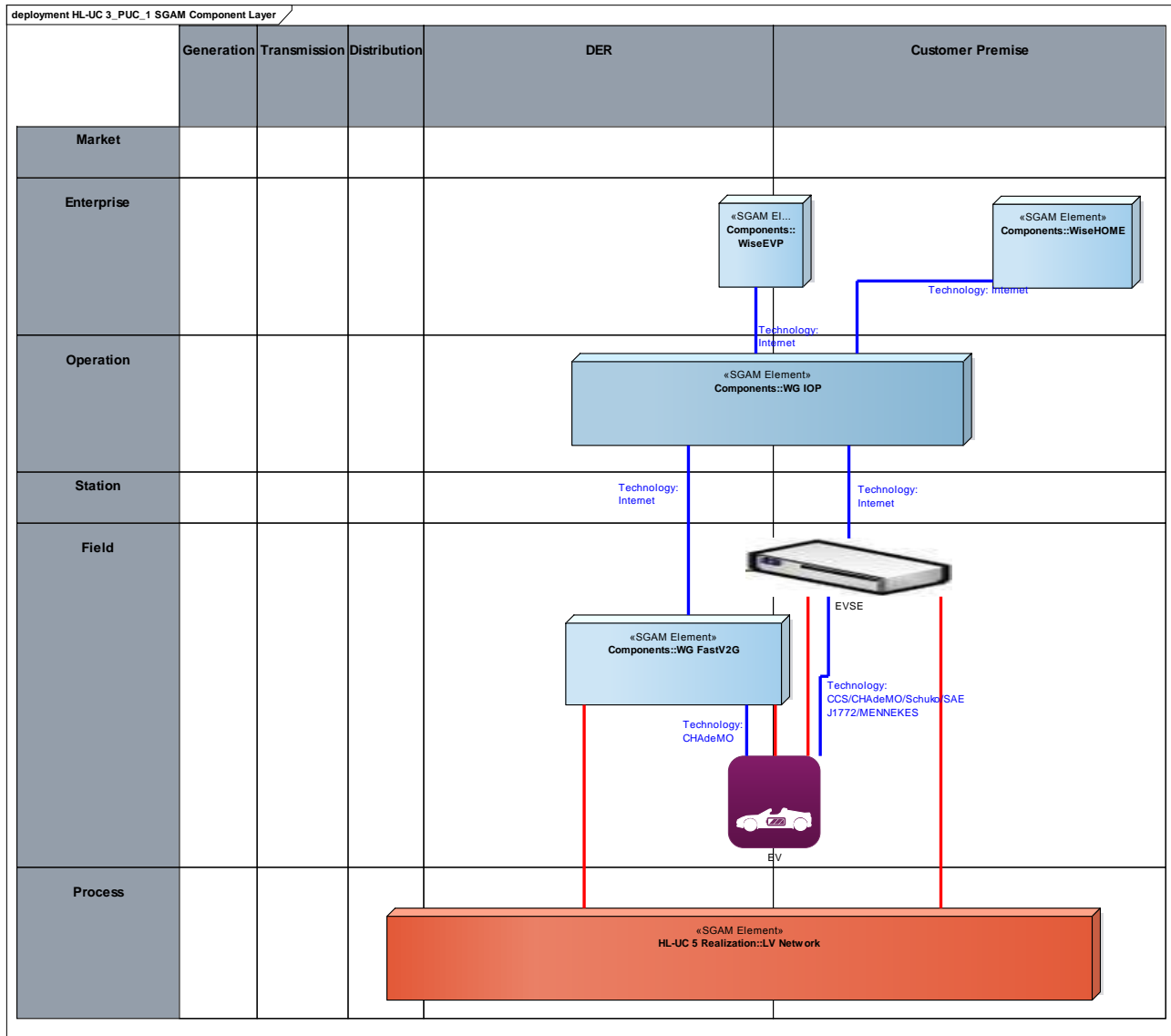


Figure 179 - SGAM Component Layer

Table 133 - List of Components Participating in the Primary Use Case

Component	Component Type
WiseEVP	SGAM Element
WiseHOME	SGAM Element
WG IOP	SGAM Element
EVSE	Device

Component	Component Type
FastV2G	SGAM Element
EV	Electric Vehicle
LV Network	SGAM Element

### 20.1.5 SGAM COMMUNICATION LAYER

The communication flows identified for this PUC can be divided into three groups:

- Communication between car and EVSE, which will depend on the vehicles and charging points of the pilot sites
- Communication between EVSE and control system, whose standard de-facto nowadays is the OCPP protocol
- Communications with WiseGRID components: include the protocols considered to be enabled by the WG IOP

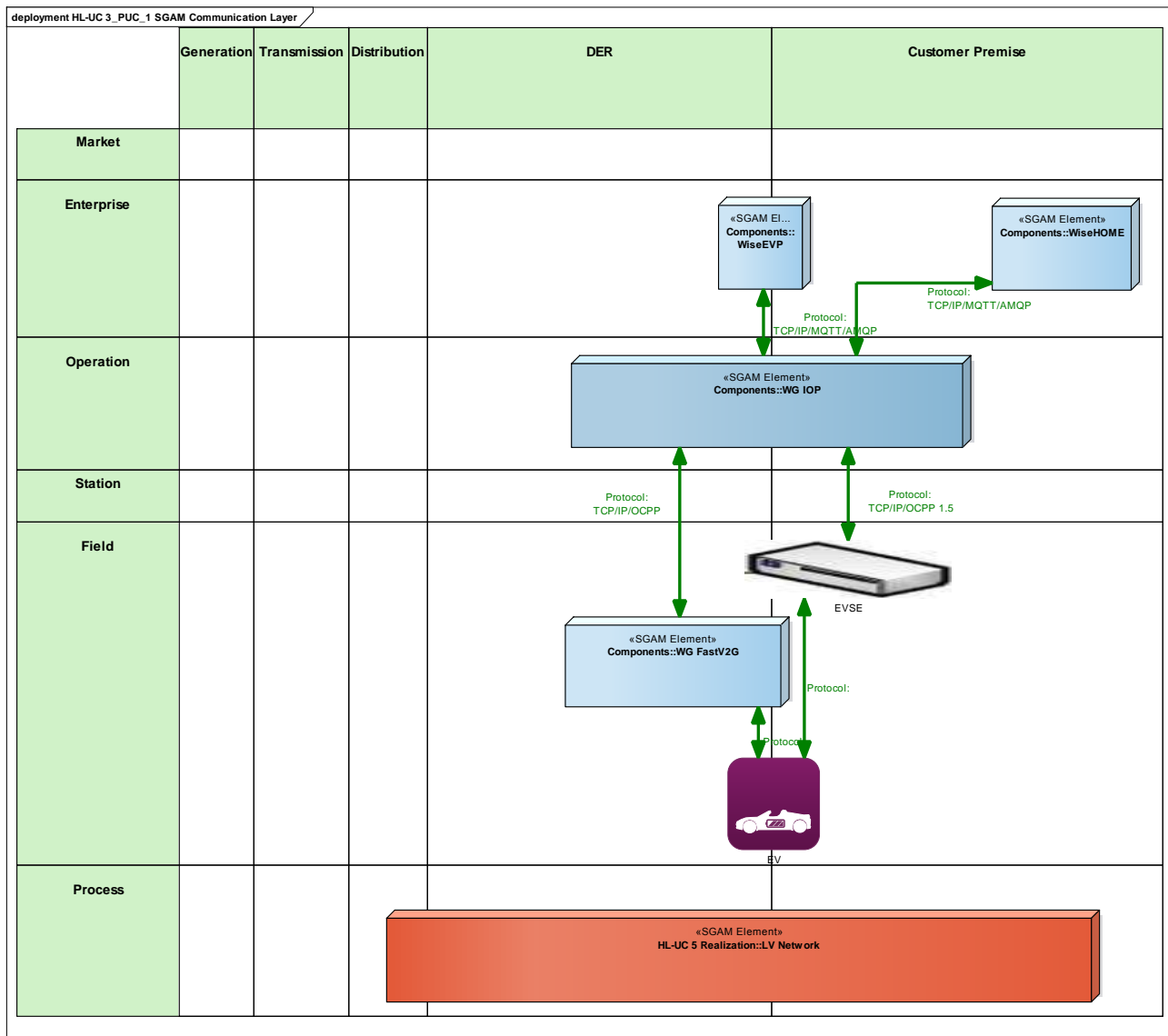


Figure 180 - SGAM Communication Layer

Table 134 - List of Communication Technologies Involved

Communication Technology	Description
TCP/IP	Group of protocols enabling communication between devices in a network up to the transport layer
AMQP	Open standard application layer protocol for message-oriented middleware, featuring message orientation, queuing, routing (including point-to-point and publish-and-subscribe), reliability and security
MQTT	ISO standard (ISO/IEC PRF 20922) publish-subscribe-based lightweight messaging protocol for use on top of the TCP/IP protocol
OCPP	Application protocol for communication between EV charging stations and a central management system

## 20.1.6 SGAM INFORMATION LAYER

Information to be retrieved from the charging points and the electric vehicles include battery details - such as capacity and SoC -, and charging session details - such as user identification, required supply, time constraints and battery supply constraints.

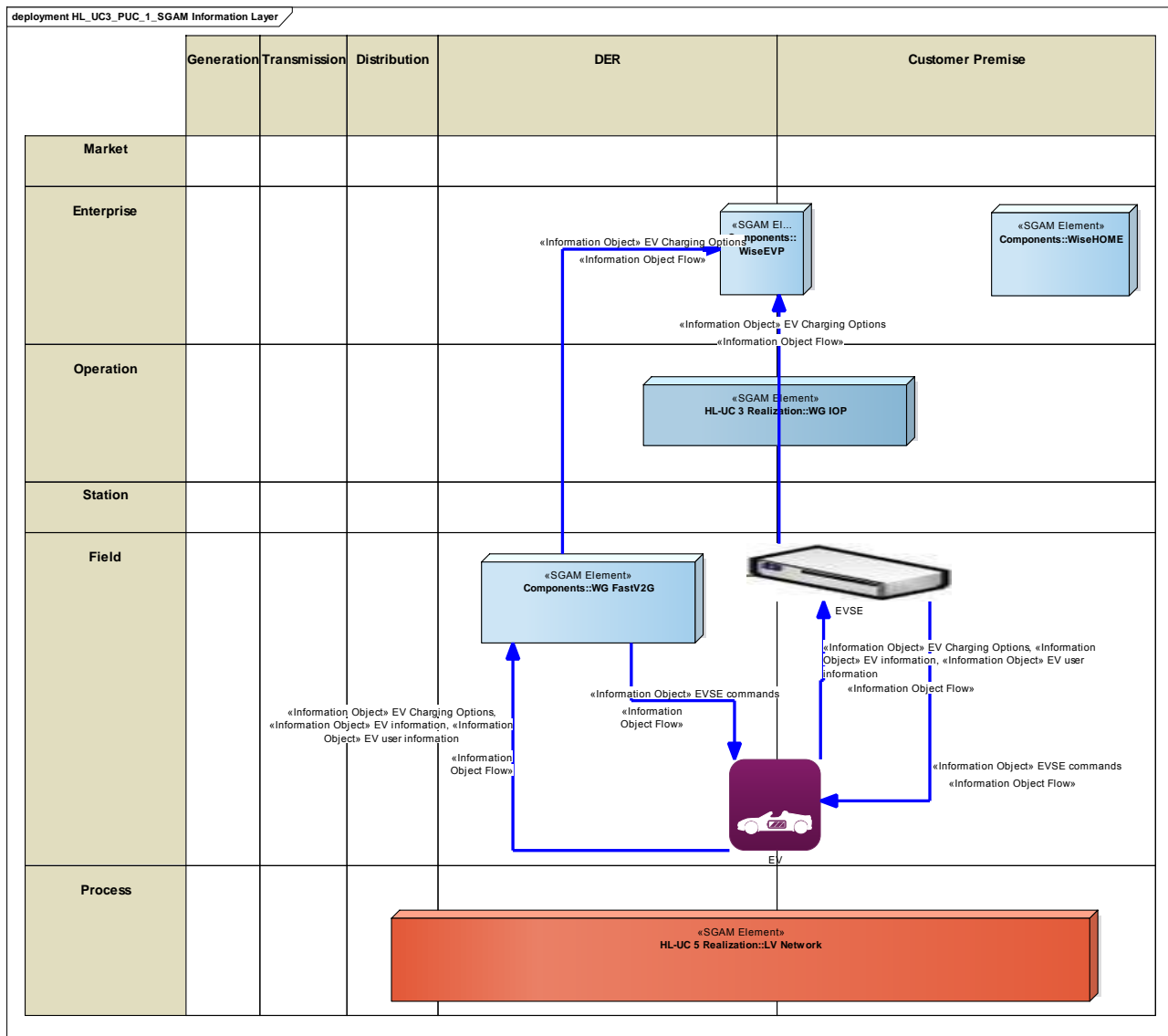


Figure 181 - SGAM Information Layer

## CANONICAL DATA MODEL

The following data models have been identified for modelling the information related to electric vehicles, charging points and charging sessions.

Table 135 - List of Data Models

Data Models
OCPP

## STANDARDS AND INFORMATION OBJECT MAPPING

Table 136 - List of Data Standards

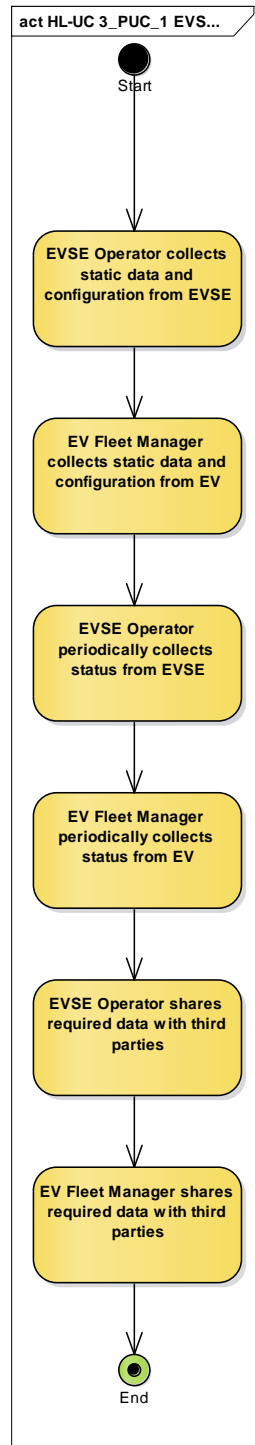
Data Standards
OCPP

Table 137 - List of Information Objects

Information Objects	Data Model
EV charging options	OCPP
EV user information	OCPP
EV information	OCPP
EVSE commands	OCPP
EVSE metering info	OCPP

### 20.1.7 ACTIVITY DIAGRAM

The following diagram depicts the steps performed by the EV/EVSE operator to retrieve the necessary data from the field devices.



**Figure 182 - Primary Use Case Activity Diagram**

## 20.1.8 SEQUENCE DIAGRAM

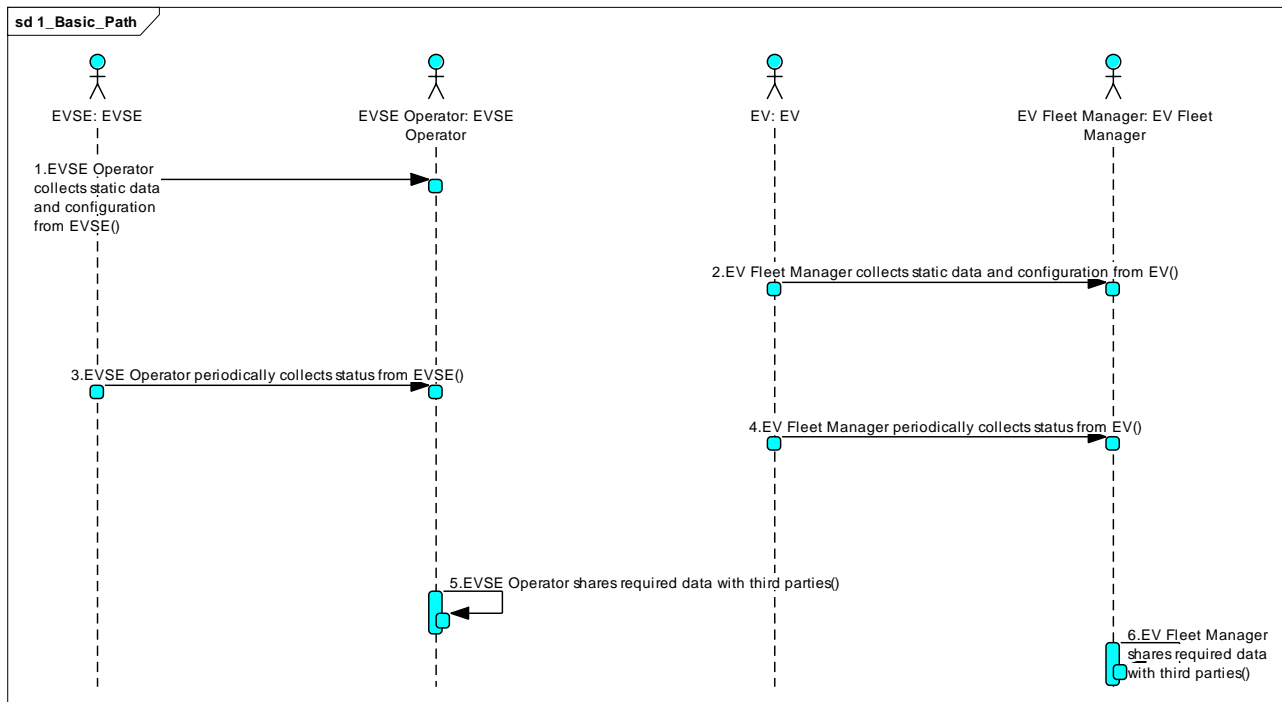


Figure 183 - Primary Use Case Sequence Diagram

## 20.2 HL-UC 3\_PUC\_2: INTERACTION OF THE USER WITH EVSE

### 20.2.1 PRIMARY USE CASE DESCRIPTION

This PUC describes the interaction of the EV user (driver) with the charging infrastructure (EVSEs) in order to authenticate, start a charging session or book an EVSE. The user will be able to select (or book in advance) three different types of charging sessions:

- Type 1: Charging on user demand. Once the EV user plugs the EV and selects the desired final SOC, the EVSE charges the EV at the maximum power.
- Type 2: Smart charging. Once the EV user plugs the EV and selects the desired final SOC and selects the time to disconnect the EV, the EVSE performs a flexible charging session managing the charging power output to follow energy prices, to avoid network congestion, to maximise the RES integration, etc.
- Type 3: Smart charging with V2G. The principle is exactly the same as type 2 but allowing power injection in the electrical network (V2G), meaning that enhanced network services can be provided.

Note: The EVSEs just “perform” the charging sessions. The charging sessions and charging characteristics are scheduled at a high level at the WiseEVP.

It includes the following SUCs:

### **USER'S AUTHENTICATION**

This SUC describes the authentication process through an EVSE before starting the charging session (also WiseEVP involved). The same process will be applied if the EV user needs to log through Smartphone Apps or web applications to the WiseEVP for booking or other purposes (if they are in the scope of WiseGRID).

### **CHARGING ON USER DEMAND**

This SUC describes how the user starts and ends a “charging on demand” session through an EVSE. Required information: only final SOC.

### **EVSE BOOKING**

This SUC describes how the user books a charging session through an EVSE or through other interfaces to the WiseEVP providing the required information about the user's EV and the aforementioned information depending on the charging type.



## 20.2.2 SECONDARY USE CASE INTERACTIONS

HL-UC 3\_PUC2 invokes 3 SUCs to obtain data from EV user and EVSEs to customer identification, define infrastructures availability and process charging requests. In addition, driver authentication invokes data from the charging infrastructure (it which in turn handles information from the network configuration) and requested recharge data

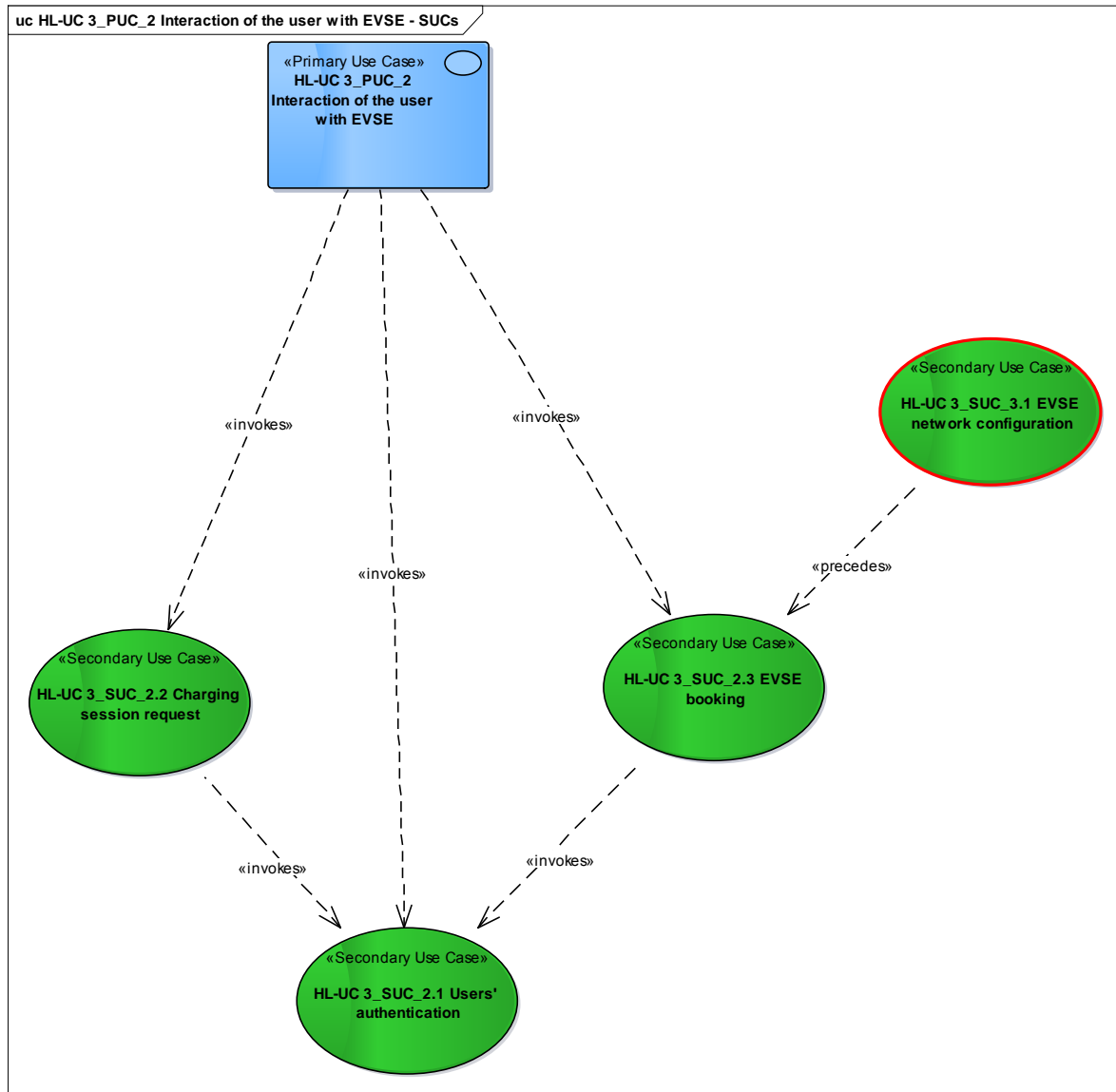


Figure 184 - SUCs Interactions Diagram

Table 138 - Table of list of participating SUCs

SUC Name	Description	Relation	PUC/SUC
HL-UC 3_SUC_2.1	Users' authentication		
HL-UC 3_SUC_2.2	Charging session request	invokes	HL-UC 3_SUC_2.1
HL-UC 3_SUC_2.3	EVSE booking	invokes preceded	HL-UC 3_SUC_2.1 HL-UC 3_SUC_3.1

### 20.2.3 SGAM FUNCTION LAYER

The SUCs that contains this PUC are considered in the customer premise domain consisting of facilities designated to attend end users of electricity. There are located on field zone allowing the interaction of the EV user with the EV charging infrastructure making use of several functionalities through intelligent electronic devices which acquire and use process data from the power system to control and monitor of it.

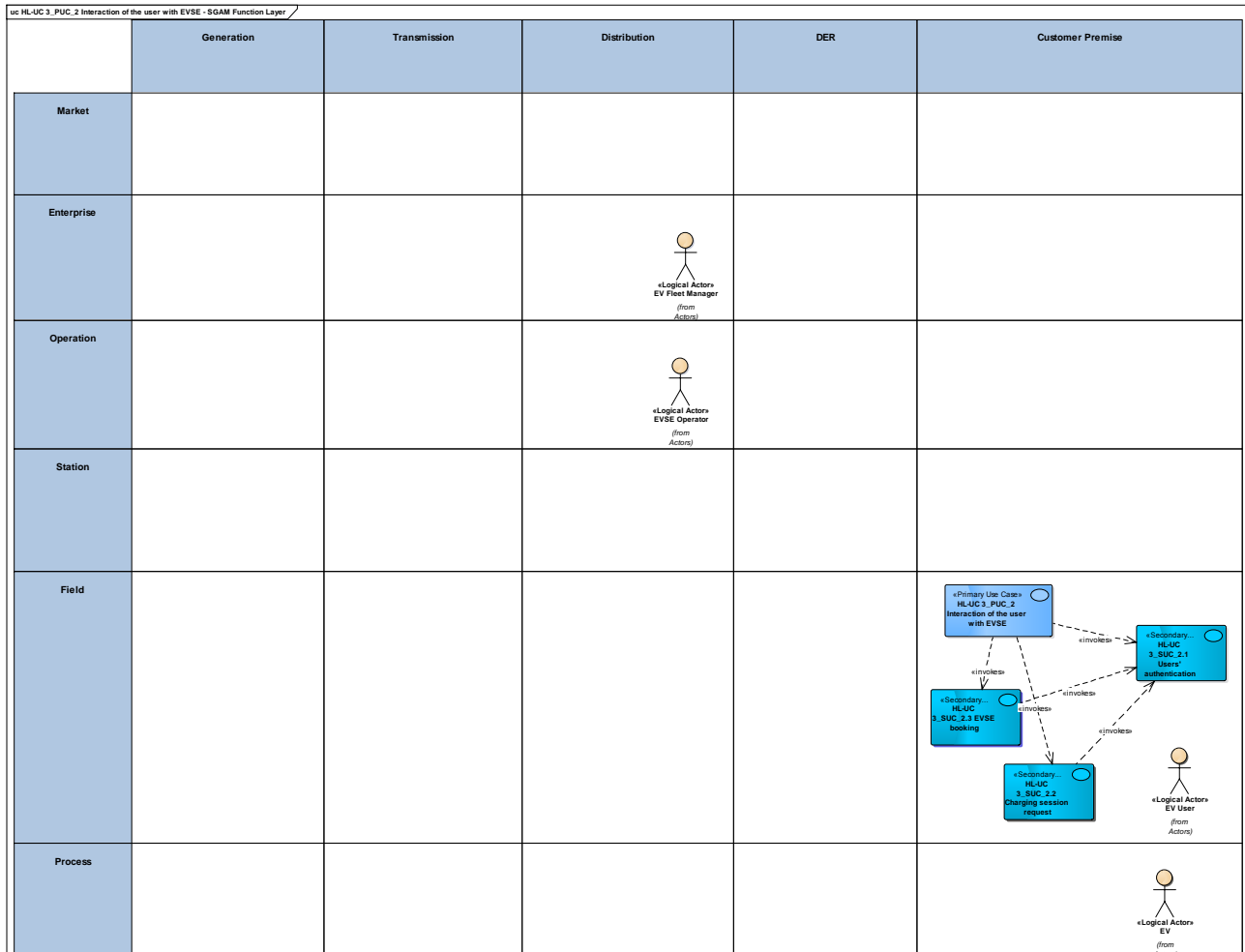


Figure 185 - SGAM Function Layer

The related actors are those in position of either providing information or getting benefit from the availability of an interaction function that defines kind of the supply.

Table 139: Participating actors

Actor Name	Actor Type
EV user	Person
EV	Device
EVSE Operator	Organization
EV Fleet manager	Organization

## 20.2.4 SGAM COMPONENT LAYER

The main component of this PUC is the WiseEVP which will interact with others components under the customer premise domain to obtain all require information to executed the demand functionalities.

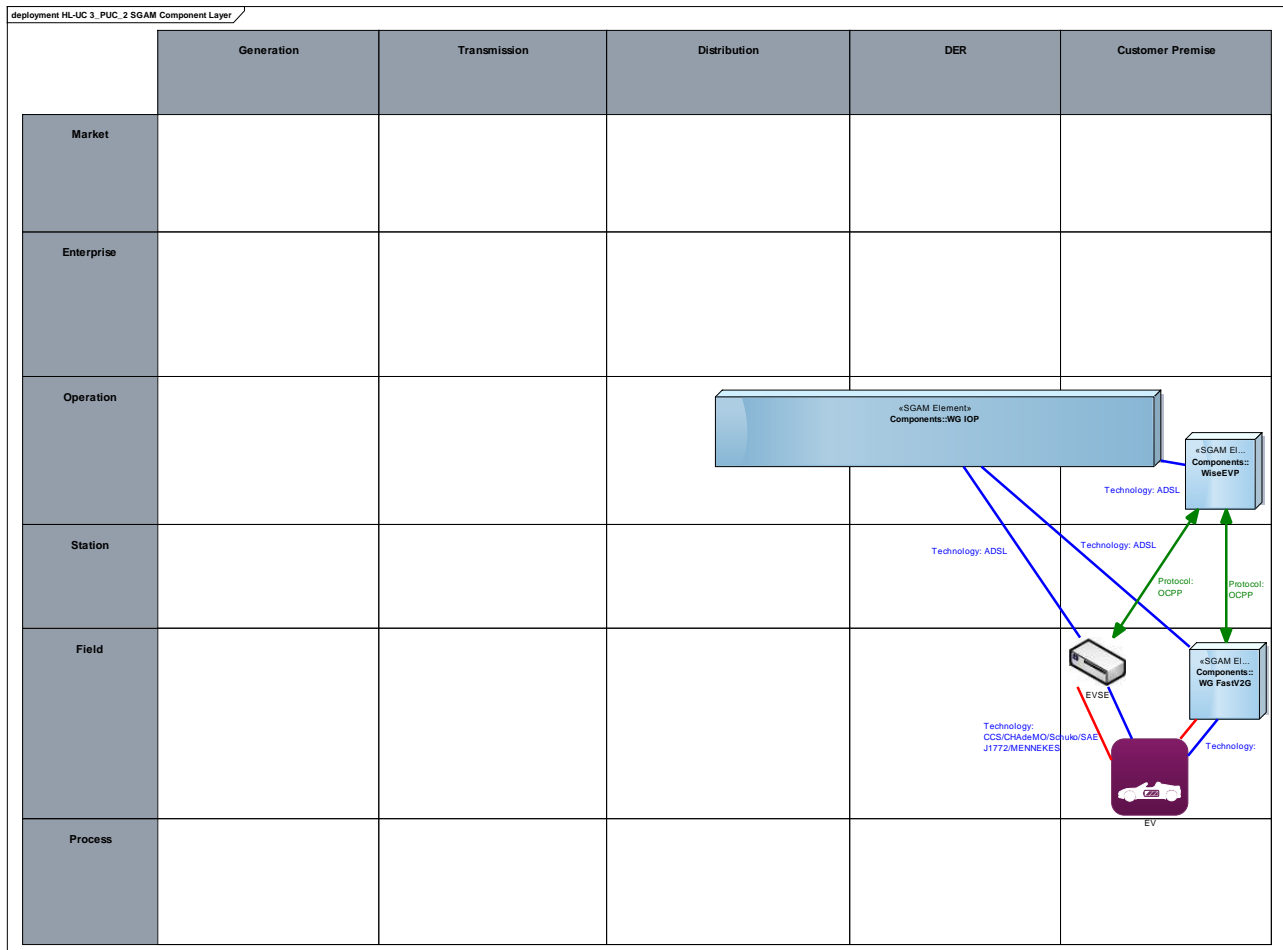


Figure 186 - SGAM Component Layer

WG FastV2G is another component comprehend by this PUC which allows for user is able to configure a charging station, developed as part of the project, and start a type 2 or type 3 charging session interacting with directly on EVSE.

**Table 140 - List of Components Participating in the Primary Use Case**

Component	Component Type
WiseEVP	SGAM Element
WG FastV2G	SGAM Element
EV	Electric Vehicle
EVSE	Device
WG IOP	SGAM Element

## 20.2.5 SGAM COMMUNICATION LAYER

Communications to implement in this PUC can be identified in two different types:

- WG IOP connectivity with WiseGRID components: include the protocols considered to be enabled
- Communications between WISE EVP and facility devices that constitute control system of charging modes

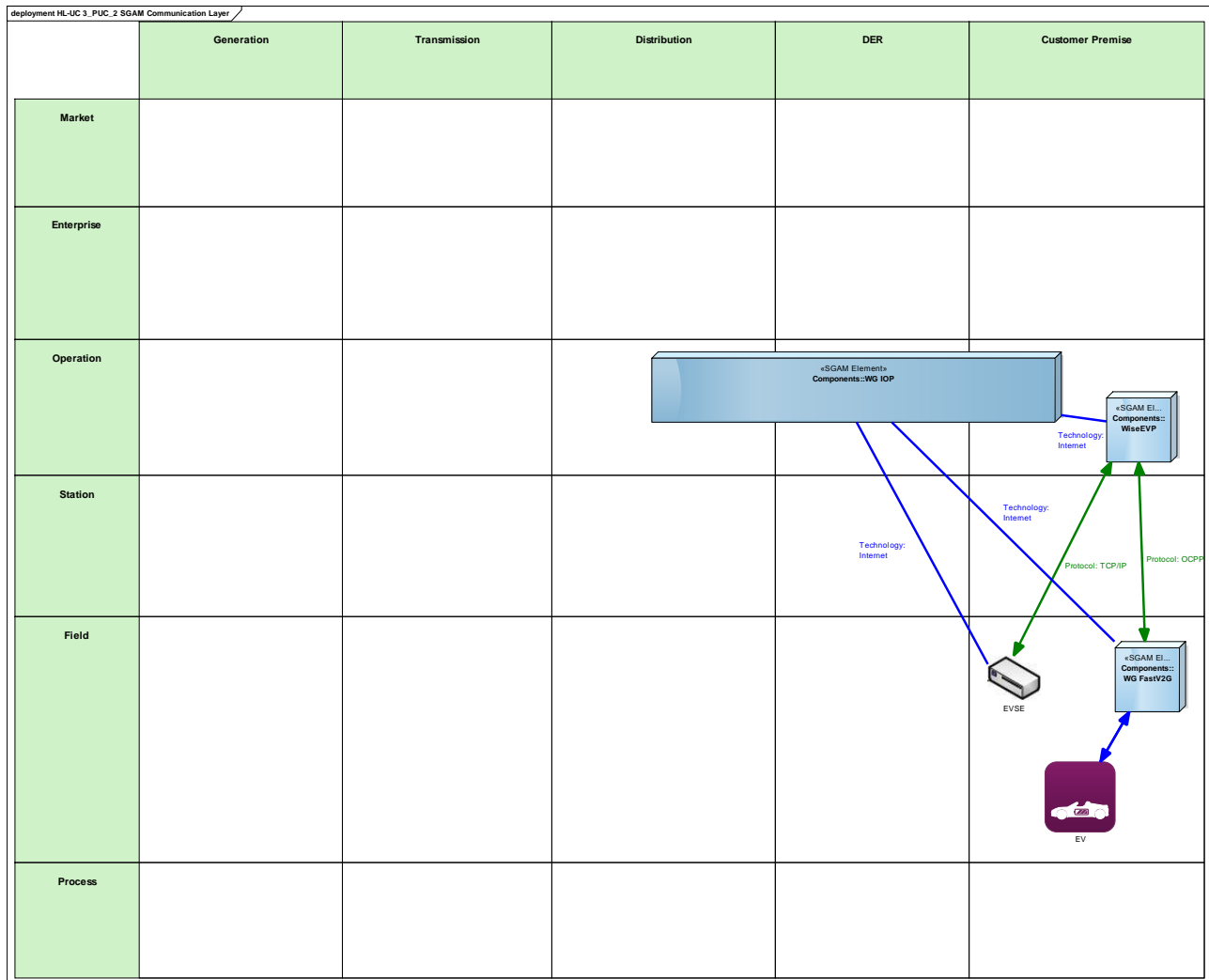


Figure 187 - SGAM Communication Layer

Table 141 - List of Communication Technologies involved

Communication Technology	Description
OCPP	Application protocol for communication between EV charging stations and a central management system
IEC61850	Specification for narrow band powerline communication
TCP/IP	Group of protocols enabling communication between devices in a network up to the transport layer

## 20.2.6 SGAM INFORMATION LAYER

The main information items handled in this PUC are related to electrical vehicle and charging stations that imply retrieved data from field device (EVSE) and WG FASTV2G, included details such battery, charging session or user identification, required to define supply, time and battery constraints.

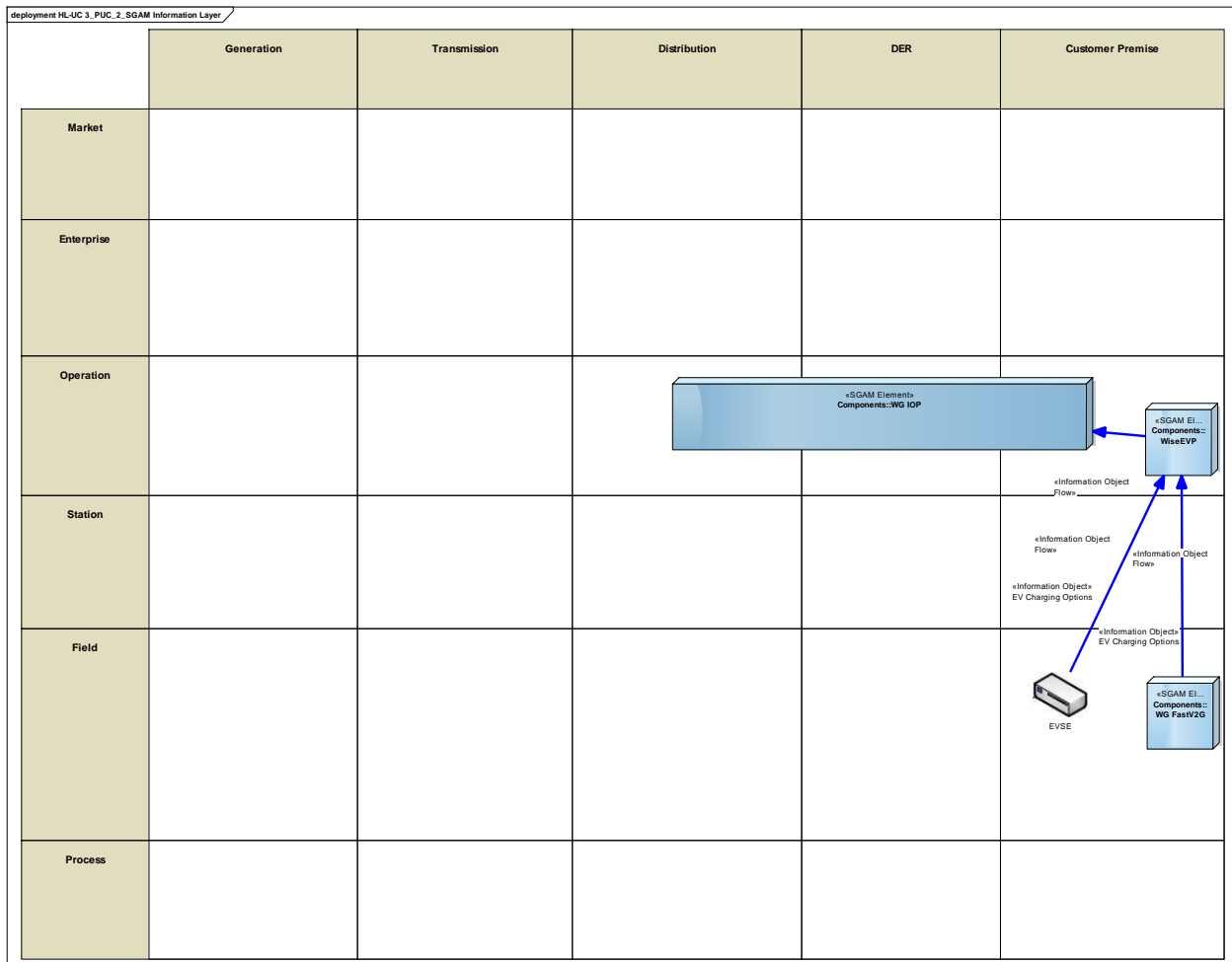


Figure 188 - SGAM Information Layer

## CANONICAL DATA MODEL

OCPP protocol is standard data model information related to EV charging stations and charging sessions.

**Table 142 - List of Data Models**

<b>Data Models</b>
OCPP

## STANDARDS AND INFORMATION OBJECT MAPPING

**Table 143 - List of Data Standards**

<b>Data Standards</b>
OCPP

**Table 144 - List of Information Objects**

<b>Information Objects</b>	<b>Data Model</b>
EV charging options	OCPP
EV user information	OCPP
EV information	OCPP
EVSE commands	OCPP
EVSE metering info	OCPP
Charging mode	OCPP

### 20.2.7 ACTIVITY DIAGRAM

The following activity diagram resumes the steps executed under this PUC to retrieve the necessary data from the field devices of the controlled facilities.

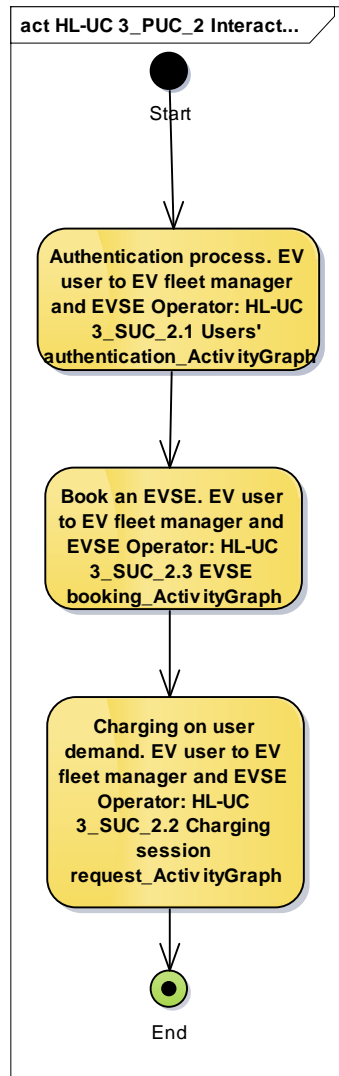


Figure 189 - Primary Use Case Activity Diagram



## 20.2.8 SEQUENCE DIAGRAM

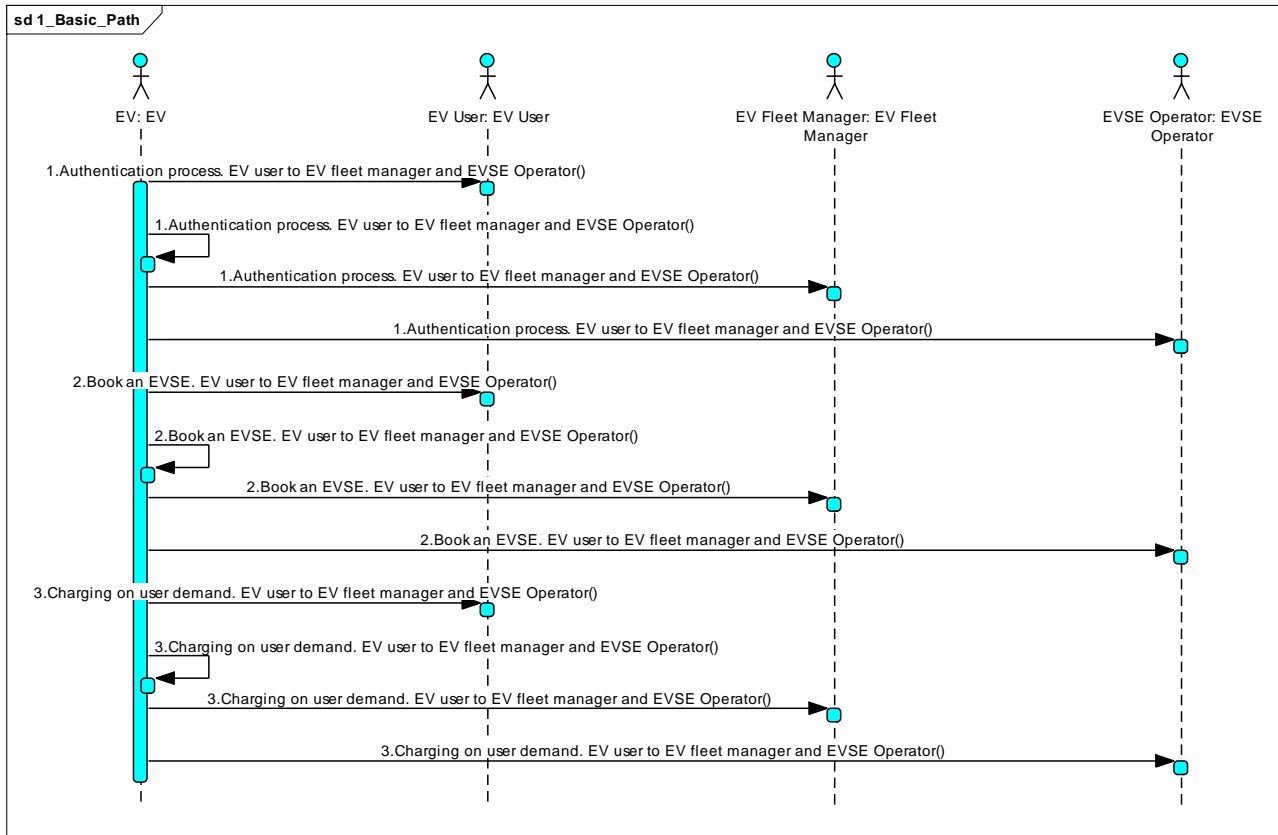


Figure 190 - Primary Use Case Sequence Diagram

## **20.3 HL-UC 3\_PUC\_3: EV CHARGING MANAGEMENT**

### **20.3.1 PRIMARY USE CASE DESCRIPTION**

This PUC describes all the processes that take place in the WiseEVP to manage the charging sessions of the EVSE and to schedule the charging session according to the EV user preferences.

It includes the following SUCs:

#### **EVSE NETWORK CONFIGURATION**

This SUC describes how the EVSE network in the WiseEVP is configured grouping the EVSEs under its management in regulation areas and providing the main characteristics of each EVSE: location, number of sockets, maximum power, charging modes, V2G capabilities, public/private management, plugged directly in the network or inside a household, etc.

#### **EV LOAD FORECASTING**

This secondary use case describes how the WiseEVP performs EV load forecasting with in different time frames (following day, following number of hours, etc.) and how often they are updated to provide them to the Wise Tools interacting with the market and managing the electrical network.

#### **EV FLEXIBILITY ESTIMATION**

This SUC describes how management of multiple EVSE connected to the same 'regulation area' allows for offering flexibility in the energy demand for charging EVs, in order to respond to demands of the grid operator based on the current status of the grid.

#### **REFERENCE LOAD PROFILE CALCULATION**

This SUC describes how WiseEVP calculates the reference load profile per regulation area. The reference load profile will be the default charging session profile used by the EVSEs (per regulation area) if the user selects types 2-3 charging sessions. Then, according to the RES and grid needs, this profile will be periodically updated (or not) as a result of the rescheduling processes (see HL-UC 3\_SUC\_4.1 and HL-UC 3\_SUC\_4.2).

#### **CHARGING SESSION SCHEDULE**

This SUC describes how the WiseEVP schedules the type 2-3 charging sessions of its EVSE network when no flexibility requests are triggered.

HL-UC 3 PUC3 invokes 5 SUCs to accomplished with requirements of the EVSE Operator or the Fleet Manager to manage the EV charging infrastructure (topology will be managed by WG Cockpit and offered to other applications via IOP) and calculate the potential flexibility services that might be offered to other WiseGRID tools. In addition the Wise EVP performs EV load forecasting with in different time frames, calculates the reference load profile per regulation area and schedules the type 2-3 charging sessions.



**Table 145 - Table of list of participating SUCs**

SUC Name	Description	Relation	PUC/SUC
HL-UC 3_SUC_3.1	EVSE network configuration	precedes precedes precedes	HL-UC 3_SUC_3.2 HL-UC 3_SUC_3.3 HL-UC 3_SUC_3.4
HL-UC 3_SUC_3.2	EV load forecasting	uses preceded	HL-UC 3_SUC_3.5 HL-UC 3_SUC_1.1
HL-UC 3_SUC_3.3	EV flexibility estimation	uses preceded uses uses	HL-UC 3_SUC_3.5 HL-UC 3_SUC_1.1 HL-UC 3_SUC_4.1 HL-UC 3_SUC_4.2
HL-UC 3_SUC_3.4	Reference charging load profile calculation	preceded uses uses	HL-UC 3_SUC_1.1 HL-UC 3_SUC_4.1 HL-UC 3_SUC_4.2
HL-UC 3_SUC_3.5	Charging session schedule	precedes precedes	HL-UC 3_SUC_4.1 HL-UC 3_SUC_4.2

### 20.3.3 SGAM FUNCTION LAYER

The SUCs that contains this PUC are considered in the distribution domain representing the infrastructure and organization which distributes electricity to customers. There are located on different zones reflecting the possible market operations (flexibility estimation), including commercial and organizational processes (fleet manager) or hosting power system control operation (DSO, charging stations, loads).

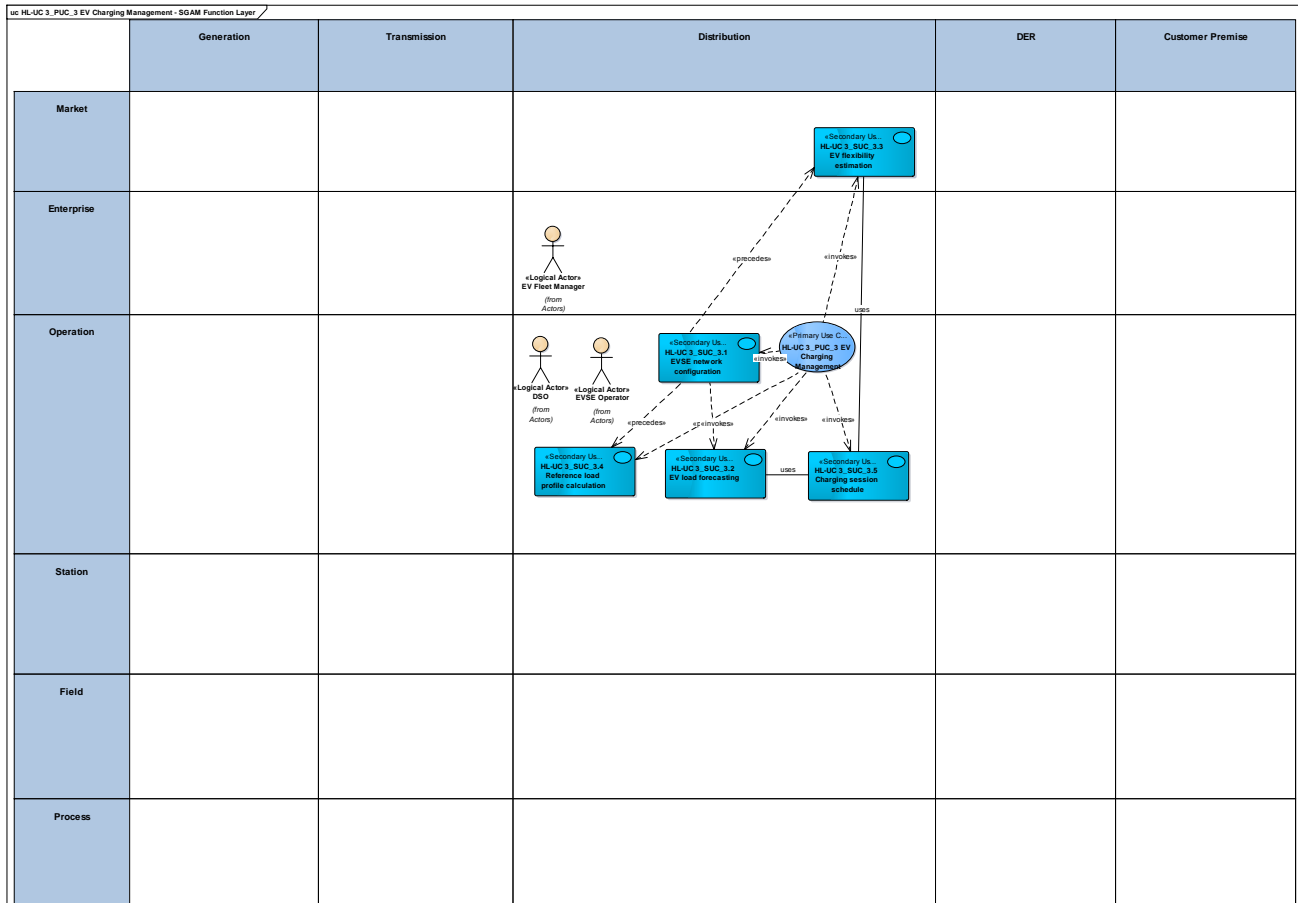


Figure 192 - SGAM Function Layer

Table 146 - List of Actors Involved

Actor Name	Actor Type
EVSE Operator	Organization
Fleet manager	Organization
DSO	Organization

### 20.3.4 SGAM COMPONENT LAYER

The main component of this PUC is the WiseEVP which will interact with others components under the customer premise domain to obtain all require information to executed the demand functionalities.

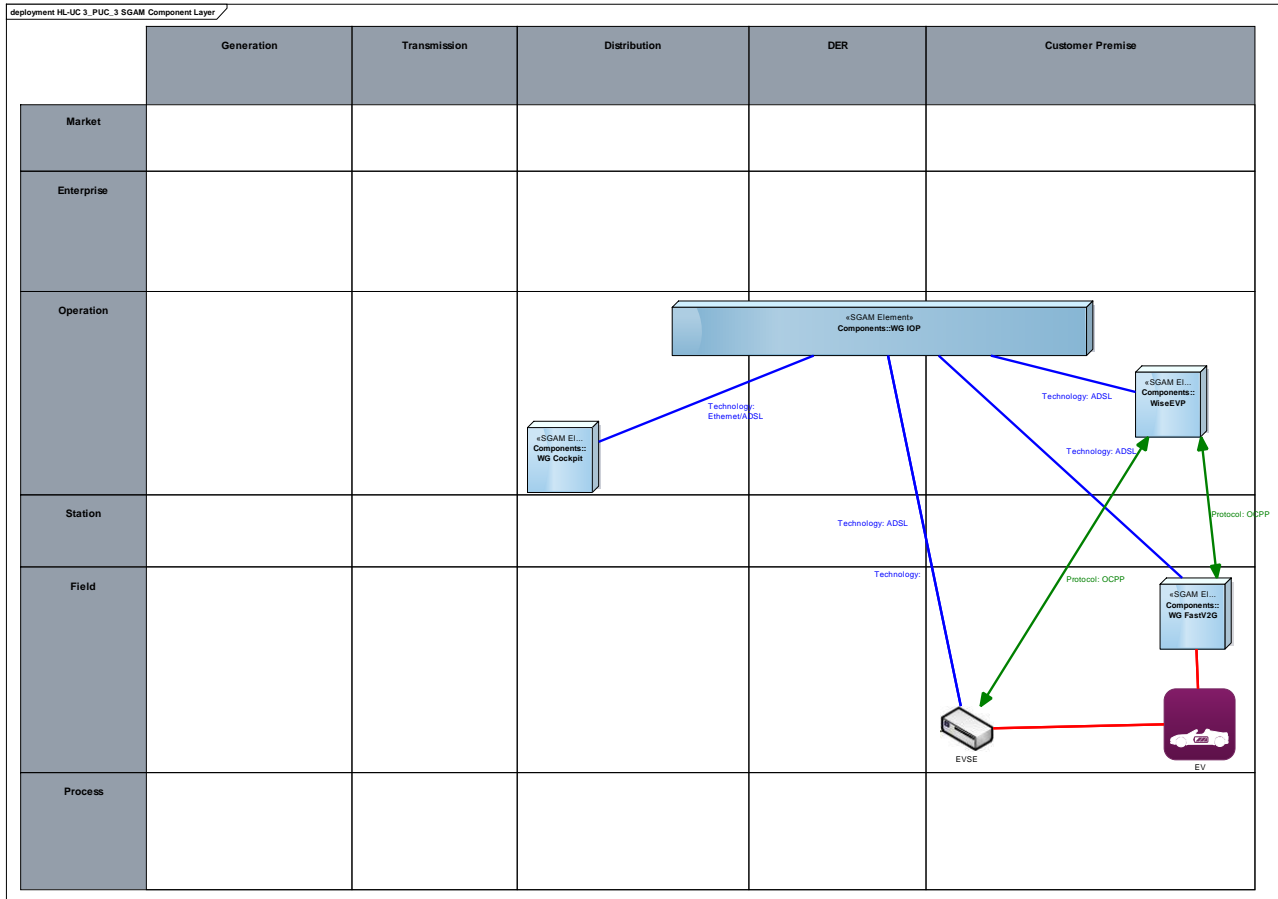


Figure 193 - SGAM Component Layer

WG Cockpit asks the WiseEVP via the WG IOP for available flexibility in a regulation area

Table 147 - List of Components Participating in the Primary Use Case

Component	Component Type
WiseEVP	SGAM Element
WG FastV2G	SGAM Element
EV	Electric Vehicle
EVSE	Device
WG IOP	SGAM Element
WG Cockpit	SGAM Element

### 20.3.5 SGAM COMMUNICATION LAYER

Communications to implement in this PUC can be identified in three different types:

- WG IOP connectivity with WiseGRID components: include the protocols considered to be enabled
- Communication of already deployed field devices and control systems: include a variety of industrial and smart grid protocols

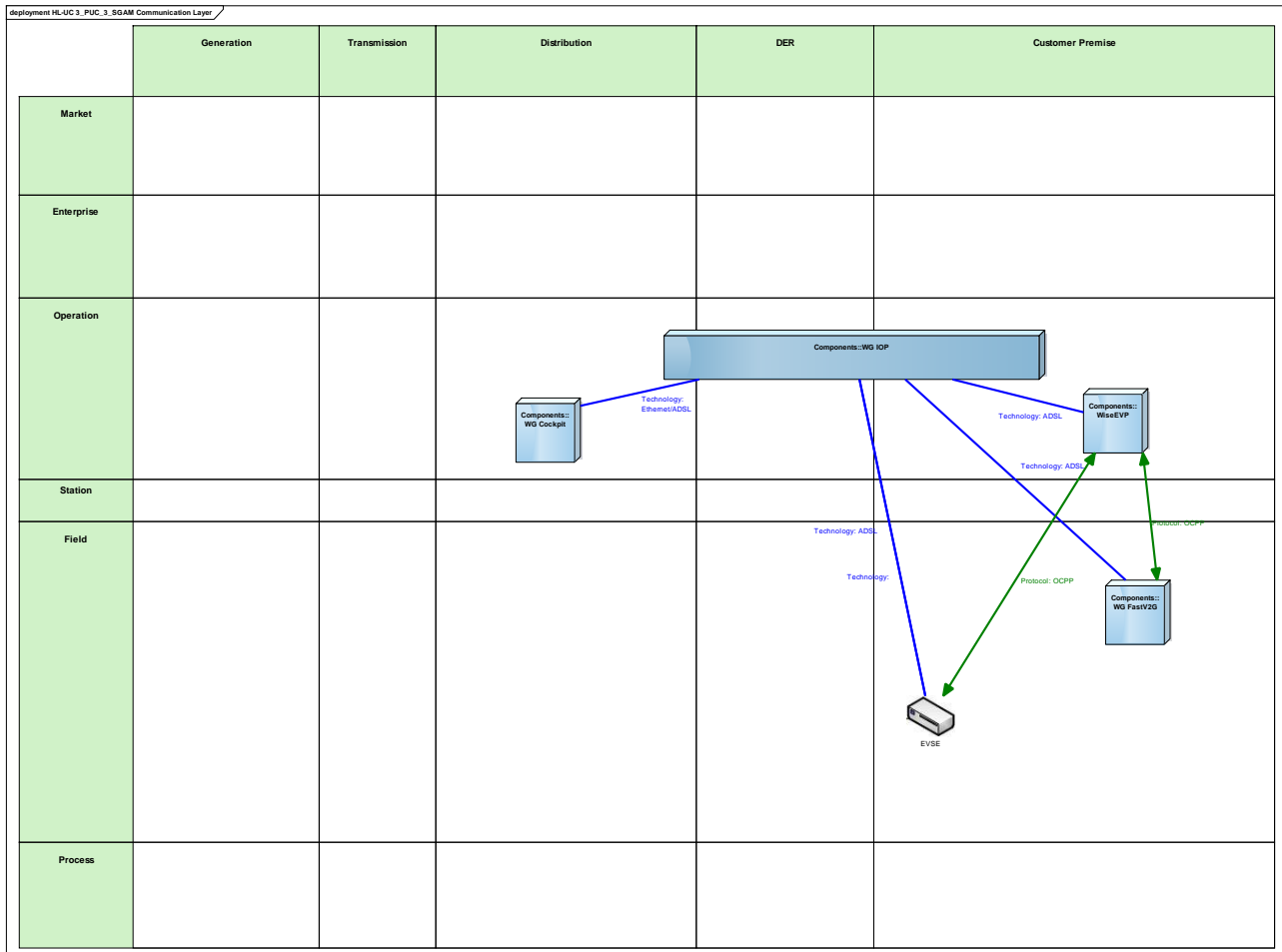


Figure 194 - SGAM Communication Layer

Table 148 - List of Communication Technologies involved

Communication Technology	Description
OCPP	Application protocol for communication between EV charging stations and a central management system
IEC61850	Specification for narrow band powerline communication
TCP/IP	Group of protocols enabling communication between devices in a network up to the transport layer
MQTT	ISO standard (ISO/IEC PRF 20922) publish-subscribe-based lightweight messaging protocol for use on top of the TCP/IP protocol

### 20.3.6 SGAM INFORMATION LAYER

The information handled in this PUC are related to electrical vehicle and charging stations that imply retrieved data from field device (EVSE) and WG FASTV2G, and flow data from field devices about state calculated or forecasted towards WG Cockpit

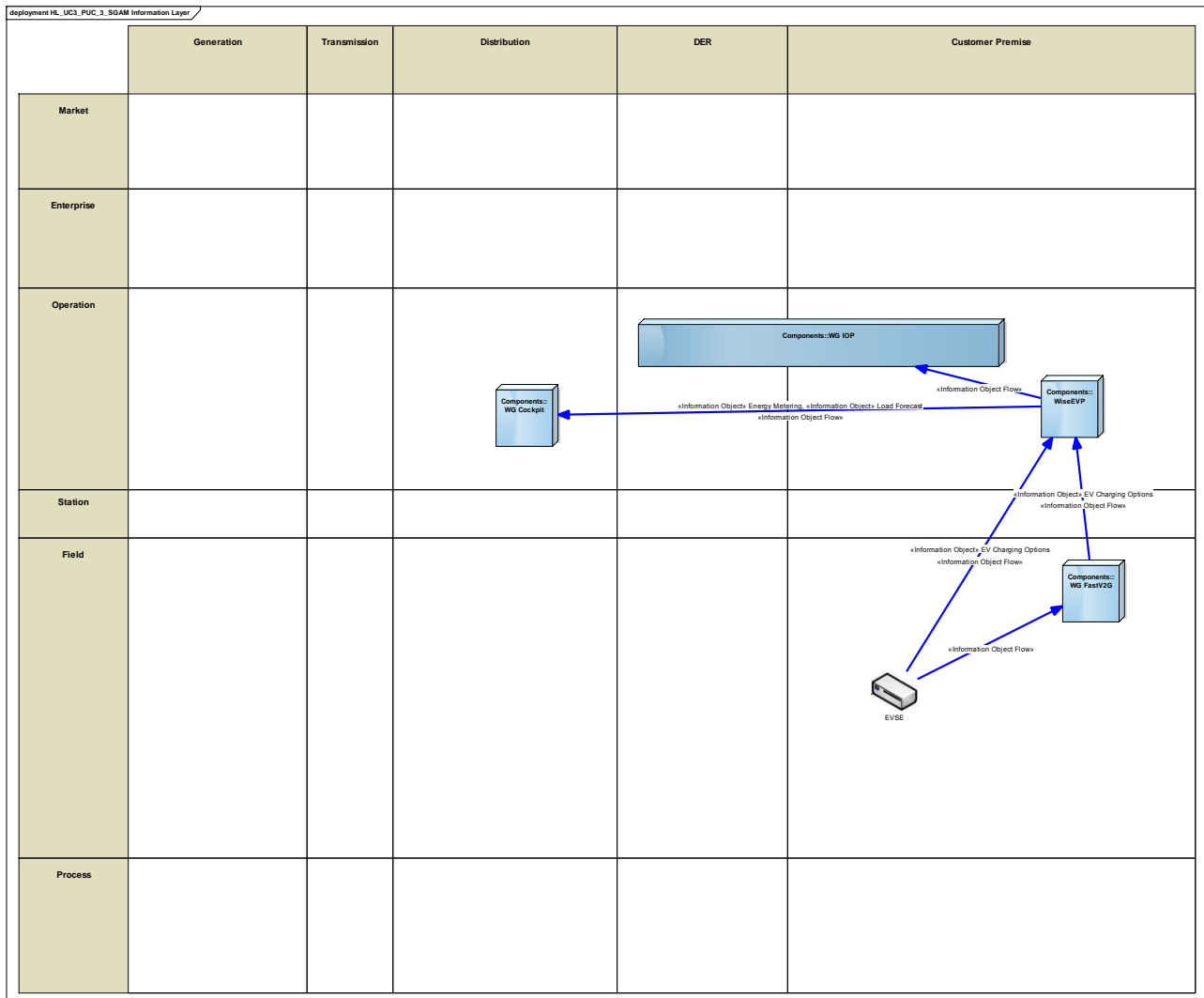


Figure 195 - SGAM Information Layer

### CANONICAL DATA MODEL

The following data models are envisaged necessary to cover the different information items identified within this PUC

Table 149 - List of Data Models

Data Models
Flexibility data model (USEF)
OCPP



## STANDARDS AND INFORMATION OBJECT MAPPING

**Table 150 - List of Data Standards**

Data Standards
Flexibility data model (USEF)
OCPP

**Table 151 - List of Information Objects**

Information Objects	Data Model
Demand Response signal	Flexibility data model (USEF)
Demand flexibility profile	Flexibility data model (USEF)
Demand response request	Flexibility data model (USEF)
Flexibility offer	Flexibility data model (USEF)
Flexibility request	Flexibility data model (USEF)
EV charging options	OCPP
EV user information	OCPP
EV information	OCPP
EVSE commands	OCPP
EVSE metering info	OCPP
Charging mode	OCPP

### 20.3.7 ACTIVITY DIAGRAM

The following activity diagram resumes the steps executed under this PUC to retrieve the necessary data from the field devices of the controlled facilities.

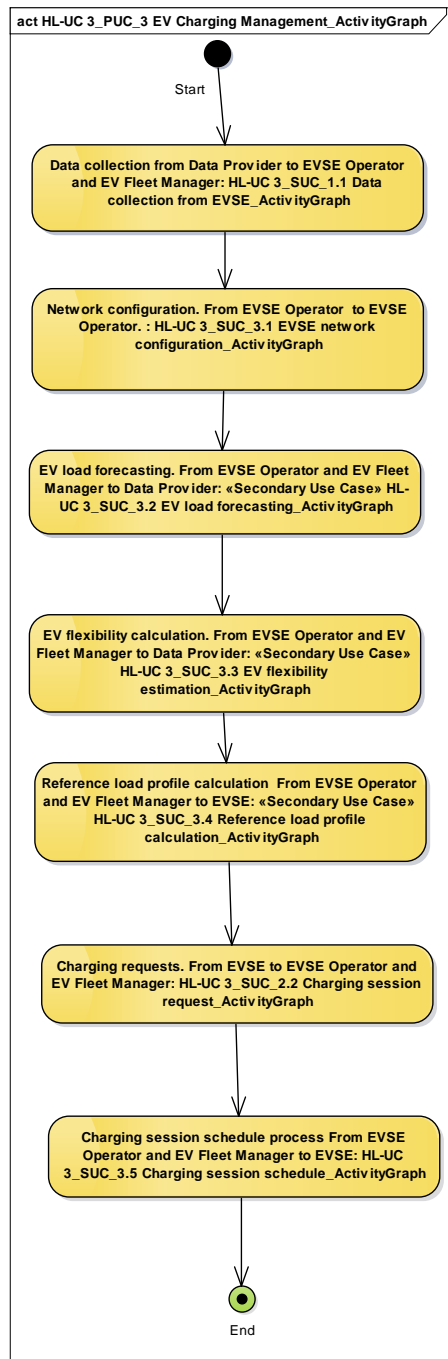


Figure 196 - Primary Use Case Activity Diagram

## 20.3.8 SEQUENCE DIAGRAM

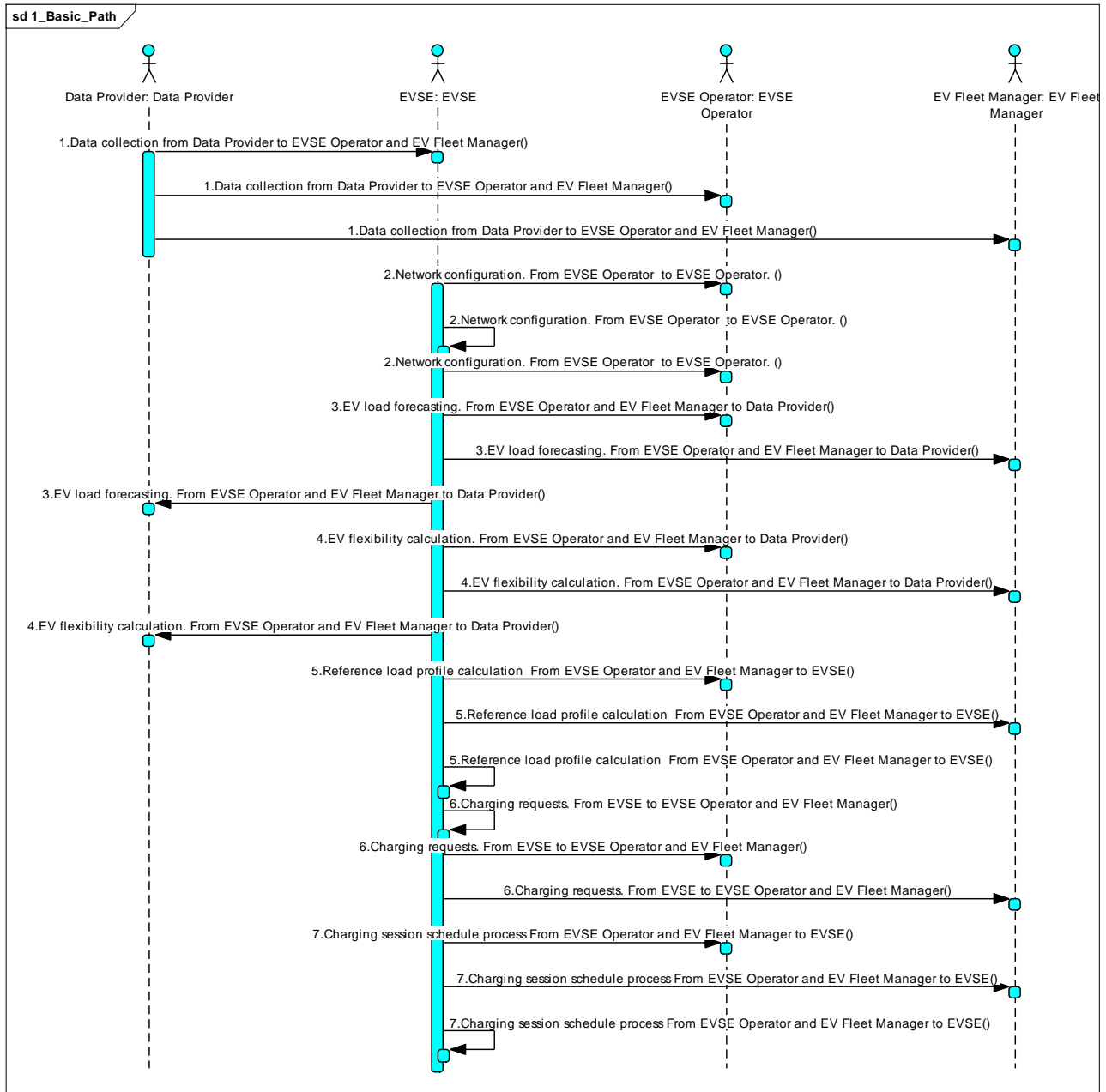


Figure 197 - Primary Use Case Sequence Diagram

## **20.4 HL-UC 3\_PUC\_4: INTERACTION WITH THE ENERGY INFRASTRUCTURE**

### **20.4.1 PRIMARY USE CASE DESCRIPTION**

This PUC describes how the EV charging infrastructure might modulate its power output to provide flexibility to the grid, to maximize the RES integration and to participate in the house energy management process (V2H). It includes the following SUCs:

#### **CHARGING RESCHEDULE TO FOLLOW GRID REQUESTS**

This SUC describes how an EVSE network might modulate its power output after a grid request from the grid operator (DSO). This means that the power output of each socket is regulated (lowered or increased) based on the status of the grid (local net excess or shortage of energy).

#### **CHARGING RESCHEDULE TO MAXIMISE GRID INTEGRATION**

This SUC describes how the Wise EVP reschedules the type 2-3 charging session of its EVSE network after a RES request received from the RESCOs/Aggregators through the WG STaaS/VPP to execute a portion or all the flexibility defined for each regulation area.

#### **EV PROVIDING V2H SERVICES**

This SUC describes how an EVSE installed in a home environment can participate in the house energy management process modulating the power consumption and even injecting power to the household electric installation.

## 20.4.2 SECONDARY USE CASE INTERACTIONS

HL-UC 3 PUC4 invokes 3 SUCs to manage the EV infrastructure (it contemplates not only actions under DSO tasks, but also third parties ancillary services), to integrate RES (consisting of different strategies to reduce RES curtailment) and to support the household energy management process (residential storage systems for self-consumption and demand response).

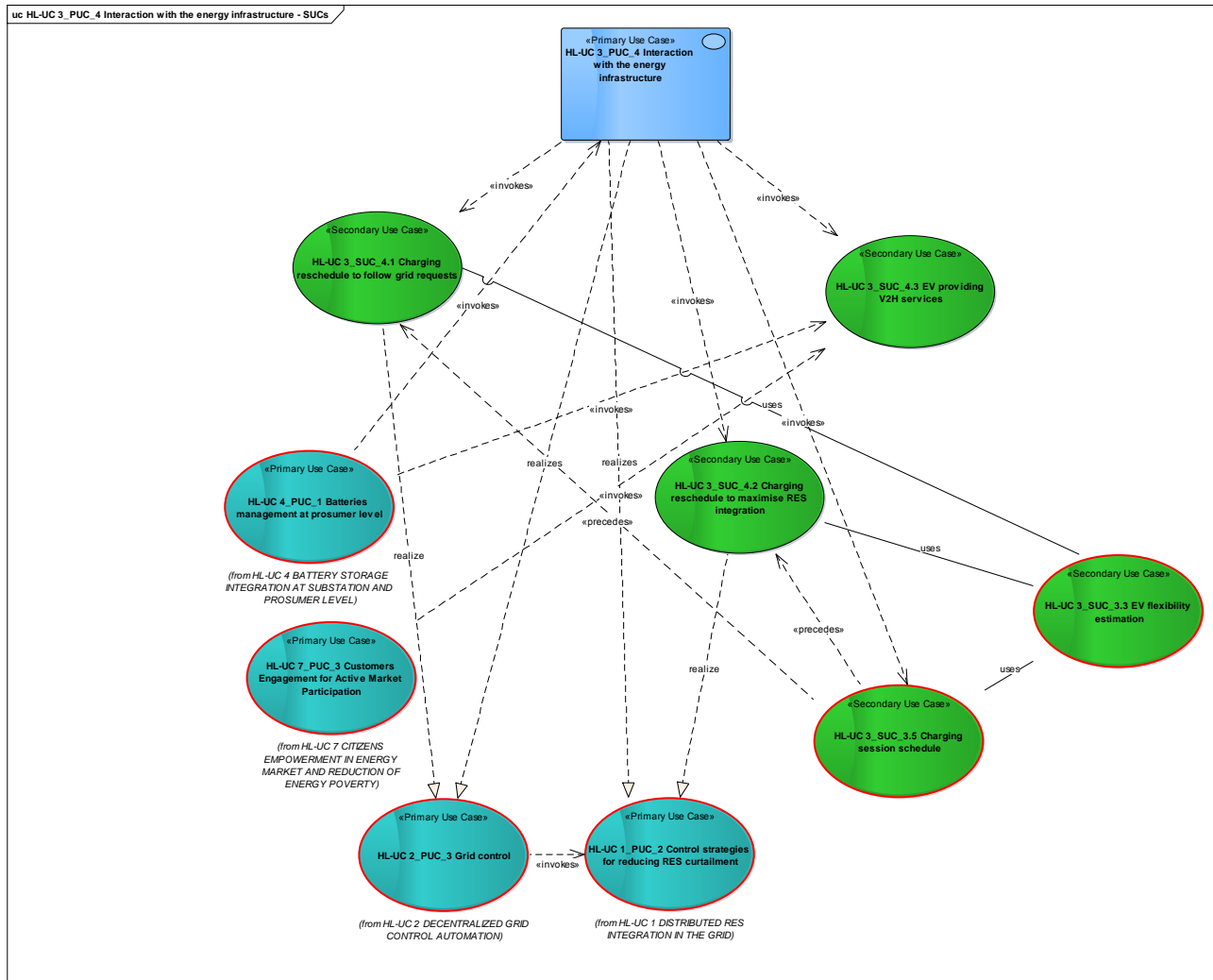


Figure 198 - SUCs Interactions Diagram

**Table 152 - Table of list of participating SUCs**

SUC Name	Description	Relation	PUC/SUC
HL-UC 3_SUC_4.1	Charging reschedule to follow grid requests	uses preceded realize	HL-UC 3_SUC_3.3 HL-UC 3_SUC_3.5 HL-UC 2_PUC_3
HL-UC 3_SUC_4.2	Charging reschedule to maximize RES integration	uses preceded realize	HL-UC 3_SUC_3.3 HL-UC 3_SUC_3.5 HL-UC 1_PUC_2
HL-UC 3_SUC_4.3	EV providing V2H services	invoked invoked	HL-UC 4_PUC_1 HL-UC 7_PUC_3

### 20.4.3 SGAM FUNCTION LAYER

The SUCs that contains this PUC are considered different domains distribution (infrastructure and operator representations related electricity management), DER (distributed electrical resources activity) and customer premise (to provide services for power system end-users). Consequently, there are located on separate zones (operator, market, field or enterprise) according interaction levels with power system control and monitoring.

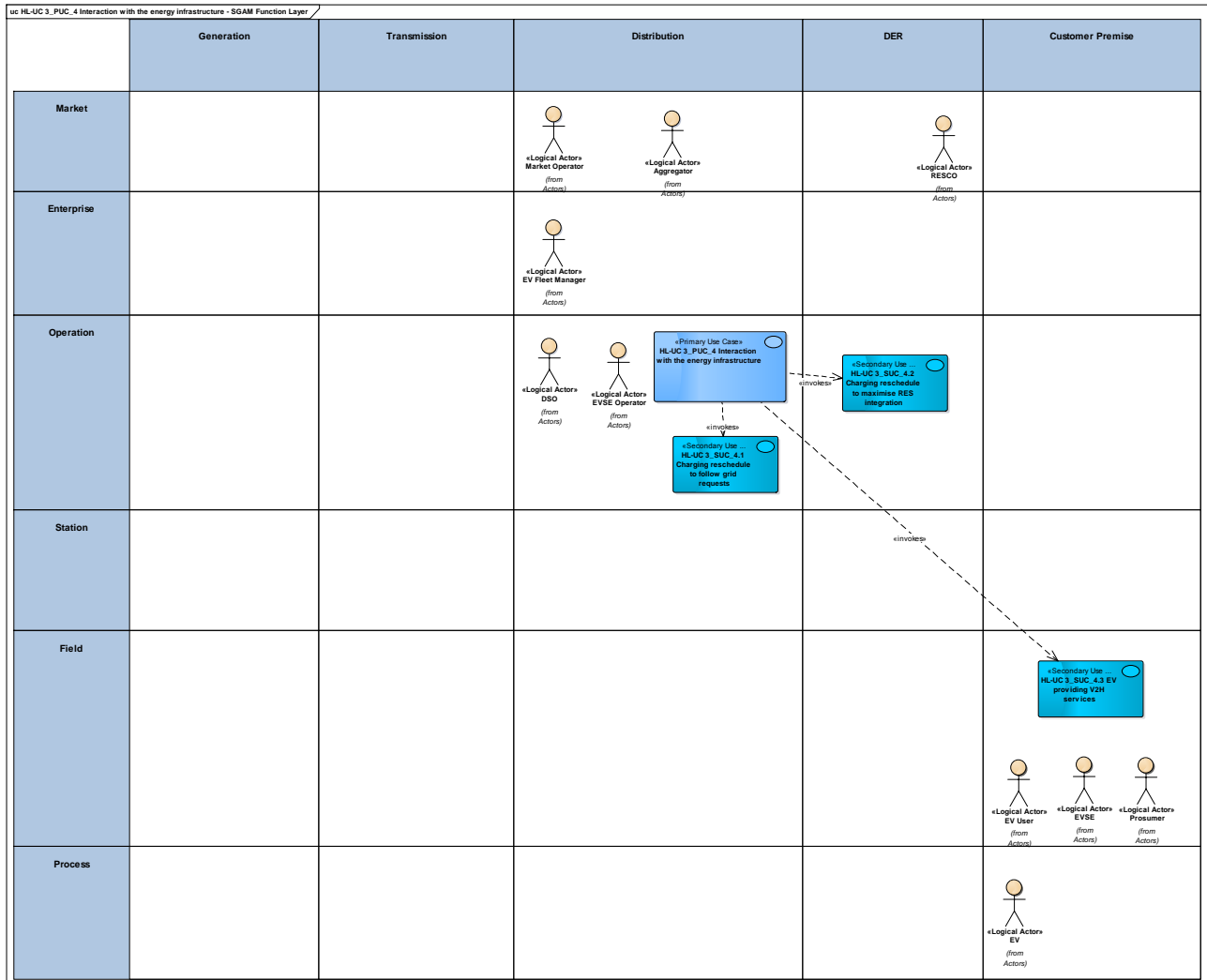


Figure 199 - SGAM Function Layer

The related actors are those in position of either providing information or getting benefit from the grid.

Actor Name	Actor Type
DSO	Organization
EV Fleet Manager	Organization
EV user	Person
Prosumer	Person
EVSE	Device
EV	Device
Aggregator	Organization

Actor Name	Actor Type
RESCO	Organization
Market Operator	Organization
EVSE Operator	Organization

Table 153 - List of Actors Involved

#### 20.4.4 SGAM COMPONENT LAYER

There are 3 featured components: WiseEVP and WG STaaS/VPP (which will interact with others components under the customer premise domain to obtain all required information demand); and WG Cockpit (which will control and monitor grid performance to support power efficiency goals).

WG FastV2G is another component comprehended by this PUC which allows for user is able to configure a charging station and start different types of charging session. WiseHOME would use to perform the domestic charging propection to integrate, monitor and operate within the grid.

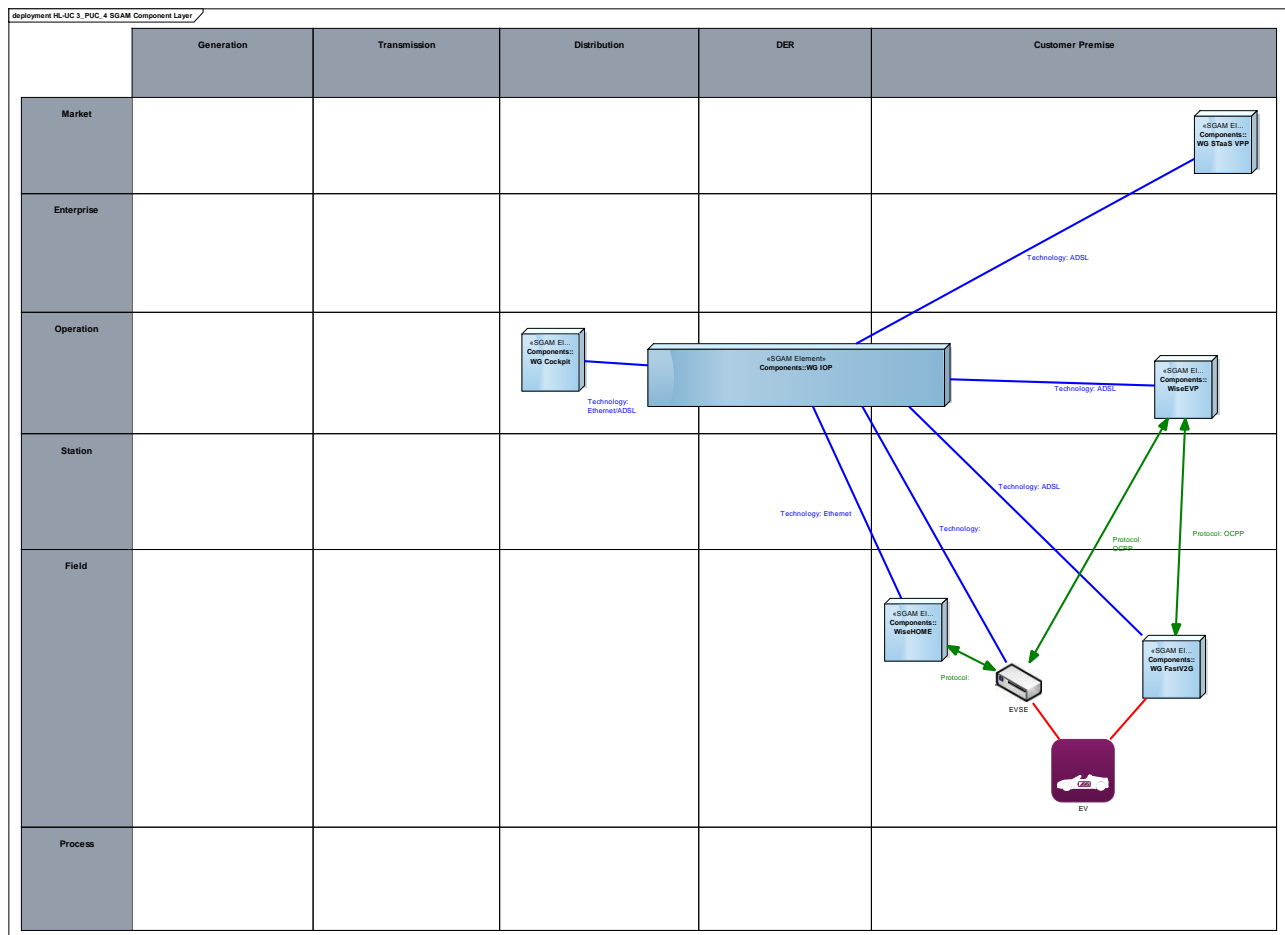


Figure 200 - SGAM Component Layer



Component	Component Type
WG IOP	SGAM Element
WG Cockpit	SGAM Element
WiseHOME	SGAM Element
WG Fast2VG	SGAM Element
WiseEVP	SGAM Element
WG STaaS/VPP	SGAM Element
EV	Electric Vehicle
EVSE	Device

**Table 154 - List of Components Participating in the Primary Use Case**

## 20.4.5 SGAM COMMUNICATION LAYER

Communications to implement in this PUC can be identified in two different types:

- WG IOP connectivity with WiseGRID components: include the protocols considered to be enabled
- Communications between WISE EVP and facility devices that constitute control system of charging modes

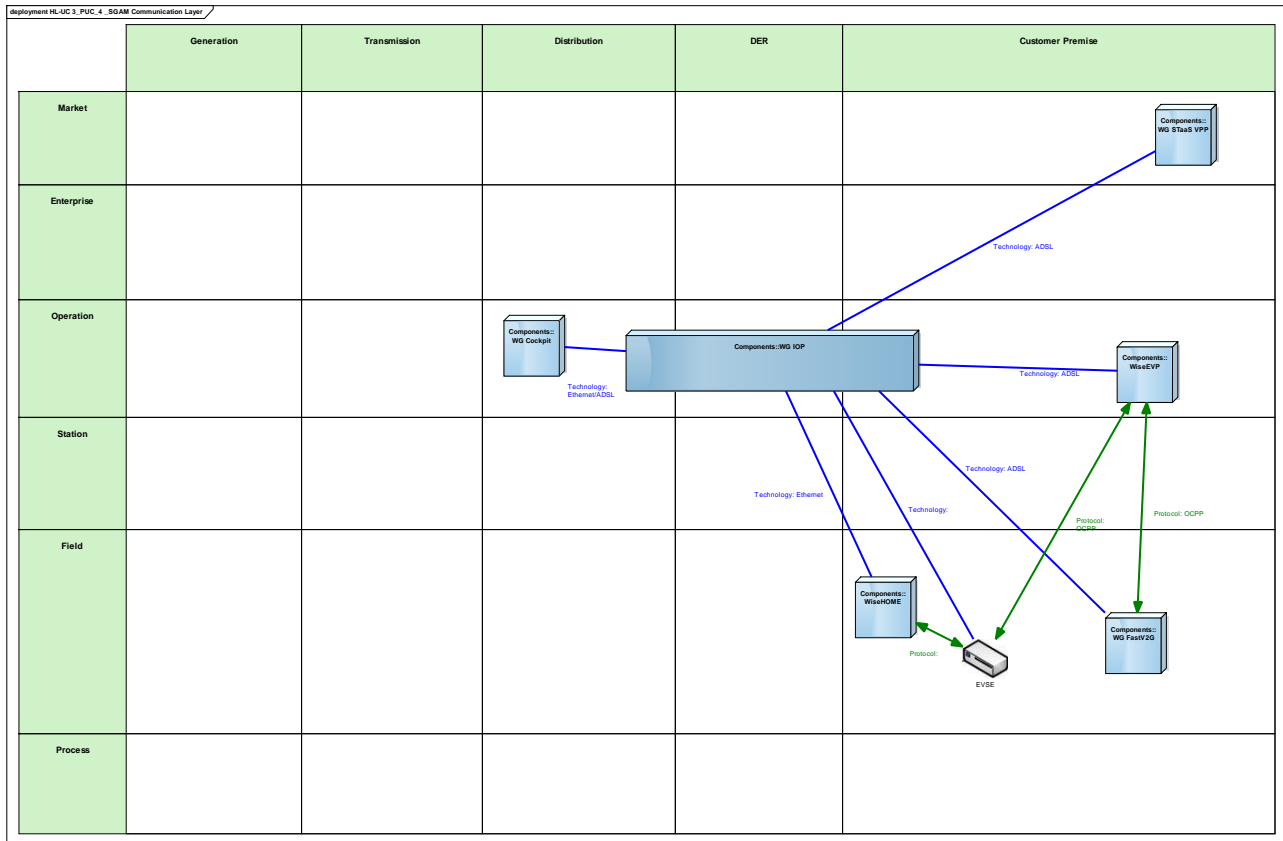


Figure 201 - SGAM Communication Layer

**Table 155 - List of Communication Technologies Involved**

Communication Technology	Description
OCPP	Application protocol for communication between EV charging stations and a central management system
TCP/IP	Group of protocols enabling communication between devices in a network up to the transport layer
MQTT	ISO standard (ISO/IEC PRF 20922) publish-subscribe-based lightweight messaging protocol for use on top of the TCP/IP protocol
IEC61850	Specification for narrow band powerline communication

## 20.4.6 SGAM INFORMATION LAYER

The main information items handled within this PUC include:

- EV and charging stations that imply retrieved data from field device (EVSE) and WG FASTV2
- Load and production forecasts
- Flexibility requests and offers for providing ancillary services
- Domestic demand response
- Wholesale market energy bids.

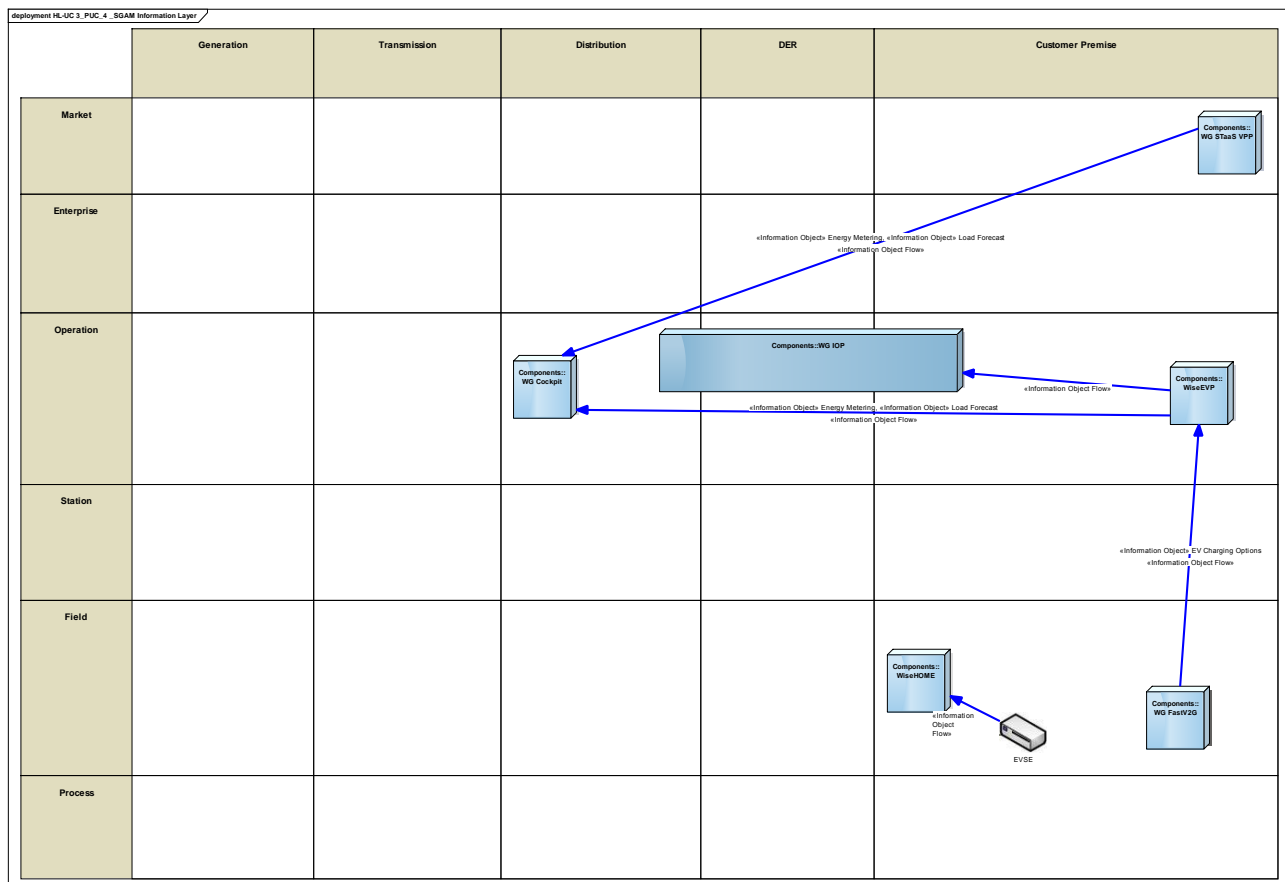


Figure 202 - SGAM Information Layer

## CANONICAL DATA MODEL

Table 156 - List of Data Models

Data Models
Flexibility data model (USEF)
OCPP
V2H Flexibility Data Model

## STANDARDS AND INFORMATION OBJECT MAPPING

Table 157 - List of Data Standards

Data Standards
Flexibility data model (USEF)
OCPP
V2H Flexibility Data Model

Table 158 - List of Information Objects

Information Objects	Data Model
Demand Response signal	Flexibility data model (USEF)
Demand flexibility profile	Flexibility data model (USEF)
Demand response request	Flexibility data model (USEF)
Flexibility offer	Flexibility data model (USEF)
Flexibility request	Flexibility data model (USEF)
EV charging options	OCPP
EV user information	OCPP
EV information	OCPP
EVSE commands	OCPP
EVSE metering info	OCPP

## 20.4.7 SEQUENCE DIAGRAM

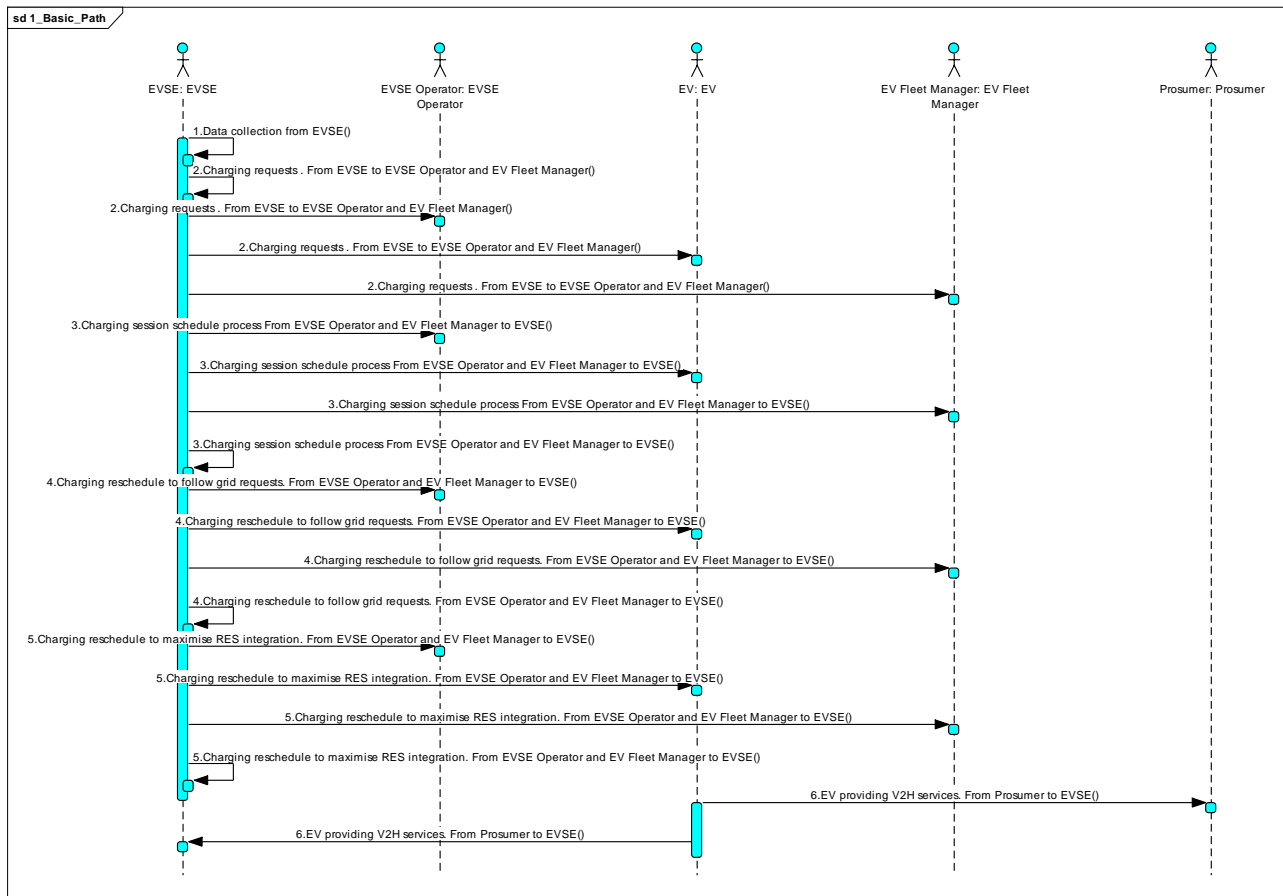


Figure 203 - Primary Use Case Sequence Diagram

## **21 APPENDIX D - ARCHITECTURE**

### **HL-UC 4: BATTERY STORAGE INTEGRATION AT SUBSTATION AND PROSUMER LEVEL**

## **21.1 HL-UC 4\_PUC\_1: BATTERIES MANAGEMENT AT PROSUMER LEVEL**

### **21.1.1 PRIMARY USE CASE DESCRIPTION**

To get a more flexible RES generation and more efficient distributed generation system on the grid, it is necessary to set up storage facilities and most feasible would be batteries together with a management system at consumer/prosumer level. This control would facilitate higher energy generated by distributed renewable energy resources and optimize the grid availability at the consumer group level.

This system also enables consumers to become prosumers, as active grid-users that would maximize the generation from RES both with balance between generation and consumption but also grid load control.



## 21.1.2 SECONDARY USE CASE INTERACTIONS

This Secondary Use Case illustrates the potential use of residential storage systems as enablers for critical business cases such as self-consumption and demand response.

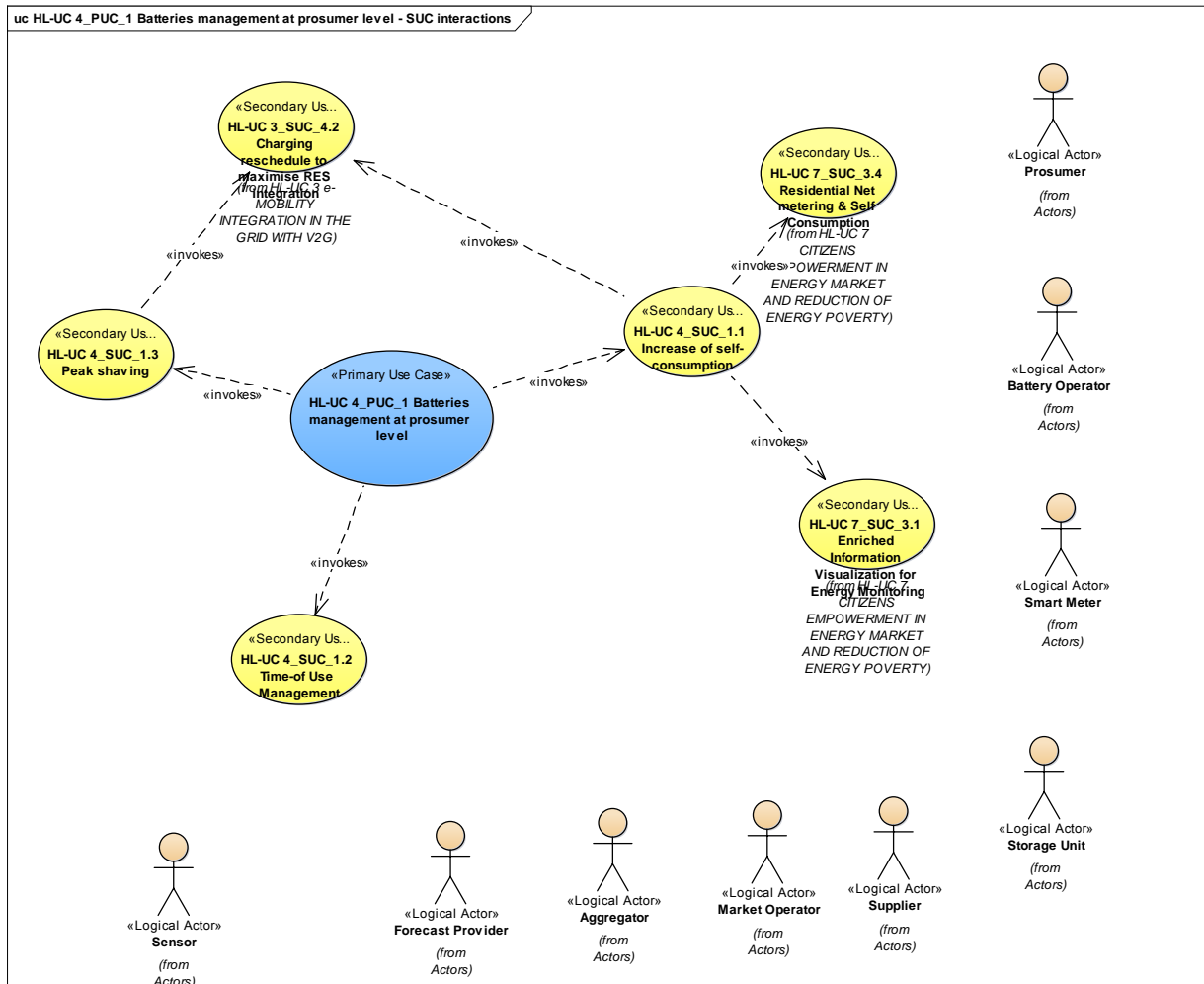


Figure 204 - SUCs Interactions Diagram

Table 159 - Table of list of participating SUCs

SUC Name	Description	Relation	PUC/SUC
Increase of self-consumption	This SUC describes the operation of the battery that maximizes self-consumption in the presence of local generation resources.	Invokes	SUC_1.1
Time-of Use Management	SUC highlight how the battery can leverage ToU tariffs to reduce energy cost.	Invokes	SUC_1.2
Peak shaving	This SUC describes how the battery can be used to limit the maximum power consumption of the building by utilizing stored energy.	Invokes	SUC_1.3

### 21.1.3 SGAM FUNCTION LAYER

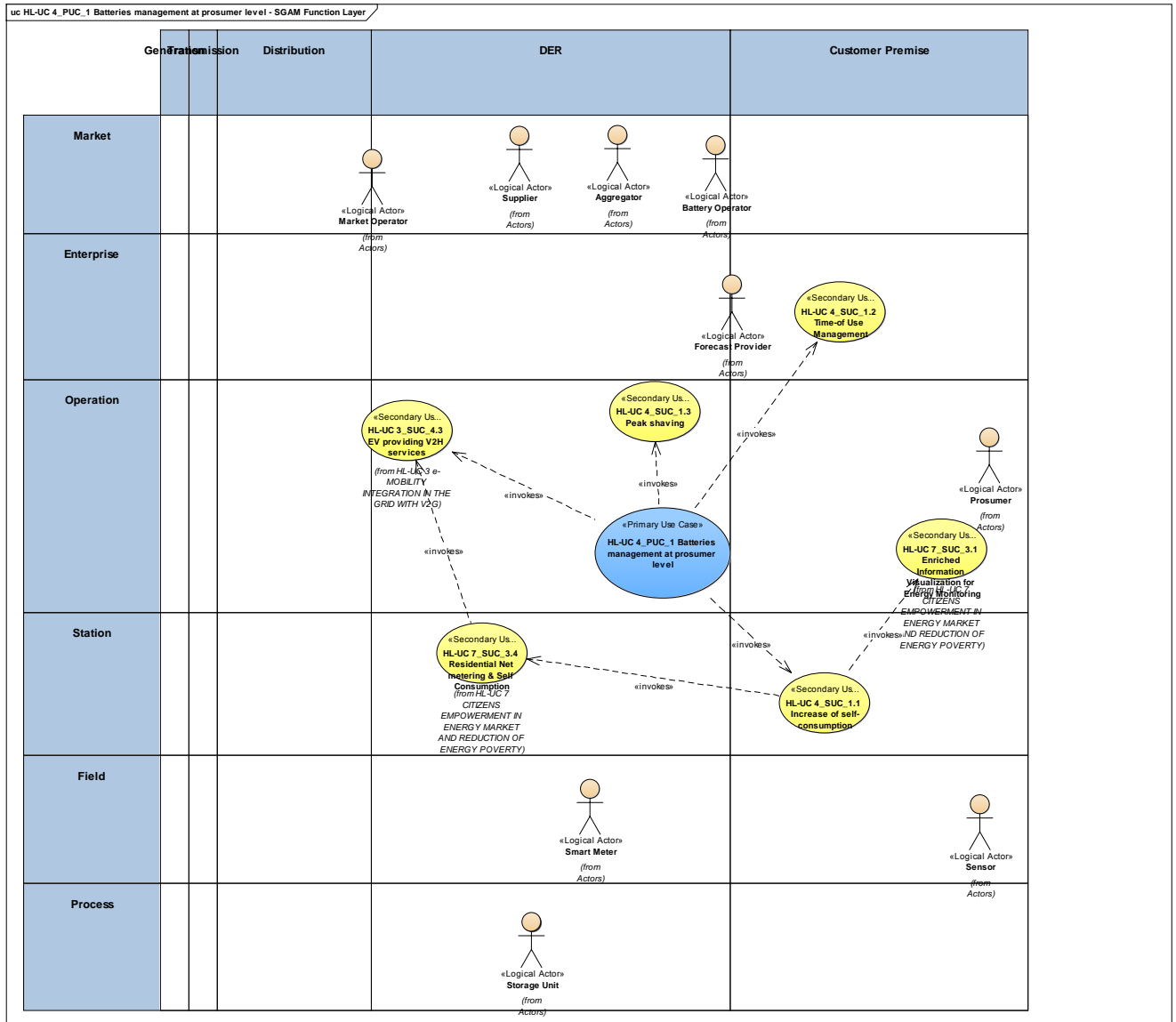


Figure 205 - SGAM Function Layer

Table 160 - List of Actors Involved

Actor Name	Actor Type
Market Operator	Organization
Battery Operator	Organization
Supplier	Organization
Aggregator	Organization
Forecast Provider	Organization
Prosumer	Person
Smart Meter	Device

### 21.1.4 SGAM COMPONENT LAYER

deployment HL-UC 4_PUC_1_SGAM Component Layer					
	Generation	Transmission	Distribution	DER	Customer Premise
Market					
Enterprise					
Operation					
Station					
Field					
Process					

The diagram illustrates the SGAM Component Layer architecture, showing the flow of information and components across different layers and domains.

**Layers and Components:**

- Market:** Contains five SGAM Elements: «SGAM El... Components:: WG Cockpit», «SGAM El... Components:: WG STaaS VPP», «SGAM El... Components:: WiseCOOP», «SGAM El... Components:: WiseHOME», and «SGAM El... Components:: WiseCORP».
- Enterprise:** (Empty layer)
- Operation:** Contains a central «SGAM Elements» Components::WG IOP block.
- Station:** Contains a VPP Component.
- Field:** Contains a Storage Controller.
- Process:** Contains a DER (Distributed Energy Resource) component.

**Connections and Technologies:**

- Market to Operation:** Connections from WG Cockpit, WG STaaS VPP, WiseCOOP, WiseHOME, and WiseCORP to the WG IOP block. Technologies include Ethernet, Ethernet/ADSL, and Ethernet.
- Operation to Station:** Connection from WG IOP to VPP Component. Technology: Protocol.
- Station to Field:** Connection from VPP Component to Storage Controller. Technology: Ethernet.
- Field to Process:** Connection from Storage Controller to DER. Technology: Ethernet.
- Information Flow:** An arrow labeled «Information Object Flow» points from the Storage Controller to the DER.

### Table 161 - List of Components Participating in the Primary Use Case

428

Component	Component Type
WiseHOME	SGAM Element
WiseCORP	SGAM Element
WiseIOP	SGAM Element
VPP Controller	Device
Storage Controller	Device
Storage	Device

## 21.1.5 SGAM COMMUNICATION LAYER

This section outlines the main communication technologies that will be utilised in the reference implementation of the WiseGRID project.

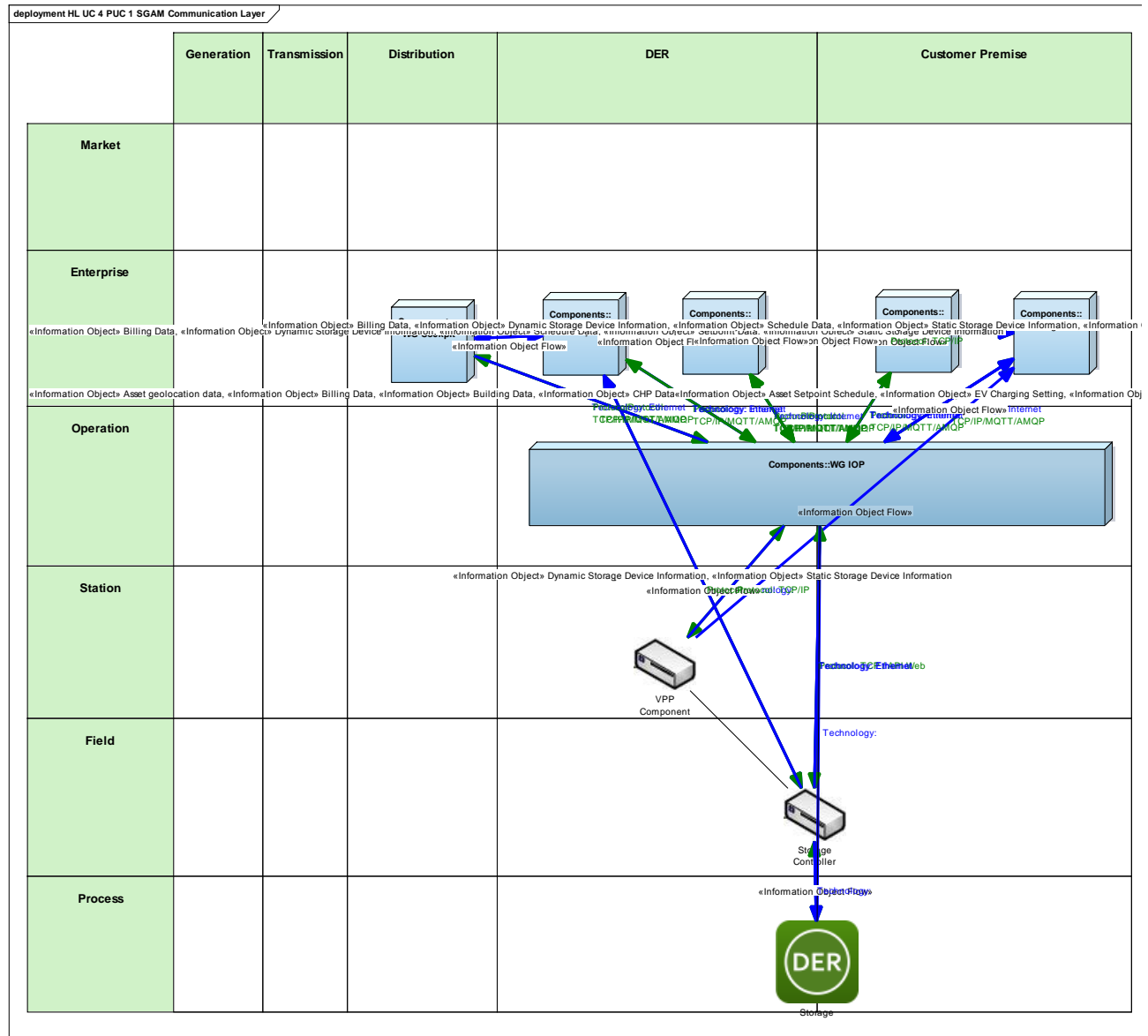


Figure 207 - SGAM Communication Layer

**Table 162 - List of Communication Technologies Involved**

Communication Technology	Description
TCP/IP	Group of protocols enabling communication between devices in a network up to the transport layer
AMQT	Open standard application layer protocol for message-oriented middleware, featuring message orientation, queuing, routing (including point-to-point and publish-and-subscribe), reliability and security
MQTT	ISO standard (ISO/IEC PRF 20922) publish-subscribe-based lightweight messaging protocol for use on top of the TCP/IP protocol

## 21.1.6 SGAM INFORMATION LAYER

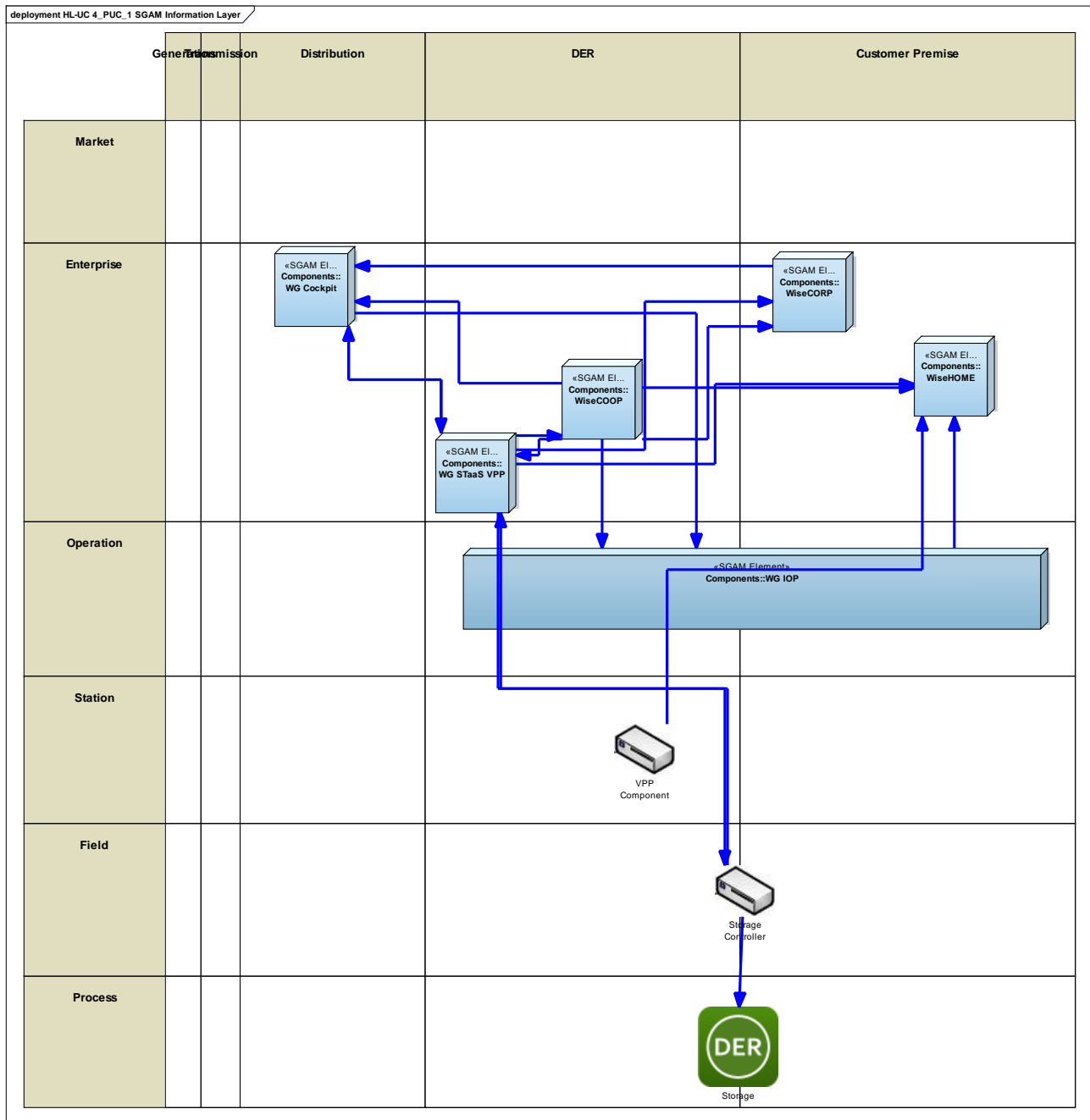


Figure 208 - SGAM Information Layer

## CANONICAL DATA MODELS

**Table 163 - List of Data Models**

Data Models
Building Information Model (BIM)
Universal Smart Energy Framework (USEF)
DLMS/COSEM
OpenADR
Energy asset/device operational status models
Static energy asset information
User preference models

## STANDARDS AND INFORMATION OBJECT MAPPING

This secondary use case will leverage the following standards in order to align its outputs with ongoing activities by other parties so as to ensure replicability of the WiseGRID solution.

**Table 164 - List of Data Standards**

Data Standards
Building Information Model (BIM)
Universal Smart Energy Framework (USEF)
DLMS/COSEM
OpenADR

The correspondence between the information objects of the previous models and the relevant standards is illustrated in the table below.

**Table 165 - List of Information Objects**

Information Objects	Data Model
Asset Geolocation Data	BIM
Billing Data	OpenADR
Building Data	BIM
Demand Response Offer	USEF
Demand Response Request	USEF
Dynamic Storage Device Information	OpenADR
Energy Metering	DLMS/COSEM
Gas Meter Data	DLMS/COSEM
Indoor Environmental Conditions	BIM
Load Forecast	USEF
PV Forecast	USEF



Information Objects	Data Model
PV Production Data	USEF
Retail Electricity Price	OpenADR
Tariff Definition	OpenADR
Grid asset status	DLMS/COSEM
Static Storage Device Information	SAREF/OpenADR
Operation Setpoint Data	SGReady/Modbus

### 21.1.7 ACTIVITY DIAGRAM

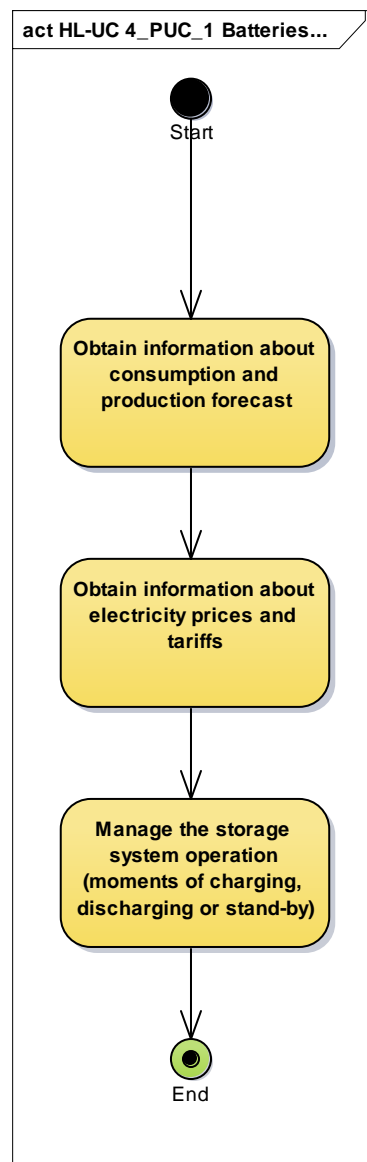


Figure 209 - Primary Use Case Activity Diagram

## 21.1.8 SEQUENCE DIAGRAM

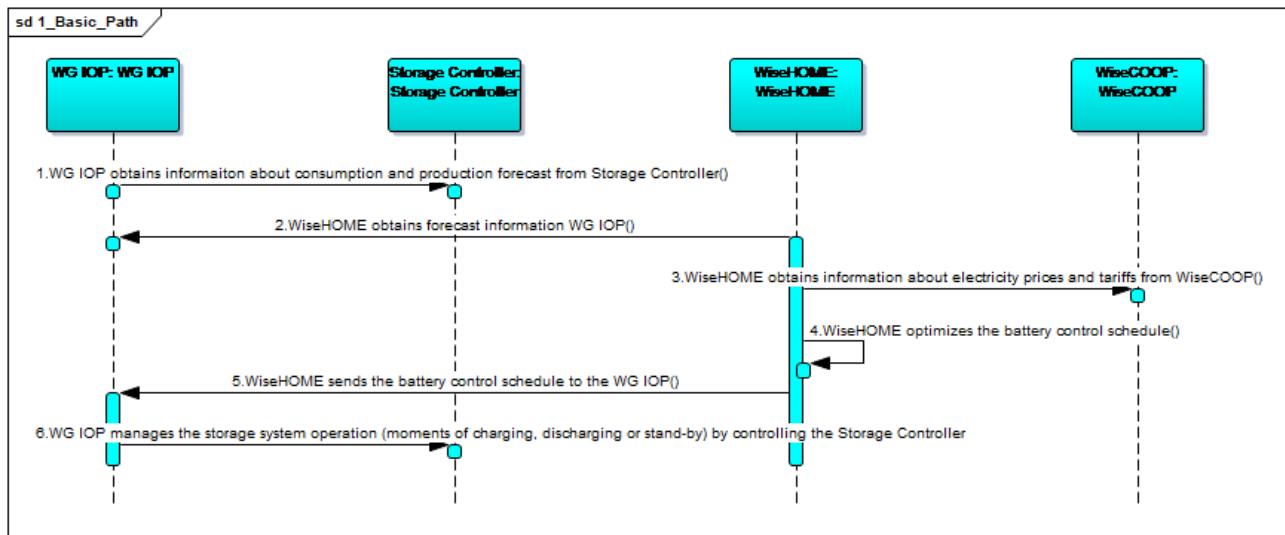


Figure 210 - Primary Use Case Sequence Diagram

## 21.2 HL-CU 4\_PUC\_2: BATTERIES MANAGEMENT AT AGGREGATOR LEVEL

### 21.2.1 PRIMARY USE CASE DESCRIPTION

Batteries enable the grid to become more stable for several reasons. If batteries are managed by a system, they can reduce the grid's fluctuations by means of coordinated control of the grid's voltage and frequency. They can, as well, ensure a quick response in case of a grid outage (fast restoration), reducing the blackout duration and improve the consumer's security of supply. The following services regarding grid support can be provided by battery storage systems:

- Load frequency control
- Grid capacity management
  - Deliver peak load electricity
  - Load-following power generation at short notice (DRES + batteries combined)
- Voltage support
- Power quality support
- Blackstart and backup capabilities

### 21.2.2 SECONDARY USE CASE INTERACTIONS

HL-UC 4\_PUC\_2\_Batteries management at aggregator level (grid support) is closely related to HL-UC 7\_PUC\_2\_Dynamic aggregation of distributed energy assets and active participation into energy market, HL-UC 6\_PUC\_2\_VPP market participation and HL-UC 6\_PUC\_3\_VPP Real time control.

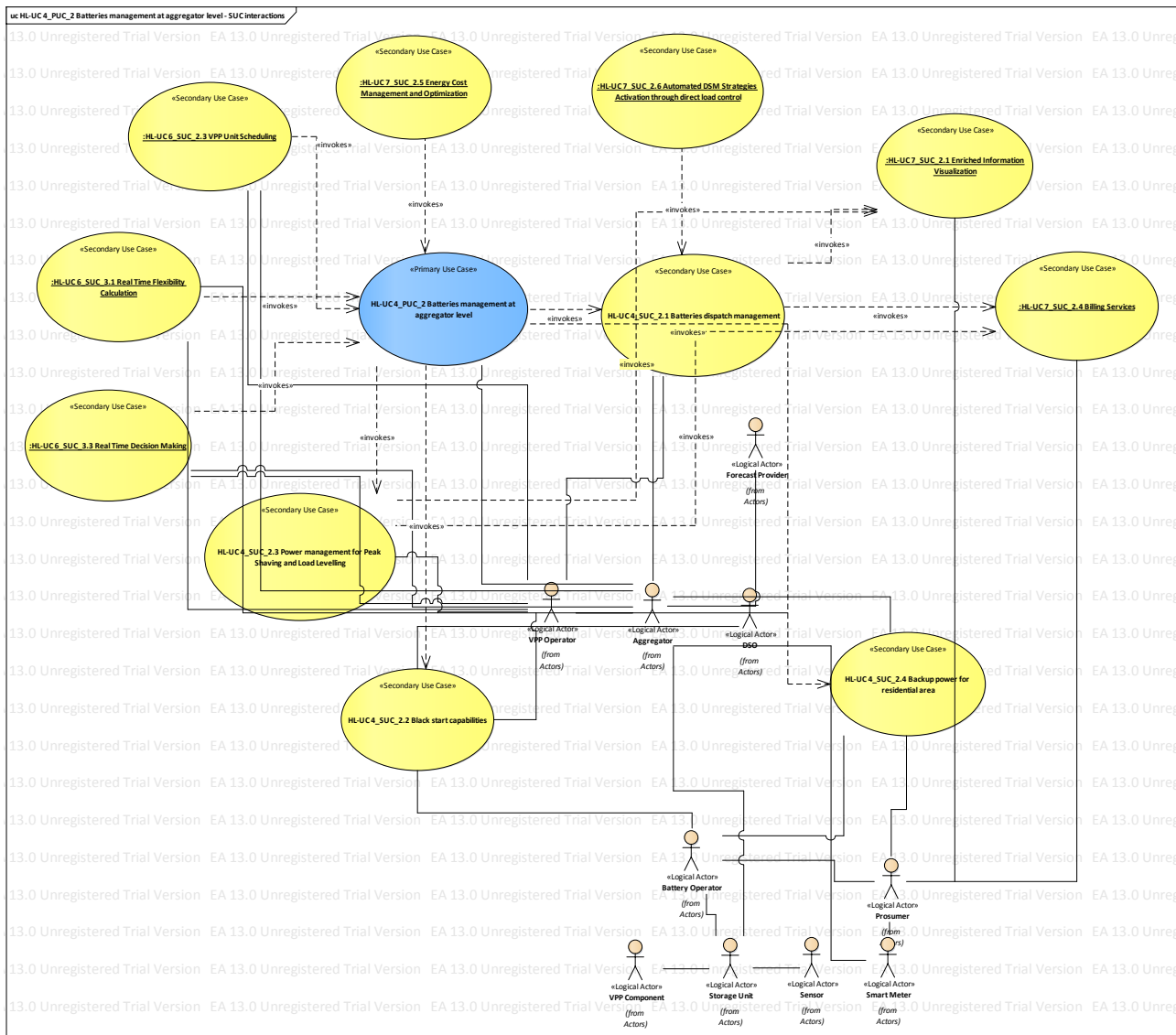


Figure 211 - SUCs Interactions Diagram

**Table 166 - Table of list of participating SUCs**

SUC Name	Description	Relation	PUC/SUC
HL-UC 4_SUC_2.1_Batteries dispatch management	Dispatch management of batteries	invokes	HL-UC 7_SUC_2.1_Enriched information visualization HL-UC 7_SUC_2.4_Billing services
HL-UC 4_SUC_2.2_Black start capabilities	Using batteries for providing black start capabilities	gets invoked by	HL-UC 4_PUC_2_Batteries management at aggregator level (grid support)
HL-UC 4_SUC_2.3_Power management for peak-shaving and load harmonization	Providing peak shaving and load harmonization services	gets invoked by	HL-UC 4_PUC_2_Batteries management at aggregator level (grid support)
HL-UC 4_SUC_2.4_Backup power for residential area	Providing backup power on residential level	invokes	
HL-UC 6_SUC_2.3_VPP unit scheduling	Scheduling of VPP units including aggregated batteries	invokes	HL-UC 4_PUC_2_Batteries management at aggregator level (grid support)
HL-UC 6_SUC_3.1_Real time flexibility calculation	Flexibility estimation of VPP including aggregated batteries	invokes	HL-UC 4_PUC_2_Batteries management at aggregator level (grid support)
HL-UC 6_SUC_3.3_Real time decision making	Real time decision making for VPP including aggregated	invokes	HL-UC 4_PUC_2_Batteries management at aggregator level (grid support)
HL-UC 7_SUC_2.5_Energy cost management and optimization	Energy cost management optimization including aggregated batteries	invokes	HL-UC 4_PUC_2_Batteries management at aggregator level (grid support)
HL-UC 7_SUC_2.6_Automated DSM strategies activation through direct load control	Providing DSM with aggregated batteries	invokes	HL-UC 4_SUC_2.1_Batteries dispatch management

### 21.2.3 SGAM FUNCTION LAYER

The player related to this HL-UC can be found either on the distribution/enterprise (VPP Operator, Aggregator, Forecast provider) or on the field/customer premise level (Prosumer, Battery Operator, VPP component, Sensor, Smart Meter).

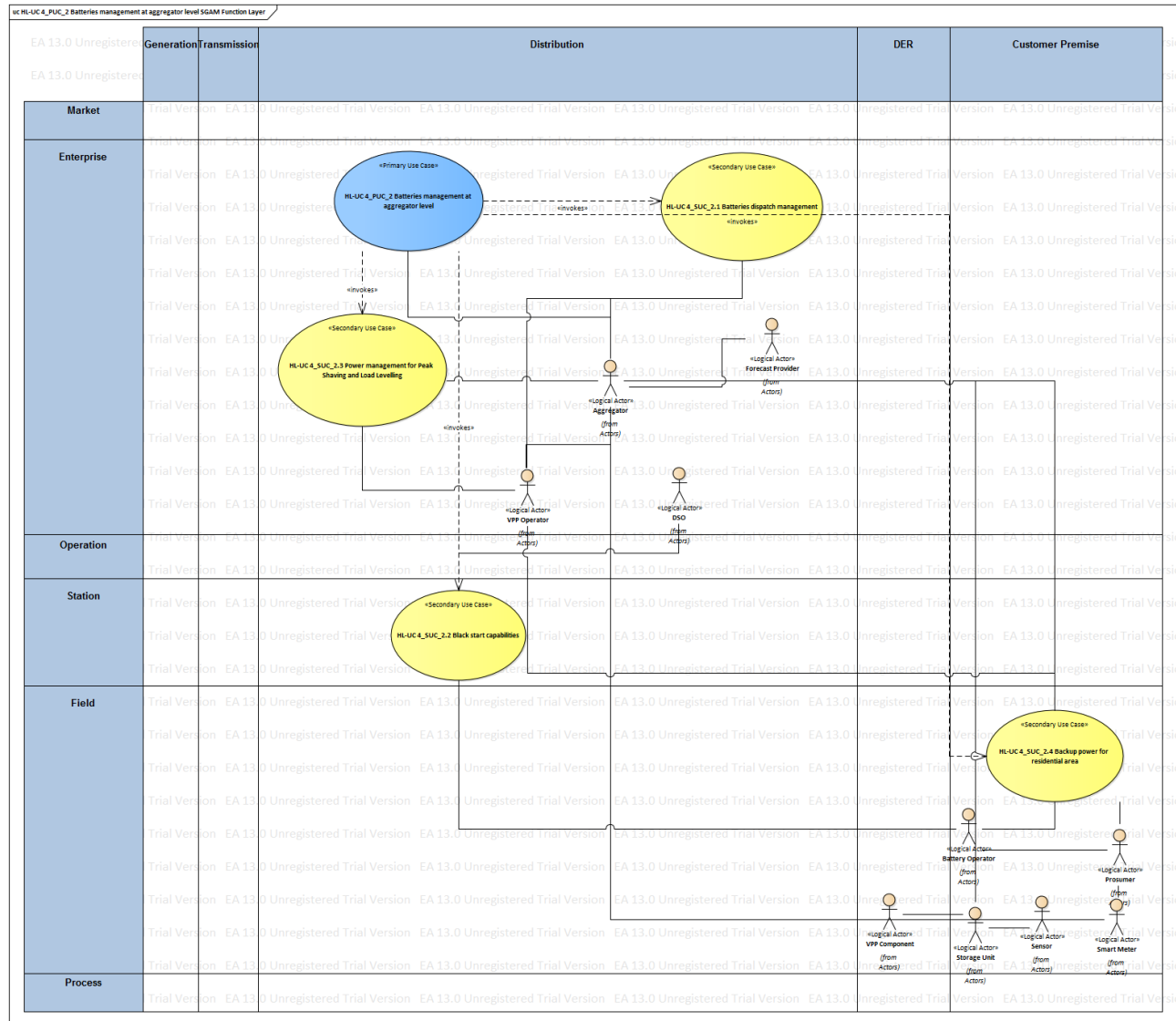


Figure 212 - SGAM Function Layer

**Table 167 - List of Actors Involved**

Actor Name	Actor Type
Aggregator	Organization
Forecast provider	Organization
VPP Operator	Organization
DSO	Organization
Battery Operator	Organization
Prosumer	Person
Smart Meter	Device
Sensor	Device
Storage Unit	Device
VPP component	Device

## 21.2.4 SGAM COMPONENT LAYER

The component layer for HL-UC 4 PUC 2 includes several SGAM elements. WG StaaS/VPP is the most important one for the presented use case since this tool manages the batteries actively. Other WiseGRID tools are directly linked to WG StaaS/VPP. Besides, several components related to Storage Units and metering infrastructure are included.

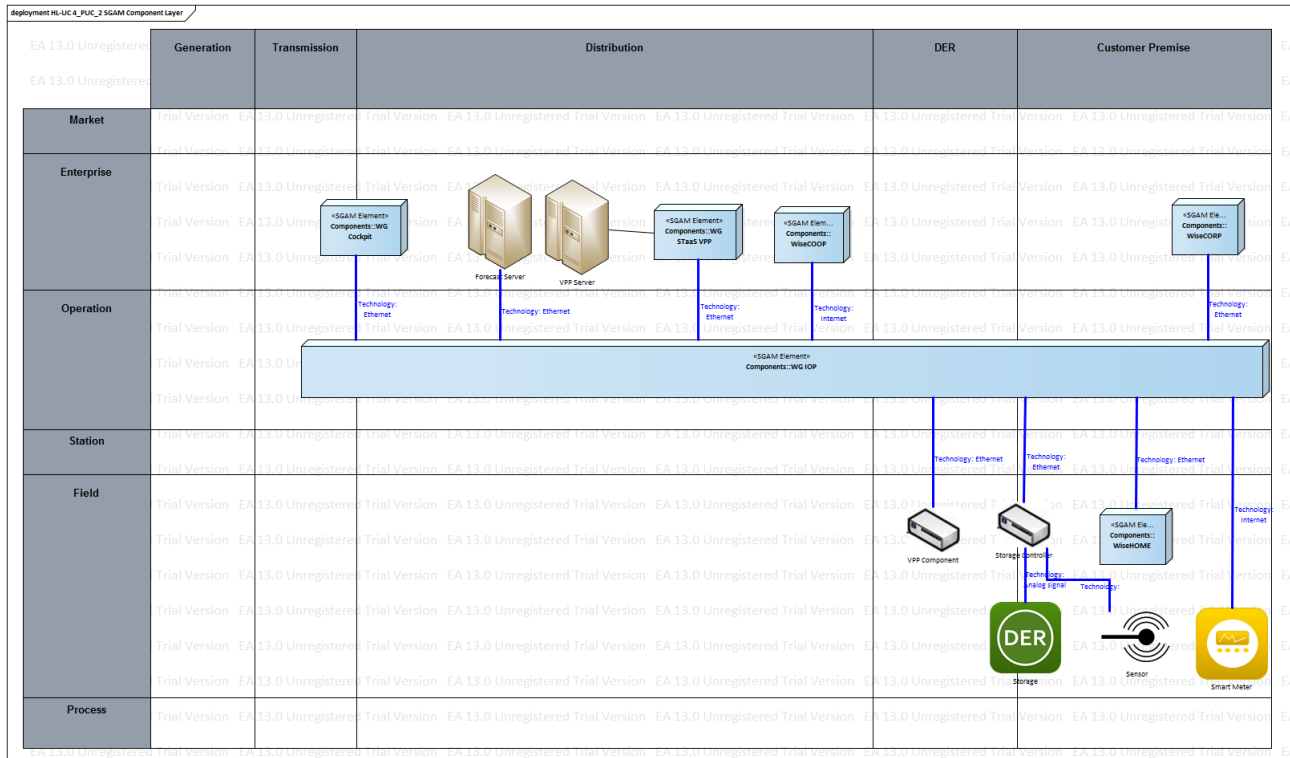


Figure 213 - SGAM Component Layer

Table 168 - List of Components Participating in the Primary Use Case

Component	Component Type
WG Cockpit	SGAM Element
WG StaaS VPP	SGAM Element
WiseCOOP	SGAM Element
WiseCORP	SGAM Element
WiseHOME	SGAM Element
Sensor	Device
Smart Meter	Device
Storage	Device
Storage Controller	Device
VPP Component	Device



The communication structure between the devices and different WG tool is based on TCP/IP. On top different standardized and proprietary protocols will be used.



### Table 169 - List of Communication Technologies Involved

Communication Technology	Description
TCP/IP	Group of protocols enabling communication between devices in a network up to the transport layer
MQTT	ISO standard (ISO/IEC PRF 20922) publish-subscribe-based lightweight messaging protocol for use on top of the TCP/IP protocol
AMQP	Open standard application layer protocol for message-oriented middleware, featuring message orientation, queuing, routing (including point-to-point and publish-and-subscribe), reliability and security
Proprietary	For storage units it is likely that proprietary protocols will be used

## 21.2.6 SGAM INFORMATION LAYER

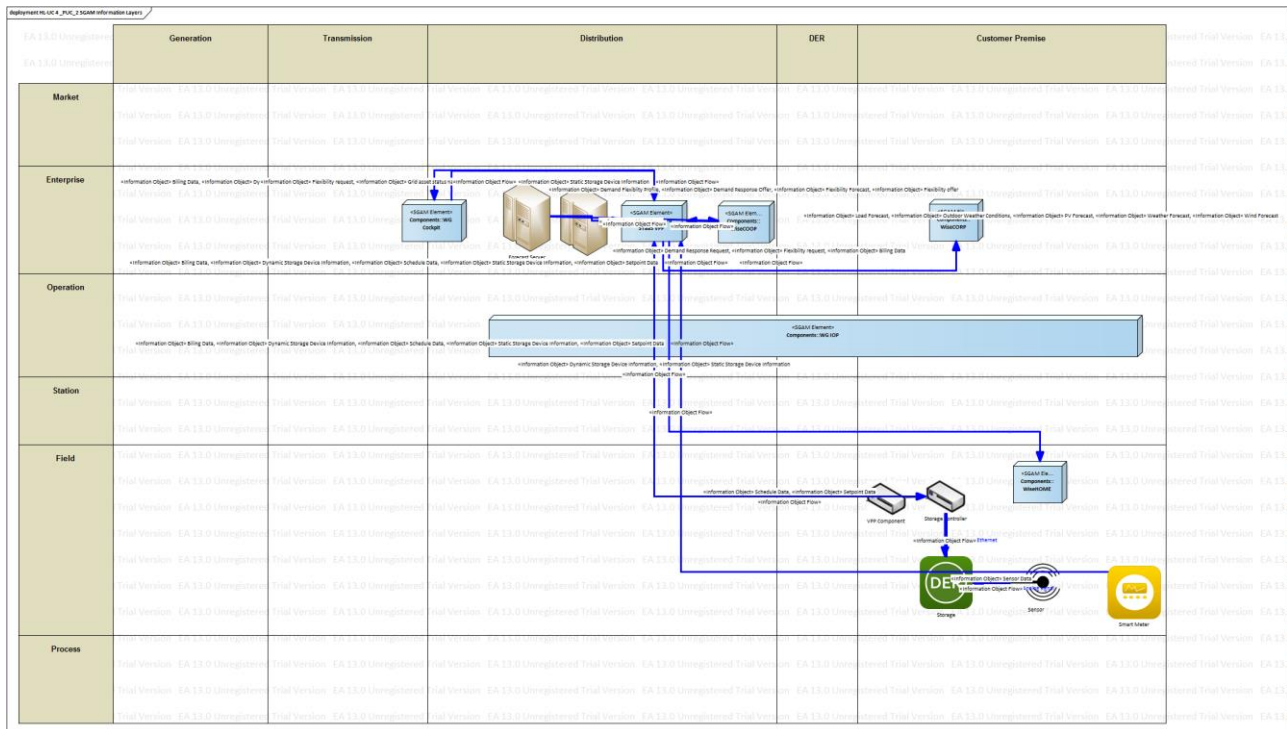


Figure 215 - SGAM Information Layer

## CANONICAL DATA MODEL

The identified canonical data models include those models related to flexibility estimation, monitoring and scheduling of battery storage systems as well as billing processes.

Data Models
Flexibility Data Model
Schedule and Setpoint Data Model
Storage Data Model
Billing Data Model

Table 170 - List of Data Models

## STANDARDS AND INFORMATION OBJECT MAPPING

Necessary data standards have to be analysed in the further course of the project.

Table 171 - List of Data Standards

Data Standards
To be analyzed

In order to offer demand response services to the DSO flexibility offer, flexibility request, demand response

flexibility profile, demand response requests and demand response offer information objects are included. Static and dynamic Storage Device Information serve as input for flexibility estimation whereas Schedule data and Setpoint data are for operation purposes. Billing and remuneration is based on the information object Billing data.

**Table 172 - List of Information Objects**

Information Objects	Data Model
Demand response request	Flexibility Data Model
Demand flexibility profile	Flexibility Data Model
Demand response offer	Flexibility Data Model
Flexibility offer	Flexibility Data Model
Flexibility request	Flexibility Data Model
Schedule data	Schedule and Setpoint Data Model
Setpoint data	Schedule and Setpoint Data Model
Static Storage Device Information	Storage Data Model
Dynamic Storage Device Information	Storage Data Model
Billing data	Billing Data Model

## 21.2.7 ACTIVITY DIAGRAM

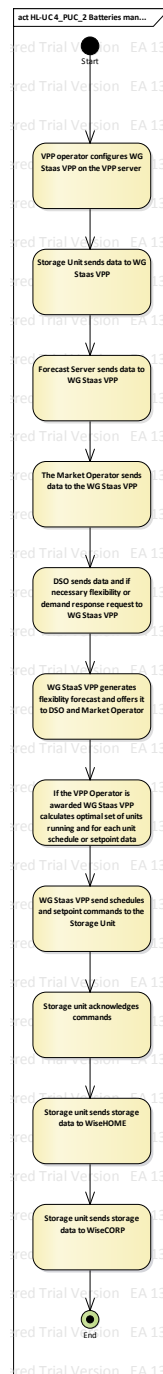


Figure 216 - Primary Use Case Activity Diagram

## 21.2.8 SEQUENCE DIAGRAM

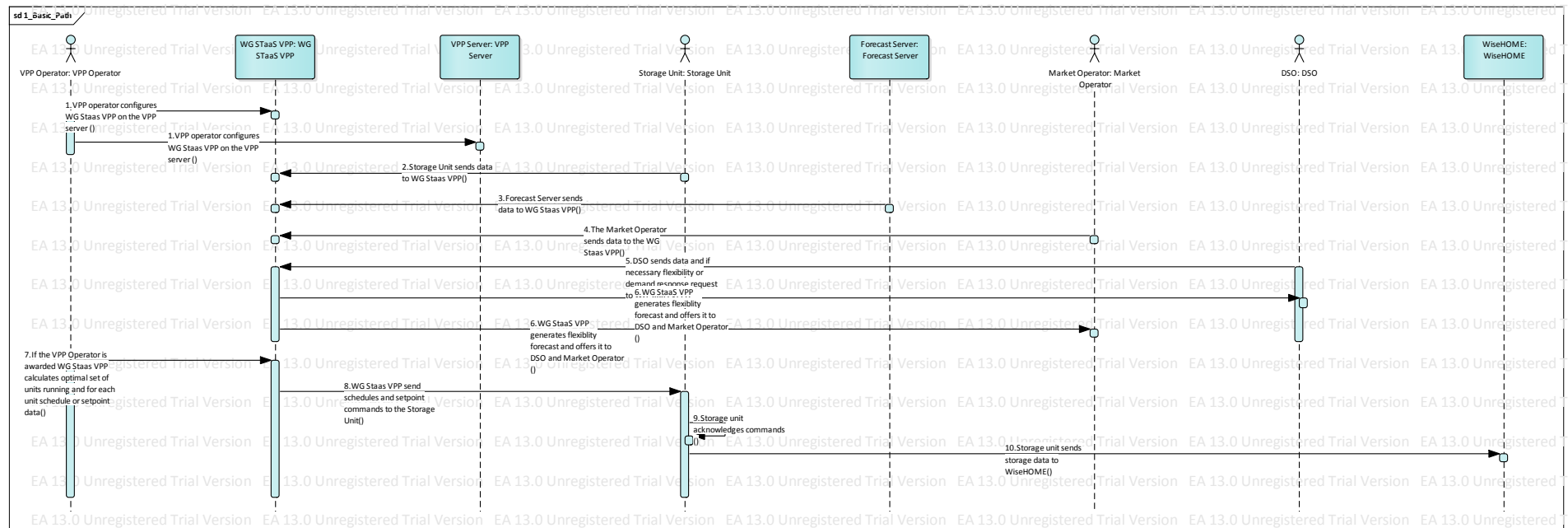


Figure 217 - Primary Use Case Sequence Diagram

## 21.3 HL-UC 4\_PUC\_3: ANCILLARY SERVICES

### 21.3.1 PRIMARY USE CASE DESCRIPTION

Energy Storage Systems can provide services that are important for a satisfactory operation of the network, such as reactive power support, load following, back-up service, peak shaving, power quality (PQ) and disturbance compensation to name a few. Through various control algorithms, such as droop control, virtual inertia, etc., generation and storage units can coordinate their operations offering significant benefits for the utility grid.

The aggregation of battery systems based on modern communication, at any level, can offer several services related indirectly with the energy storage as the market regulation.

Ancillary services like “active power reserves” and “frequency response”, would be possible based on energy and power availability.

### 21.3.2 SECONDARY USE CASE INTERACTIONS

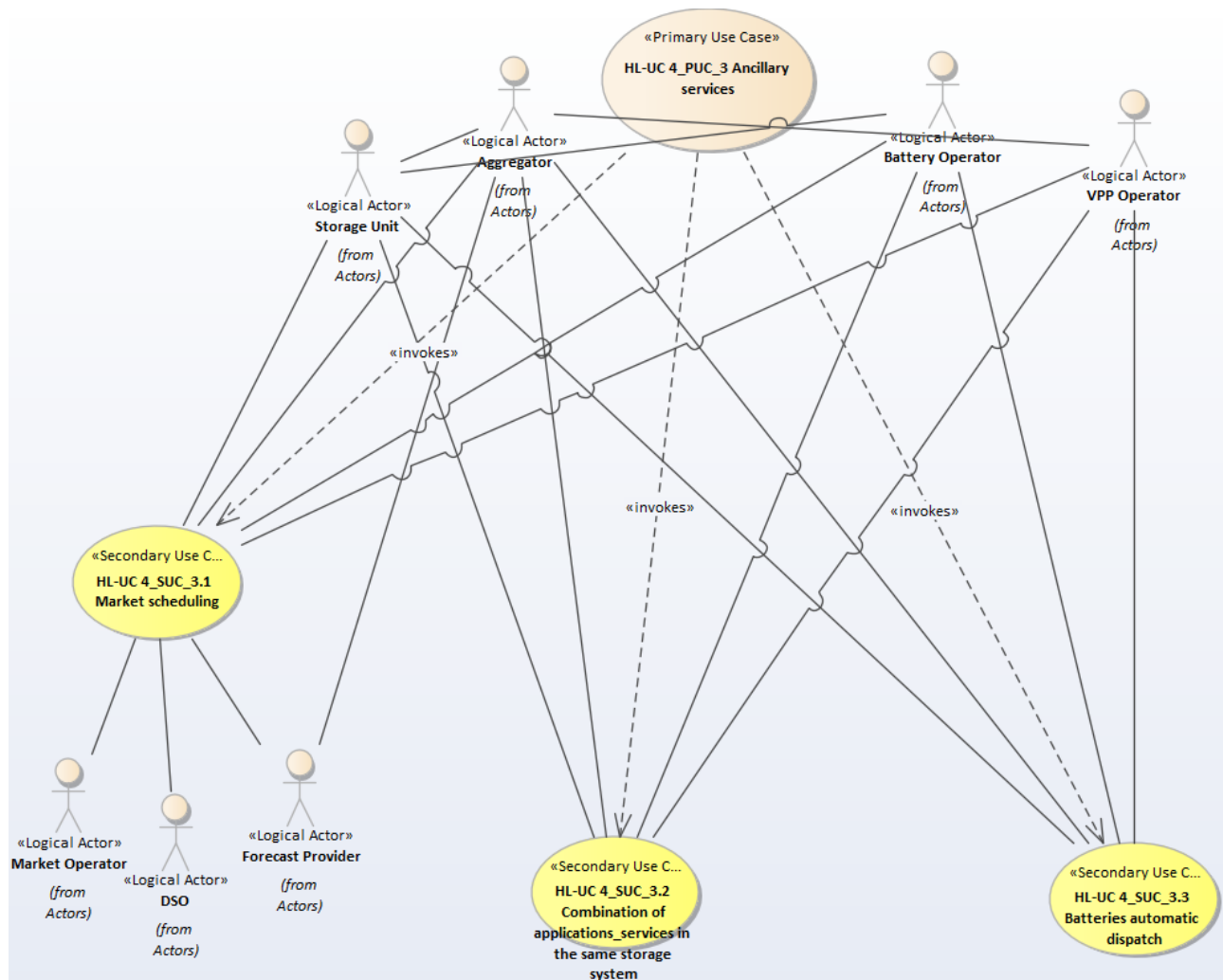


Figure 218 - SUCs Interactions Diagram

Table 173 - Table of list of participating SUCs

SUC Name	Description	Relation	PUC/SUC
Market scheduling	Storage facilities are making the grid more flexible as the battery system can attenuate the demand fluctuations. This service lets the grid work in a larger variety of regimes with variable production levels. Information on the production and consumer forecast and market prices are needed in order to anticipate the potential use of the portfolio.	Invokes	3.1
Combination of applications services in the same storage system	The storage system (unit) needs to estimate the optimal dispatch in order to achieve the applications and services configured. In this direction, suitable priority	Invokes	3.2

SUC Name	Description	Relation	PUC/SUC
	and cost functions need to be established, in order to provide a coherent use of the system when receiving different commands from different applications/users.		
Battery automatic dispatch	The batteries, in order to provide ancillary services, need to operate automatically. The dispatch should be authorized by the user or aggregator, but the loop control needs to be implemented in the battery in order to achieve a fast and secure response.	Invokes	3.3

### 21.3.3 SGAM FUNCTION LAYER

The SGAM Function layer for this use case is presented below.

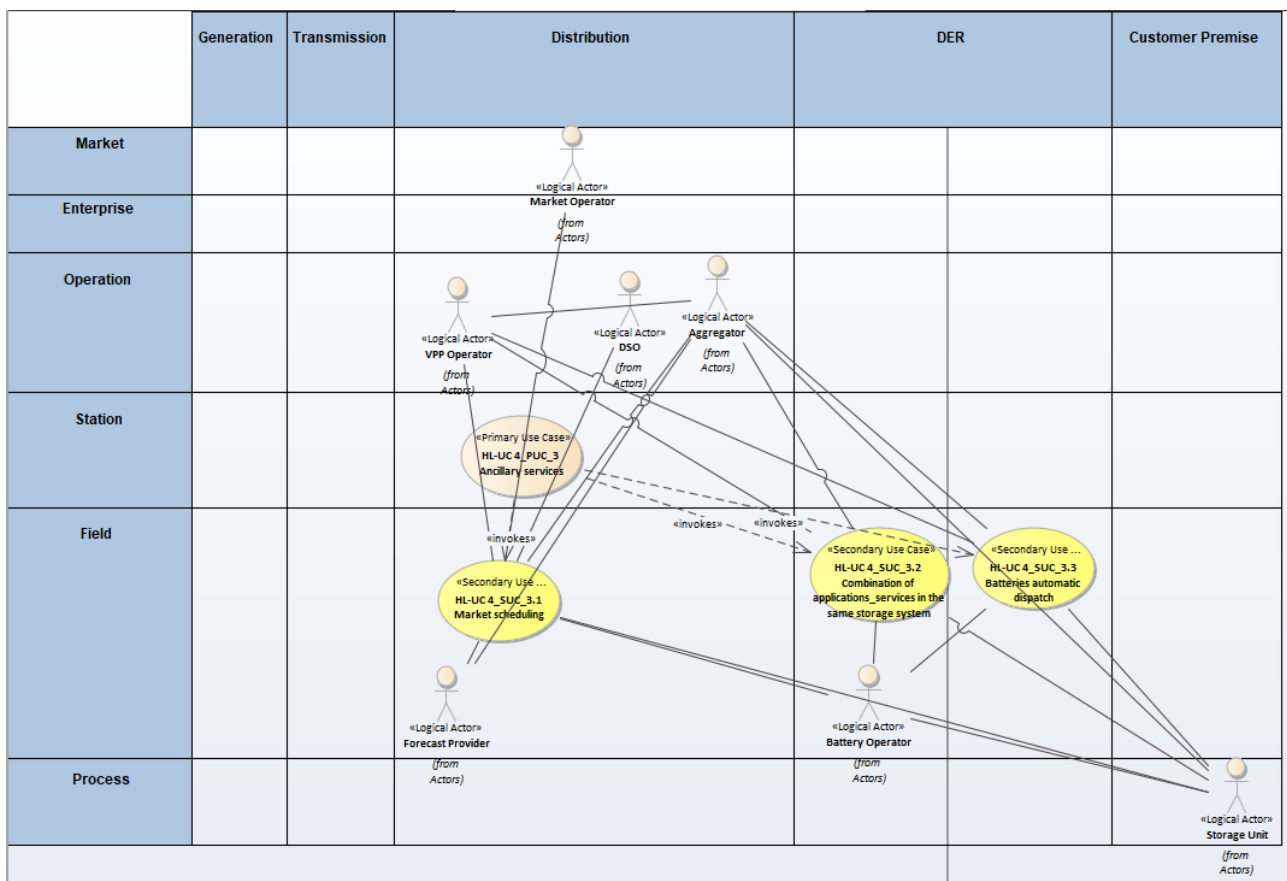


Figure 219 - SGAM Function Layer

Table 174 - List of Actors Involved

Actor Name	Actor Type
Market operator	Organization
VPP operator	Organization



Actor Name	Actor Type
DSO	Organization
Aggregator	Organization
Forecast provider	Device
Battery operator	Organization
Storage unit	Device

### 21.3.4 SGAM COMPONENT LAYER

The SGAM Component layer for this use case is presented below.

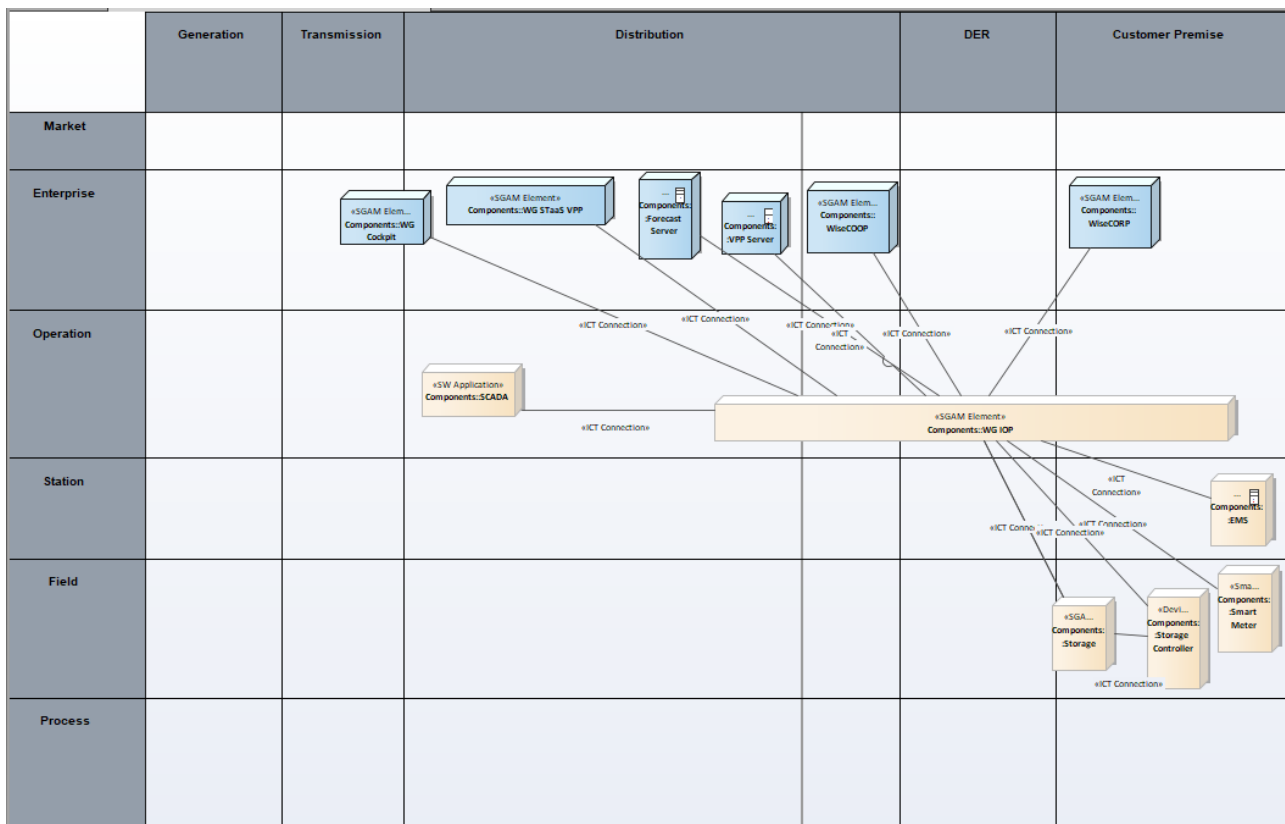


Figure 220 - SGAM Component Layer

Table 175 - List of Components Participating in the Primary Use Case

Component	Component Type
EMS	Device
Smart meter	Device
Storage controller	Device
Storage	Device
WG cockpit	SGAM element
WG Staas VPP	SGAM element

Component	Component Type
Forecast server	Device
WiseCOOP	SGAM element
WiseCORP	SGAM element
SCADA	Device
WG IOP	SGAM element

### 21.3.5 SGAM COMMUNICATION LAYER

The SGAM Communication layer for this use case is presented below.

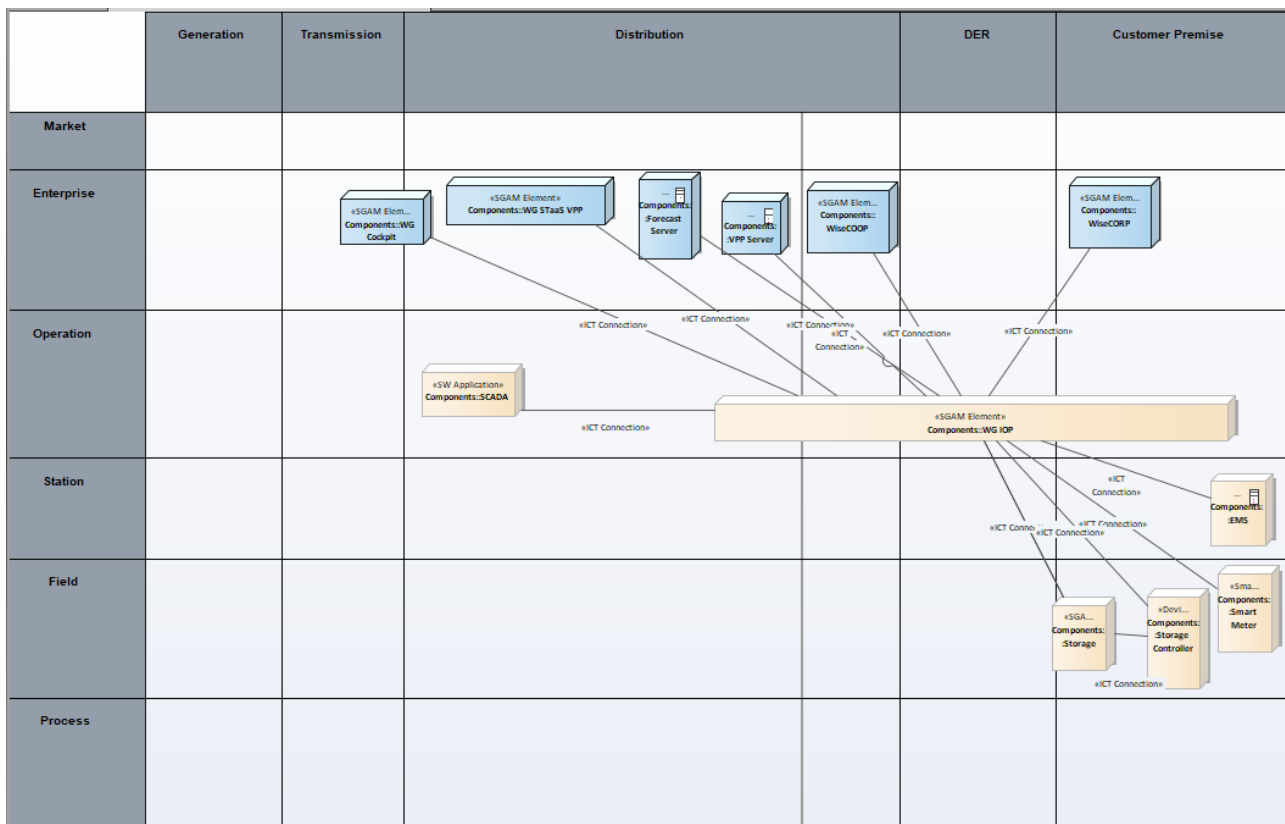


Figure 221 - SGAM Communication Layer

**Table 176 - List of Communication Technologies Involved**

Communication Technology	Description
Modbus TCP/IP	
CAN	
IEC61850	
Web services	

### 21.3.6 SGAM INFORMATION LAYER

The SGAM Information layer for this use case is presented below.

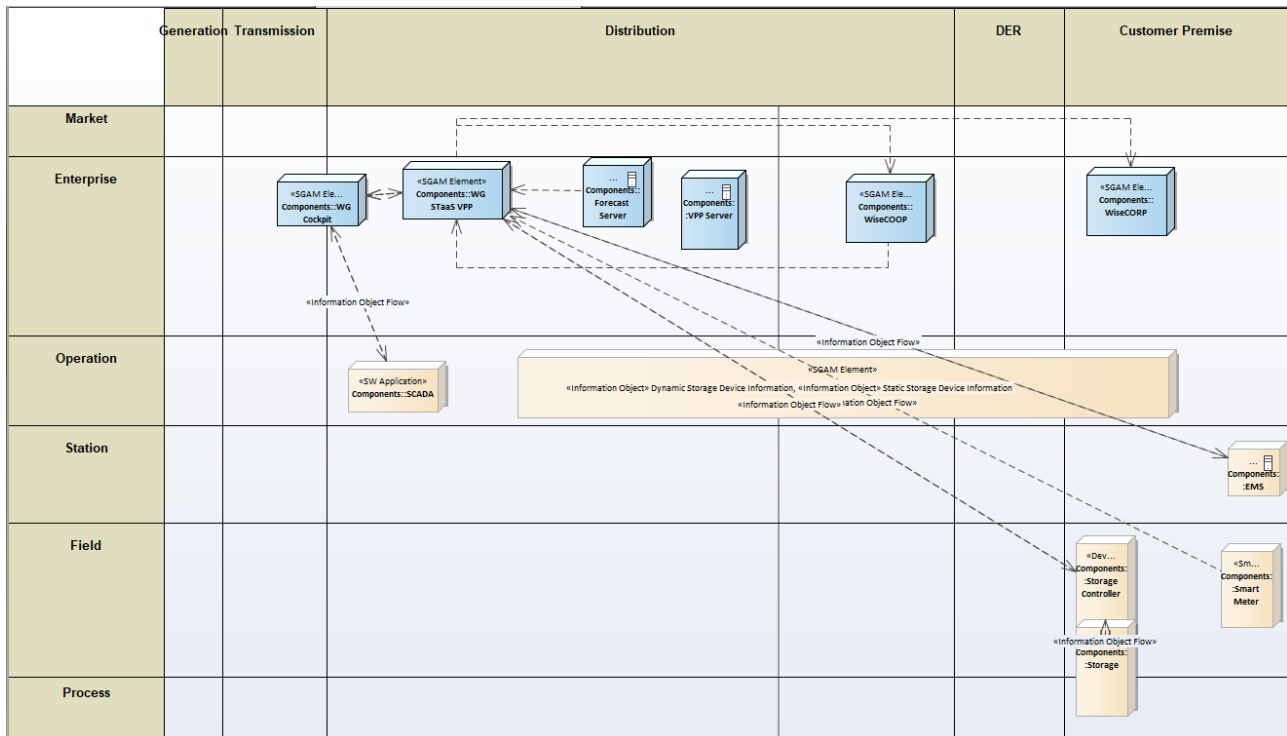


Figure 222 - SGAM Information Layer

### CANONICAL DATA MODEL

Table 177 - List of Data Models

Data Models
Flexibility data model
OpenADR
CIM

## STANDARDS AND INFORMATION OBJECT MAPPING

**Table 178 - List of Data Standards**

Data Standards
Flexibility data model
Billing data model
Schedule and setpoint data model
Storage data model

**Table 179: List of Information Objects**

Information Objects	Data Model
Demand response request	Flexibility data model
Demand flexibility profile	Flexibility data model
Demand response	Flexibility data model
Flexibility offer	Flexibility data model
Flexibility request	Flexibility data model
Schedule data	Schedule and setpoint data model
Setpoint data	Schedule and setpoint data model

### 21.3.7 ACTIVITY DIAGRAM

The activity for this use case is presented below.

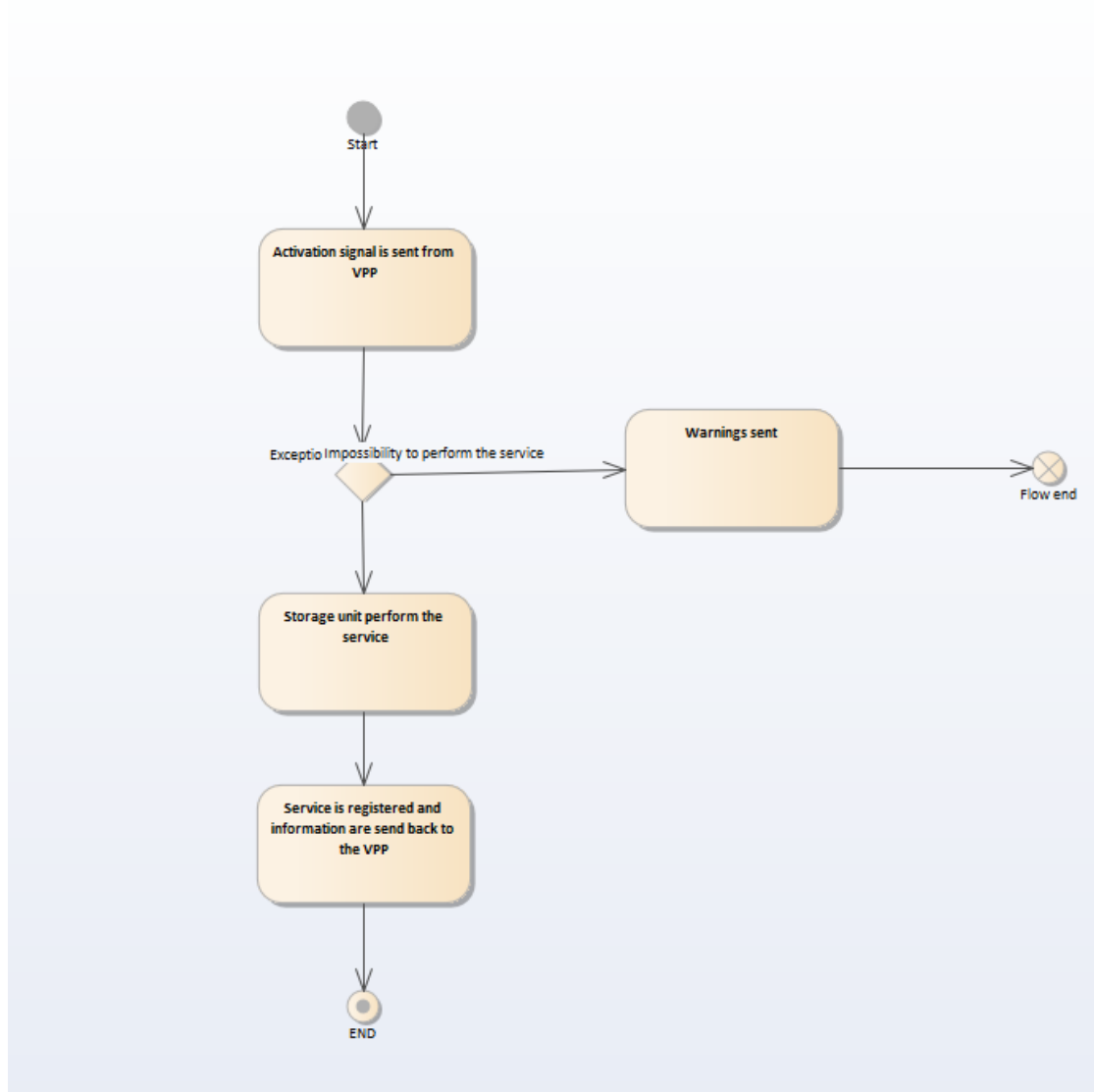


Figure 223 - Primary Use Case Activity Diagram

### 21.3.8 SEQUENCE DIAGRAM

The sequence diagram for this use case is presented below.

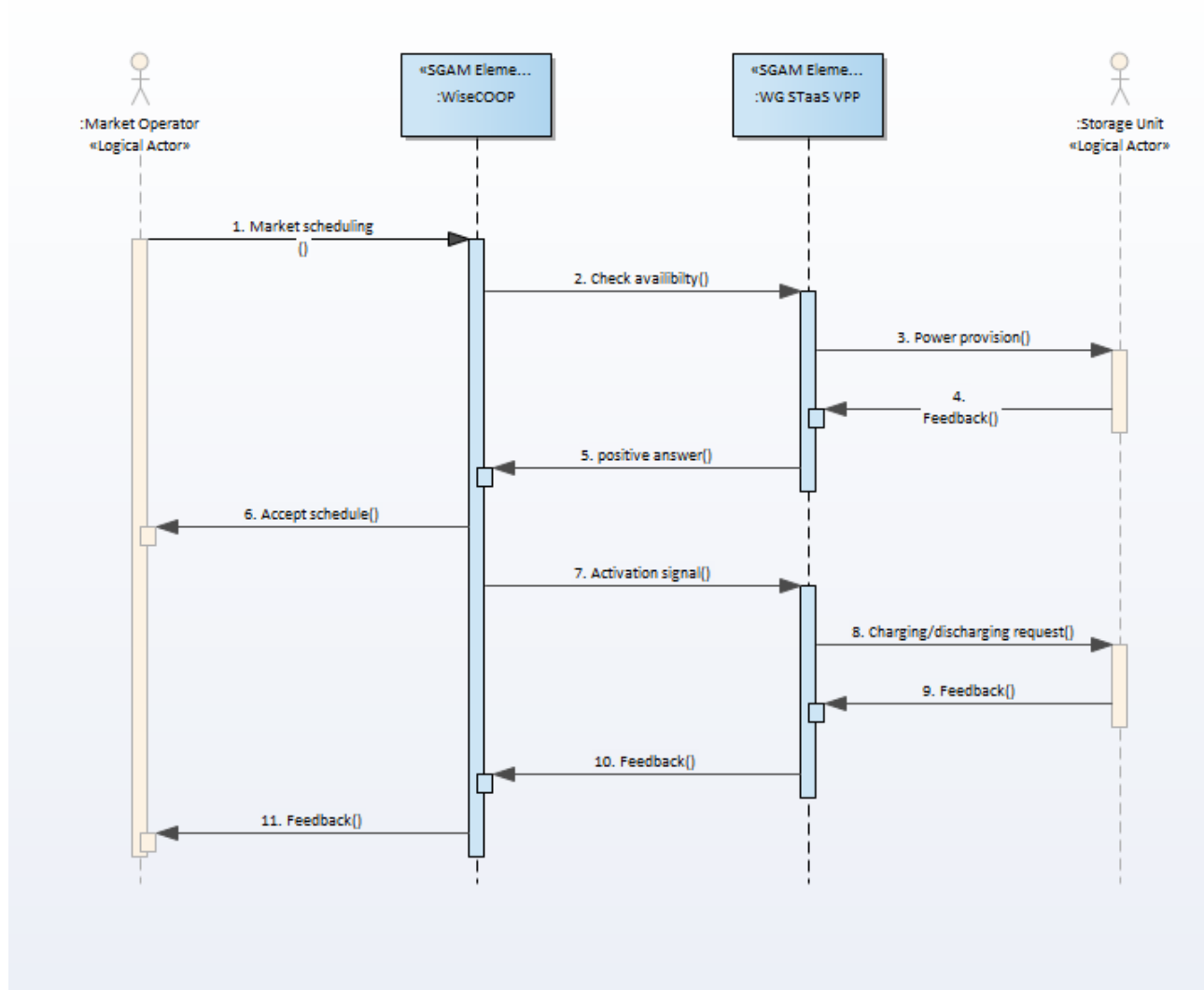


Figure 224 - Primary Use Case Sequence Diagram

## 21.4 HL-UC 4\_PUC\_4: COMBINATION OF BATTERY STORAGE SYSTEMS

### 21.4.1 PRIMARY USE CASE DESCRIPTION

With the combination of different storage technologies high power (e.g. ultracapacitors) and energy (e.g. batteries) contents can be achieved at the same system.

In common uses, it is necessary to obtain information about the status of every unit by means of a standard of information trading. This information can be used for managing in a coordinated manner the area system for interest.

Technical specifications of any battery connected to the system will be available for “grid operators” and “management systems” and used for both administrative and operative (controlling) functions. This information about the specifications of every battery model included in the system must be available for both reading and controlling

### PARAMETER IDENTIFICATION OF STORAGE SYSTEMS

The operating parameters and configurations need to be established and modeled in a standard way so that all the systems are compatible with the management system.

These parameters are necessary to be set up on to get a correct function of the system; every storage system needs be correctly configured by the end users or the Battery Operator indeed.

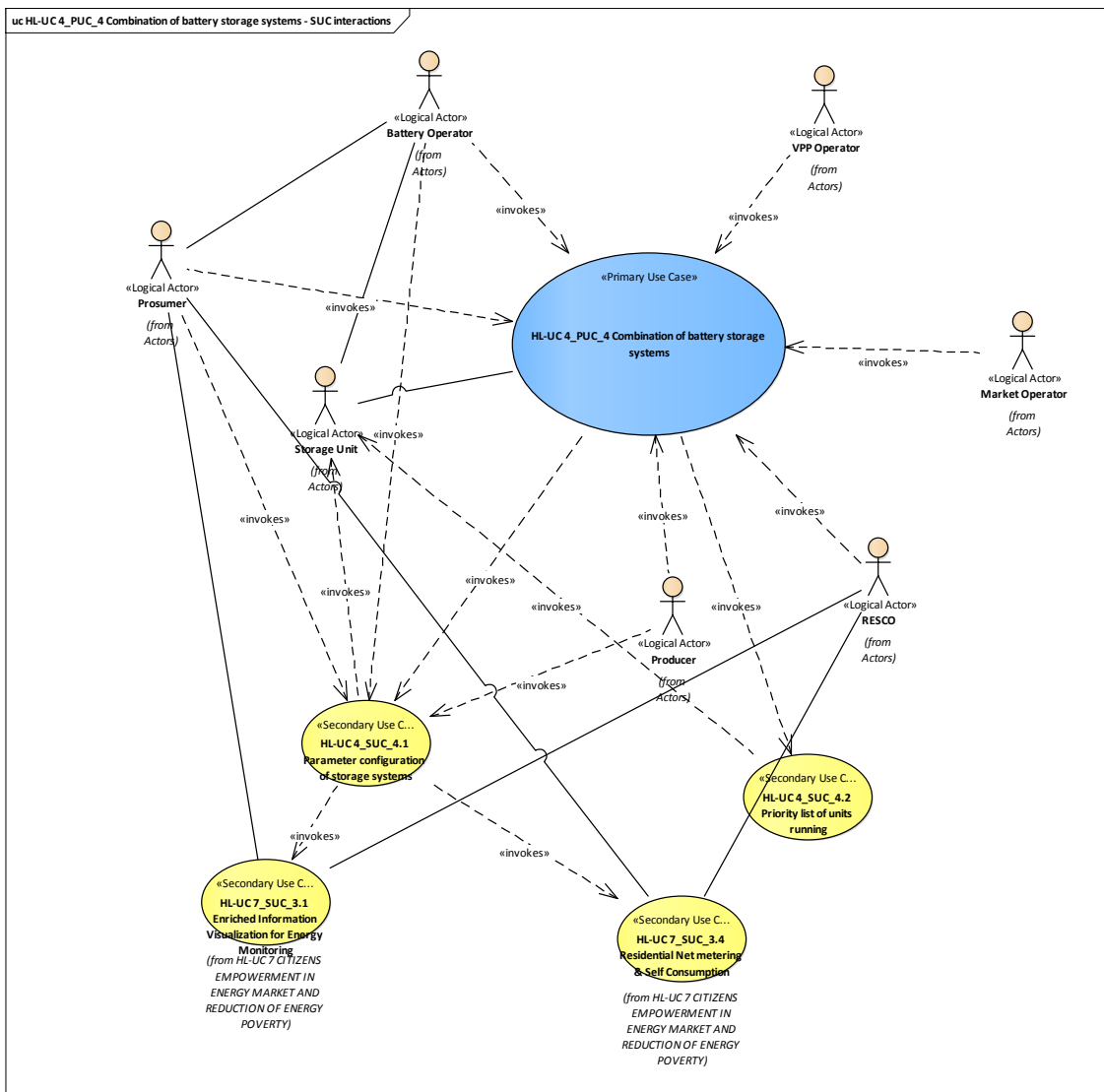
### PRIORITY LIST OF UNITS RUNNING

Depending on the operation parameters and status, a priority list needs to be performed in order to guarantee the same usage of each battery due to ageing and profitability. Algorithms for selection of best suited combinations of storage units have to consider type of storage, availability of storage system, power capability, remaining energy content, current aging status, efficiency, demand and production forecasts. Algorithms have to define if participation of storage systems in energy market/energy transfer is beneficial or not. (Aging of system + loss of energy + unavailability during period vs. income)

### 21.4.2 SECONDARY USE CASE INTERACTIONS

The following diagram shows all SUCs considered under this Combination of battery storage systems PUC, in order to understand the behaviour of combine batteries under determinate grid conditions to improve the supply quality. Also, this system can increase user profit working all together sharing ESS capacity to VPP aggregate.

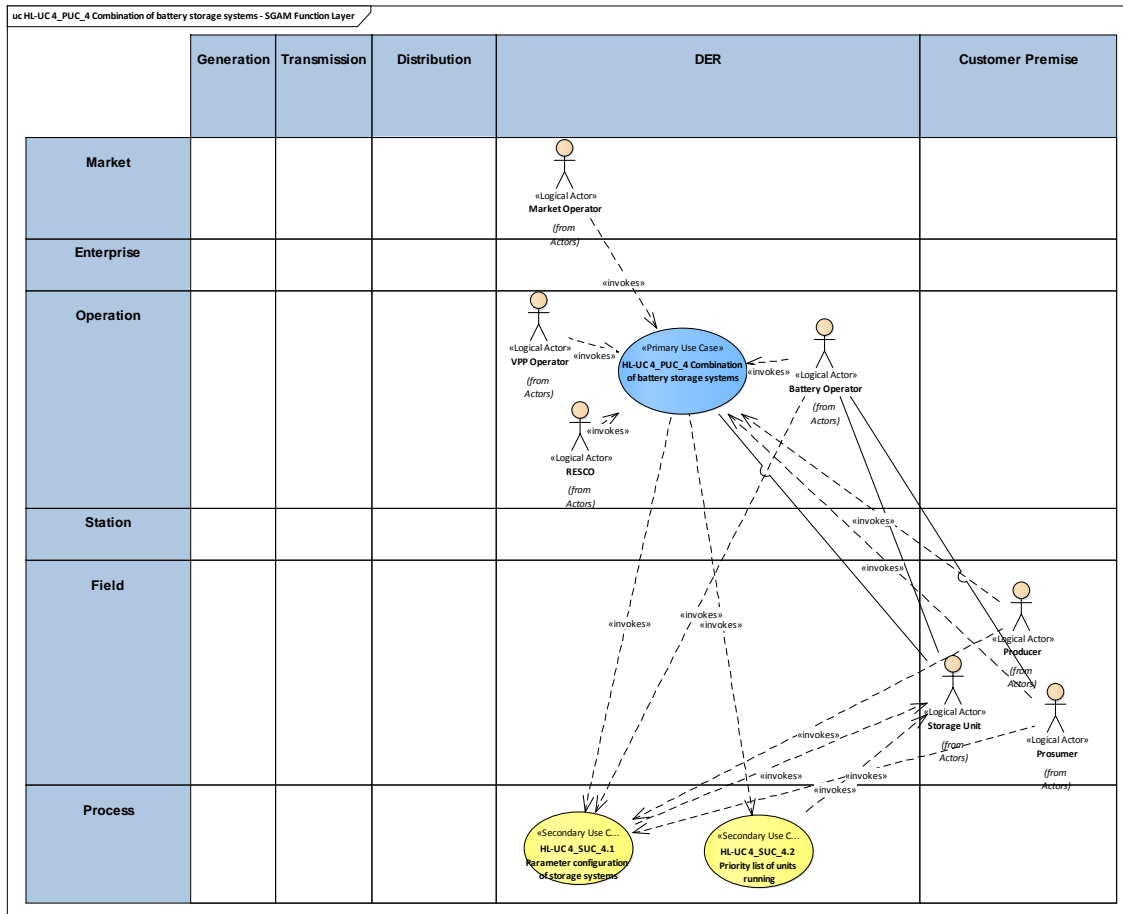




SUC Name	Description	Relation	PUC/SUC
Enriched information visualization for Energy	This SUC provides an enriched visualization tool for a better understanding of Pro/Consumers about their energy consumption.	Invoke	HLUC 7_SUC_3.1
Residential Net metering & Self Consumption	The main objective of this SUC is to allow the end-users of the application (residential clients) to participate in net metering & self-consumption concepts, promoting that way the idea of green, carbon-free living.	Invoke	HLUC 7_SUC_3.4
Parameter configuration of Storage System	This SUC establish a parameter configuration code standard.	Invoke	HLUC 4_SUC_4.1
Priority list of units running	This SUC contains the selection algorithm which determines the next status of ever system.	Invoke	HLUC 4_SUC_4.2

### 21.4.3 SGAM FUNCTION LAYER

In the figure below the actor and SUCs involved in the HL 4 PUC 4 are positioned on the SGAM Layer.

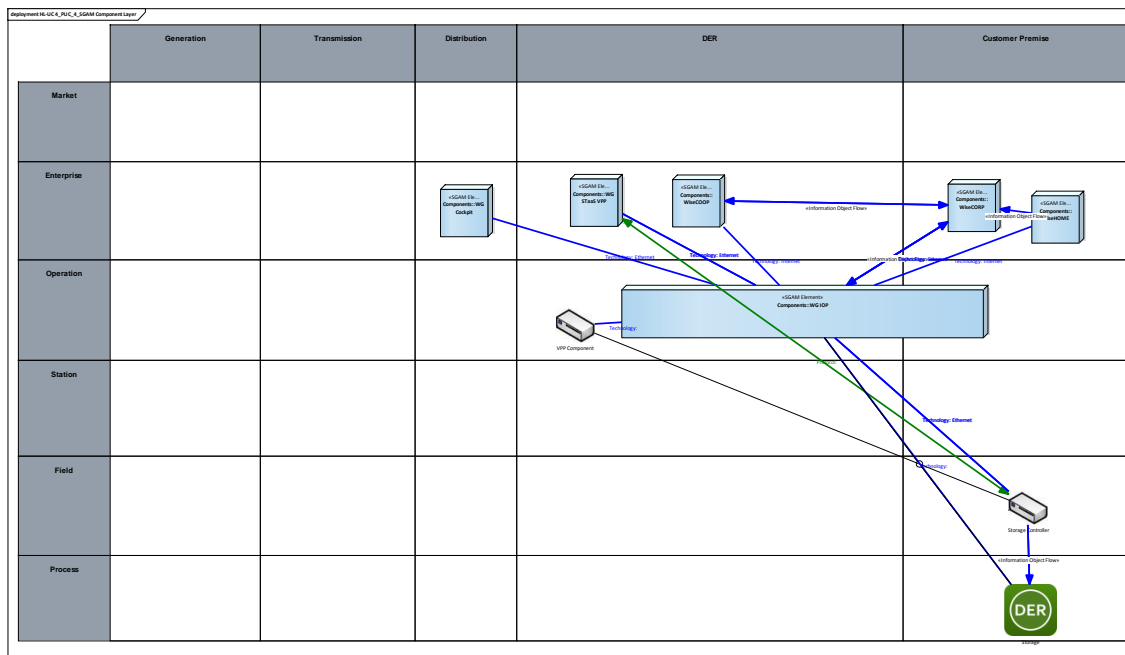


The table shows the actors involved in the HL UC 4 PUC 4

Actor Name	Actor Type
VPP Operator	Logical actor
Market Operator	Logical actor
RESCO	Logical actor
Battery Operator	Logical actor
Producer	Logical actor
Storage Unit	Logical actor
Prosumer	Logical actor

### 21.4.4 SGAM COMPONENT LAYER

The figure below shows the components involved in the HL UC PUC 4 and how they are positioned on the SGAM layer.

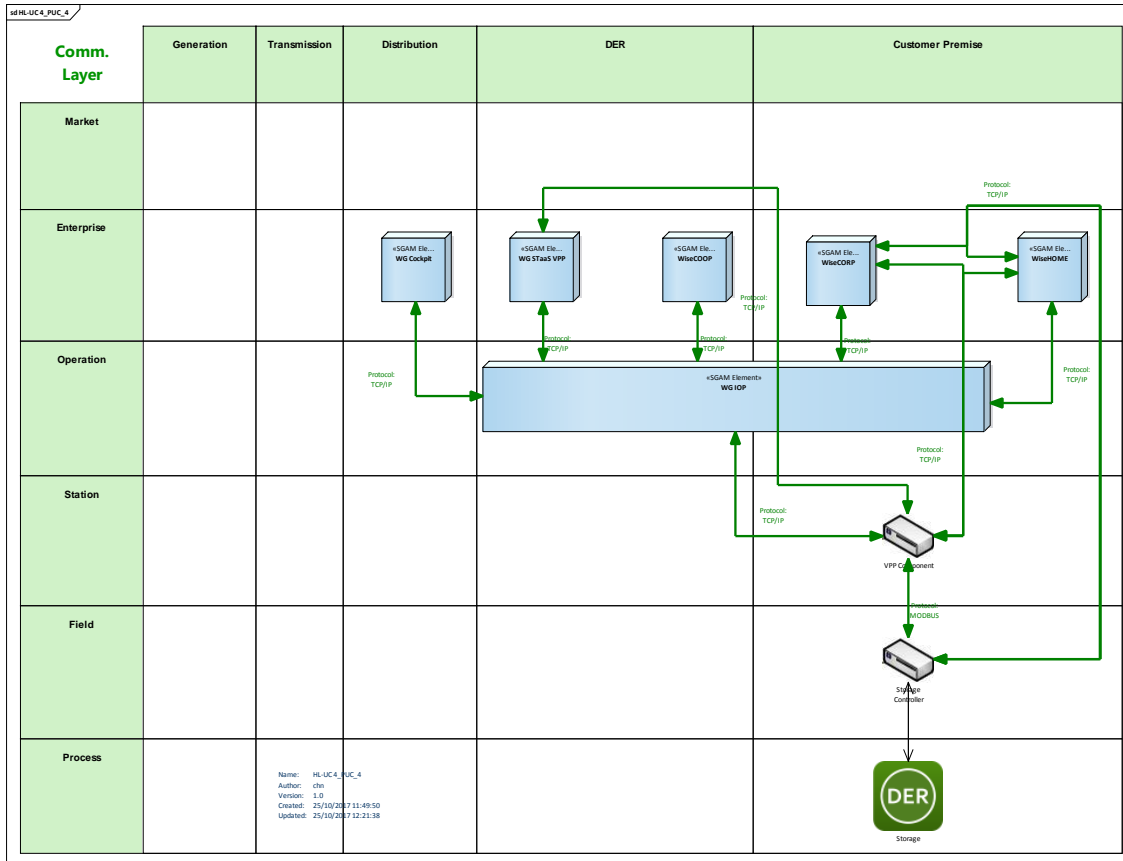


The table below shows the components involved in the PUC.

Component	Component Type
WG Cockpit	SGAM Element
WG StaaS/VPP	SGAM Element
WiseCOOP	SGAM Element
WiseCORP	SGAM Element
WiseHOME	SGAM Element
Storage	Device
Storage Controller	Device
VPP Component	Device

## 21.4.5 SGAM COMMUNICATION LAYER

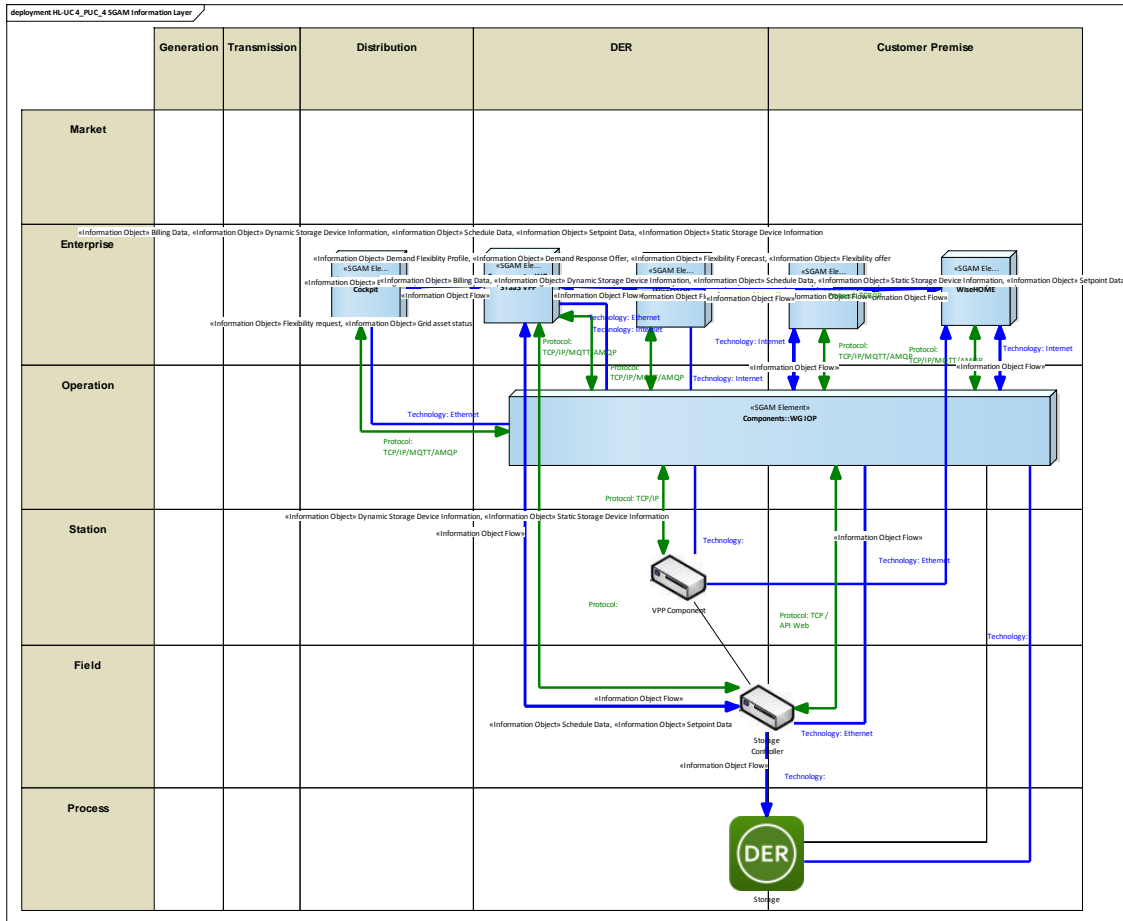
The SGAM communication layer for this Primary Use Case is depicted below.



Communication Technology	Description
TPC/IP	Transmission Control Protocol/Internet Protocol is a Communications protocol for computer networks, the main protocol used on the Internet. It follows specific rules to get data from one network device to another assuring that data will not be lost in transmission
MODBUS	Serial communications protocol originally published for use with programmable logic controllers (PLCs). Simple and robust, it has become a de facto standard communication protocol and is now a commonly available means of connecting industrial electronic devices

## 21.4.6 SGAM INFORMATION LAYER

The SGAM information layer for this Primary Use Case is illustrated below.



## CANONICAL DATA MODELS

Data Models
CIM
Universal Smart Energy Framework (USEF)
DLMS/COSEM
OpenADR
User preference models

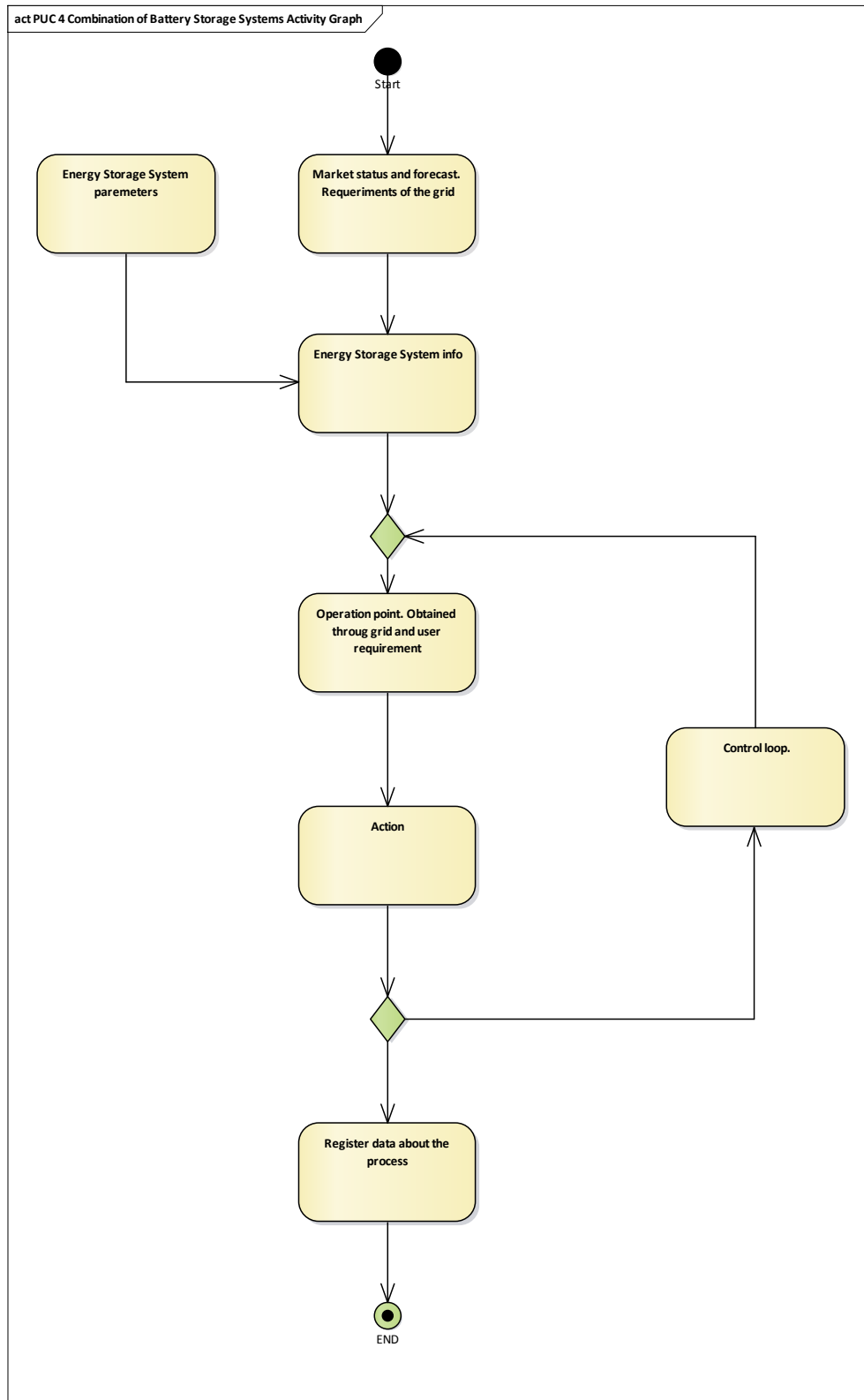
## STANDARDS AND INFORMATION OBJECT MAPPING

Data Standards
CIM
DLMS/COSEM
OpenADR
Universal Smart Energy Metering (USEF)

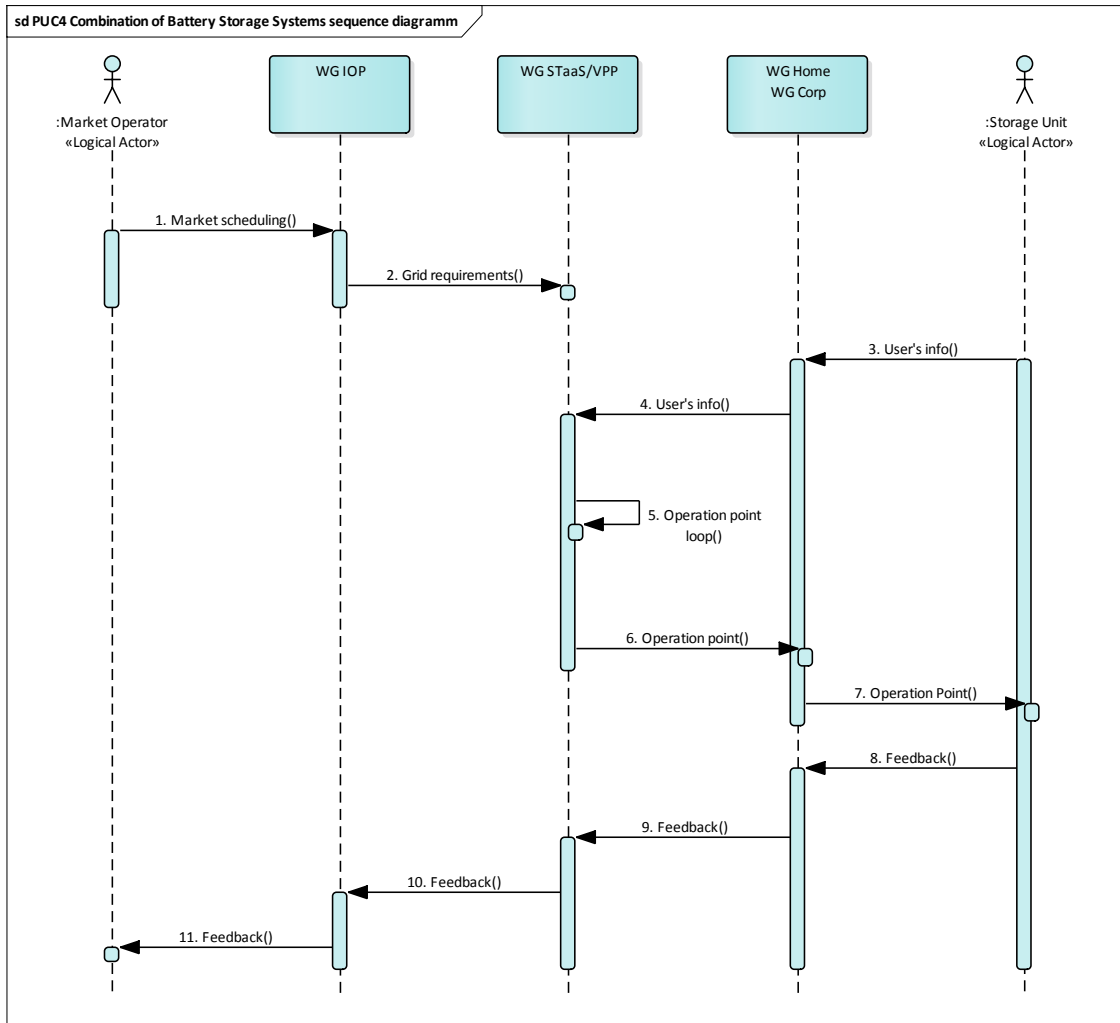
Information Objects	Data Model
Billing Data	OpenADR
Demand Response Offer	USEF
Demand Response Request	USEF
Dynamic Storage Device Information	OpenADR
Energy Metering	DLMS/COSEM

### 21.4.7 ACTIVITY DIAGRAM

The following activity diagram resumes the steps executed under this PUC to retrieve the necessary data from the field devices of the controlled facilities



## 21.4.8 SEQUENCE DIAGRAM





## **22 APPENDIX E - ARCHITECTURE**

### **HL-UC 5: COGENERATION INTEGRATION IN PUBLIC BUILDINGS/HOUSING**

## **22.1 HL-UC 5\_PUC\_1: THERMAL MONITORING**

### **22.1.1 PRIMARY USE CASE DESCRIPTION**

This PUC deals with the integration of Cogeneration in WiseCORP and the efficient management of CHPs and Thermal Storage. Three system components (as well as the relevant critical values of thermal storage) are monitored:

- Gas Consumption in Households
- Combined Heat and Power
- Buildings

### **22.1.2 SECONDARY USE CASE INTERACTIONS**

The interaction between this Primary Use Case and the Secondary Use Cases is depicted below.

uc HL-UC 5\_PUC\_1 Thermal monitoring - SUCs Interactions

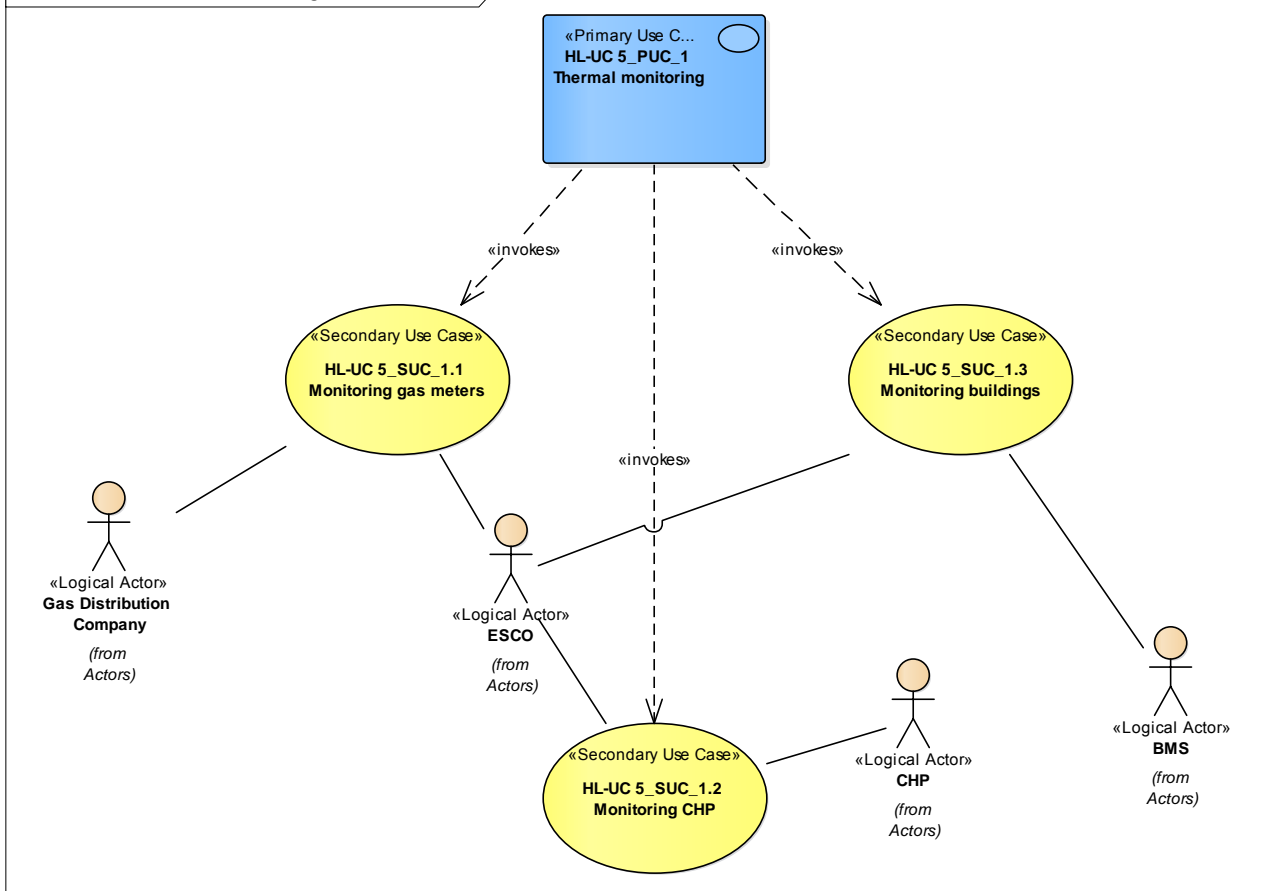


Figure 225 - SUCs Interactions Diagram

Table 180 - Table of list of participating SUCs

SUC Name	Description	Relation	PUC/SUC
Monitoring gas meters	This SUC describes the process of data exchange between the ESCO and the Gas Distribution Company	Invokes	HL-UC 5_PUC_1 Thermal Monitoring
Monitoring CHP	SUC highlights the complex processes of monitoring the CHPs	Invokes	HL-UC 5_PUC_1 Thermal Monitoring
Monitoring buildings	SUC describes the monitoring of different buildings throughout a BMS.	Invokes	HL-UC 5_PUC_1 Thermal Monitoring

### 22.1.3 SGAM FUNCTION LAYER

The SGAM function layer for the Primary Use Case is depicted below.

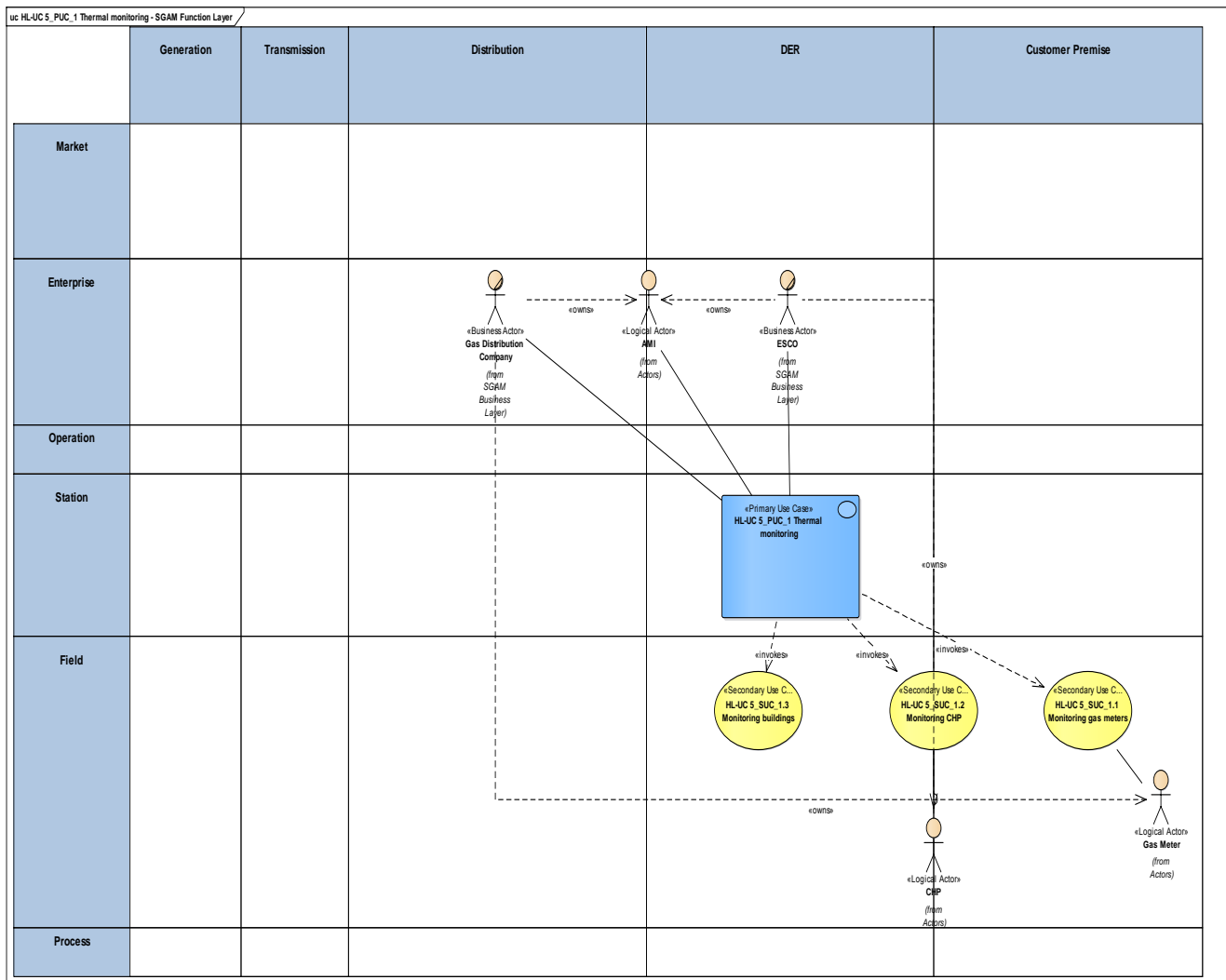


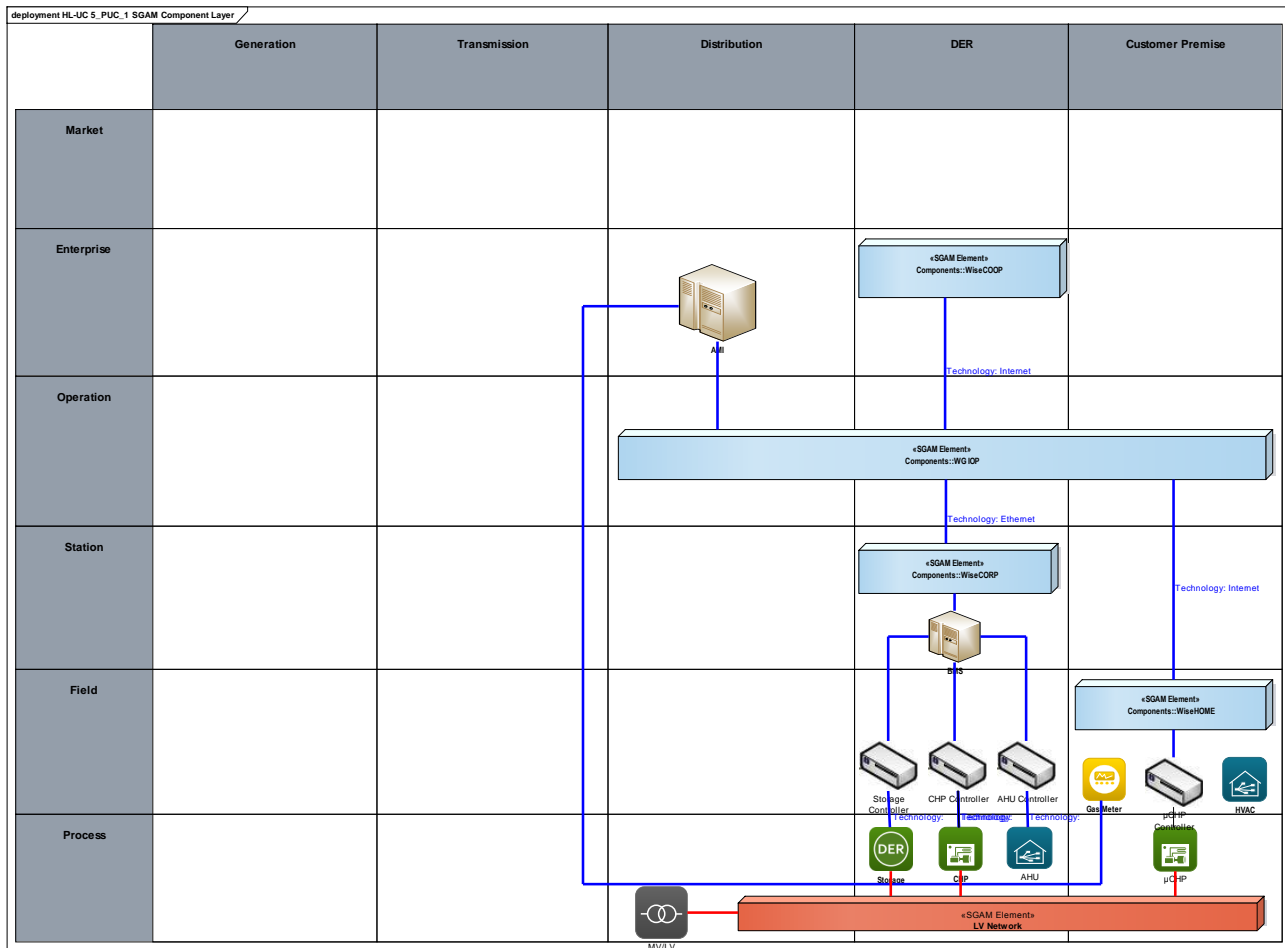
Figure 226 - SGAM Function Layer

Table 181 - List of Actors Involved

Actor Name	Actor Type
AMI	System
ESCO	Organization
BMS	System
Gas Distribution Company	Organization
VPP Operator	Organization
Gas Meter	Device
CHP	Device

#### 22.1.4 SGAM COMPONENT LAYER

The SGAM component layer for this Primary Use Case is illustrated below.



### Figure 227 - SGAM Component Layer

### Table 182 - List of Components Participating in the Primary Use Case

Component	Component Type
WiseCOOP	SGAM Element
WiseIOP	SGAM Element
WiseCORP	SGAM Element
WiseHOME	SGAM Element

## 22.1.5 SGAM COMMUNICATION LAYER

This section outlines the main communication technologies that will be utilized in the reference implementation of the WiseGRID project.

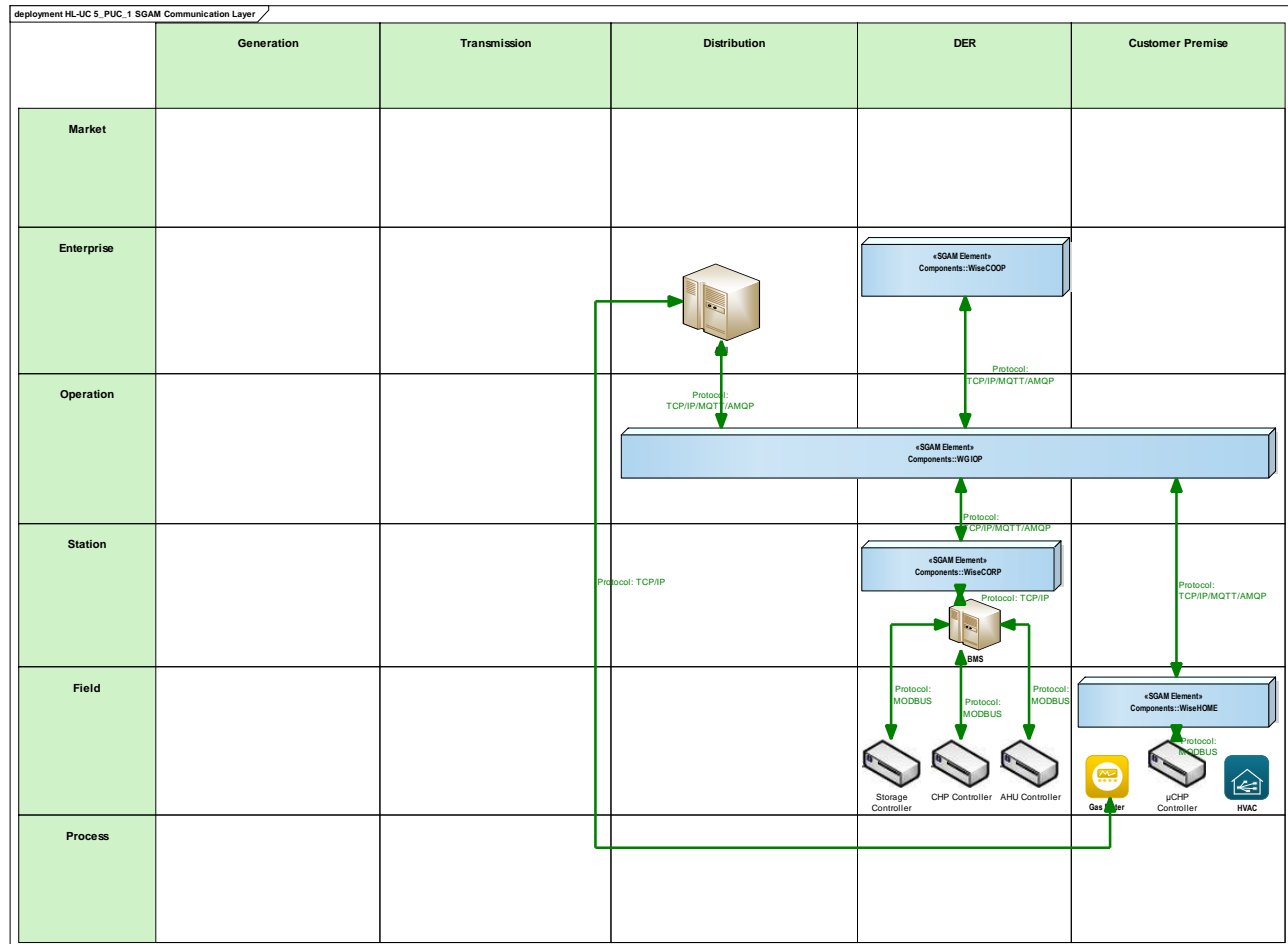


Figure 228 - SGAM Communication Layer

Table 183 - List of Communication Technologies Involved

Communication Technology	Description
TCP/IP	Group of protocols enabling communication between devices in a network up to the transport layer
AMQP	The Advanced Message Queuing Protocol (AMQP) is an open standard application layer protocol for message-oriented middleware. It is a binary, application layer protocol, designed to efficiently support a wide variety of messaging applications and communication patterns.
MQTT	ISO standard (ISO/IEC PRF 20922) publish-subscribe-based lightweight messaging protocol for use on top of the TCP/IP protocol
MODBUS	Serial communications protocol originally published for use with programmable logic controllers (PLCs). Simple and robust, it has become a de facto standard communication protocol and is now a commonly available means of connecting industrial electronic devices

## 22.1.6 SGAM INFORMATION LAYER

The SGAM information layer for this Primary Use Case is illustrated below.

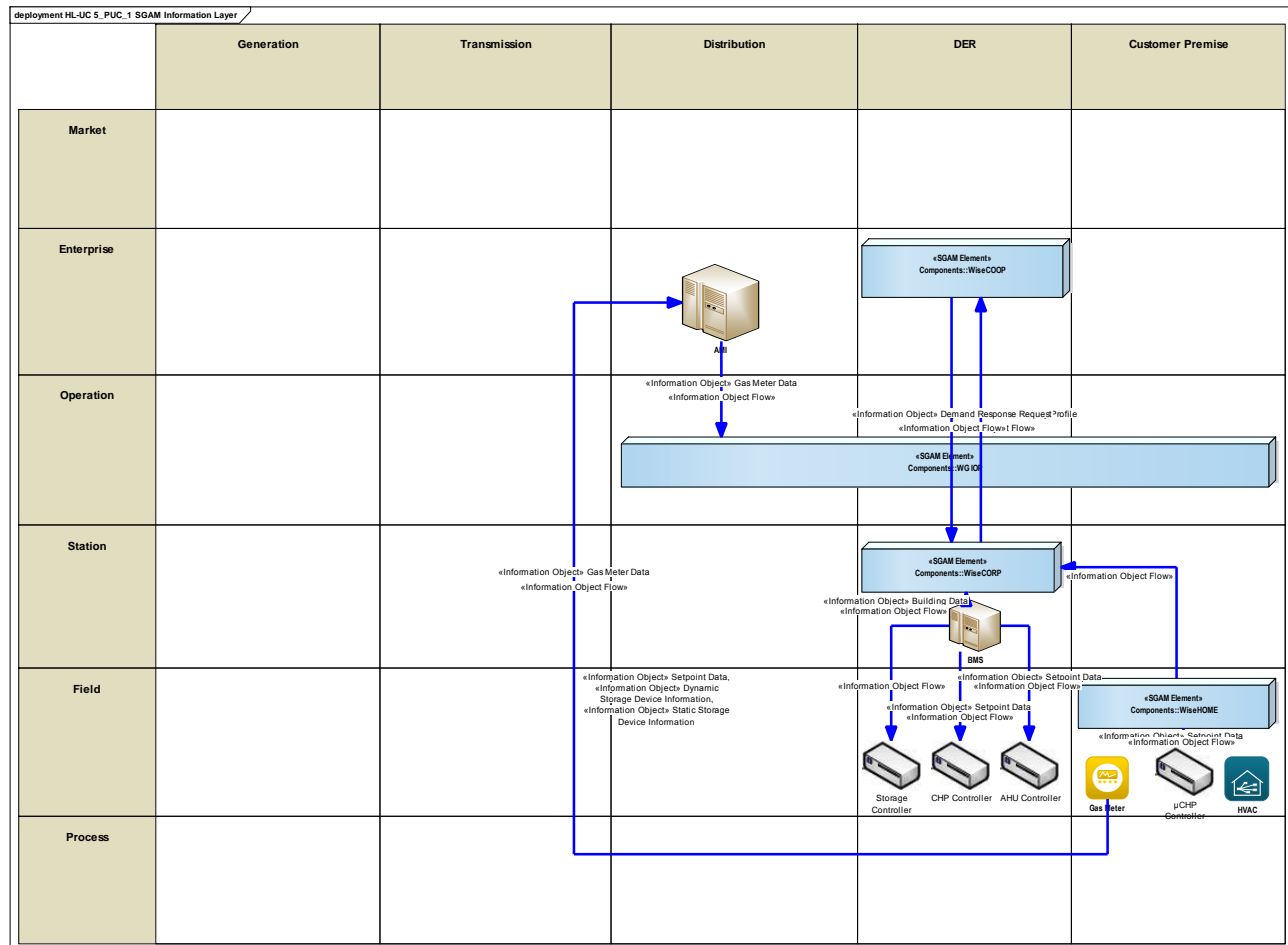


Figure 229 - SGAM Information Layer

## CANONICAL DATA MODELS

The data models used for this Primary Use Case are listed below.

Table 184 - List of Data Models

Data Models
DLMS/COSEM
Building Data Model
OPC-UA

## STANDARDS AND INFORMATION OBJECT MAPPING

The standard and information object mapping for this Primary Use Case is illustrated below.

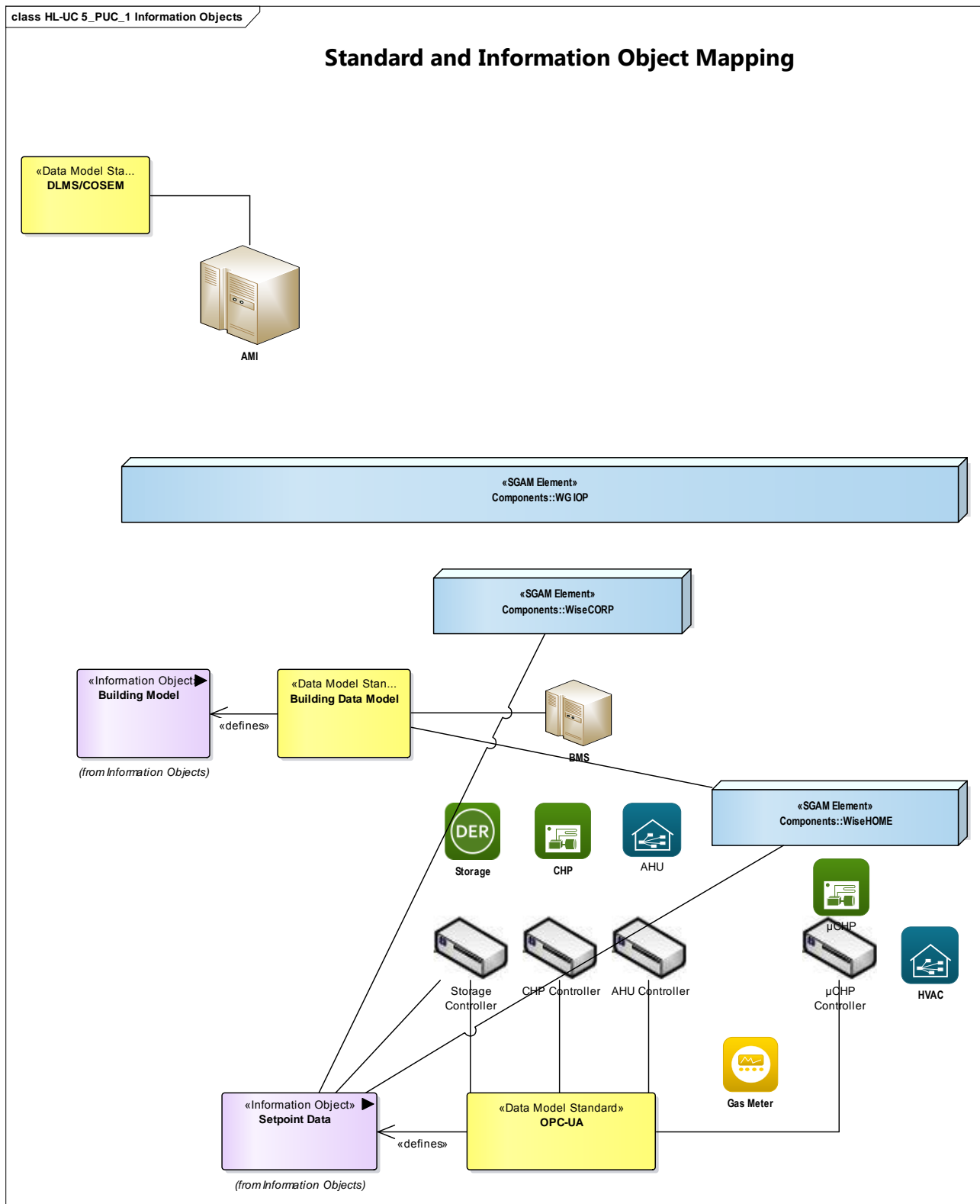


Figure 230 - Standard and Information Object Mapping diagram



Table 185 - List of Data Standards

Data Standards
Building Data Model
OPC-UA

Table 186: List of Information Objects

Information Objects	Data Model
Building Model	Building Data Model
Setpoint Data	OPC-UA

### 22.1.7 ACTIVITY DIAGRAM

The activity diagram for this Primary Use Case is illustrated below.

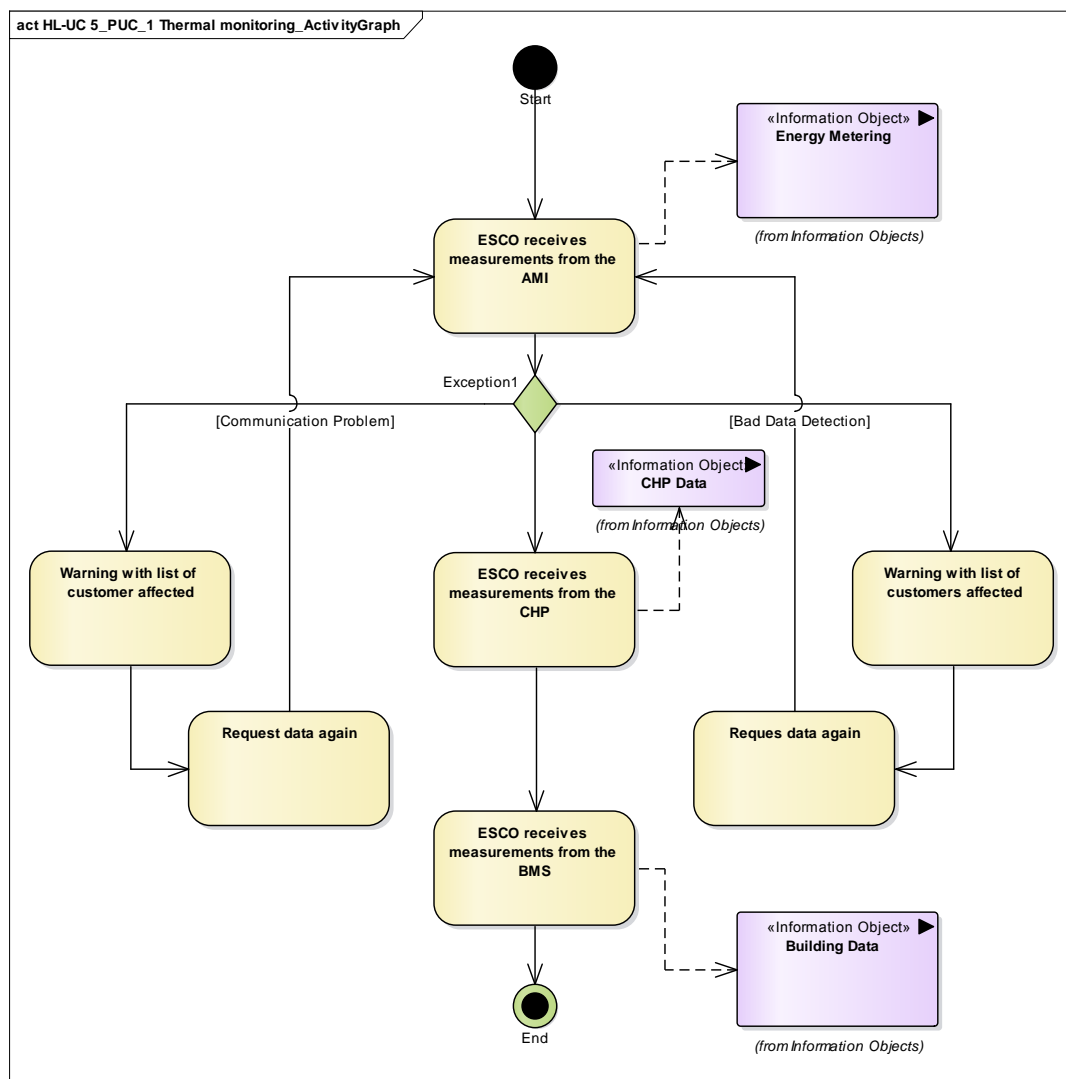


Figure 231 - Primary Use Case Activity Diagram

## 22.1.8 SEQUENCE DIAGRAM

The sequence diagrams associated with the Primary Use Case are listed below.

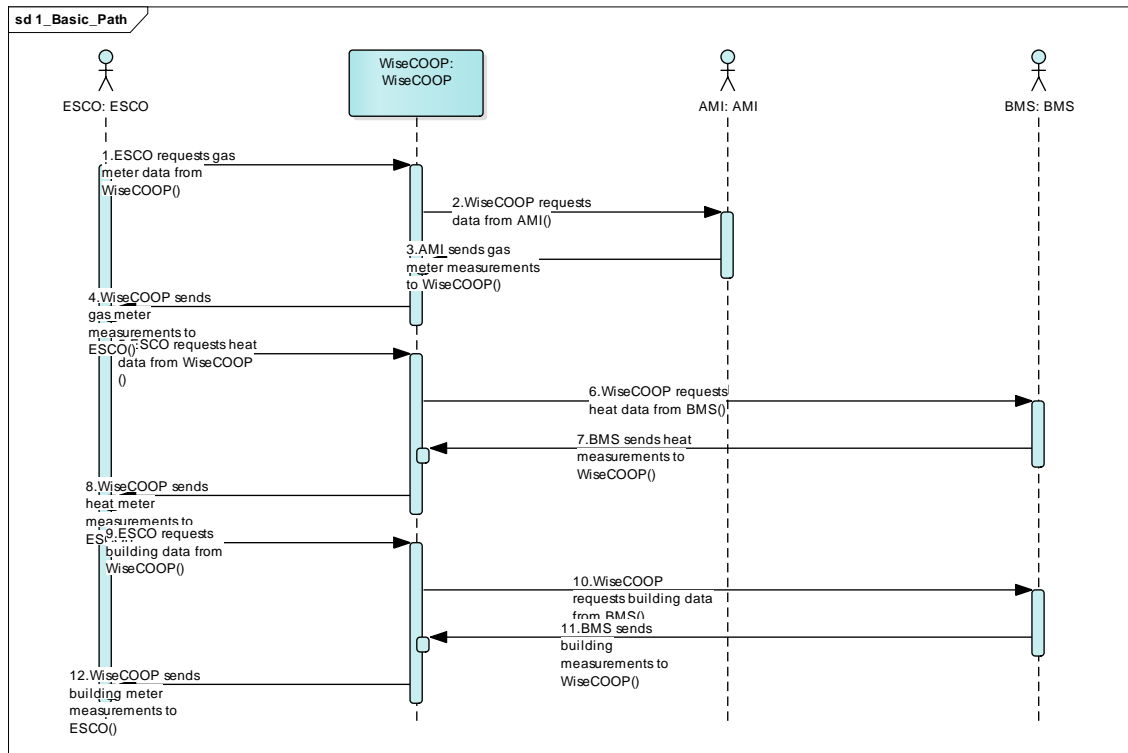


Figure 232: Basic path sequence diagram for HL-UC 5 PUC 1

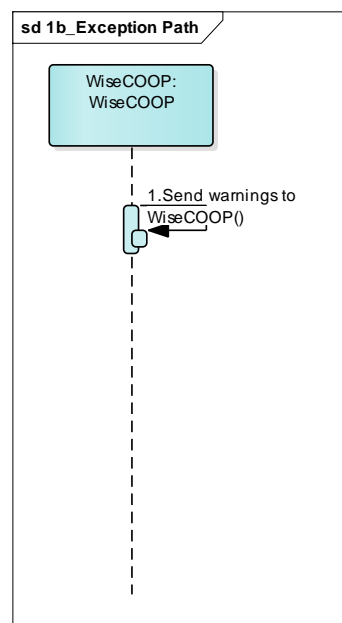


Figure 233: Exception path sequence diagram for HL-UC 5 PUC 1

## 22.2 HL-UC 5\_PUC\_2: COGENERATION AND HVAC MANAGEMENT

### 22.2.1 PRIMARY USE CASE DESCRIPTION

This PUC is associated with the control of CHP, HVAC and thermal loads of buildings. It must take under consideration the schedules proposed by HL-UC 5\_PUC\_4, without being bound by them (PUC must proceed if deviations are detected). Forecasting of thermal needs (taking into account models from HL-UC 5\_PUC\_3 and measurements from HL-UC 5\_PUC\_1) is part of this process, as well as the alarm management

### 22.2.2 SECONDARY USE CASE INTERACTIONS

The interaction between this Primary Use Case and the Secondary Use Cases is depicted below.

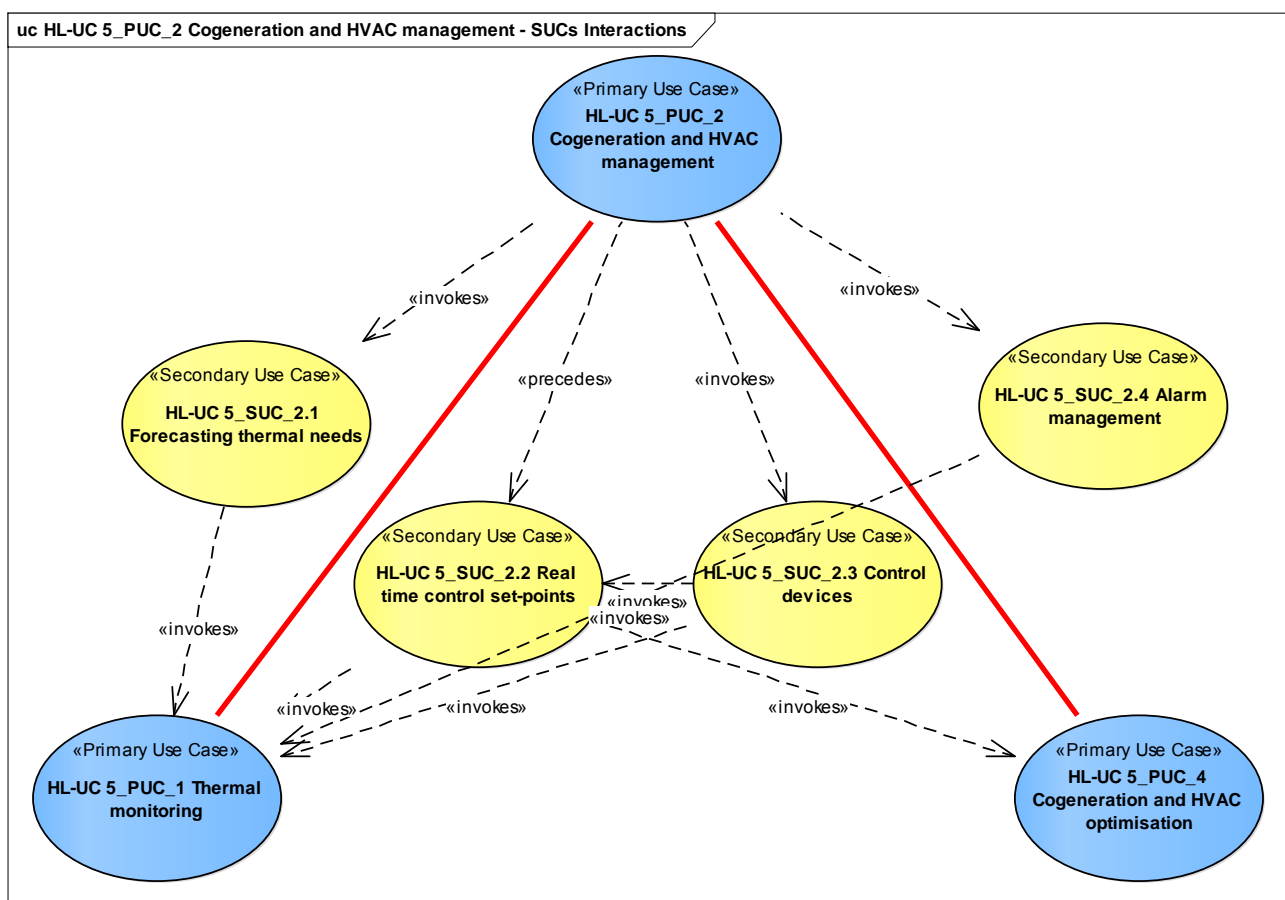


Figure 234 - SUCs Interactions Diagram

Table 187 - Table of list of participating SUCs

SUC Name	Description	Relation	PUC/SUC
Forecasting thermal needs	This SUC will use field measurements and the developed thermal models to estimate the thermal needs in buildings and the infrastructure that belongs to ESCO	Invokes	HL-UC 5_PUC_2 Co-generation and HVAC Management

SUC Name	Description	Relation	PUC/SUC
Real-time control set-points	SUC will use field measurements and will calculate the necessary real-time set-points for various devices	Invokes	HL-UC 5_PUC_2 Co-generation and HVAC Management
Control devices	SUC will deliver set-points/commands to various devices/assets	Invokes	HL-UC 5_PUC_2 Co-generation and HVAC Management
Alarm management	This SUC aims at collecting and managing the alarms coming from the field devices	Invokes	HL-UC 5_PUC_2 Co-generation and HVAC Management

### 22.2.3 SGAM FUNCTION LAYER

The SGAM function layer for the Primary Use Case is depicted below.

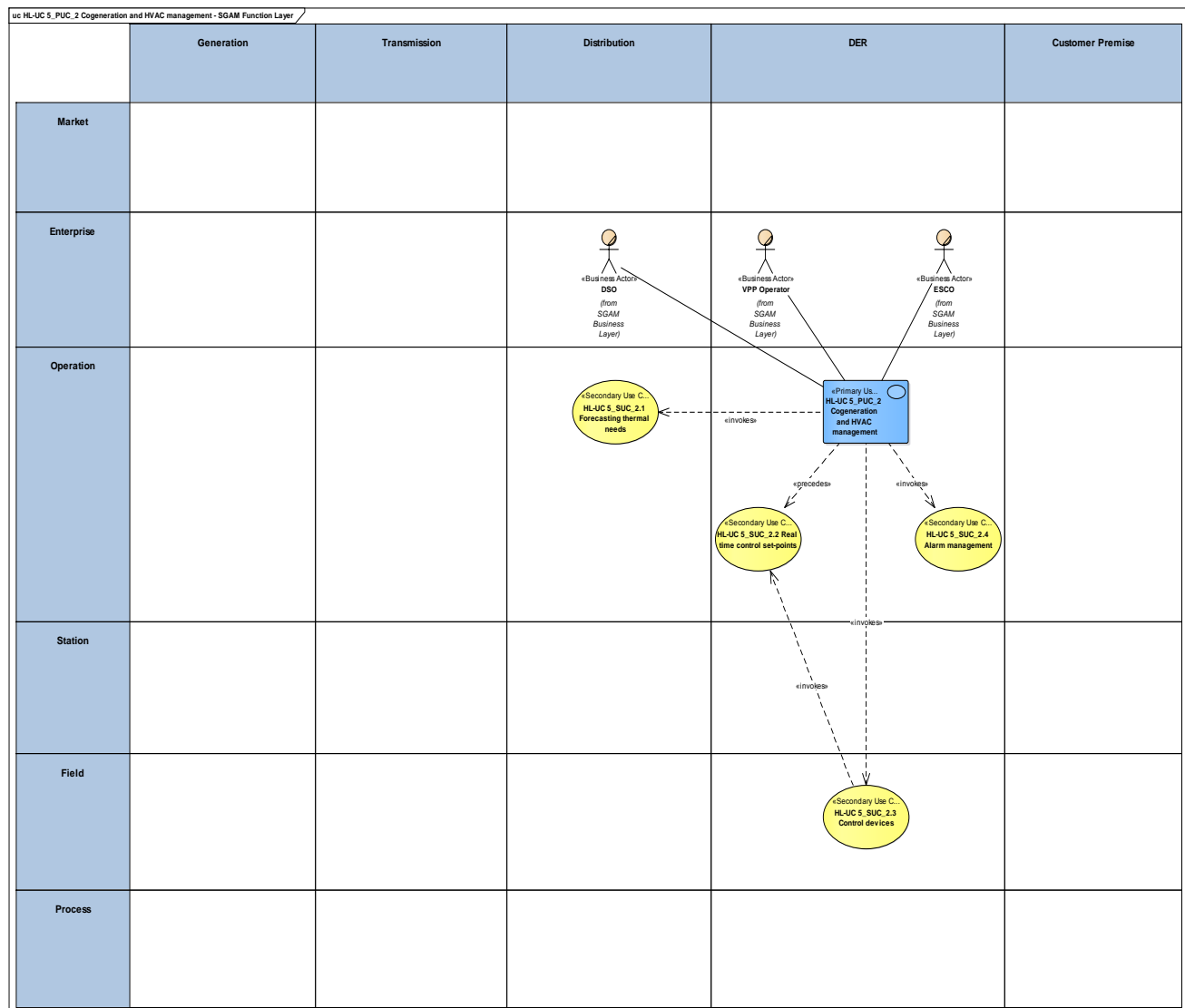


Figure 235 - SGAM Function Layer

Table 188 - List of Actors Involved

Actor Name	Actor Type
AMI	System
ESCO	Organization
BMS	System
Gas Distribution Company	Organization
VPP Operator	Organization
Gas Meter	Device

### 22.2.4 SGAM COMPONENT LAYER

The SGAM component layer for the Primary Use Case is illustrated below.

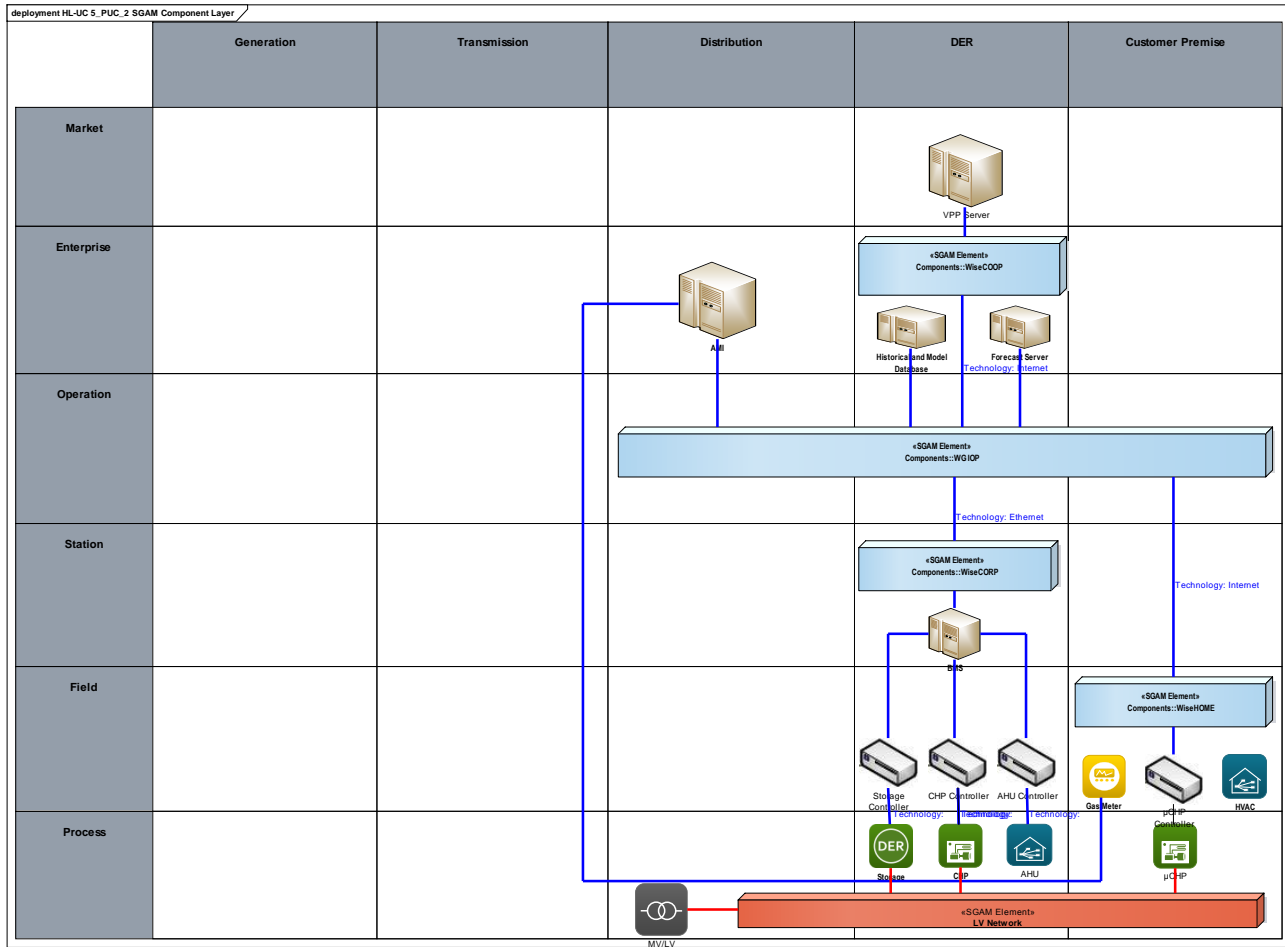


Figure 236 - SGAM Component Layer

Table 189 - List of Components Participating in the Primary Use Case

Component	Component Type
WiseCOOP	SGAM Element
WiseIOP	SGAM Element
WiseCORP	SGAM Element
WiseHOME	SGAM Element

## 22.2.5 SGAM COMMUNICATION LAYER

This section outlines the main communication technologies that will be utilized in the reference implementation of the WiseGRID project.

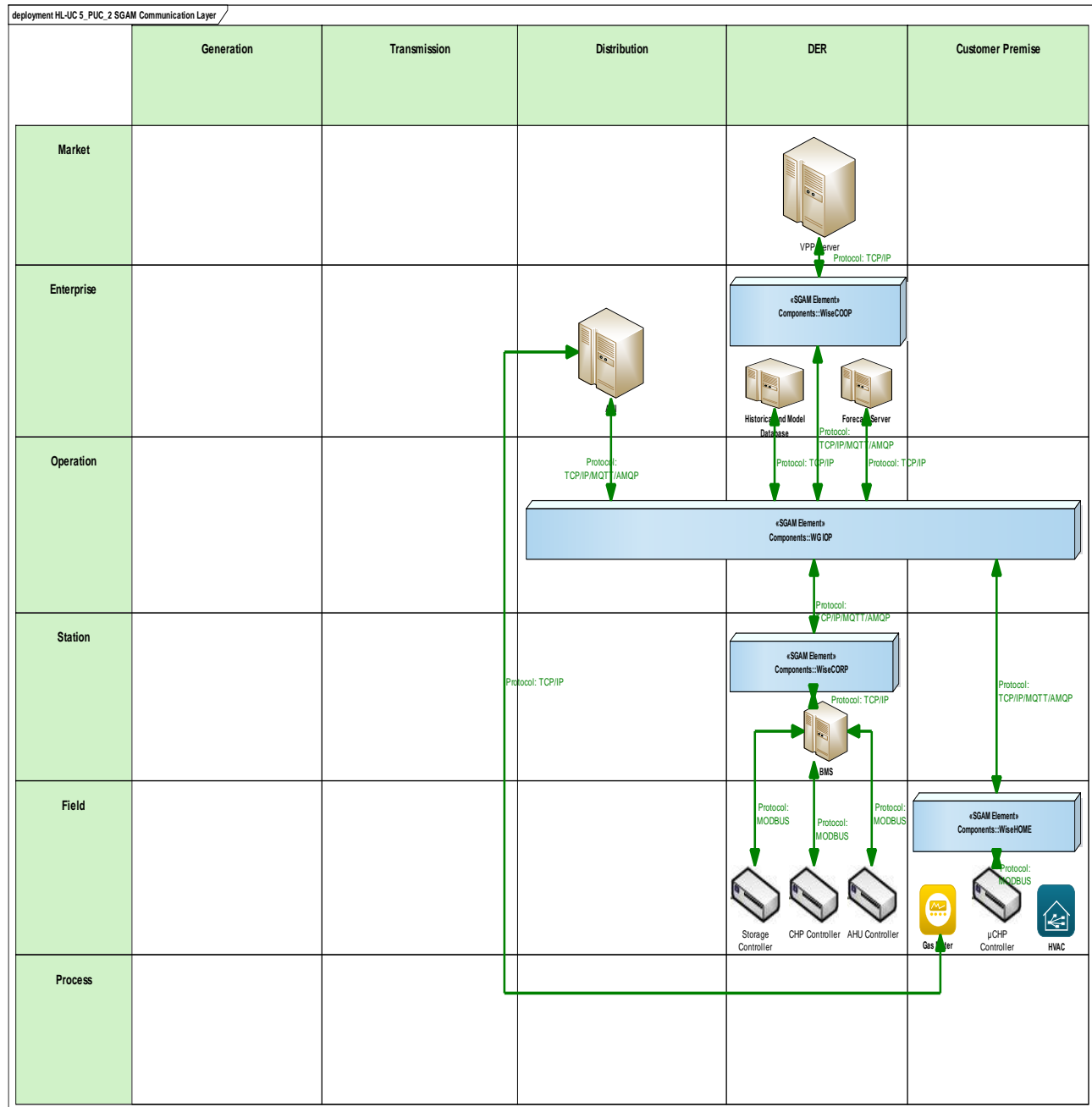


Figure 237 - SGAM Communication Layer

**Table 190 - List of Communication Technologies Involved**

Communication Technology	Description
TCP/IP	Group of protocols enabling communication between devices in a network up to the transport layer
AMQP	The Advanced Message Queuing Protocol (AMQP) is an open standard application layer protocol for message-oriented middleware. It is a binary, application layer protocol, designed to efficiently support a wide variety of messaging applications and communication patterns.
MQTT	ISO standard (ISO/IEC PRF 20922) publish-subscribe-based lightweight messaging protocol for use on top of the TCP/IP protocol
MODBUS	Serial communications protocol originally published for use with programmable logic controllers (PLCs). Simple and robust, it has become a de facto standard communication protocol and is now a commonly available means of connecting industrial electronic devices



## 22.2.6 SGAM INFORMATION LAYER

The SGAM information layer for the Primary Use Case is depicted below.

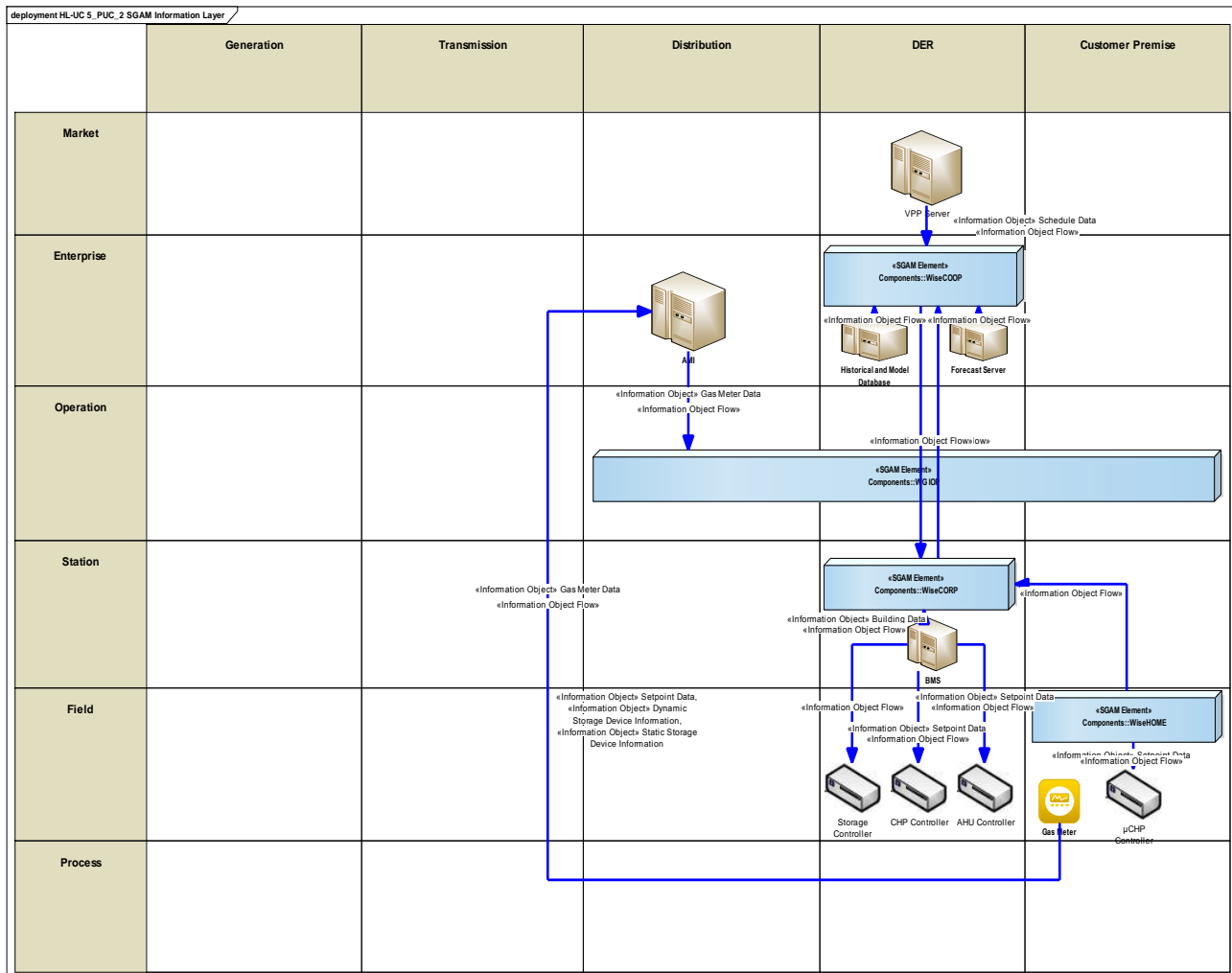


Figure 238 - SGAM Information Layer

## Canonical data models

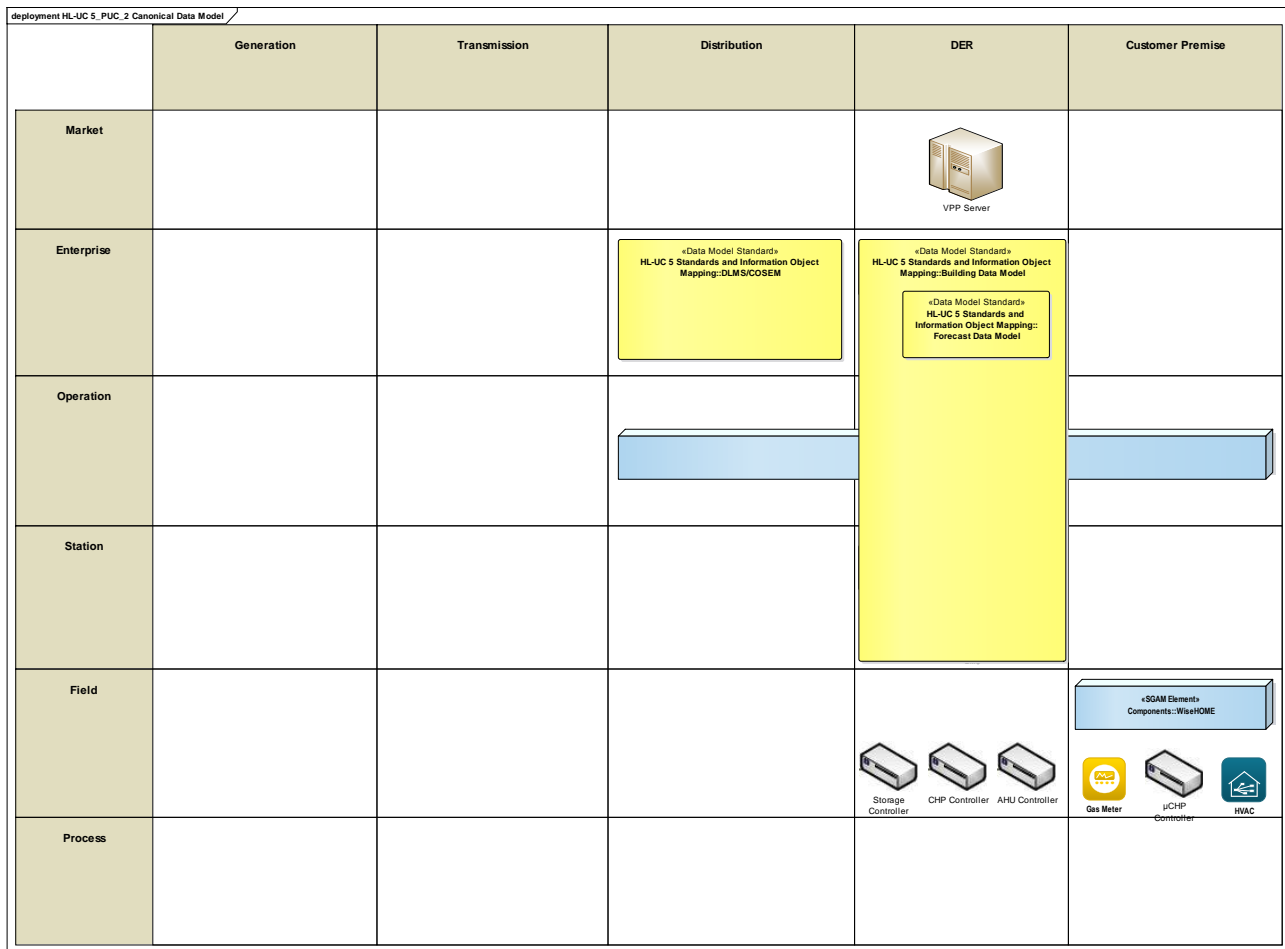


Figure 239 - Canonical Data Model diagram

Table 191 - List of Data Models

Data Models
DLMS/COSEM
Building Data Model
Forecast Data Model

## STANDARDS AND INFORMATION OBJECT MAPPING

The standards and information object mapping associated with the Primary Use Case is depicted below.

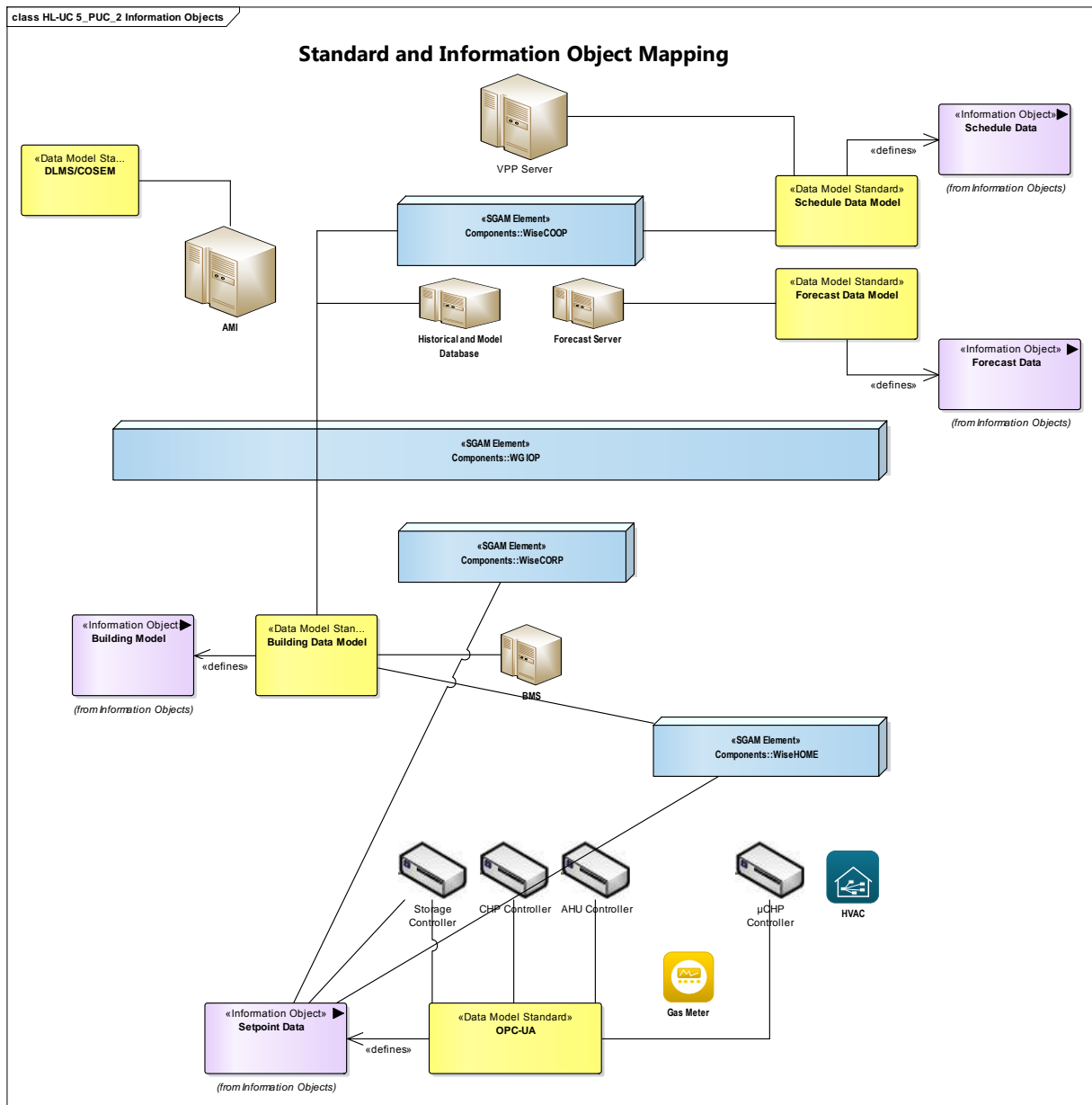


Figure 240 - Standard and Information Object Mapping diagram

Table 192 - List of Data Standards

Data Standards
DLMS/COSEM
Schedule Data Model
Forecast Data Model
Building Data Model
OPC-UA

**Table 193: List of Information Objects**

Information Objects	Data Model
Schedule Data	Schedule Data Model
Forecast Data	Forecast Data Model
Building Model	Building Data Model
Setpoint Data	OPC-UA

## 22.2.7 ACTIVITY DIAGRAM

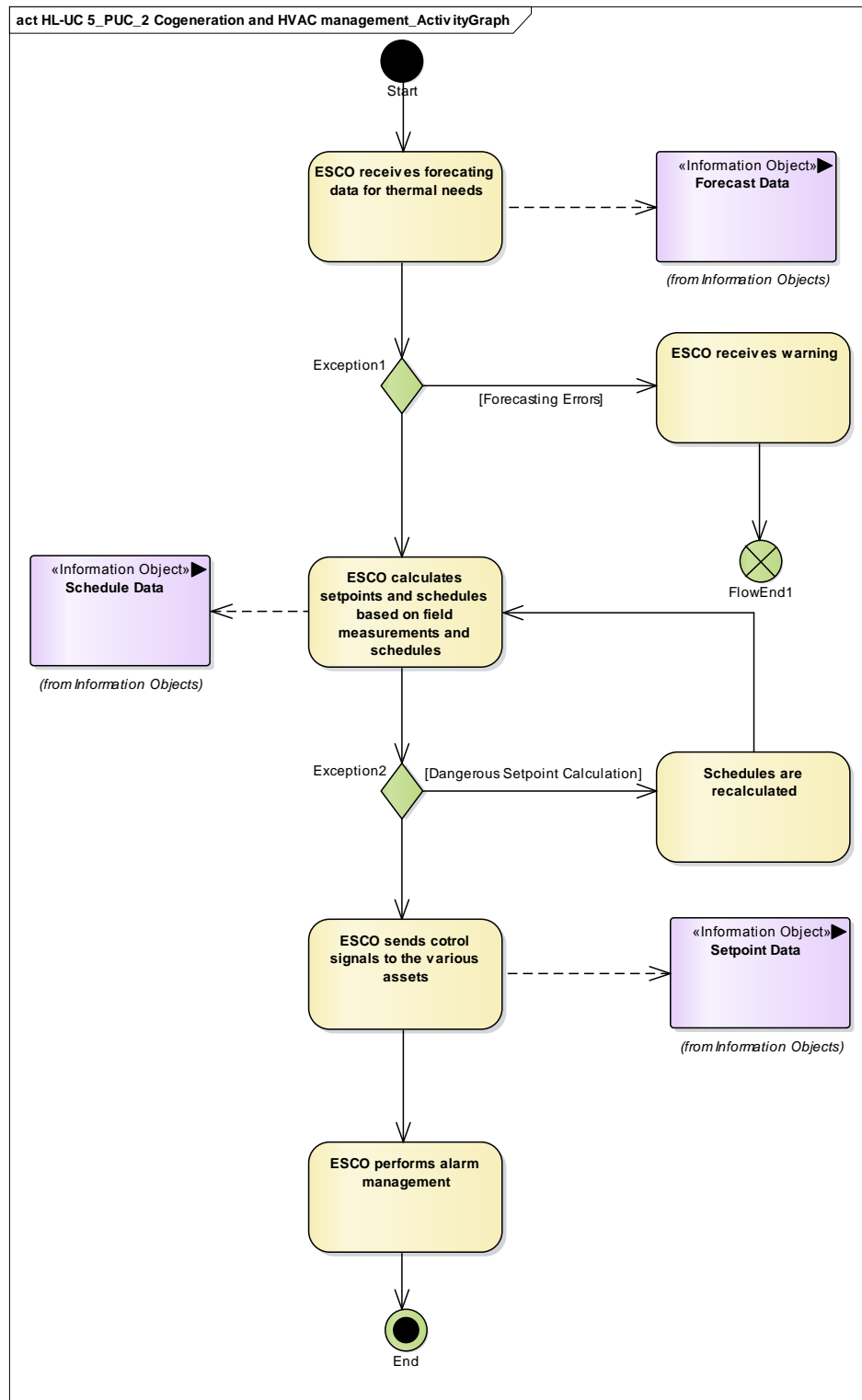


Figure 241 - Primary Use Case Activity Diagram

## 22.2.1 SEQUENCE DIAGRAM

The sequence diagrams associated with this Primary Use Case are listed below.

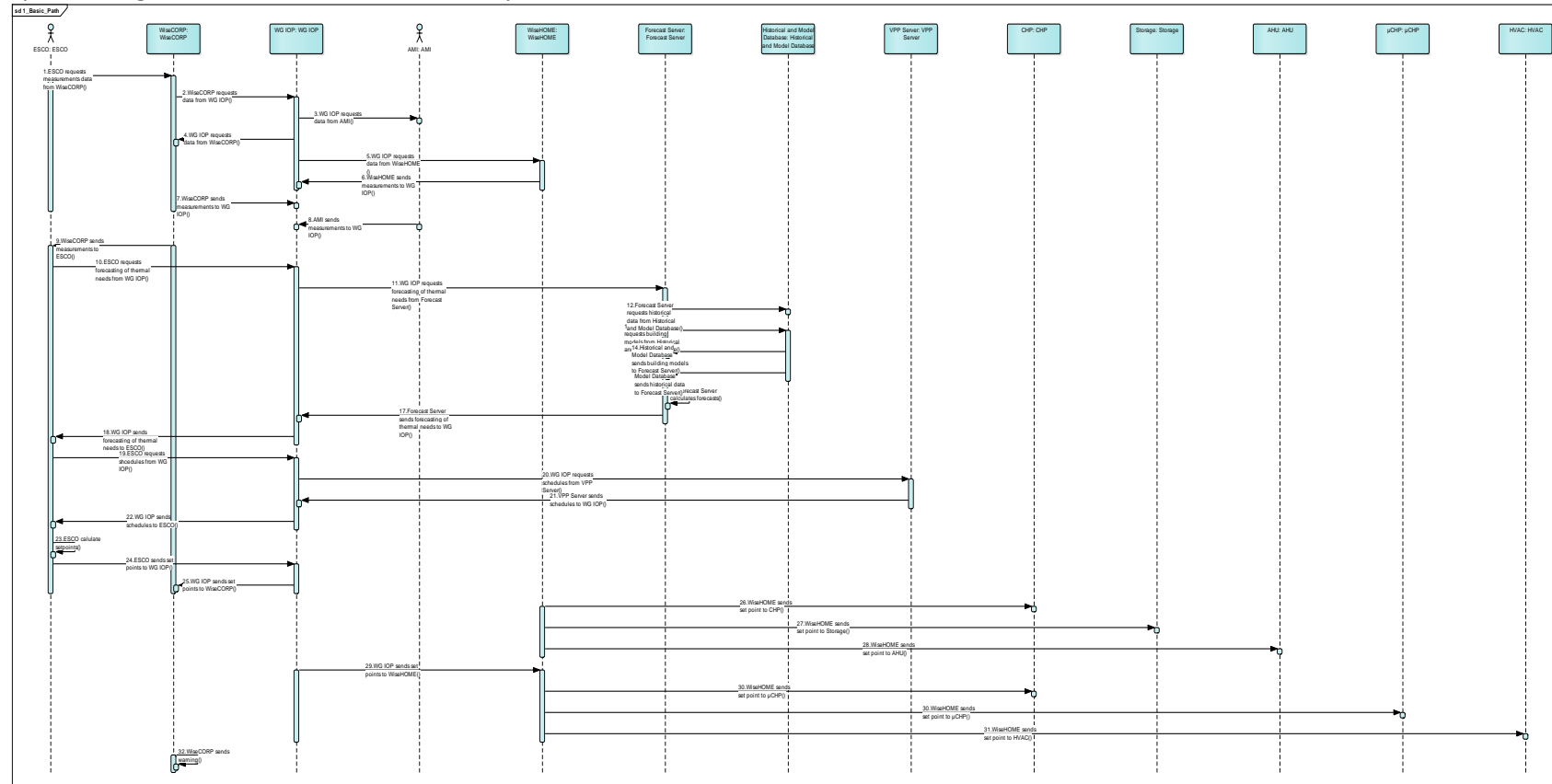
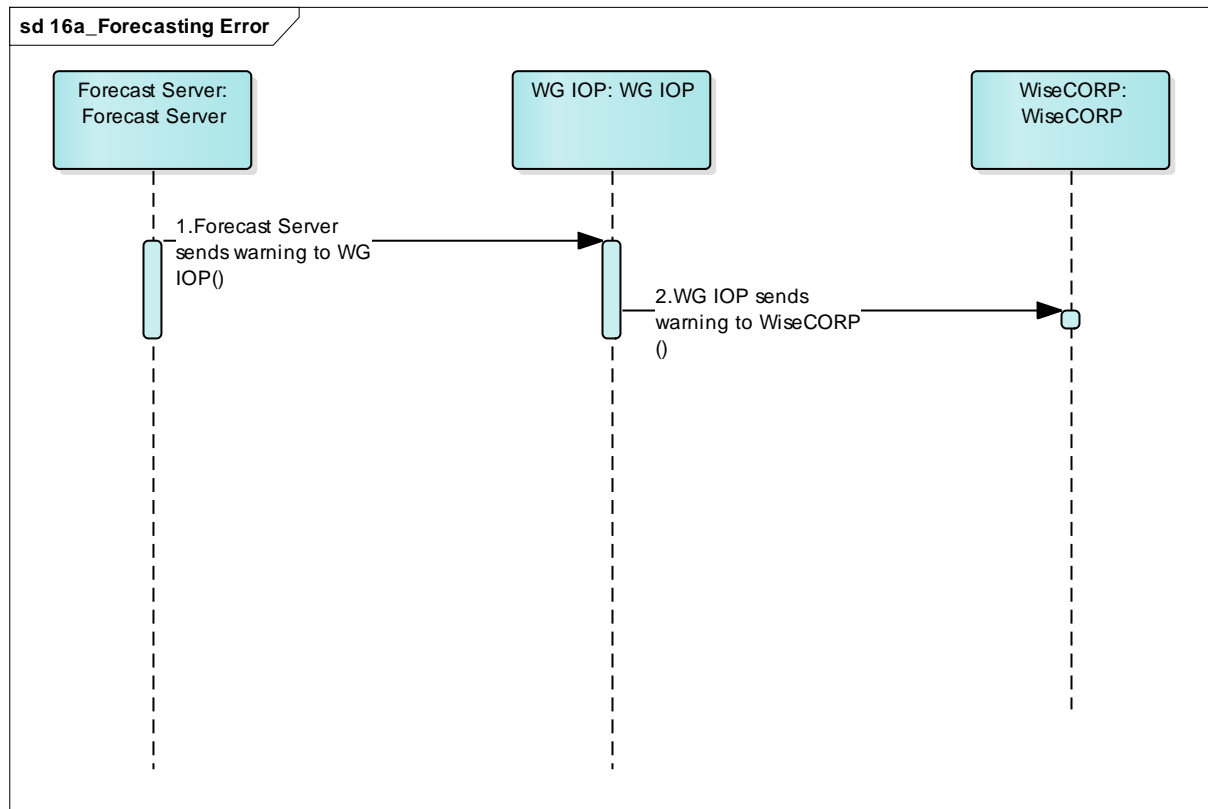
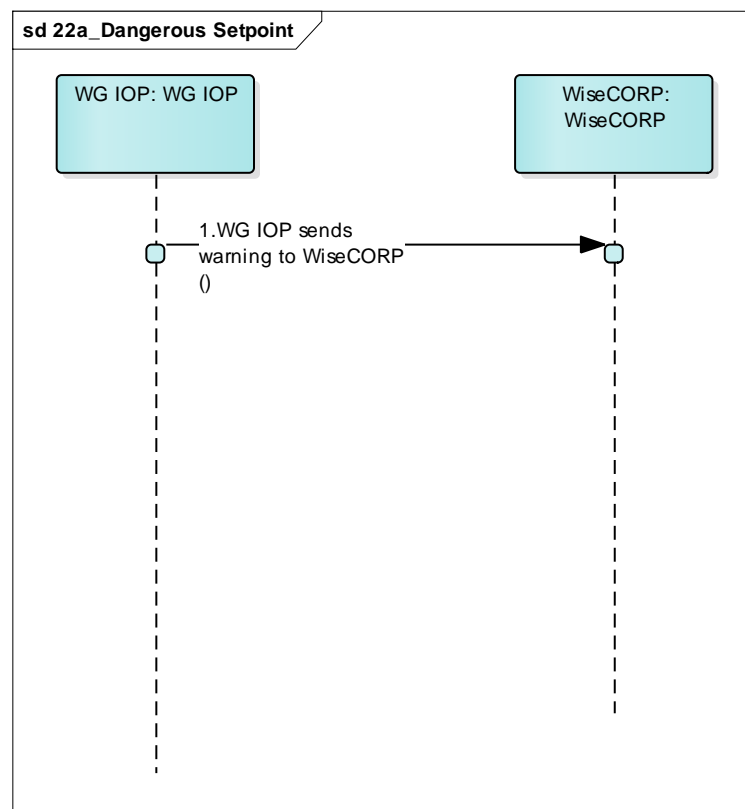


Figure 242 - Basic path sequence diagram for HL-UC 5 PUC 2



**Figure 243 - Forecasting error exception path sequence diagram for HL-UC 5 PUC 2**



**Figure 244 - Dangerous setpoint exception path sequence diagram for HL-UC 5 PUC 2**



## **22.3 HL-UC 5\_PUC 3: COMFORT-BASED DEMAND FLEXIBILITY MODELS**

### **22.3.1 PRIMARY USE CASE DESCRIPTION**

This PUC is responsible for the development of models of buildings/households and the associated usage patterns, that have an impact on energy demand. A model of thermal behavior will be created, through advanced algorithms using as much information as possible. Apart from this, thermal flexibility and the amount of thermal energy that can be shifted must be estimated. Inputs from HL-UC 5\_SUC\_2.3 are to be included.

### 22.3.2 SECONDARY USE CASE INTERACTIONS

The Secondary Use Cases associated with this Primary Use Case and their associations are listed below.

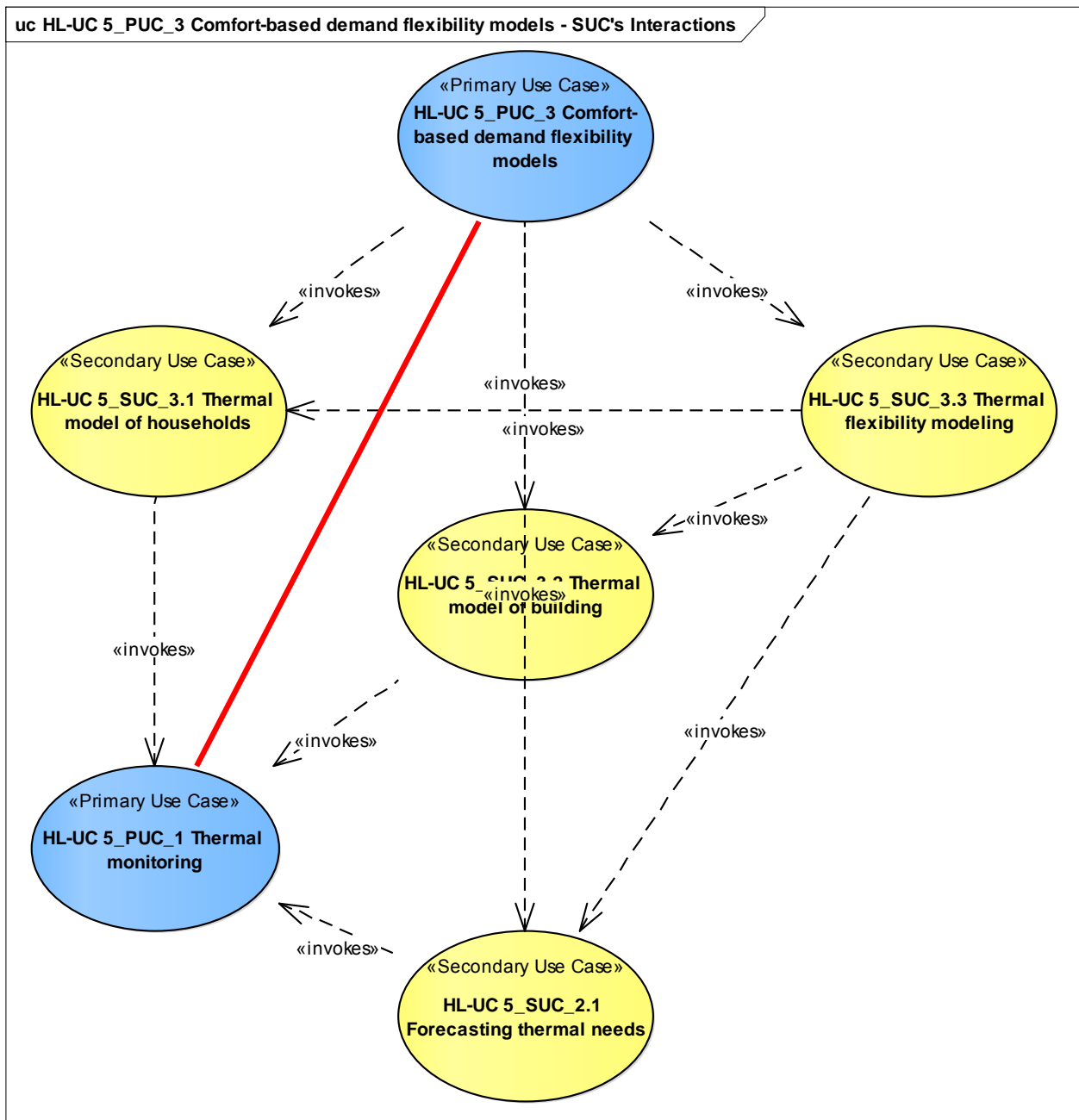


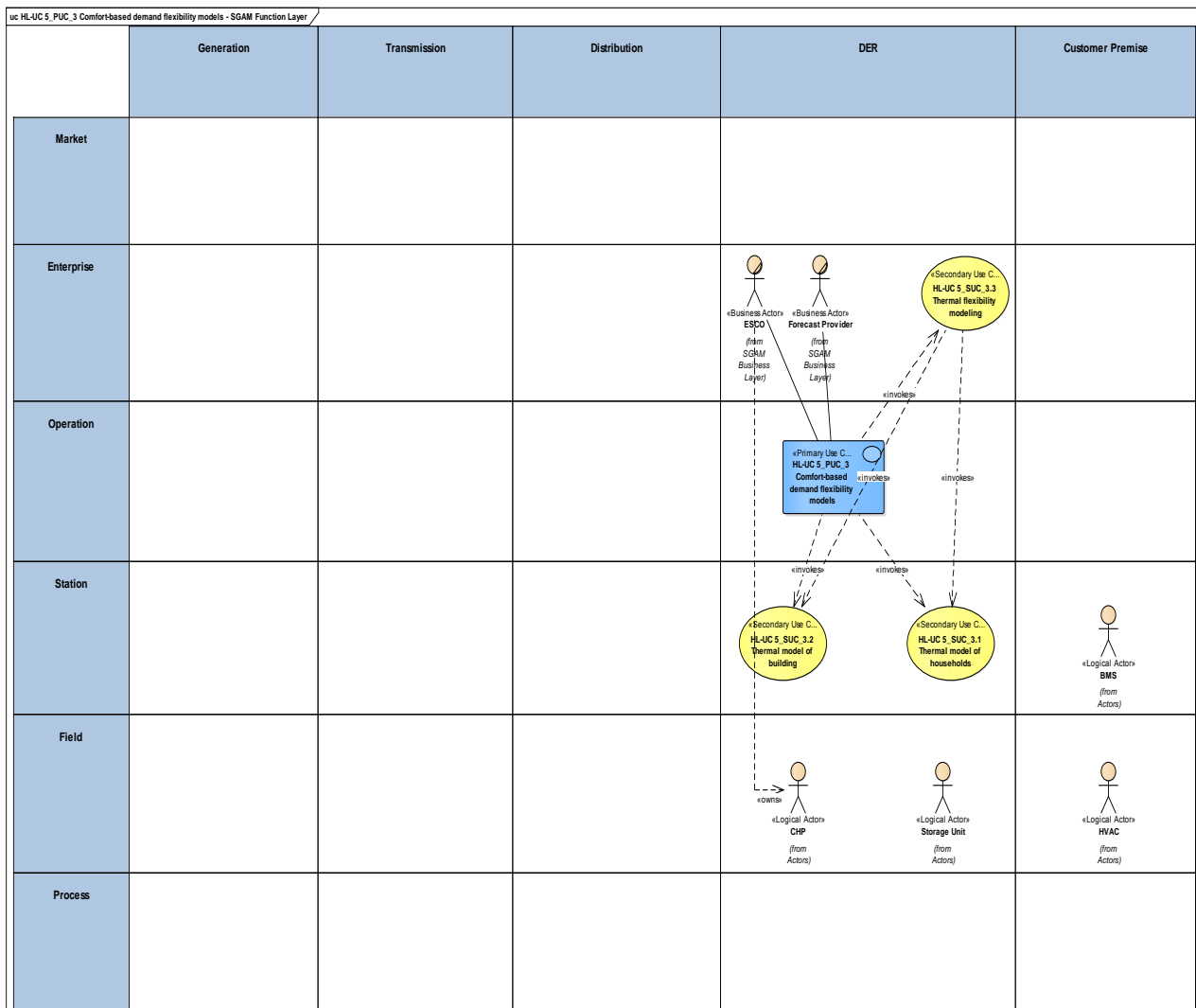
Figure 245 - SUCs Interactions Diagram

**Table 194 - Table of list of participating SUCs**

SUC Name	Description	Relation	PUC/SUC
Thermal model of households	This SUC provides the thermal models of households	Invokes	HL-UC 5_PUC_1
Thermal model of building	SUC provides the thermal model of households	Invokes	HL-UC 5_SUC_2.1
Thermal flexibility modelling	SUC responsible for calculating the availability for thermal flexibility	Invokes	HL-UC 5_SUC_2.1

### 22.3.3 SGAM FUNCTION LAYER

The SGAM function layer for this Primary Use Case is illustrated below.



**Figure 246 - SGAM Function Layer**

Table 195 - List of Actors Involved

Actor Name	Actor Type
Gas Meter	Device
BMS	System
ESCO	Organization
Gas Distribution Company	Organization
Sensor	Device
Consumer	Logical actor

### 22.3.4 SGAM COMPONENT LAYER

The SGAM component layer for this Primary Use Case is depicted below.

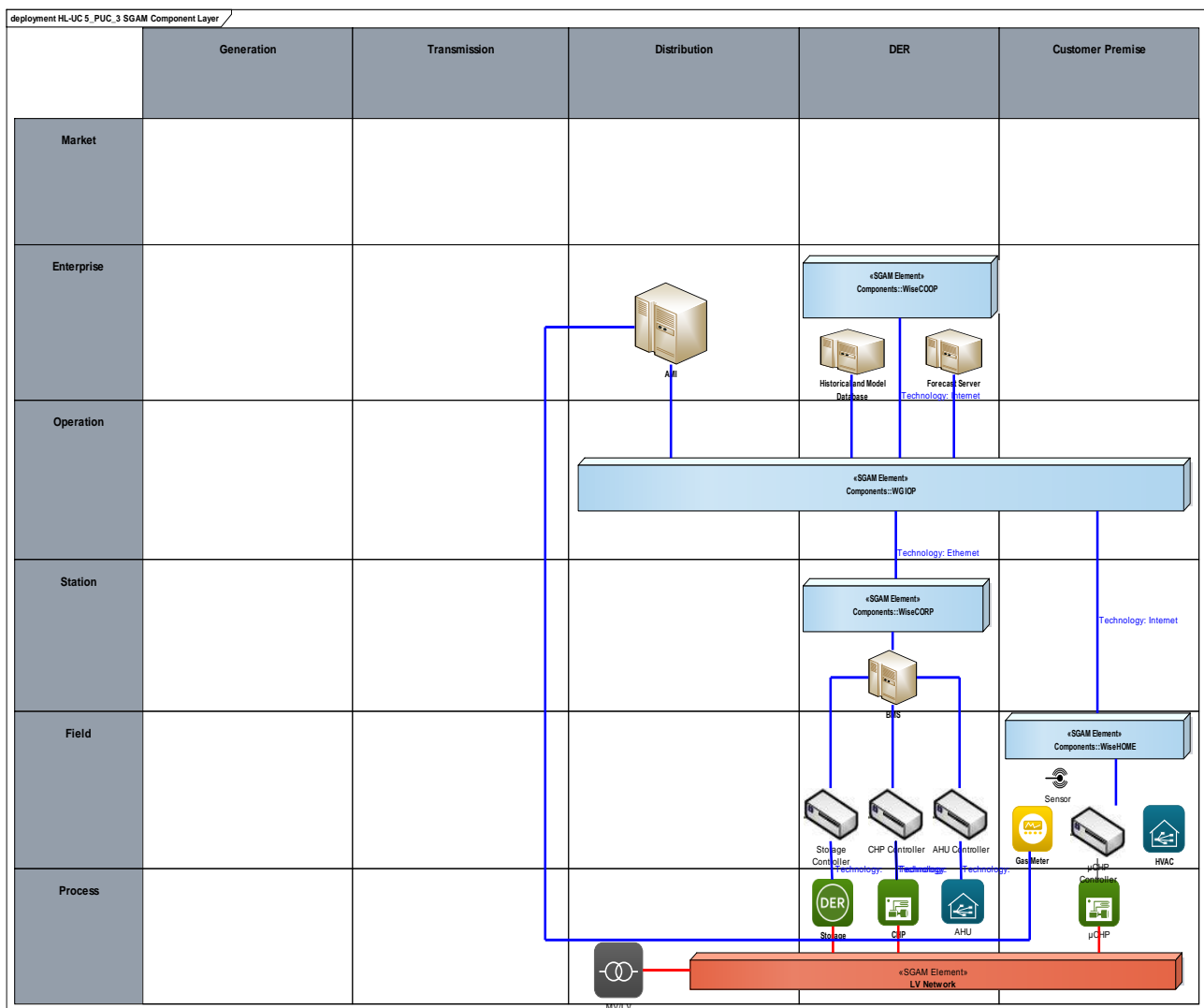


Figure 247 - SGAM Component Layer

Table 196 - List of Components Participating in the Primary Use Case

Component	Component Type
WiseCOOP	SGAM Element
WiseIOP	SGAM Element
WiseCORP	SGAM Element
WiseHOME	SGAM Element

### 22.3.5 SGAM COMMUNICATION LAYER

This section outlines the main communication technologies that will be utilised in the reference implementation of the WiseGRID project.

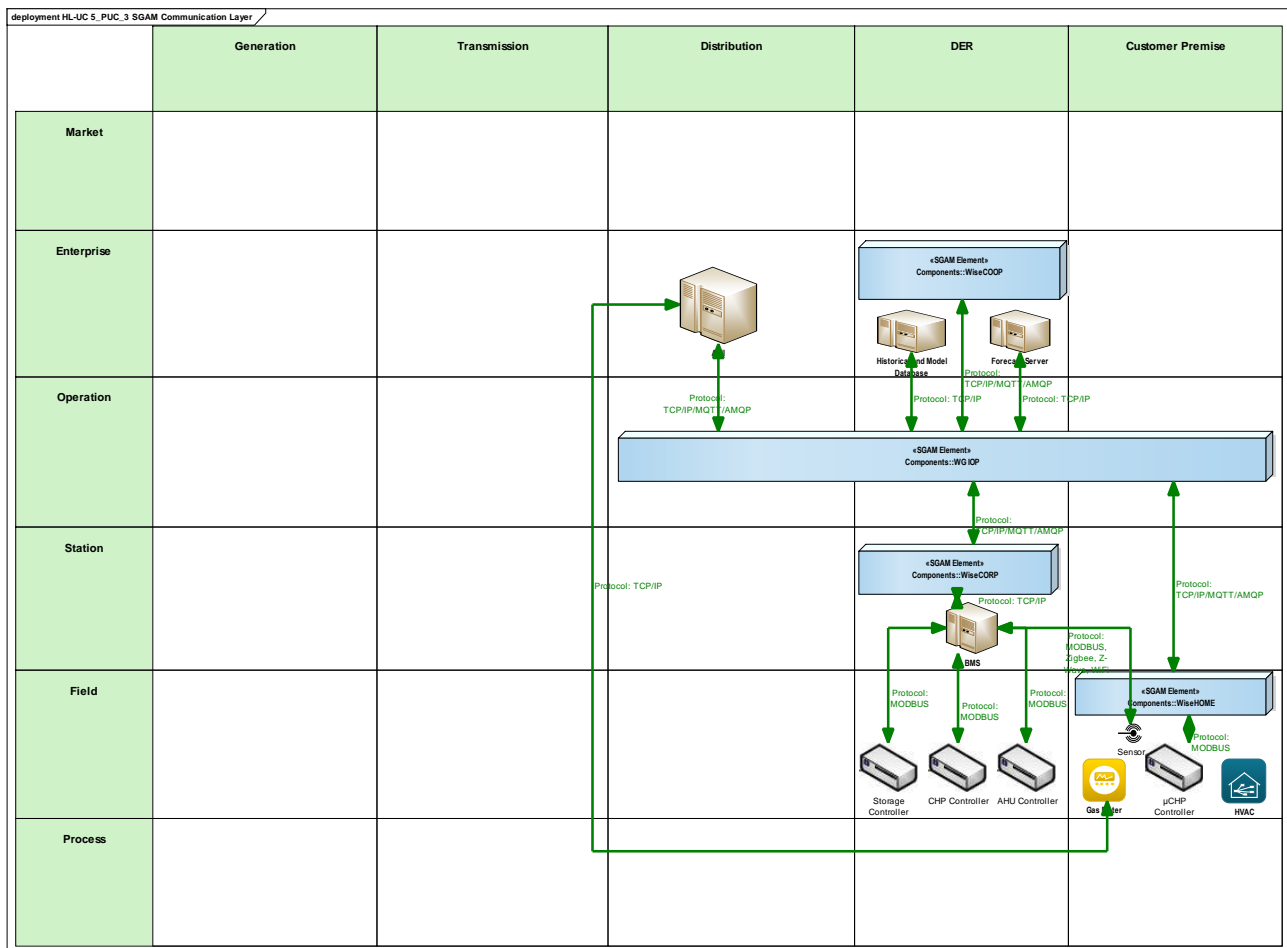


Figure 248 - SGAM Communication Layer

**Table 197 - List of Communication Technologies Involved**

Communication Technology	Description
TCP/IP	Group of protocols enabling communication between devices in a network up to the transport layer
AMQP	The Advanced Message Queuing Protocol (AMQP) is an open standard application layer protocol for message-oriented middleware. It is a binary, application layer protocol, designed to efficiently support a wide variety of messaging applications and communication patterns.
MQTT	ISO standard (ISO/IEC PRF 20922) publish-subscribe-based lightweight messaging protocol for use on top of the TCP/IP protocol
MODBUS	Serial communications protocol originally published for use with programmable logic controllers (PLCs). Simple and robust, it has become a de facto standard communication protocol and is now a commonly available means of connecting industrial electronic devices
ZigBee	It is a wireless communication protocol used to create personal area networks with small, low-power digital radios, such as for home automation. Usually it aims to be simpler and less expensive than other wireless personal area networks, such as Bluetooth or Wi-Fi.
Z-Wave	It is a wireless communications protocol used primarily for home automation. It is a mesh network using low-energy radio waves to communicate from appliance to appliance.
Wi-Fi	It is a wireless communication protocol for local area networking. It is based on the IEEE 802.11 standards.

### 22.3.6 SGAM INFORMATION LAYER

The SGAM information layer for this Primary Use Case is illustrated below.

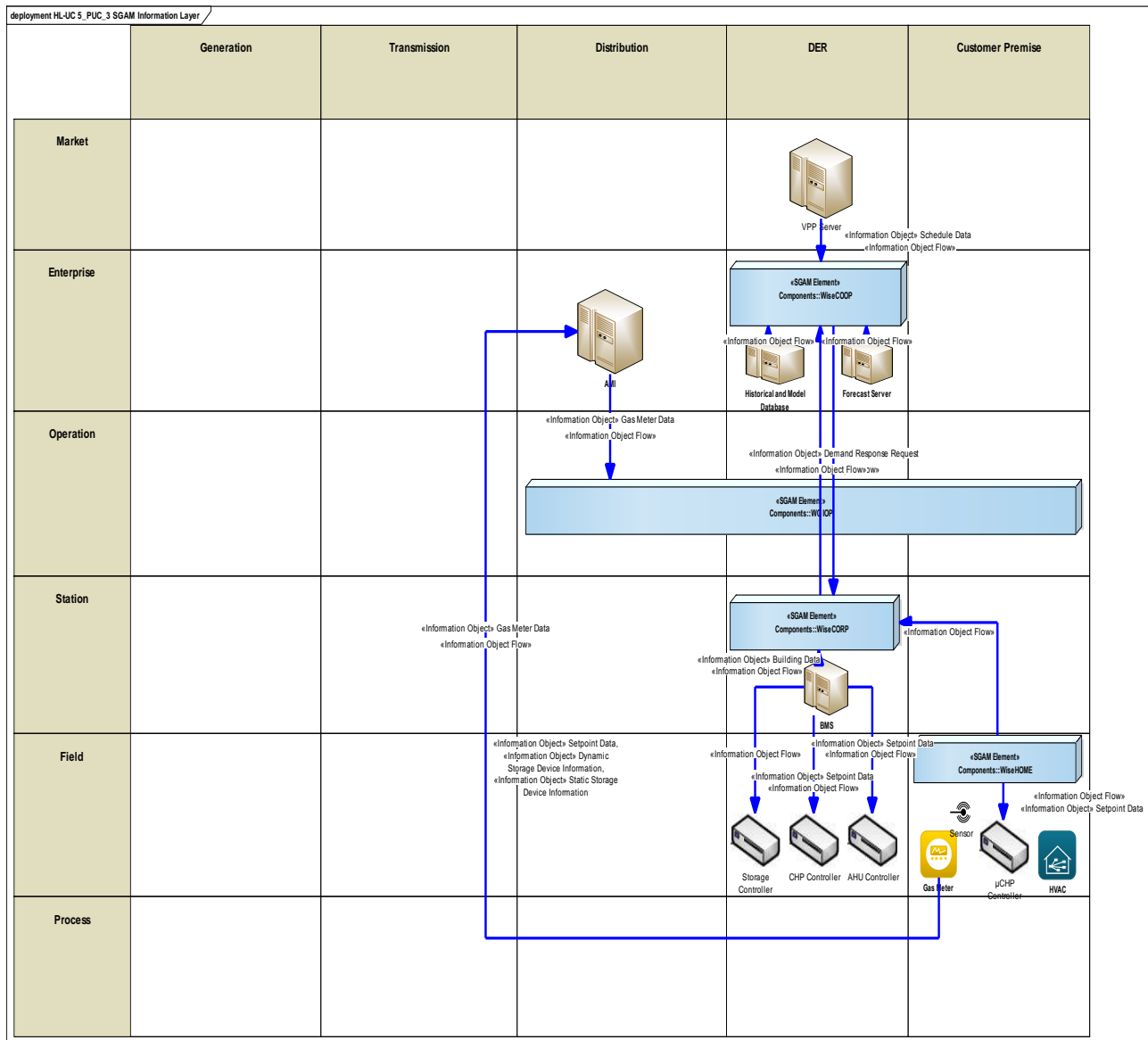


Figure 249 - SGAM Information Layer

## Canonical data models

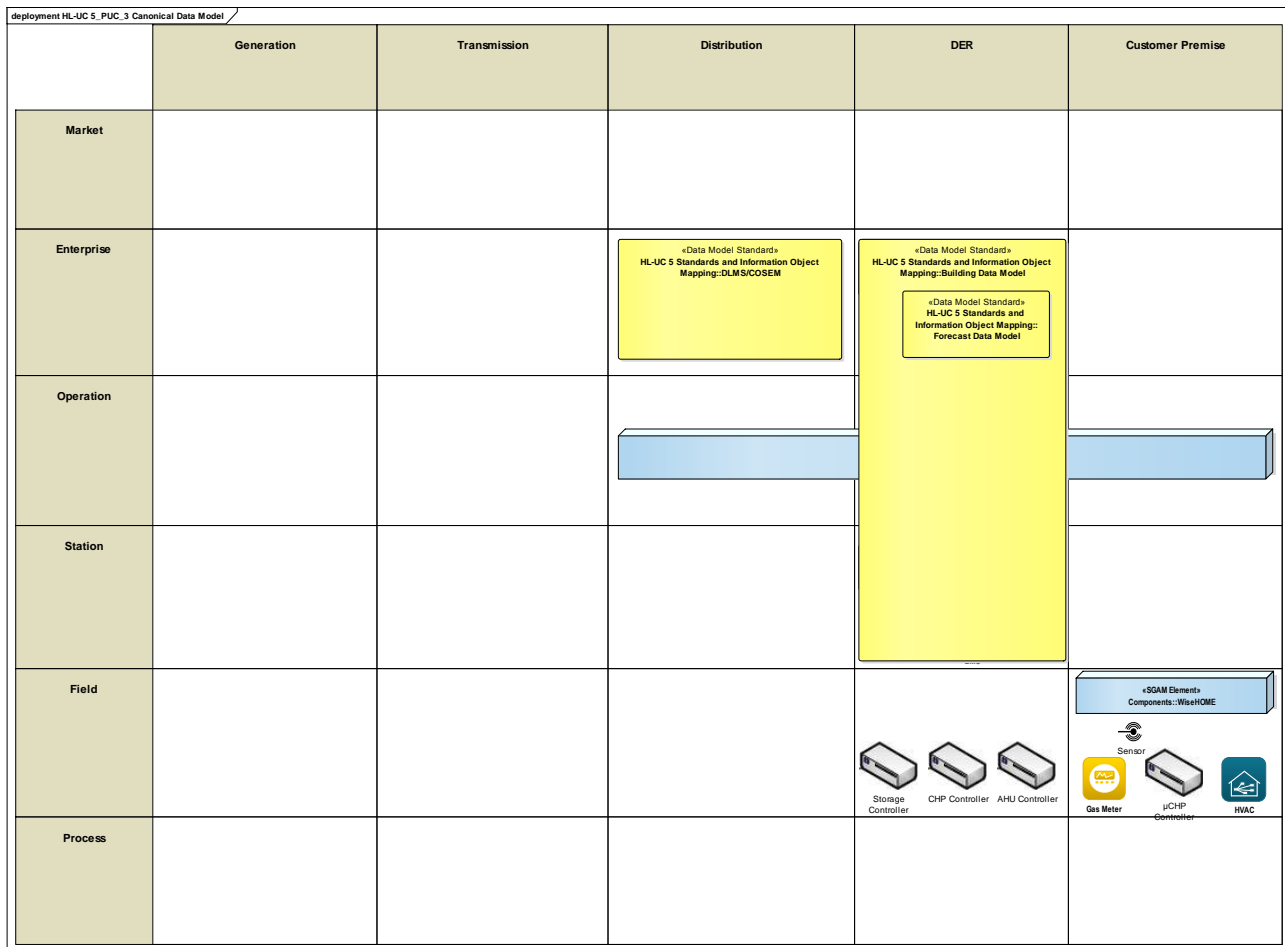


Figure 250 - Canonical Data Model diagram

Table 198 - List of Data Models

Data Models
DLMS/COSEM
Building Data Model
Forecast Data Model



## STANDARDS AND INFORMATION OBJECT MAPPING

This secondary use case will leverage the following standards in order to align its outputs with ongoing activities by other parties so as to ensure replicability of the WiseGRID solution.

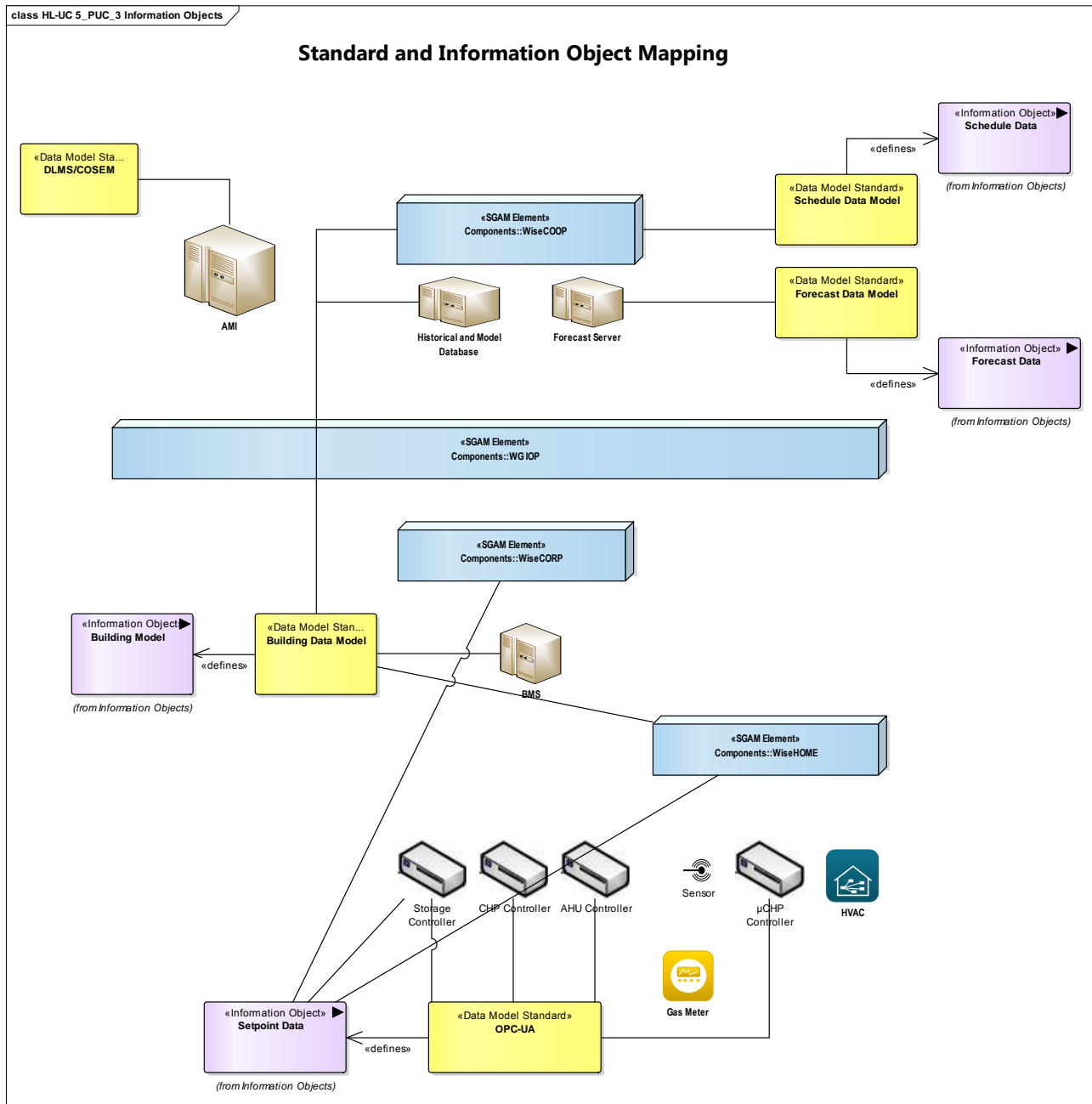


Figure 251 - Standard and Information Object Mapping diagram

Table 199 - List of Data Standards

Data Standards
DLMS/COSEM
Schedule Data Model
Forecast Data Model
Building Data Model
OPC-UA

Table 200 - List of Information Objects

Information Objects	Data Model
Schedule Data	Schedule Data Model
Forecast Data	Forecast Data Model
Building Model	Building Data Model
Setpoint Data	OPC-UA

### 22.3.7 ACTIVITY DIAGRAM

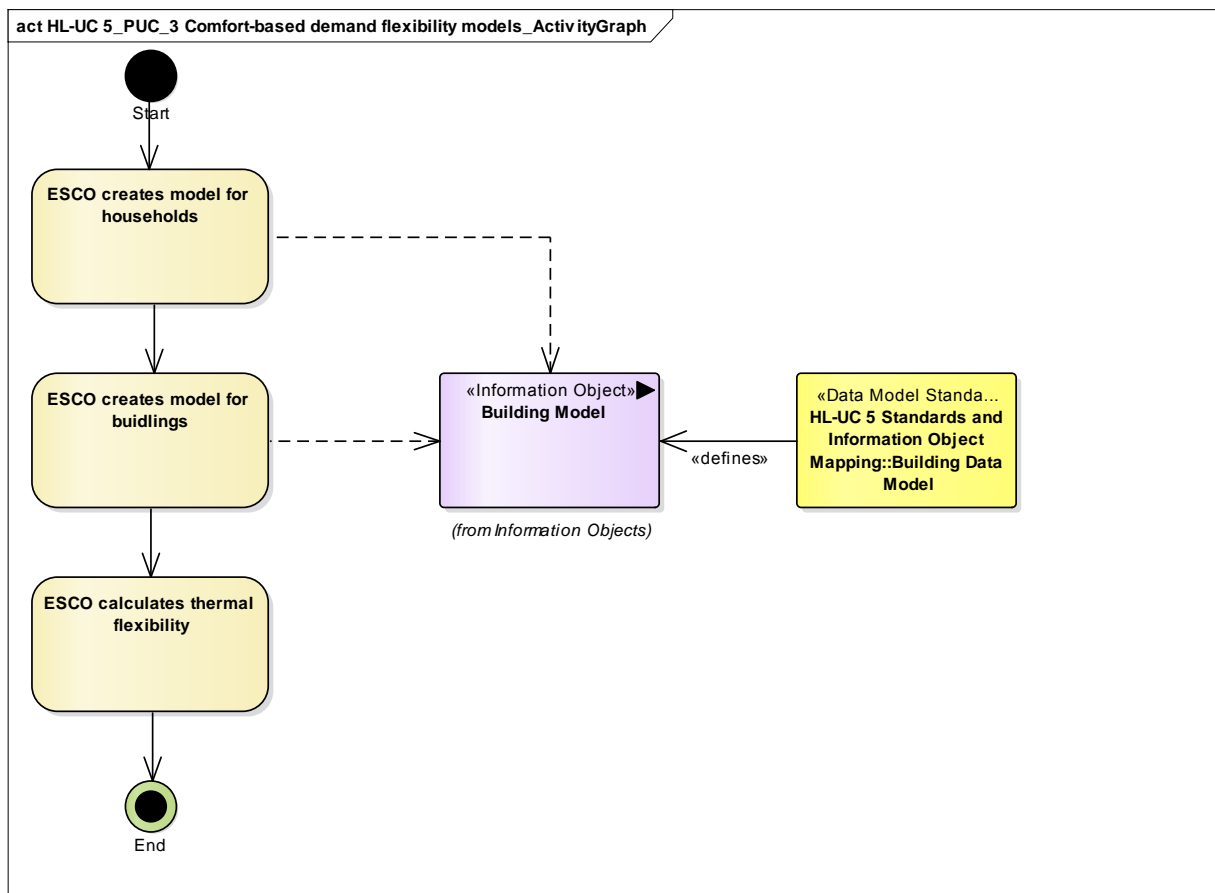


Figure 252 - Primary Use Case Activity Diagram

## 22.3.8 SEQUENCE DIAGRAM

The sequence diagram associated with this Primary Use Case is illustrated below.

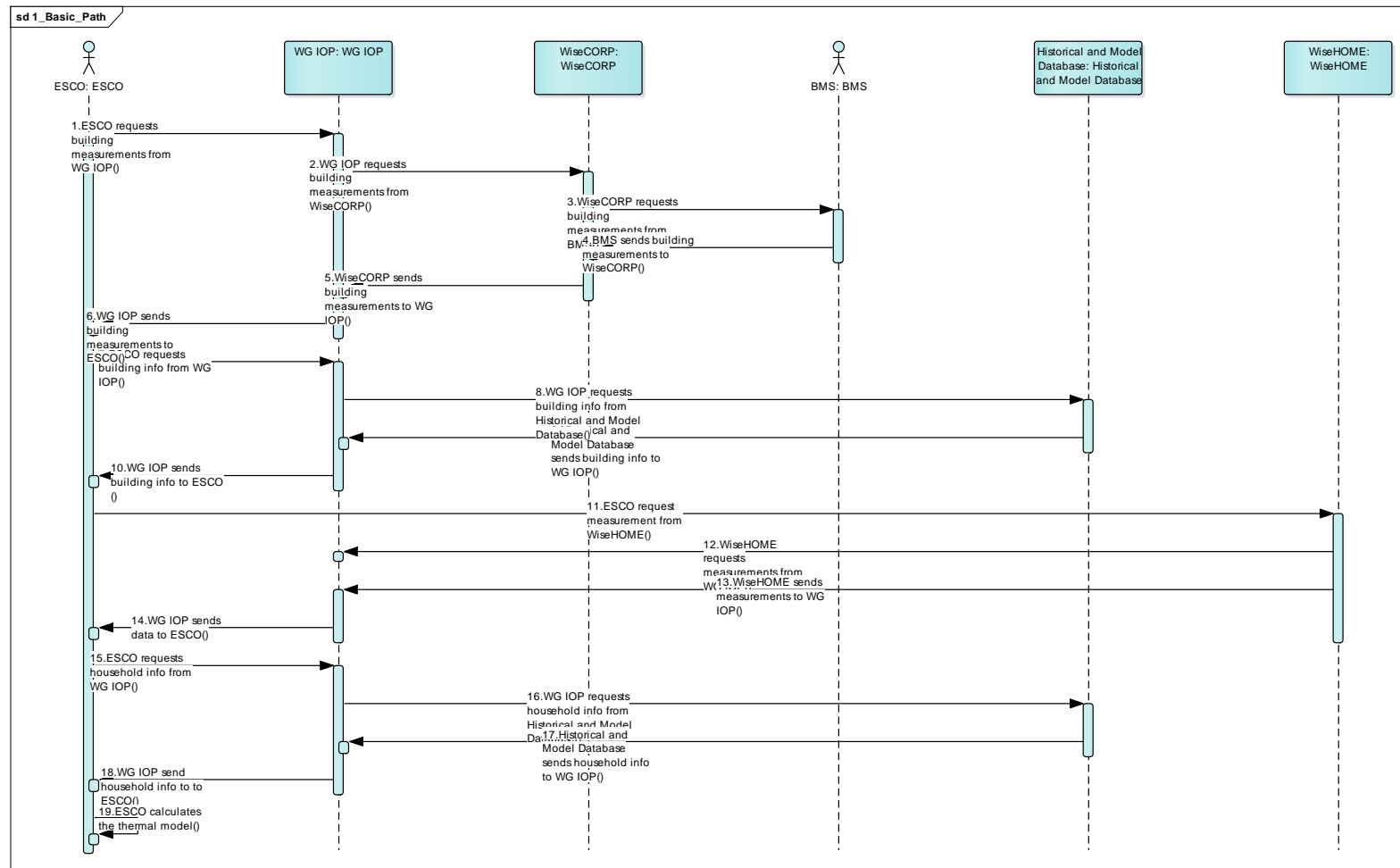


Figure 253 - Basic path sequence diagram for HL-UC 5 PUC 3

## **22.4 HL-UC 5\_PUC\_4: COGENERATION AND HVAC OPTIMISATION**

### **22.4.1 PRIMARY USE CASE DESCRIPTION**

In this PUC, the market and business aspects of CHP, HVAC and building management are examined. Firstly, the role of each asset and its participation in the VPP or provision of Ancillary Services to the distribution network is defined. The final business decisions are made by an optimization algorithm, while two different algorithms optimize the participation of the assets in VPP and the Ancillary Services. As a result, the optimal bids are identified and a set of schedules is produced.

## 22.4.2 SECONDARY USE CASE INTERACTIONS

The Secondary Use Cases associated with this Primary Use Case and their relations are illustrated in the following diagram.

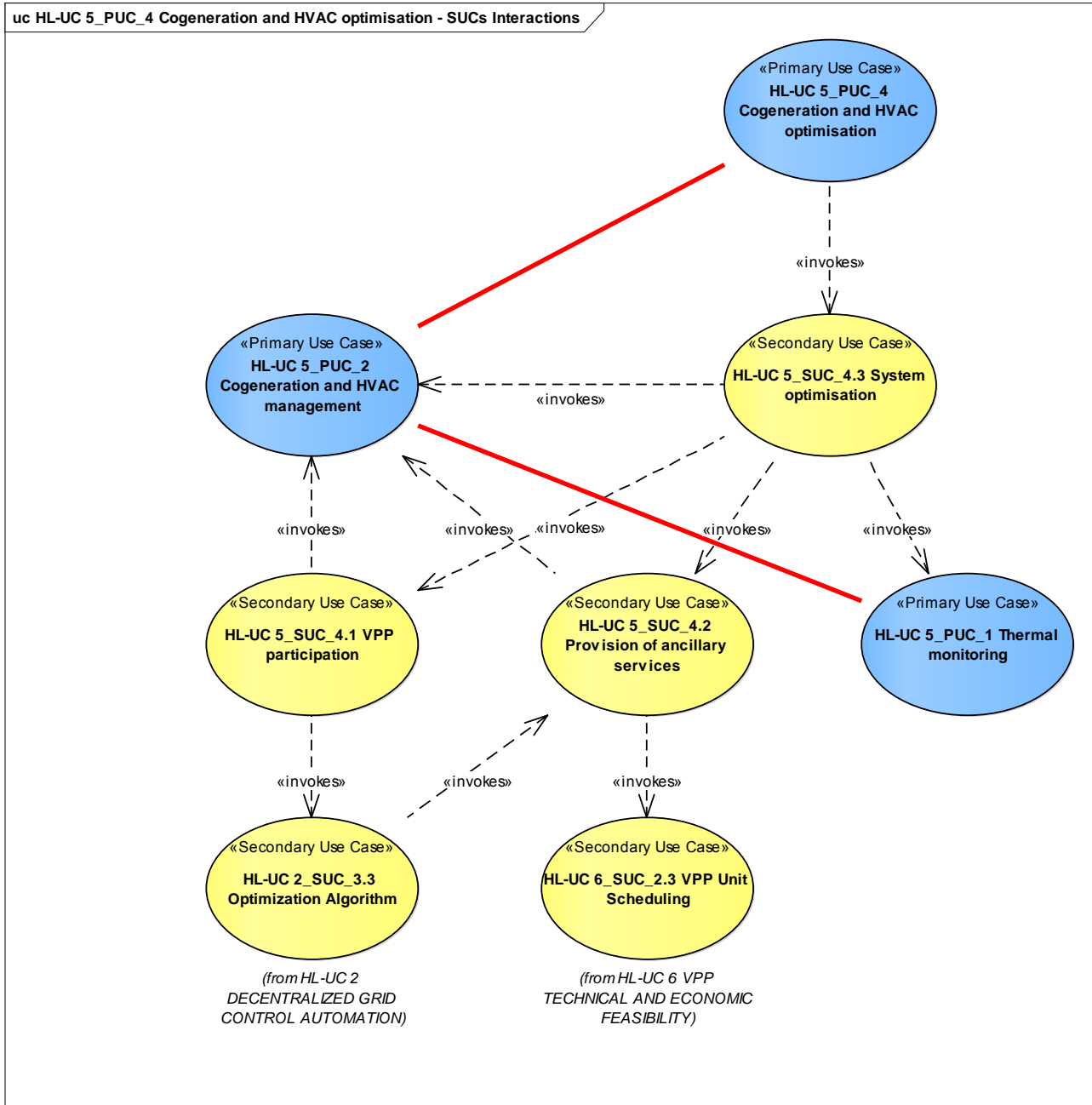


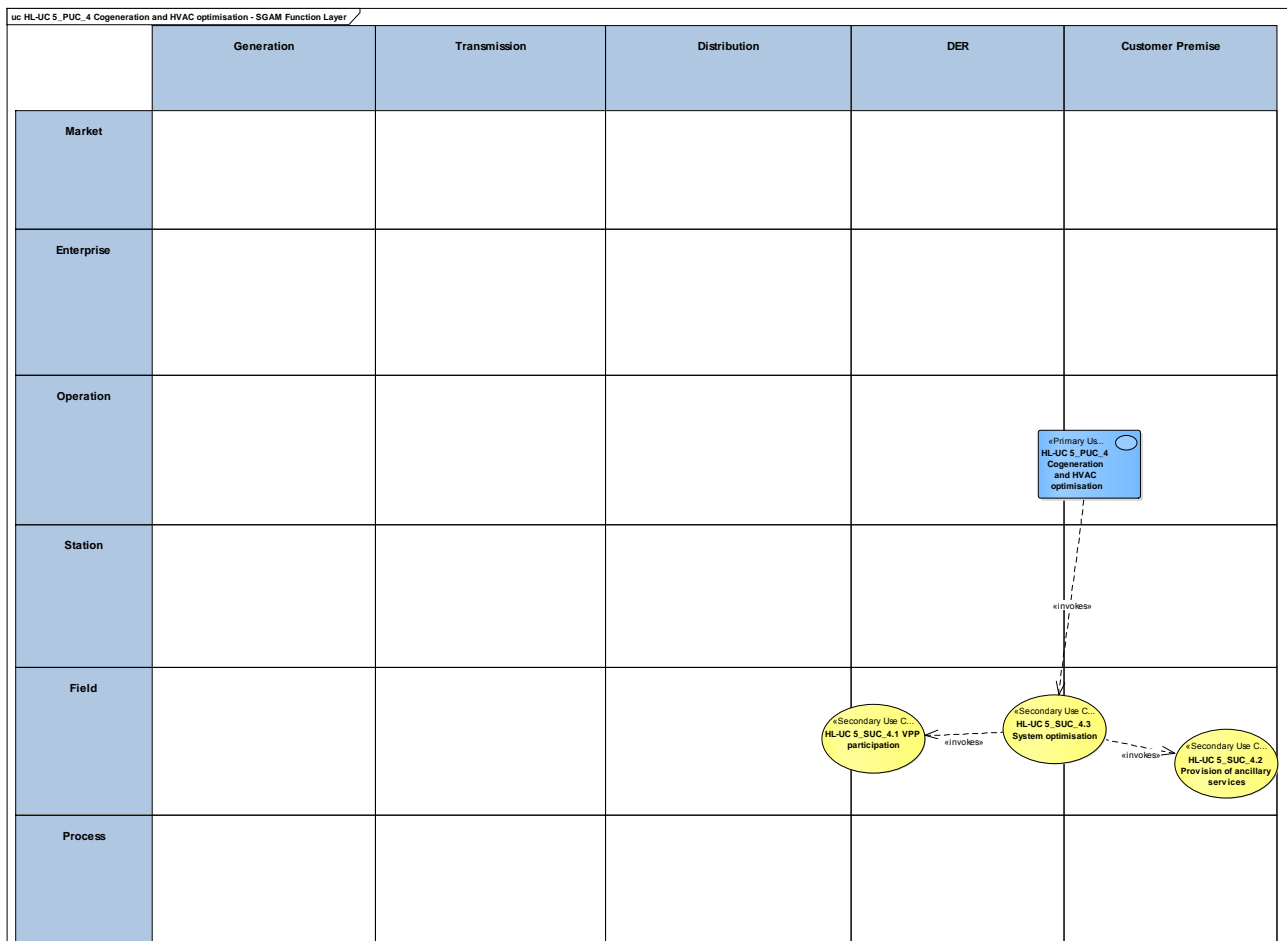
Figure 254 - SUCs Interactions Diagram

**Table 201 - Table of list of participating SUCs**

SUC Name	Description	Relation	PUC/SUC
VPP participation	SUC will provide the assets to be committed for the participation in the VPP.	Invokes	HL-UC 2_SUC_3.3
Provision of ancillary services	SUC will calculate the optimal schedule of actions for assets providing ancillary services to the DSO.	Invokes	HL-UC 5_PUC_2 HL-UC _SUC_2.3
System optimisation	SUC aims at defining the optimal participation of assets managed by this PUC, in the other 2 SUCs	Invokes	HL-UC 5_PUC_1 HL-UC 5_PUC_2

### 22.4.3 SGAM FUNCTION LAYER

The SGAM function layer for this Primary Use Case is depicted below.



**Figure 255 - SGAM Function Layer**

Table 202 - List of Actors Involved

Actor Name	Actor Type
BMS	System
ESCO	Organization
DSO	Organization
VPP Operator	Organization
Sensor	Device
Consumer	Logical actor

#### 22.4.4 SGAM COMPONENT LAYER

The SGAM component layer for this Primary Use Case is depicted below.

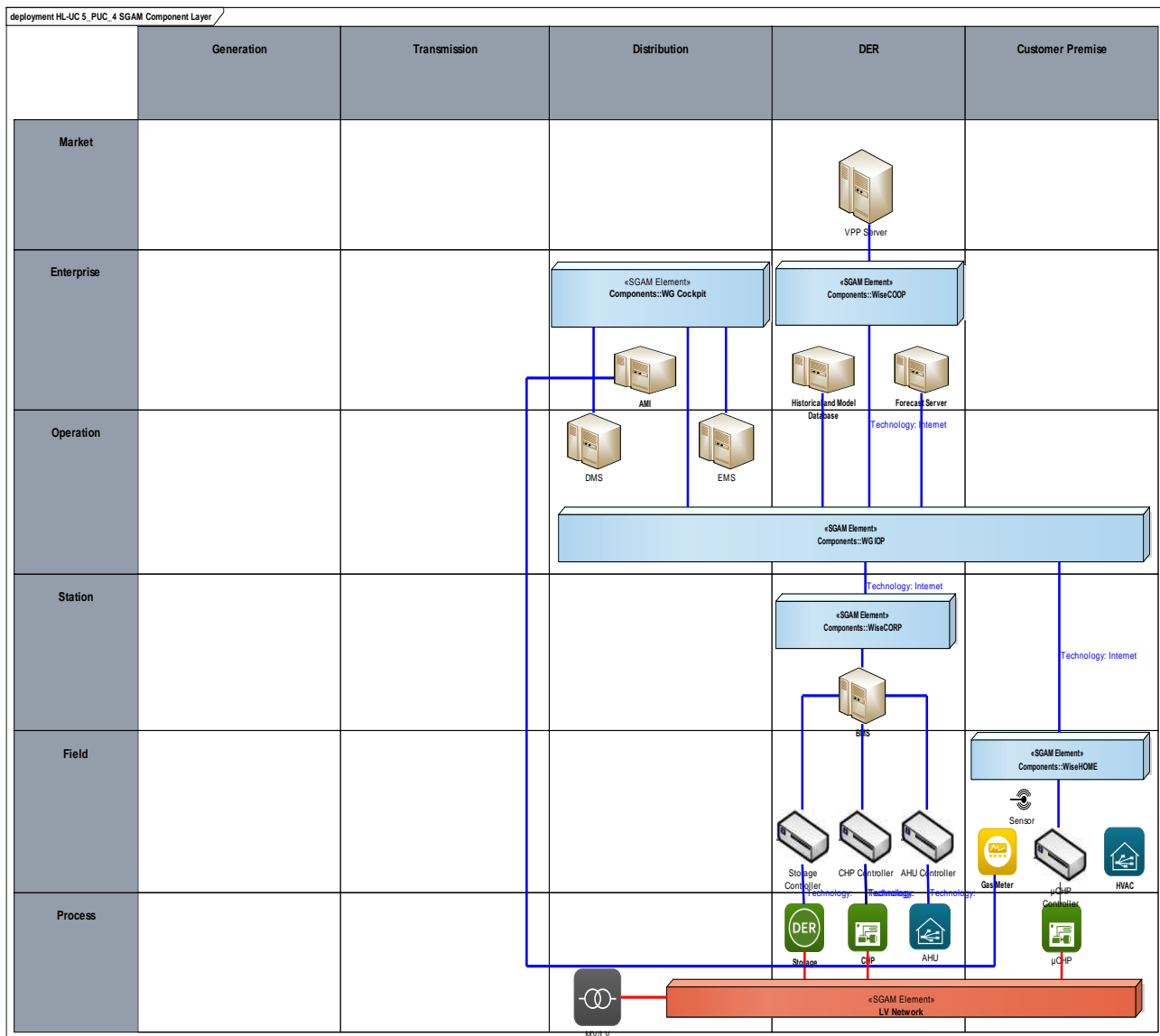


Figure 256 - SGAM Component Layer

Table 203 - List of Components Participating in the Primary Use Case

Component	Component Type
WG Cockpit	SGAM Element
WiseCOOP	SGAM Element
WiseIOP	SGAM Element
WiseCORP	SGAM Element
WiseHOME	SGAM Element



## 22.4.5 SGAM COMMUNICATION LAYER

The SGAM communication layer for this Primary Use Case is depicted below.

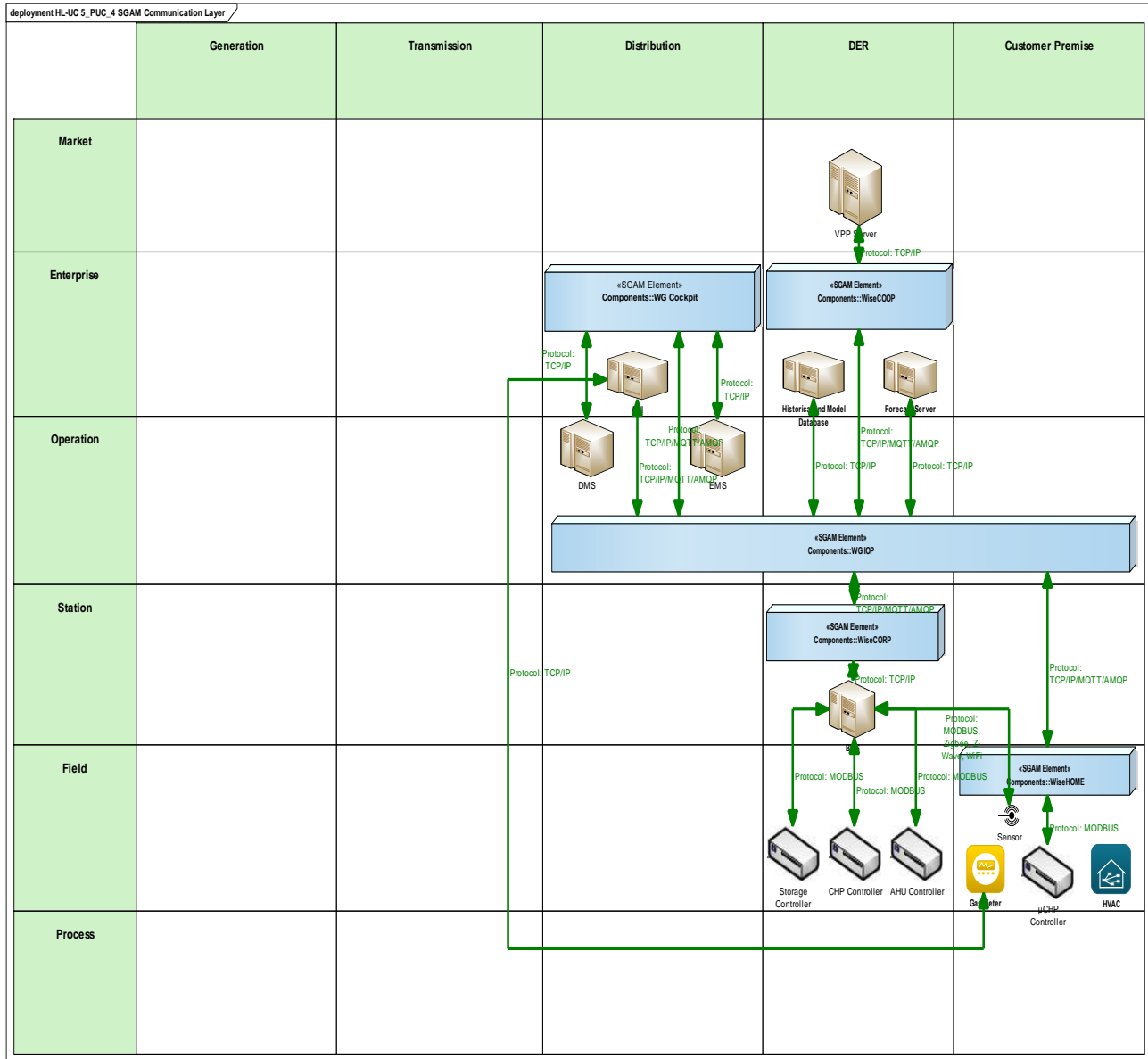


Figure 257 - SGAM Communication Layer

**Table 204 - List of Communication Technologies Involved**

Communication Technology	Description
TCP/IP	Group of protocols enabling communication between devices in a network up to the transport layer
AMQP	The Advanced Message Queuing Protocol (AMQP) is an open standard application layer protocol for message-oriented middleware. It is a binary, application layer protocol, designed to efficiently support a wide variety of messaging applications and communication patterns.
MQTT	ISO standard (ISO/IEC PRF 20922) publish-subscribe-based lightweight messaging protocol for use on top of the TCP/IP protocol
MODBUS	Serial communications protocol originally published for use with programmable logic controllers (PLCs). Simple and robust, it has become a de facto standard communication protocol and is now a commonly available means of connecting industrial electronic devices
ZigBee	It is a wireless communication protocol used to create personal area networks with small, low-power digital radios, such as for home automation. Usually it aims to be simpler and less expensive than other wireless personal area networks, such as Bluetooth or Wi-Fi.
Z-Wave	It is a wireless communications protocol used primarily for home automation. It is a mesh network using low-energy radio waves to communicate from appliance to appliance.
Wi-Fi	It is a wireless communication protocol for local area networking. It is based on the IEEE 802.11 standards.

## 22.4.6 SGAM INFORMATION LAYER

The SGAM information layer for this Primary Use Case is depicted below.

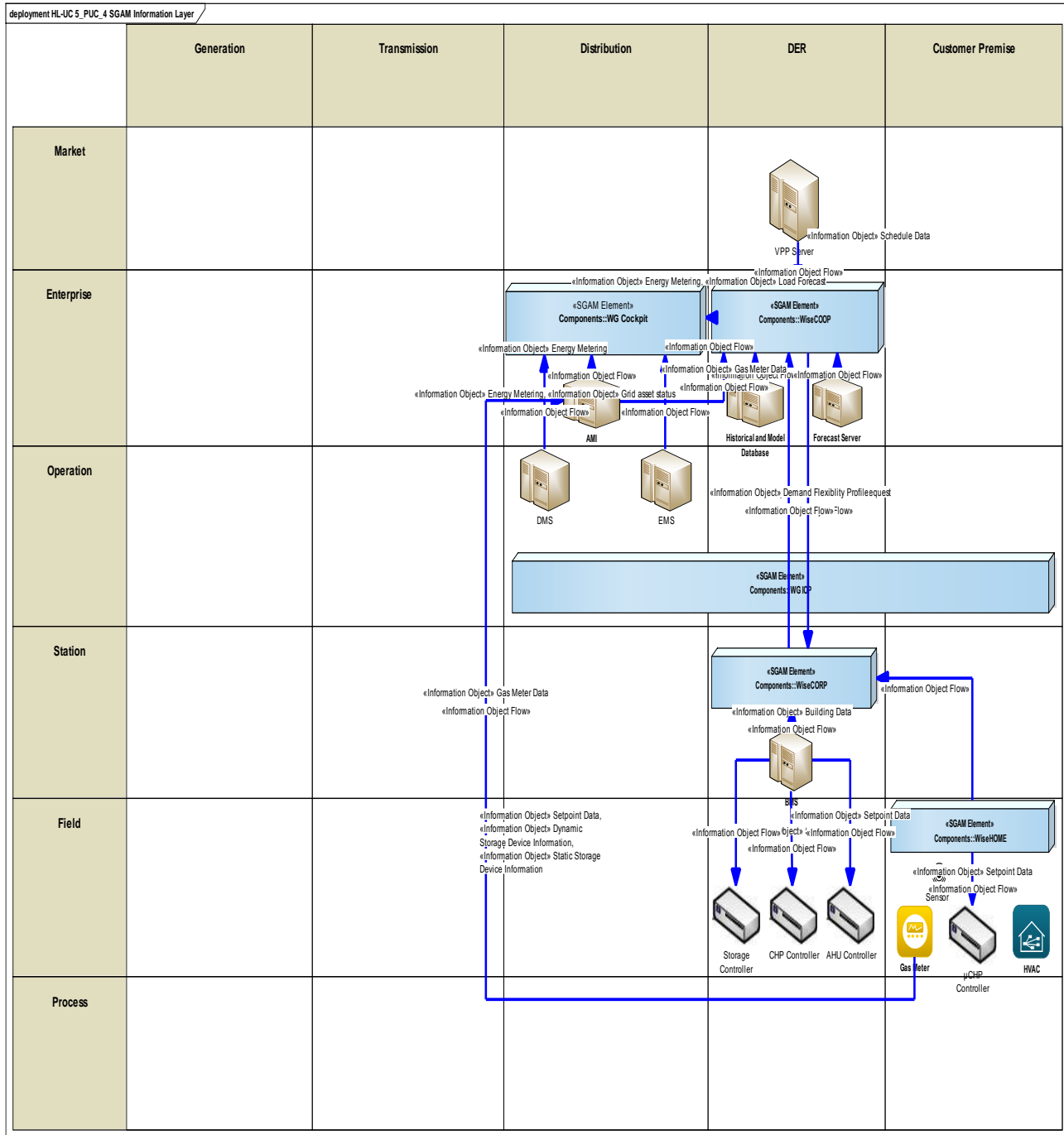


Figure 258 - SGAM Information Layer

## Canonical Data Models

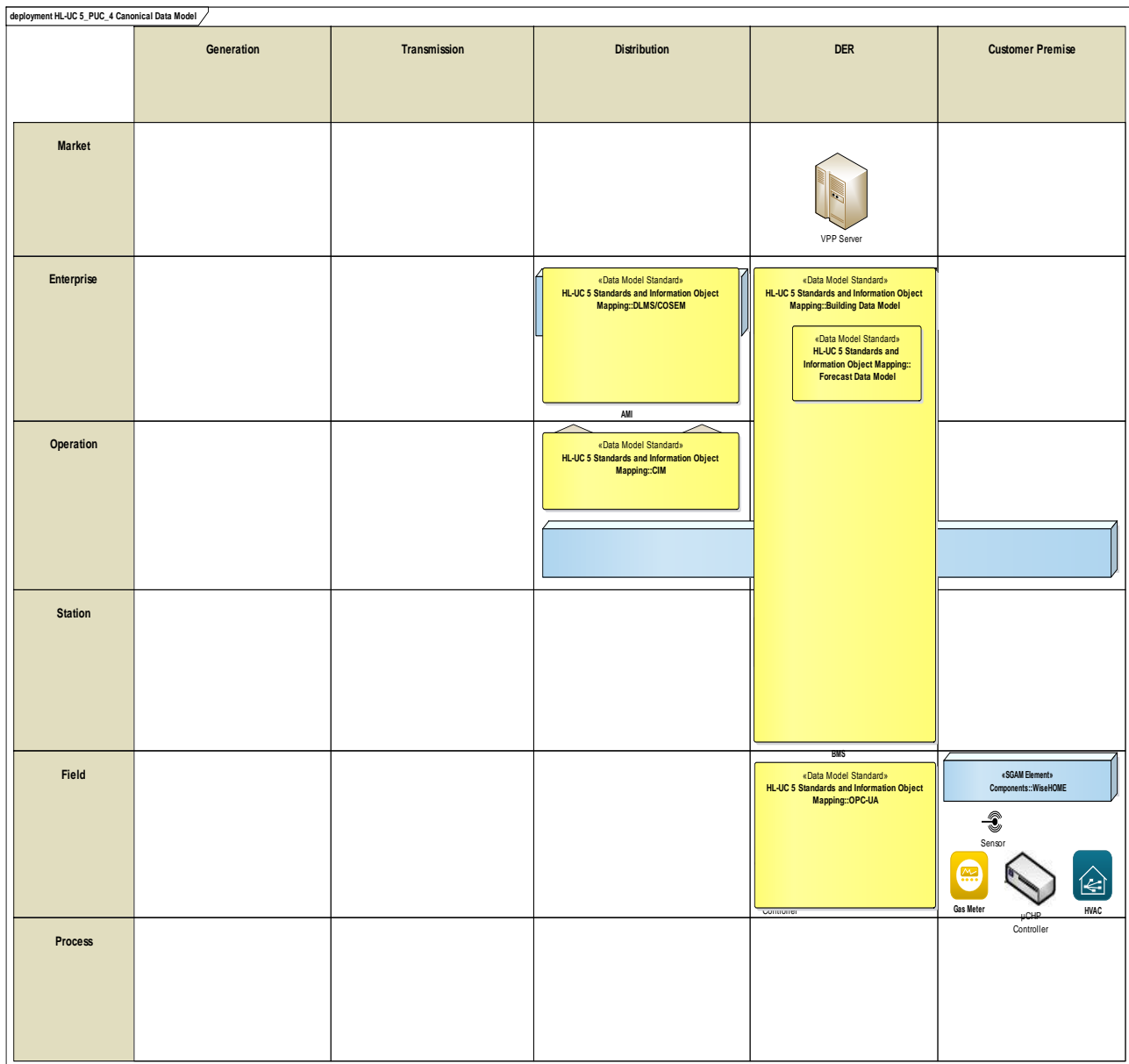


Figure 259 - Canonical Data Model diagram

Table 205 - List of Data Models

Data Models
DLMS/COSEM
CIM
Building Data Model
Building Forecast Model
OPC-UA

## STANDARDS AND INFORMATION OBJECT MAPPING

The standards and information object mappings associated with this Primary Use Case is depicted below.

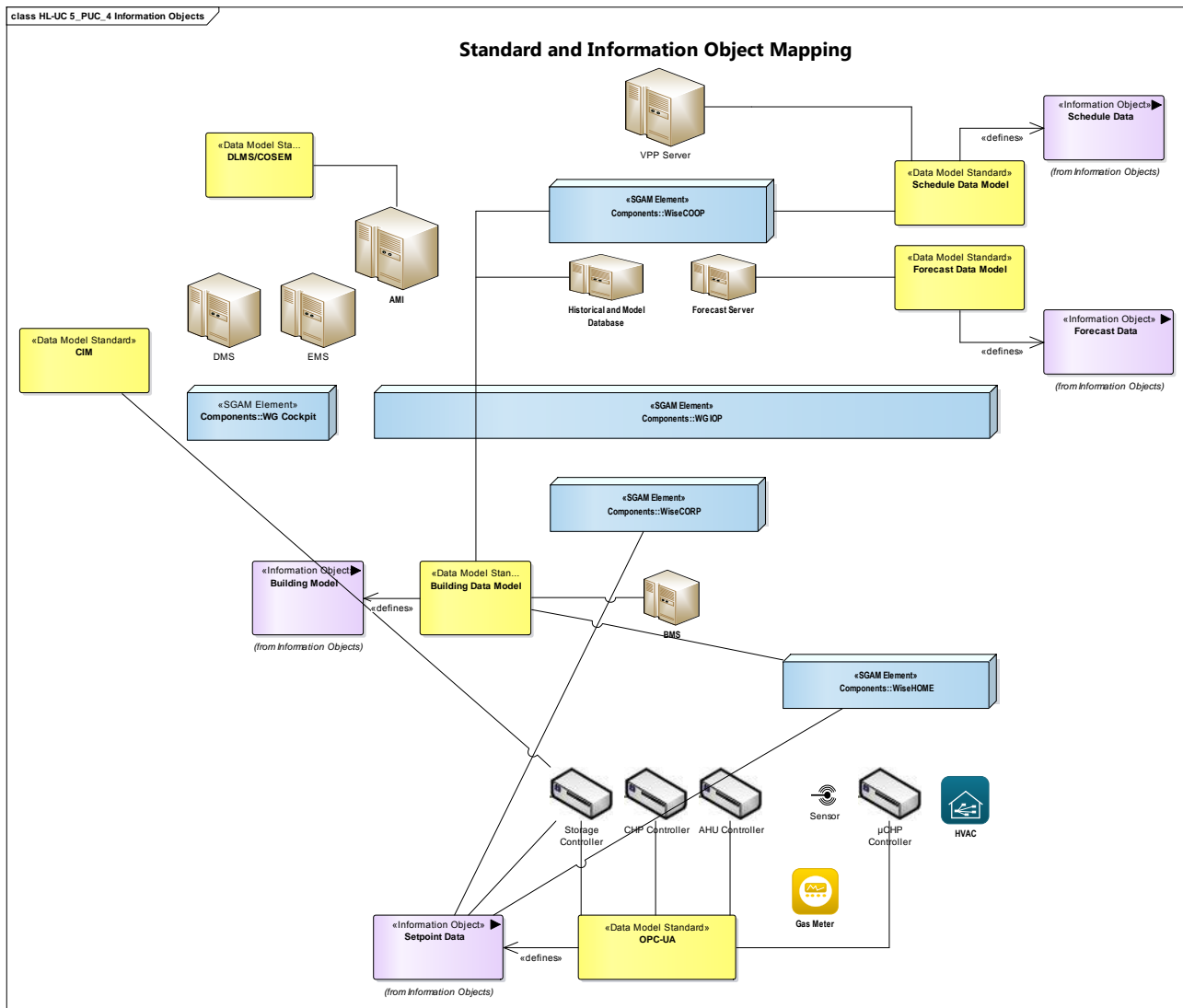


Figure 260 - Standard and Information Object Mapping diagram

**Table 206 - List of Data Standards**

<b>Data Standards</b>
DLMS/COSEM
Schedule Data Model
Forecast Data Model
CIM
Building Data Model
OPC-UA

**Table 207: List of Information Objects**

<b>Information Objects</b>	<b>Data Model</b>
Schedule Data	Schedule Data Model
Forecast Data	Forecast Data Model
Building Model	Building Data Model
Setpoint Data	OPC-UA

## 22.4.7 ACTIVITY DIAGRAM

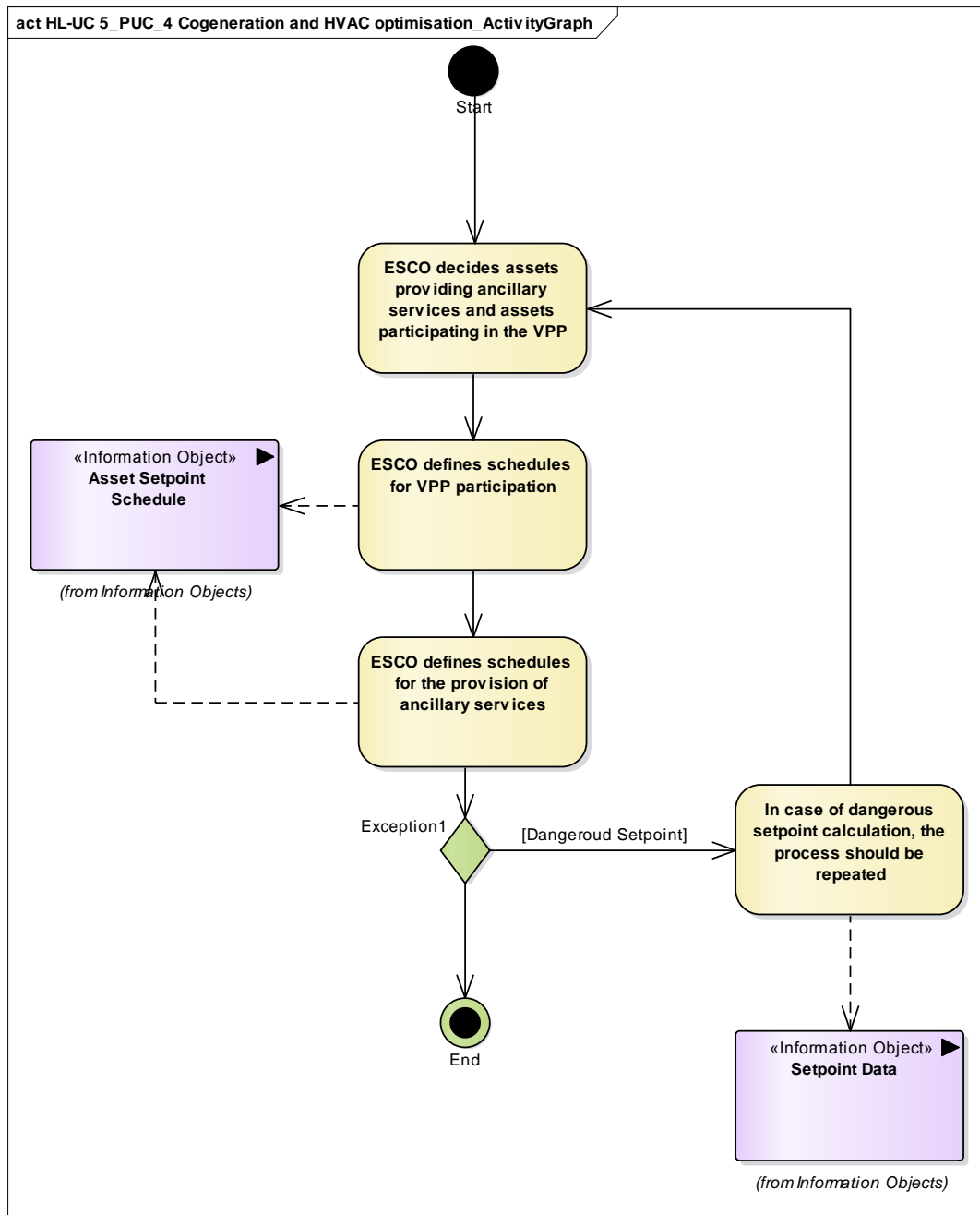


Figure 261 - Primary Use Case Activity Diagram



## 22.4.8 SEQUENCE DIAGRAM

The sequence diagram associated with this Primary Use Case is illustrated below.

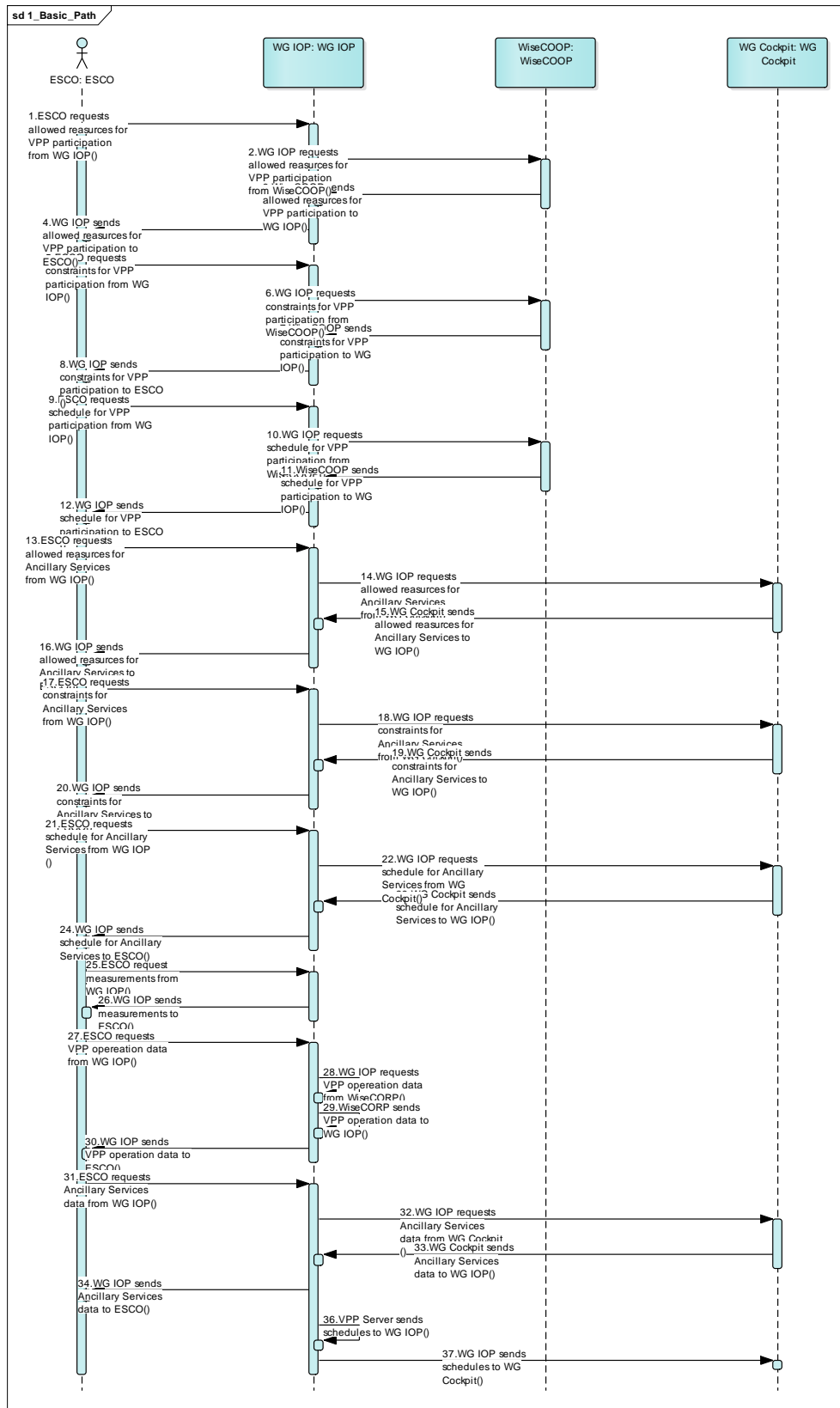


Figure 262 - Basic path sequence diagram for HL-UC 5 PUC 4

## **23 APPENDIX F - ARCHITECTURE**

### **HL-UC 6: VPP TECHNICAL AND ECONOMIC FEASIBILITY**

## 23.1 HL-UC 6\_PUC\_1: VPP MONITORING AND MANAGEMENT

### 23.1.1 PRIMARY USE CASE DESCRIPTION

According the description already provided in the D2.1, the goal of this PUC is to monitor the state of the resources (industrial, domestic and public facilities, EVs, energy storages etc.) belonging to the VPP (current status) (HL-UC 6\_SUC\_1.1) as well as to provide forecasting for RES, demand (HL-UC 6\_SUC\_1.2) and flexibility (HL-UC 6\_SUC\_1.3), and use that information for defining suitable strategies for managing (internal) grid and market issues (HL-UC 6\_SUC\_1.4).

### 23.1.2 SECONDARY USE CASE INTERACTIONS

In the figure below is showed the interactions among the primary and secondary use cases as well as with the involved actors.

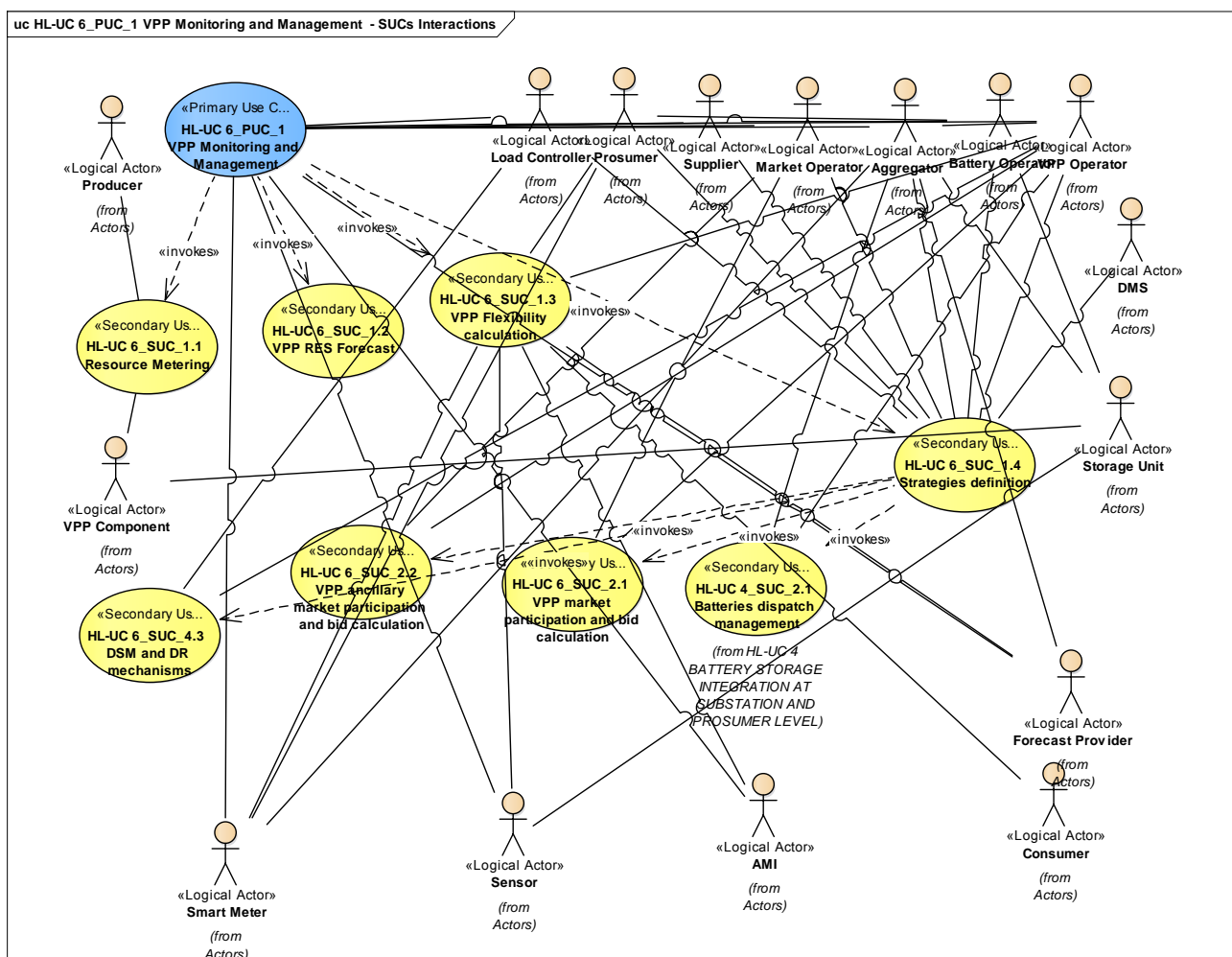


Figure 263 - SUCs Interactions Diagram

In the table below a brief description for each SUC involved in the considered PUC, as well as their relations.

**Table 208 - Table of list of participating SUCs**

SUC Name	Description	Relation	PUC/SUC
HL-UC 6_SUC_1.1_Resource metering	This HL-UC 6_SUC_1.1 provides information about the current status of the VPP. To this end, collection of metering data from all available metering infrastructure in the components of the VPP as well data coming from other WiseGRID systems is performed. Furthermore, an initial screening of the data is performed in order to detect ambiguous measurements, errors etc.	Invoke	HL-UC 6_PUC_1_VPP monitoring and management
HL-UC 6_SUC_1.2_VPP RES forecast	The production of RES units belonging to the VPP should be forecasted. The algorithms may be different from the ones developed for DSO, since data coming from the installation (e.g. weather station inside the RES facility) may be used and not only smart metering data and data from DMS. This forecasting will be used as an input to calculate the flexibility of the portfolio for further purposes.  The horizon and the dispatch periods (interval) of the forecasts should be defined according to the market rules.	Invoke	HL-UC 6_PUC_1_VPP monitoring and management
HL-UC 6_SUC_1.3_VPP flexibility forecast	Estimation in the short term (usually 24-48 hours) of the energy demand and available controllable resources for a given time horizon is performed in this SUC. The energy demand of controllable loads (from consumers) belonging to the VPP should be scheduled and by the case, forecasted. This will be an input to calculate the flexibility of the portfolio for further purposes.  The flexibility of the VPP is coming from: controllable load, storage capacity, generation regulation capability (this is depending on the primary energy source).  The HL-UC 6_SUC_1.3 should estimate the amount of energy that could be curtailed or shed. It should consider technical constraints or other requirements (e.g. regulation about the comfort level).  It is important to point out that this HL-UC 6_SUC_1.3 may use additional measurements available only to the VPP.  The horizon and the dispatchable periods of the forecasts should be defined according to the market rules.	Invoke	HL-UC 6_PUC_1_VPP monitoring and management
HL-UC 6_SUC_1.4_Strategies definition	This SUC aims to provide to the VPP the best strategies for managing the energy flexibility and the stored energy.  It takes into account the current status of the VPP as made available by HL-UC 6_SUC_1.1, the available forecasted RES resources (HL-UC 6_SUC_1.2) and the available forecasted flexibility (HL-UC 6_SUC_1.3), as well as resources committed to the execution of services already committed (energy sale or ancillary services).  The main objective is to provide suggestions in order for the VPP Operator to maximize the profit by distributing the usage of the energy managed of the VPP.  Implementation of this SUC requires an optimization	Invoke	HL-UC 6_PUC_1_VPP monitoring and management

SUC Name	Description	Relation	PUC/SUC
	<p>algorithm that will advise the distribution of the available energy among the following possible uses:</p> <ul style="list-style-type: none"> <li>• Sell energy to the wholesale market</li> <li>• Distribute energy among VPP Components (local explicit DR campaigns in order to use energy at loads controlled by the VPP)</li> <li>• Store energy for future usage at batteries controlled by VPP</li> <li>• Use energy to meet committed ancillary services (explicit DR mechanisms to shift VPP Components' consumption or production as requested by the corresponding actor - DSO/BRP)</li> </ul>		
HL-UC 6_SUC_2.1_VPP market participation and bid calculation	<p>This SUC describes a module for calculating the optimal participation of the VPP in the energy market (day-ahead and intraday) in order to sell energy surplus. The module calculates the optimal participation of the VPP units and proposes market bids that are in line with the market rules. Energy market participation is performed on the basis of price-quantity pairs for each dispatch period. The calculation considers Energy market status, unit status, technical constraints as well as information coming from the HL-UC 6_SUC_1.1.</p>	Invoke	HL-UC 6_SUC_1.4_Strategies definition
HL-UC 6_SUC_2.2_VPP ancillary market participation and bid calculation	<p>This SUC describes a module for calculating the optimal participation of the VPP in the ancillary services market providing ancillary services linked to flexibility. The module calculates the optimal participation of the VPP units and proposes market bids.</p> <p>Energy market participation is performed on the basis of price-services pairs for each dispatch period. The calculation considers unit status, technical constraints as well as information coming from the HL-UC 6_SUC_1.1.</p>	Invoke	HL-UC 6_SUC_1.4_Strategies definition
HL-UC 6_SUC_4.3_DSM and DR mechanisms	<p>This SUC includes all the tools for enabling a VPP to communicate the DSM or DR mechanism to its customers (who sign a contract with the VPP).</p> <p>VPP members offer their smart assets (controllable loads, batteries and RES) to the VPP Operator, which will operate them accordingly to the needs of the VPP. This SUC describes which information shall be shared with the VPP members to provide them an insight of the contribution of their assets to the overall operation of the VPP.</p>	Invoke	HL-UC 6_SUC_1.4_Strategies definition
HL-UC 4_SUC_2.1_Batteries dispatch management	<p>The energy control is performed at the local controller of the battery Storage Unit. The Energy Management System sets the control mode of the battery device (e.g. the batteries are given a fixed discharge/charge set-point, are in standby mode, etc.). Moreover the aggregator can give power commands to the installed battery devices, based on the load of the user, a fixed discharge/charge set-point or set the devices in standby mode (aggregator can set power if it is needed). The battery Storage Unit is operated in such a way that the customer requirements are met</p>	Invoke	HL-UC 6_SUC_1.4_Strategies definition

SUC Name	Description	Relation	PUC/SUC
	without disturbing network stability. This UC is linked to HL-UC 6_SUC_2.3.		

### 23.1.3 SGAM FUNCTION LAYER

In the figure below the actor and SUCs involved in the HL 6 PUC 1 are positioned on the SGAM Layer.

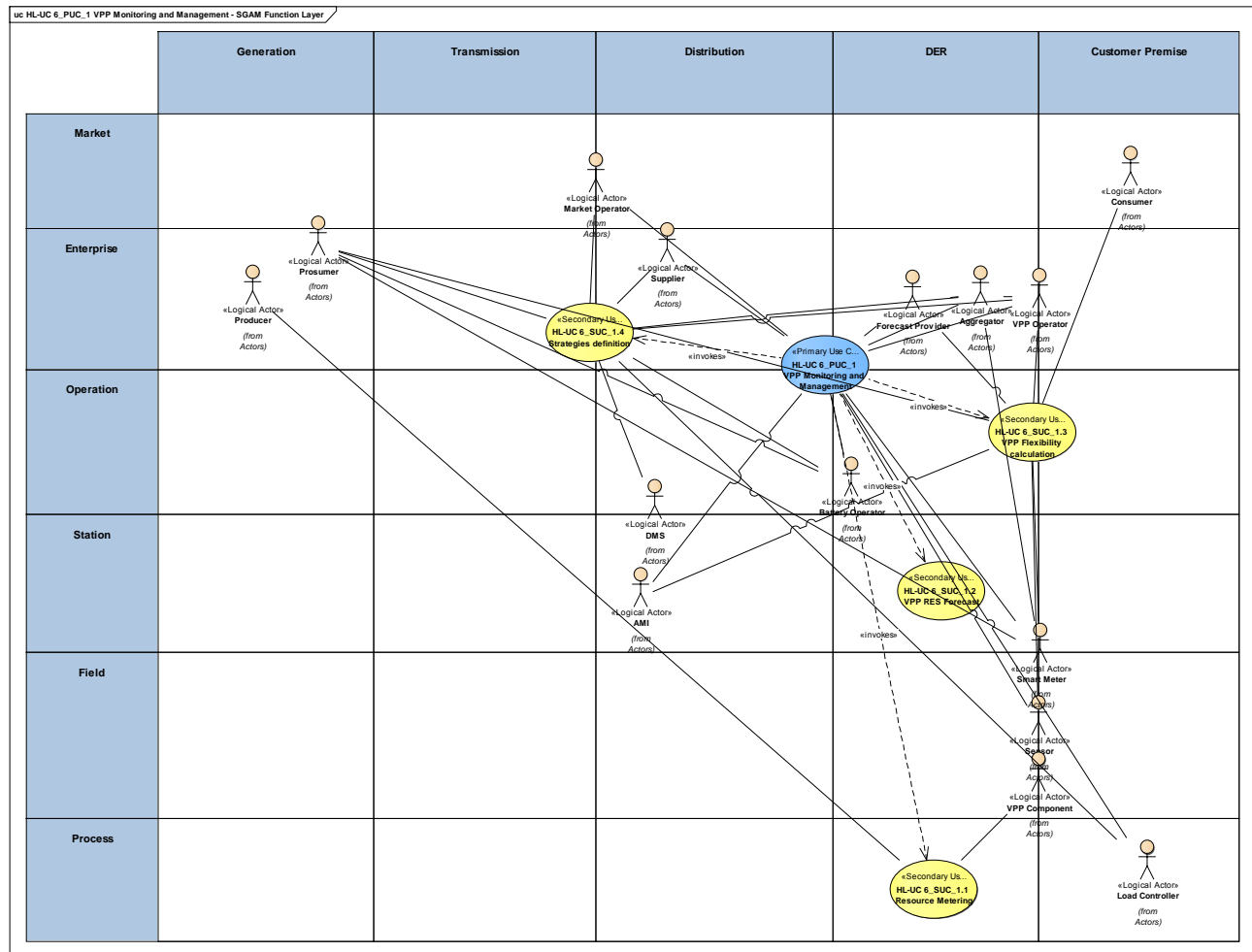


Figure 264 - SGAM Function Layer

The table shows the actors involved in the HL UC 6 PUC 1

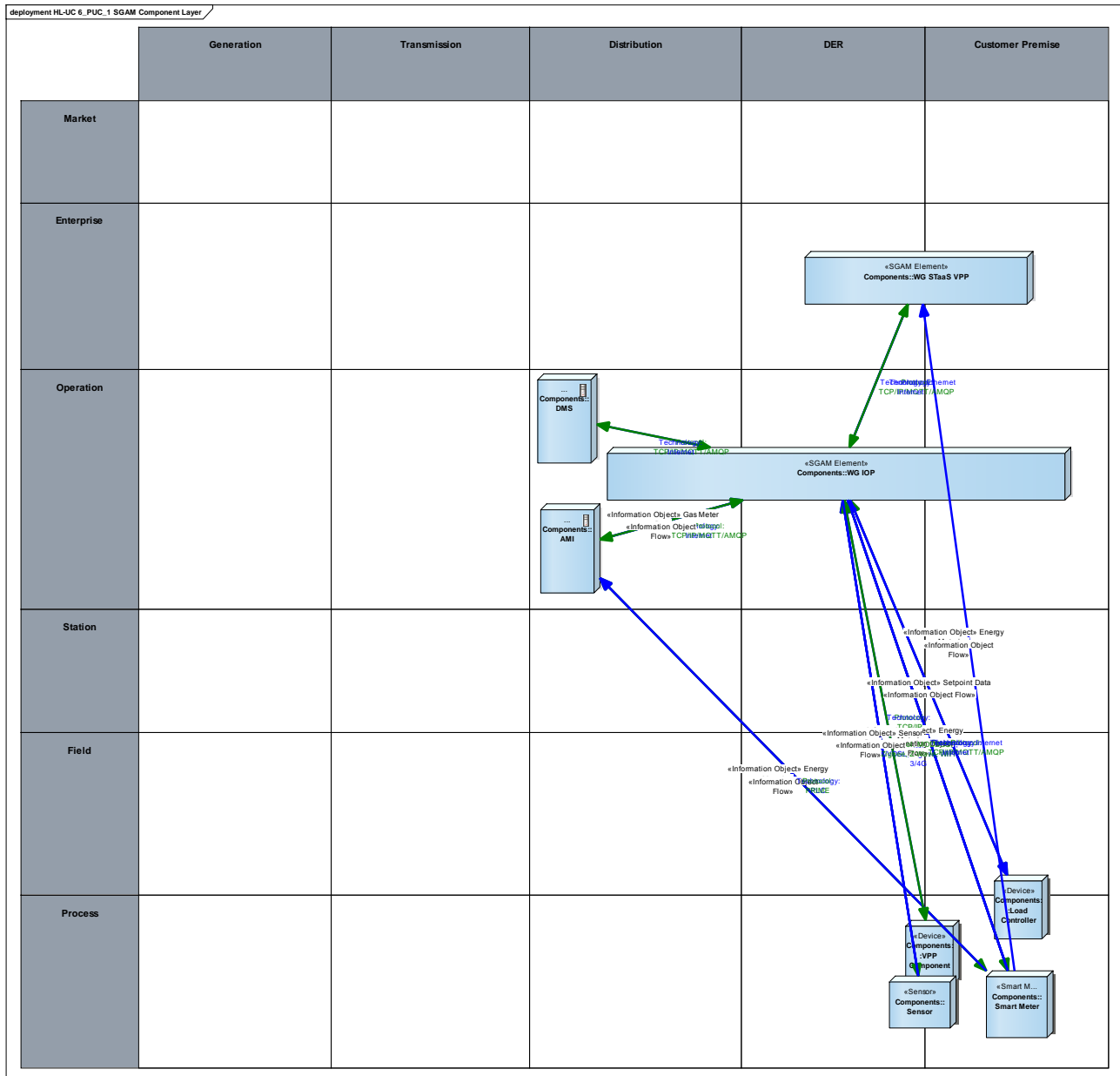
**Table 209 - List of Actors Involved**

Actor Name	Actor Type
VPP Operator	Logical Actor
Market Operator	Logical Actor
Load Controller	Logical Actor
VPP Components	Logical Actor
Producer	Logical Actor
Prosumer	Logical Actor
Supplier	Logical Actor
Forecast provider	Logical Actor
Aggregator	Logical Actor
Consumer	Logical Actor
DMS	Logical Actor
AMI	Logical Actor
Battery Operetor	Logical Actor
Smart Meter	Logical Actor
Sensor	Logical Actor



### 23.1.4 SGAM COMPONENT LAYER

The figure below show the components involved in the HL UC6 PUC 1 and how they are positioned on the SGAM layer.



### Figure 265 - SGAM Component Layer

The table below shows the components involved in the PUC.

### Table 210 - List of Components Participating in the Primary Use Case

Component	Component Type
WG STaaS/VPP	SGAM element
WG IOP	SGAM element
Load Controller	Device Component

Component	Component Type
VPP Components	Device Component
DMS	Component
AMI	Component
Smart meter	Smart meter component
Sensor	Sensor component

### 23.1.5 SGAM COMMUNICATION LAYER

In the following figure the SGAM communication layer is shown.

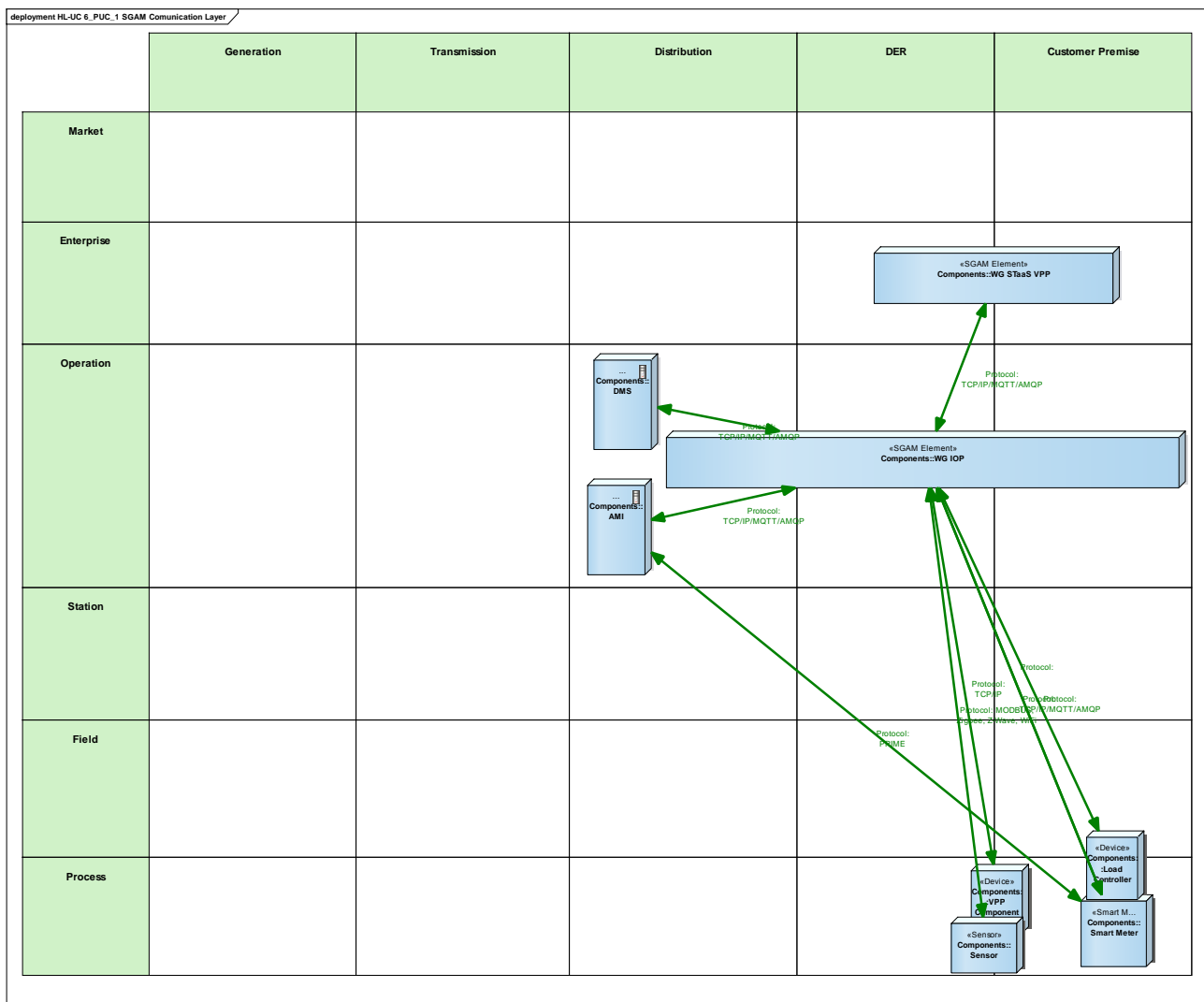


Figure 266 - SGAM Communication Layer

The table below list the main communication technologies and their brief description.

Communication Technology	Description
TPC/IP	Transmission Control Protocol/Internet Protocol is a Communications protocol for computer networks, the main protocol used on the Internet. It follows specific rules to get data from one network device to another assuring that data will not be lost in transmission
MQTT	It is an internet protocol. It is a machine-to-machine "Internet of Things" connectivity protocol. It was designed as a lightweight publish/subscribe messaging transport. It is useful for connections with remote locations where a small code footprint is required and/or network bandwidth is at a premium.
AMQP	The Advanced Message Queuing Protocol (AMQP) is an open standard application layer protocol for message-oriented middleware. It is a binary, application layer protocol, designed to efficiently support a wide variety of messaging applications and communication patterns.
ZigBee	It is a wireless communication protocol used to create personal area networks with small, low-power digital radios, such as for home automation. Usually it aims to be simpler and less expensive than other wireless personal area networks, such as Bluetooth or Wi-Fi.
Z-Wave	It is a wireless communications protocol used primarily for home automation. It is a mesh network using low-energy radio waves to communicate from appliance to appliance.
Wi-Fi	It is a wireless communication protocol for local area networking. It is based on the IEEE 802.11 standards.
PRIME	PRIME is an acronym for "PowerLine Intelligent Metering Evolution". It is a worldwide PLC standard for Advanced Metering, Grid Control and Asset Monitoring applications.

**Table 211 - List of Communication Technologies Involved**

### 23.1.6 SGAM INFORMATION LAYER

The figure below shows the information layer.

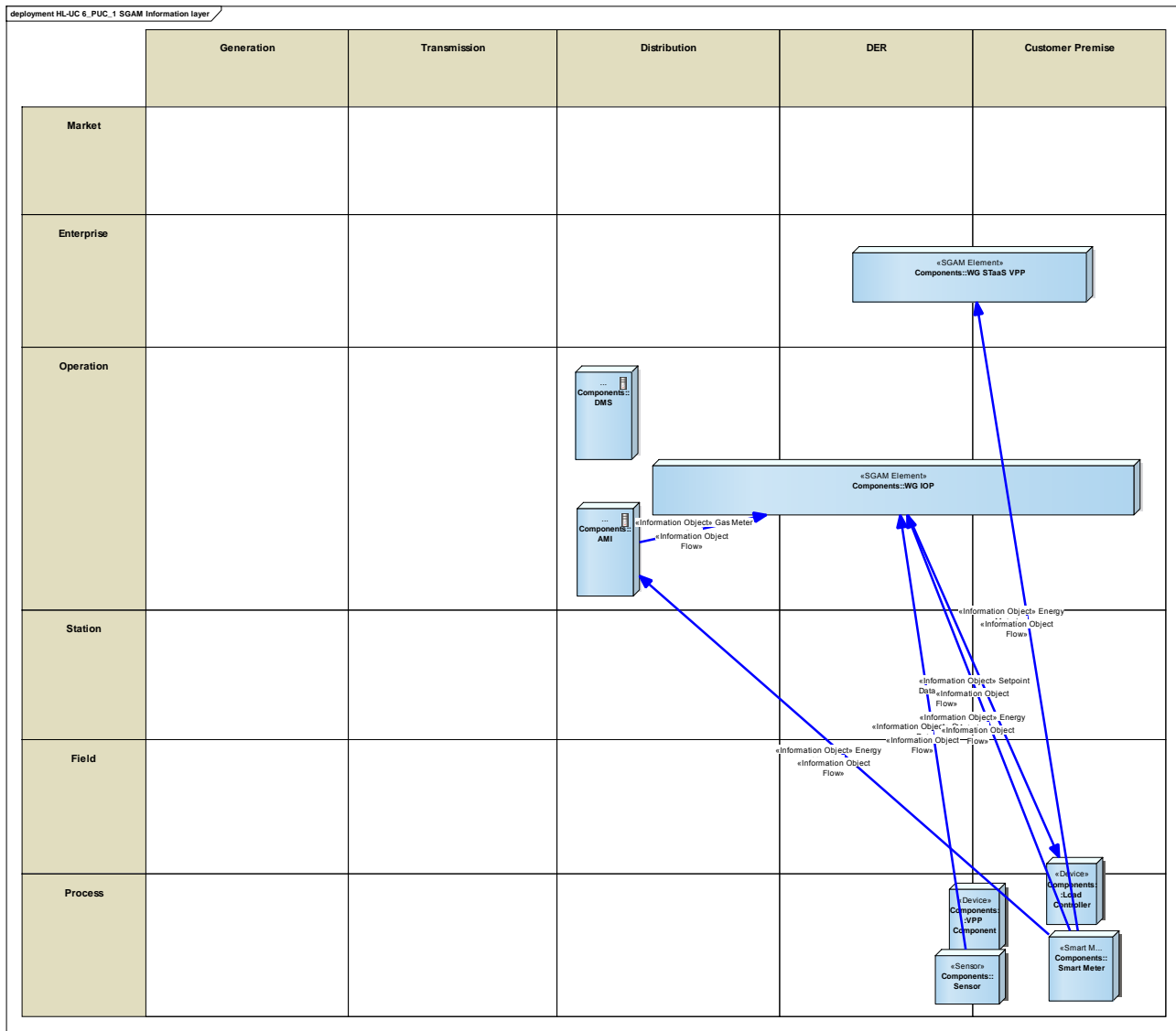


Figure 267 - SGAM Information Layer

### CANONICAL DATA MODEL

Here below some identified canonical data models.

Table 212 - List of Data Models

Data Models
VPP Billing Data Model
VPP Schedule data Model

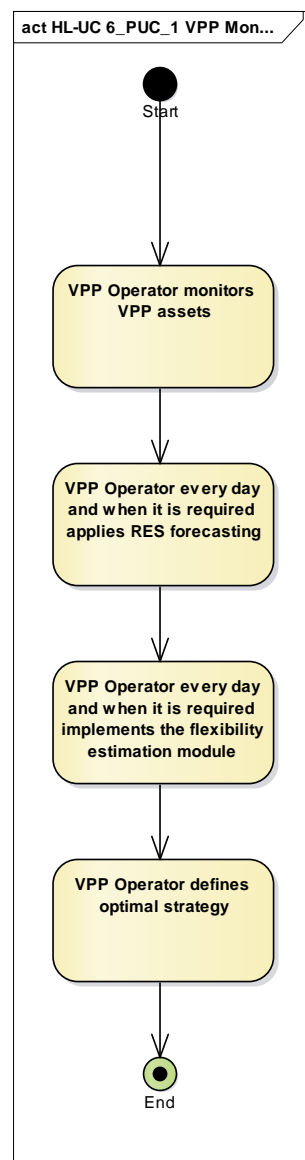
## STANDARDS AND INFORMATION OBJECT MAPPING

Here below some identified data standards.

**Table 213 - List of Data Standards**

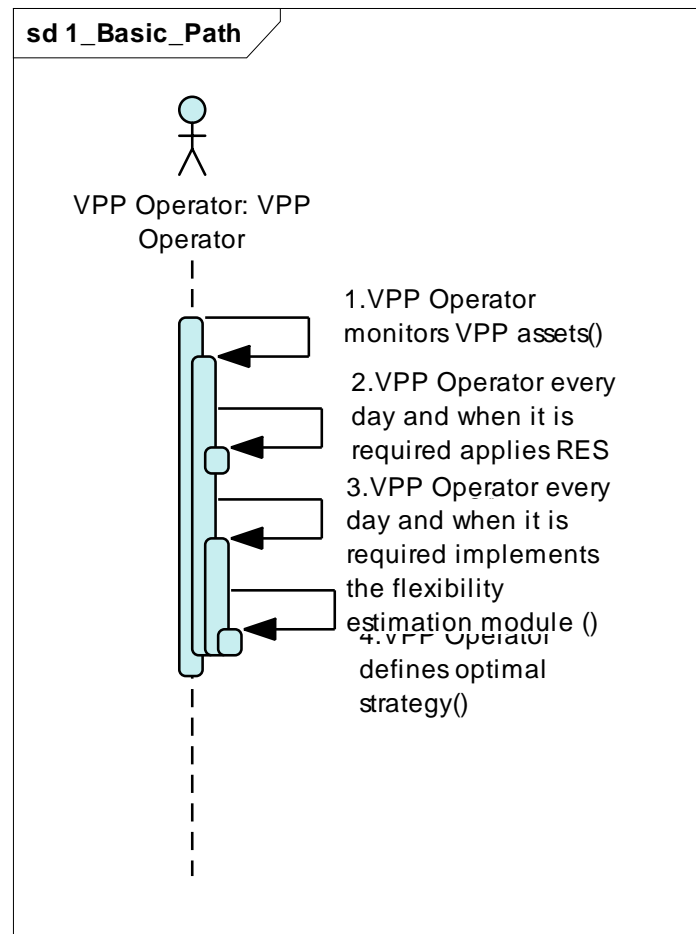
Data Standards
VPP Billing Data Model
VPP Schedule data Model

### 23.1.7 ACTIVITY DIAGRAM



**Figure 268 - Primary Use Case Activity Diagram**

### 23.1.8 SEQUENCE DIAGRAM



**Figure 269 - Primary Use Case Activity Diagram**

## 23.2 HL-UC 6\_PUC\_2: VPP MARKET PARTICIPATION

### 23.2.1 PRIMARY USE CASE DESCRIPTION

According the description already provided in the D2.1, this PUC manages the VPP within energy market participation. It helps the VPP to participate to the energy (day-ahead and intra-day) (HL-UC 6\_SUC\_2.1) as well as to the ancillary services market (HL-UC 6\_SUC\_2.2) and to calculate the most appropriate bid to be submitted in that energy market, where appropriate. Then according to these results, it supports the VPP to define a single strategy for the participation in these types of energy markets (HL-UC 6\_SUC\_2.3).

### 23.2.2 SECONDARY USE CASE INTERACTIONS

In the figure below is showed the interactions among the primary and secondary use cases as well as with the involved actors.

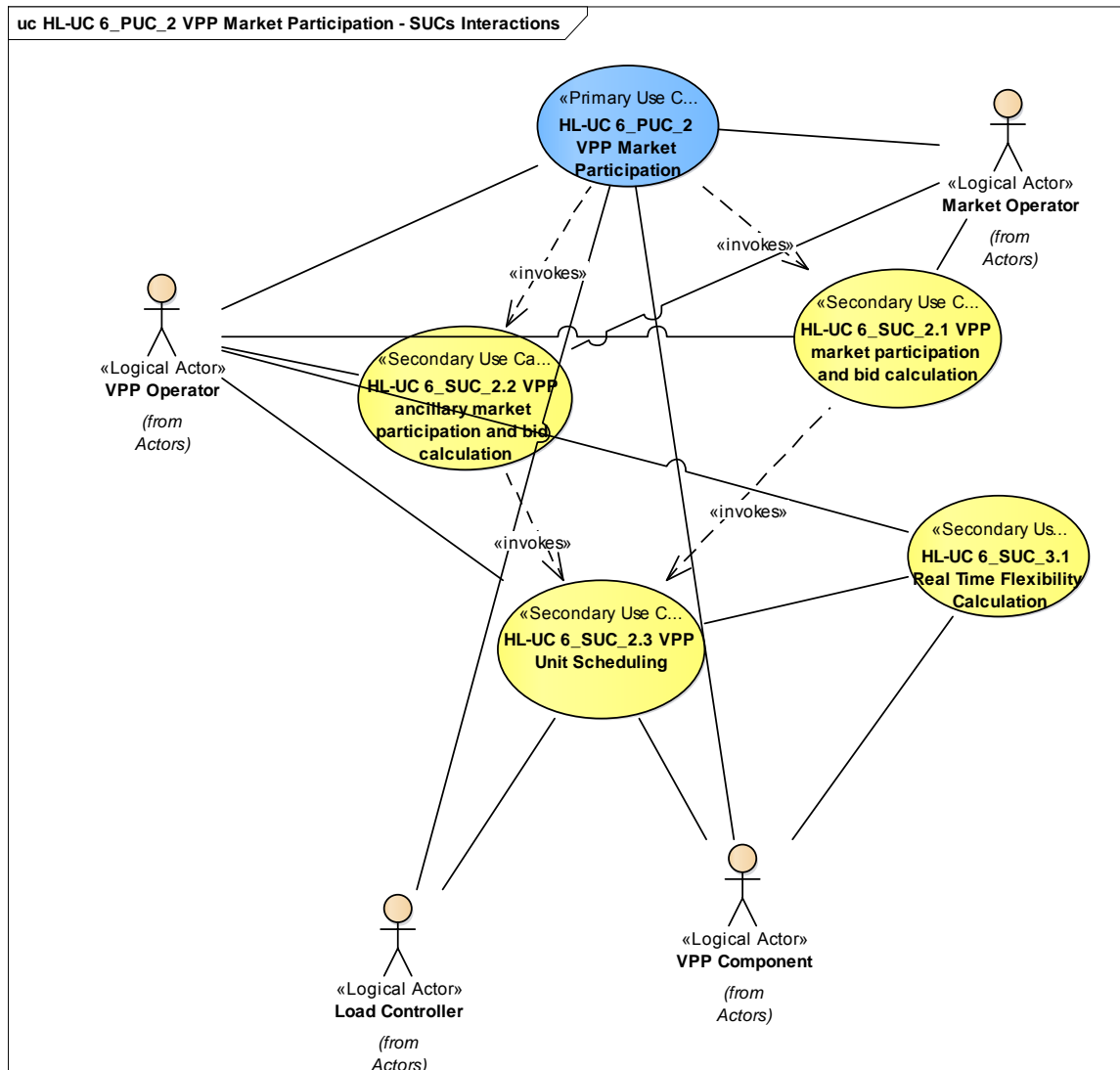


Figure 270 - SUCs Interactions Diagram

In the table below a brief description for each SUC involved in the considered PUC, as well as their relations.

**Table 214 - Table of list of participating SUCs**

SUC Name	Description	Relation	PUC/SUC
HL-UC 6_SUC_2.1_VPP market participation and bid calculation	This SUC describes a module for calculating the optimal participation of the VPP in the energy market (day-ahead and intraday) in order to sell energy surplus. The module calculates the optimal participation of the VPP units and proposes market bids that are in line with the market rules. Energy market participation is performed on the basis of price-quantity pairs for each dispatch period. The calculation considers Energy market status, unit status, technical constraints as well as information coming from the HL-UC 6_SUC_1.1.	Invoke	HL-UC 6_PUC_2, HL-UC 6_SUC_2.3_VPP unit scheduling
HL-UC 6_SUC_2.2_VPP ancillary market participation and bid calculation	This SUC describes a module for calculating the optimal participation of the VPP in the ancillary services market providing ancillary services linked to flexibility. The module calculates the optimal participation of the VPP units and proposes market bids. Energy market participation is performed on the basis of price-services pairs for each dispatch period. The calculation considers unit status, technical constraints as well as information coming from the HL-UC 6_SUC_1.1.	Invoke	HL-UC 6_PUC_2, HL-UC 6_SUC_2.3_VPP unit scheduling
HL-UC 6_SUC_2.3_VPP unit scheduling	This UC combines the results of HL-UC 6_SUC_2.1 (VPP market participation and bid calculation) and HL-UC 6_SUC_2.2 (VPP ancillary market participation and bid calculation) to define a single strategy for the participation in the energy markets. Also, within this SUC the quantities available for eventually balancing market with both components should be determined: capacity (as ancillary services) and energy (within energy market). The decision considers the optimal strategy that optimizes the benefit for the VPP and the VPP Components.	Invoke	HL-UC 6_SUC_2.1_VPP market participation and bid calculation; HL-UC 6_SUC_2.2_VPP ancillary market participation and bid calculation; HL-UC 6_SUC_3.1_Real-time flexibility calculation
HL-UC 6_SUC_3.1_Real-time flexibility calculation	This SUC identifies the available flexibility using the available real-time measurements. For example, analysing if there is any activity in a household and the level of consumption, may give an indication of the appliances in operation. This information can be used to monitor deviations and continuously adjust the calculated plan.	Invoke	HL-UC 6_SUC_2.3_VPP unit scheduling



### 23.2.3 SGAM FUNCTION LAYER

In the figure below the actor and SUCs involved in the HL 6 PUC 2 are positioned on the SGAM Layer.

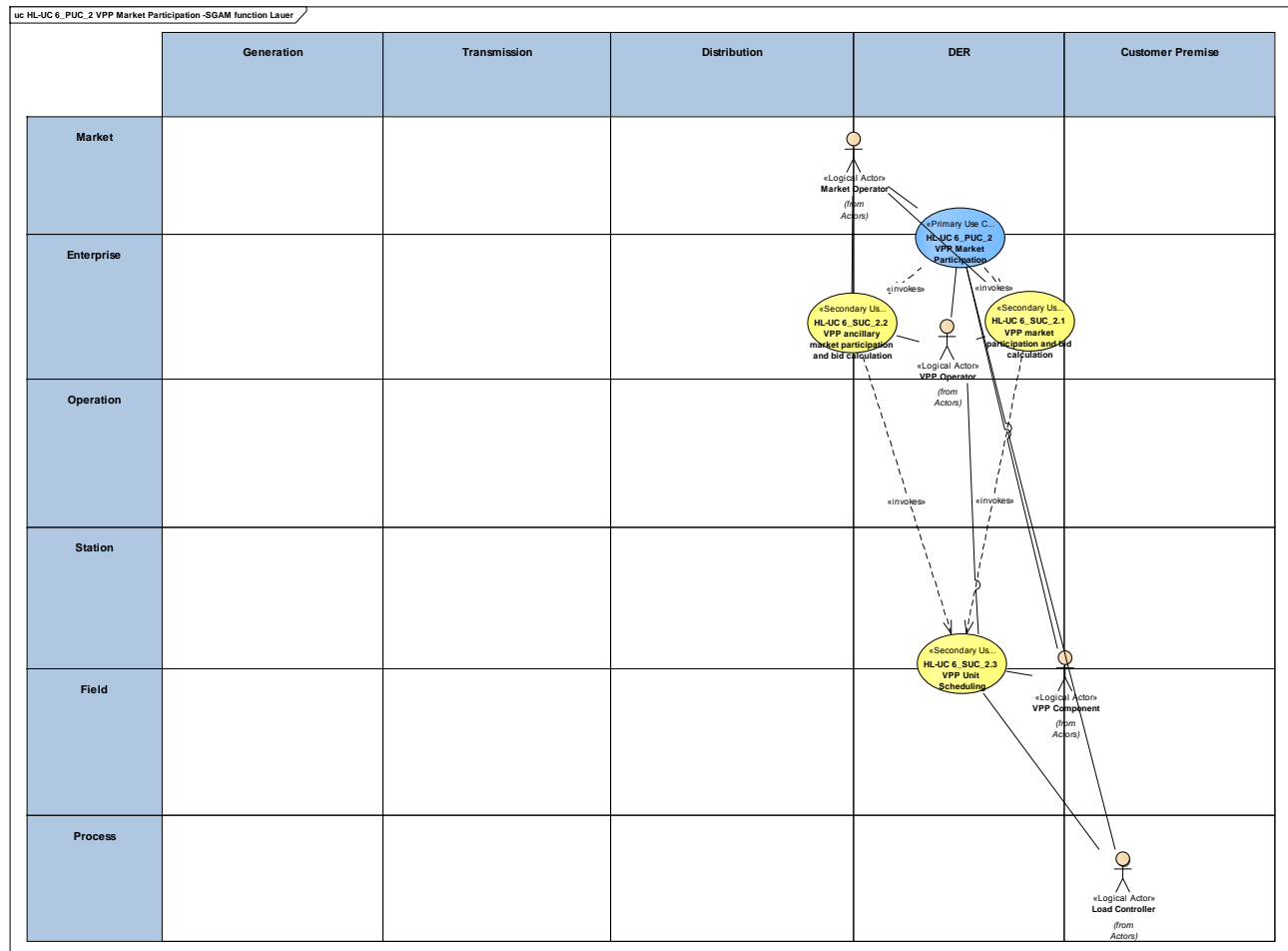


Figure 271 - SGAM Function Layer

The table shows the actors involved in the HL UC 6 PUC 2

Table 215 - List of Actors Involved

Actor Name	Actor Type
VPP Operator	Logical actor
Market Operator	Logical actor
Load Controller	Logical actor
VPP Components	Logical actor

### 23.2.4 SGAM COMPONENT LAYER

The figure below show the components involved in the HL UC6 PUC 2 and how they are positioned on the SGAM layer.

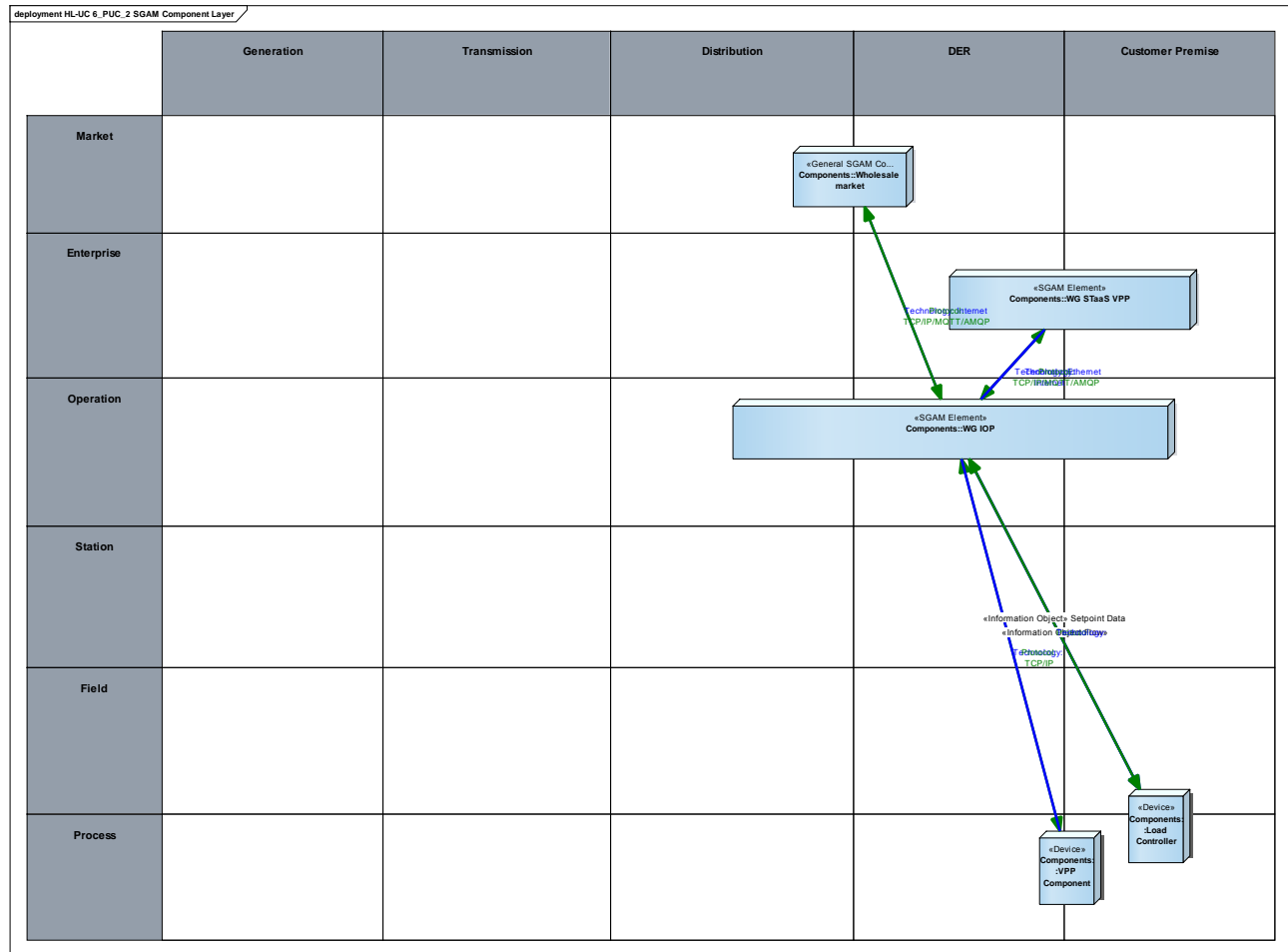


Figure 272 - SGAM Component Layer

The table below shows the components involved in the PUC.

Table 216 - List of Components Participating in the Primary Use Case

Component	Component Type
WG STaaS/VPP	SGAM element
WG IOP	SGAM element
Load Controller	Device
VPP Components	Device
Wholesale Market	General SGAM element

### 23.2.5 SGAM COMMUNICATION LAYER

In the following figure the SGAM communication layer is shown.

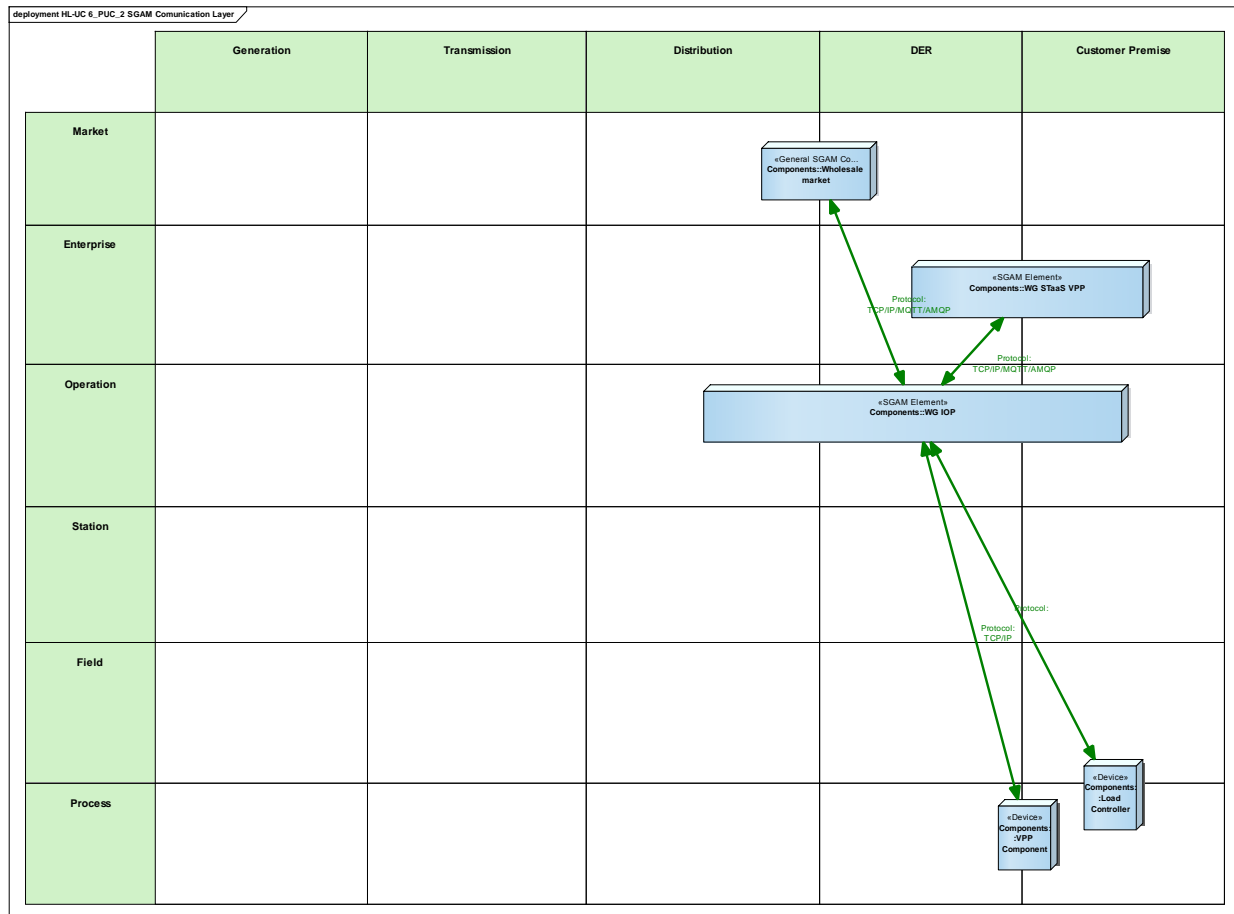


Figure 273 - SGAM Communication Layer

The table below list the main communication technologies and their brief description.

Table 217 - List of Communication Technologies Involved

Communication Technology	Description
TPC/IP	Transmission Control Protocol/Internet Protocol is a Communications protocol for computer networks, the main protocol used on the Internet. It follows specific rules to get data from one network device to another assuring that data will not be lost in transmission
MQTT	It is an internet protocol. It is a machine-to-machine "Internet of Things" connectivity protocol. It was designed as a lightweight publish/subscribe messaging transport. It is useful for connections with remote locations where a small code footprint is required and/or network bandwidth is at a premium.
AMQP	The Advanced Message Queuing Protocol (AMQP) is an open standard application layer protocol for message-oriented middleware. It is a binary, application layer protocol, designed to efficiently support a wide variety of messaging applications and communication patterns.

### 23.2.6 SGAM INFORMATION LAYER

The figure below shows the information layer.

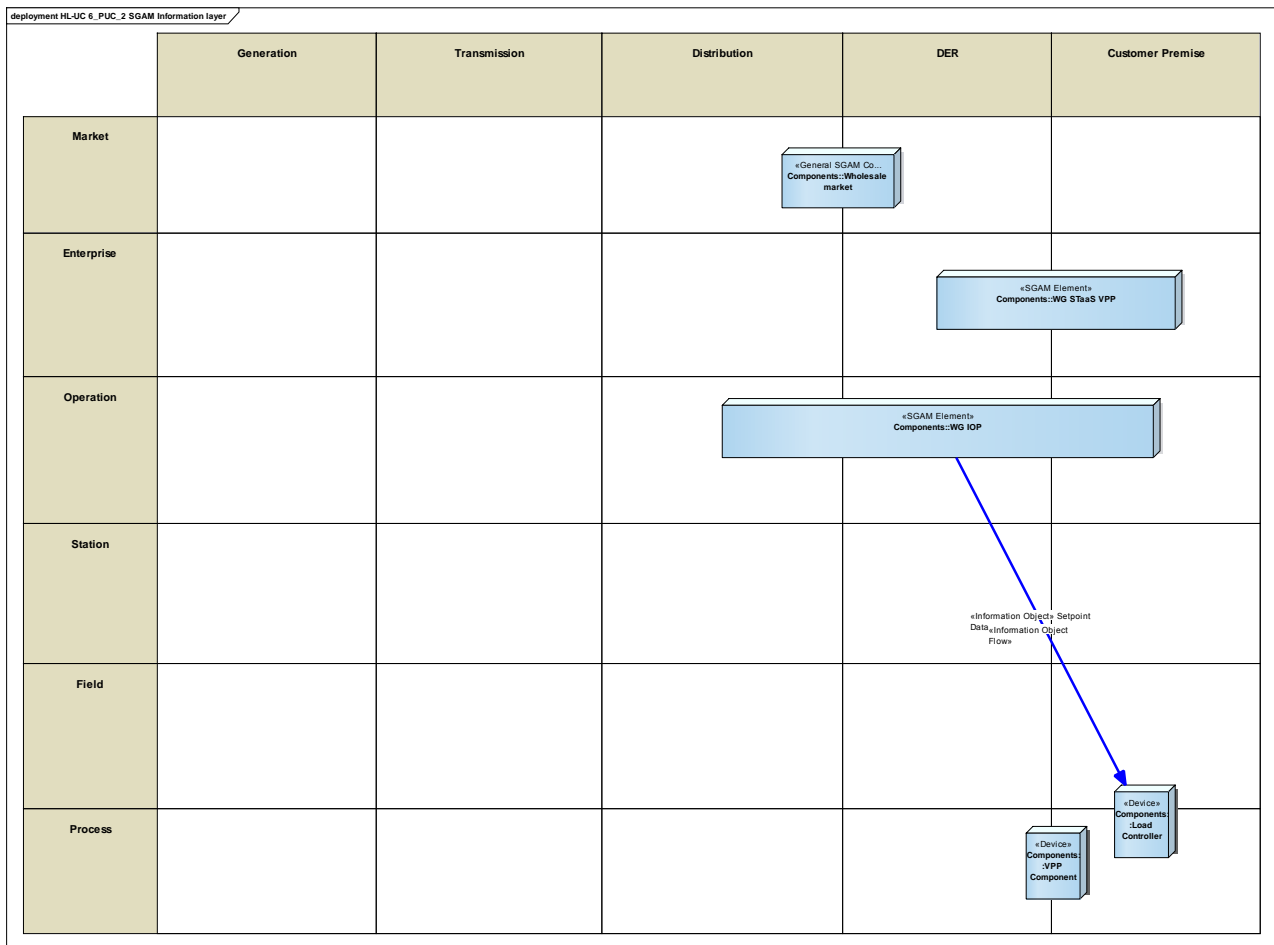


Figure 274 - SGAM Information Layer

## CANONICAL DATA MODELS

Here below some identified canonical data models.

Table 218 - List of Data Models

Data Models
VPP Billing Data Model
VPP Schedule data Model

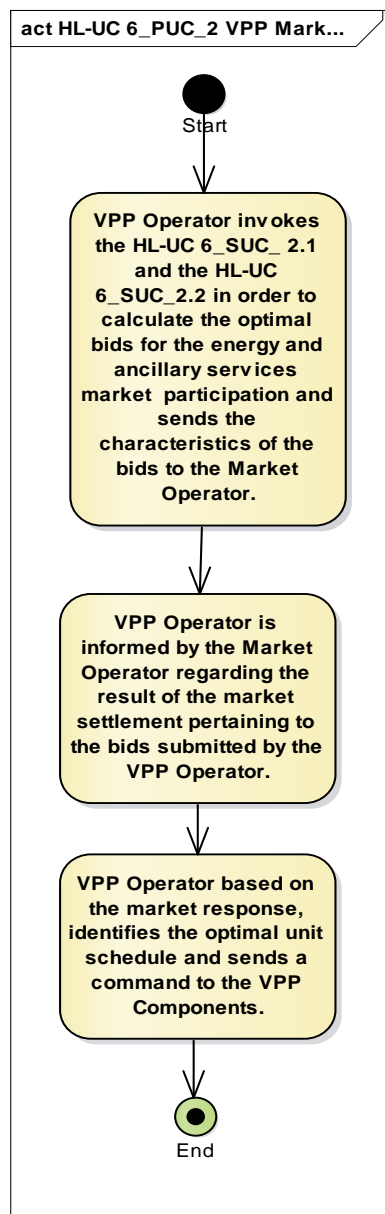
## STANDARDS AND INFORMATION OBJECT MAPPING

Here below some identified data standards.

**Table 219 - List of Data Standards**

Data Standards
VPP Billing Data Model
VPP Schedule data Model

### 23.2.7 ACTIVITY DIAGRAM



**Figure 275 - Primary Use Case Activity Diagram**

### 23.2.8 SEQUENCE DIAGRAM

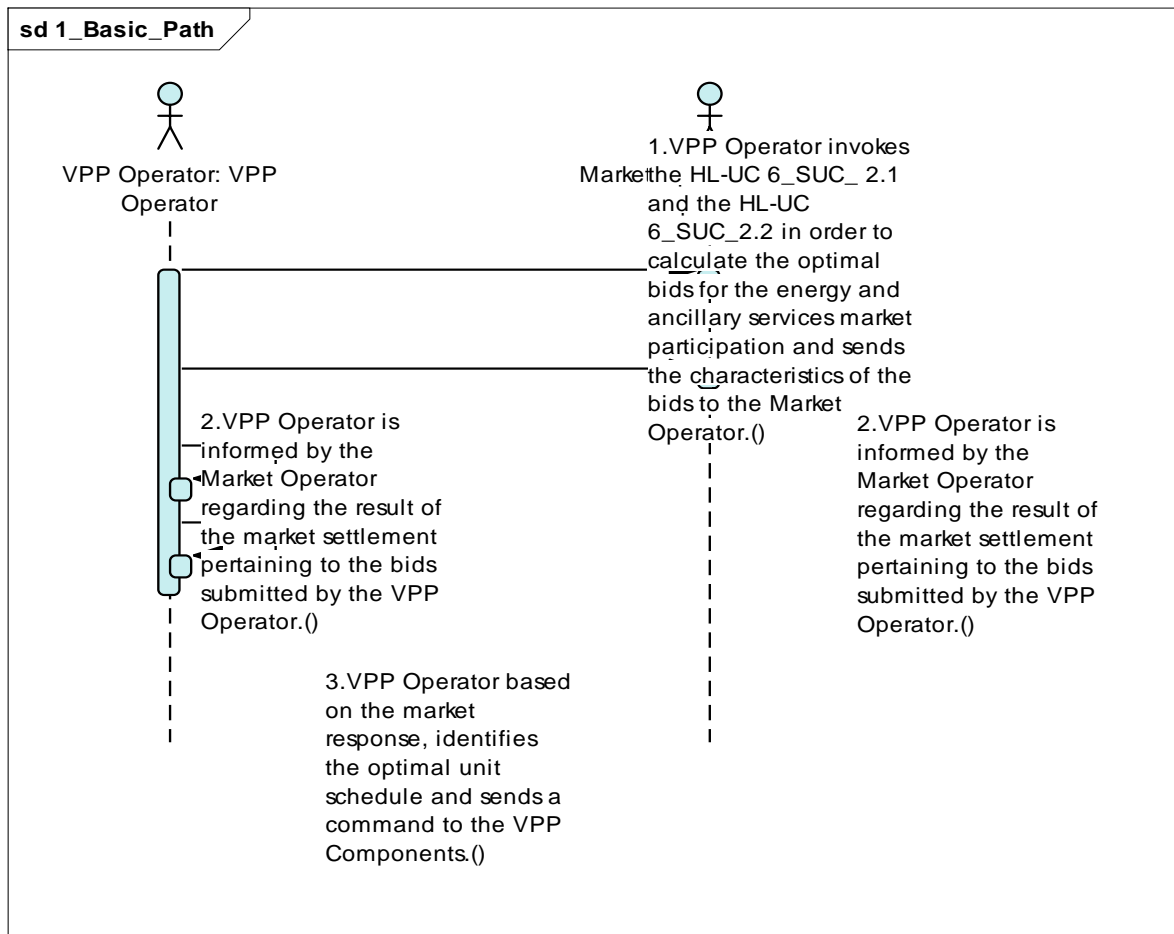


Figure 276 - Primary Use Case Sequence Diagram

## 23.3 HL-UC 6\_PUC\_3: VPP REAL TIME CONTROL

### 23.3.1 PRIMARY USE CASE DESCRIPTION

This PUC aims at providing a real time control on the VPP.

In order to do that it is necessary to identify the current available flexibility by taking into consideration the real time measurements (HL-UC 6\_SUC\_3.1), to receive notifications and requests by the local DSO through the ancillary services market in order to implement ancillary services (HL-UC 6\_SUC\_3.2), and to define the appropriate commands that the VPP Operator will send to the VPP Components (HL-UC 6\_SUC\_3.3).

### 23.3.2 SECONDARY USE CASE INTERACTIONS

This PUC invokes three SUCs to implement ancillary services through a VPP.

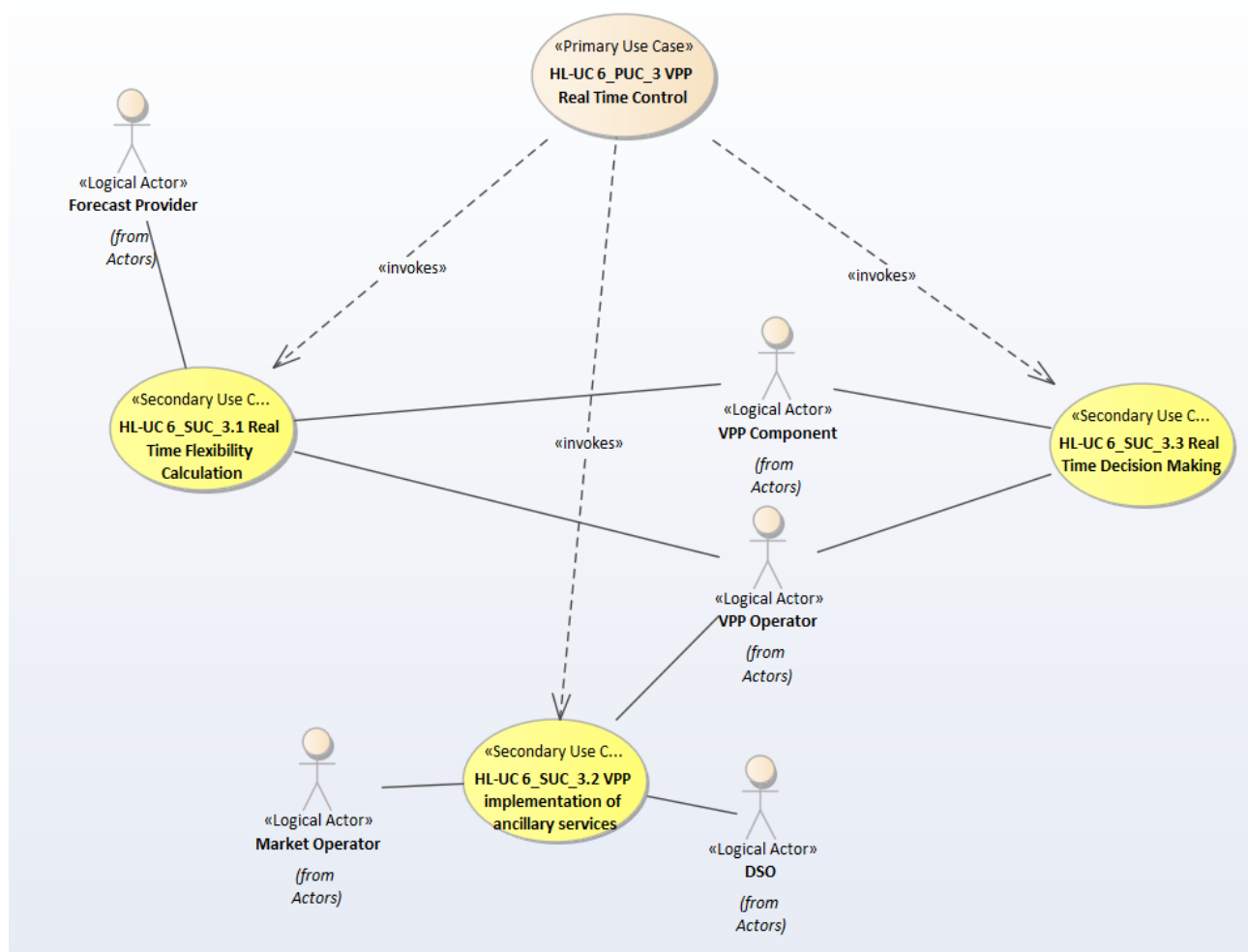


Figure 277 - SUCs Interactions Diagram

**Table 220 - Table of list of participating SUCs**

SUC Name	Description	Relation	PUC/SUC
Real time flexibility calculation	This SUC identifies the available flexibility using the available real-time measurements. For example, analyzing if there is any activity in a household and the level of consumption, may give an indication of the appliances in operation. This information can be used to monitor deviations and continuously adjust the calculated plan.	Invokes	3.1
VPP implementation of ancillary services	<p>As part of the distribution grid, the VPP is required to contribute to the smooth operation of the grid. In order to achieve that, the VPP Operator provides ancillary services to the grid considering notifications and requests by the local DSO through the ancillary services market. This SUC describes the next step, where the commands (P, Q production set points or mode of operation) to be sent to the related VPP Components should be defined. The ancillary services treated in this SUC are:</p> <ul style="list-style-type: none"> <li>• Voltage and Reactive Power (Q) control in LV network: In order to perform voltage control, the main action will be to control Q production/consumption in the network points, where possible.</li> <li>• Frequency control: The VPP can provide frequency control to the grid adjusting its consumption/generation of active power.</li> </ul> <p>Load/generation management: By increasing the generation power output during high load periods or by reducing the load, the stress on central generation can be relieved. Also, the DSO can have necessity of reallocate a RES energy surplus.</p>	Invokes	3.2
Real time decision making	The goal of the SUC is to analyse the output of previous SUCs (HL-UC 6_SUC_3.1 and HL-UC 6_SUC_3.2) as well the resource metering (HL-UC 6_SUC_1.1) and define the final schedules to be sent to the different VPP Components that form the VPP portfolio. The commands should be in line with the proposed schedules and policies but should not violate any technical and/or contractual constraint.	Invokes	3.3



### 23.3.3 SGAM FUNCTION LAYER

All SUCs under this PUC are located in the *field* zone

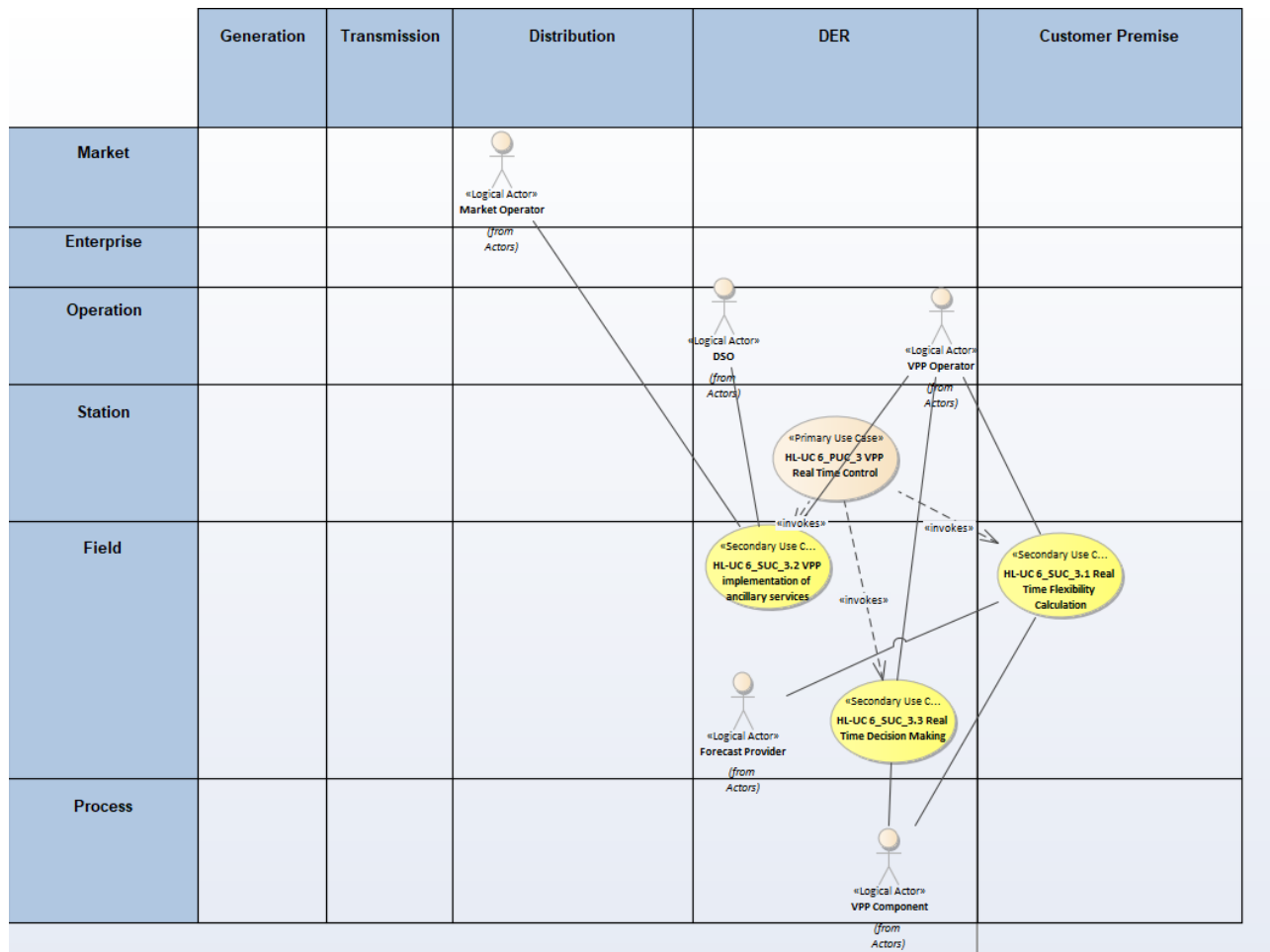


Figure 278 - SGAM Function Layer

Actor Name	Actor Type
Market operator	Organization
VPP operator	Organization
DSO	Organization
Forecast provider	Device
VPP Component	Device

Table 221 - List of Actors Involved

### 23.3.4 SGAM COMPONENT LAYER

This section illustrates the main components that will play a role in the use of storage elements as well as their associations, which will further on lead to the information flows

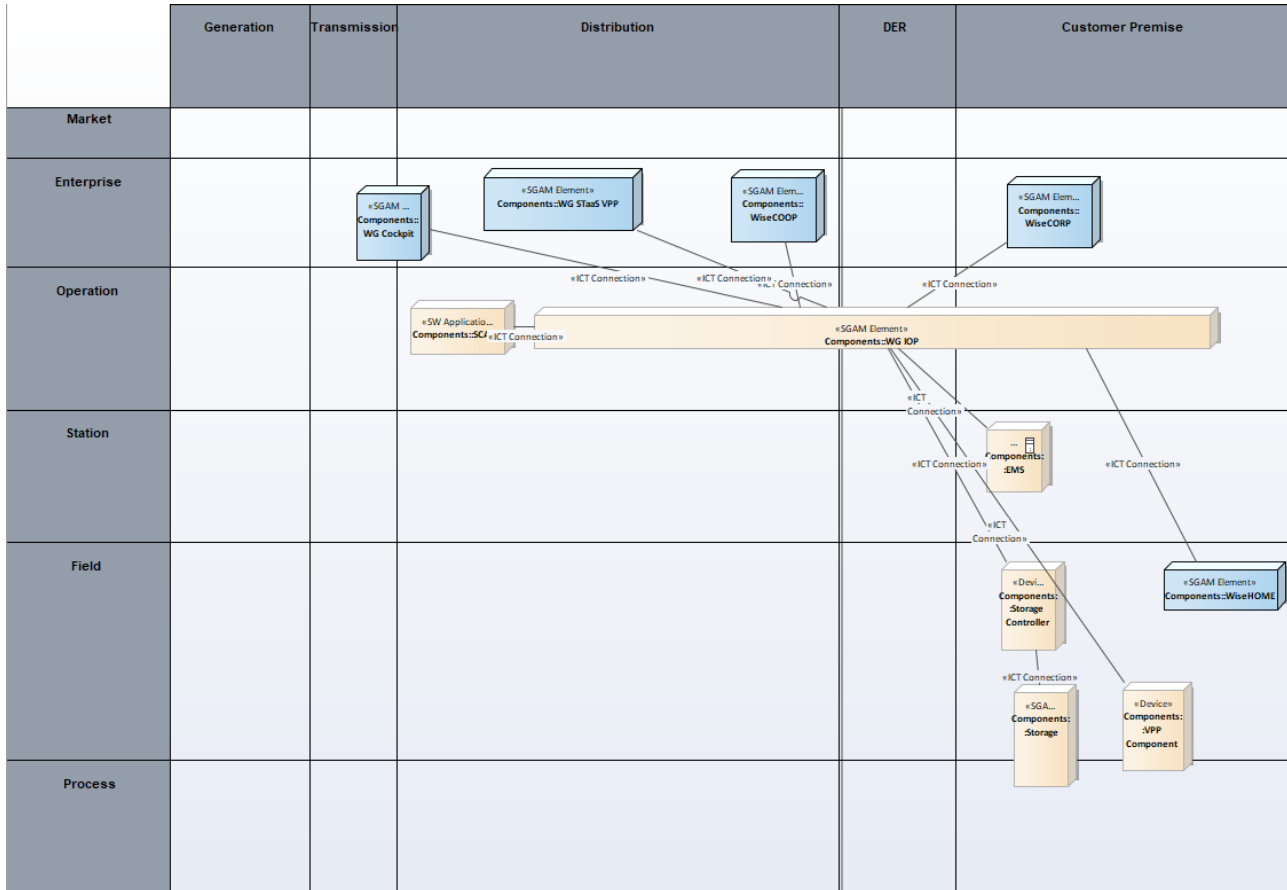


Figure 279 - SGAM Component Layer

Component	Component Type
VPP Component	Device
EMS	Device
Storage controller	Device
Storage	Device
Component SCADA	Device
WG IOP	SGAM element
WG cockpit	SGAM element
WG Staas VPP	SGAM element
WiseHOME	SGAM element
WiseCOOP	SGAM element
WiseCORP	SGAM element

Table 222 - List of Components Participating in the Primary Use Case

### 23.3.5 SGAM COMMUNICATION LAYER

This section outlines the main communication technologies that will be utilised in the reference implementation of the WiseGRID project.

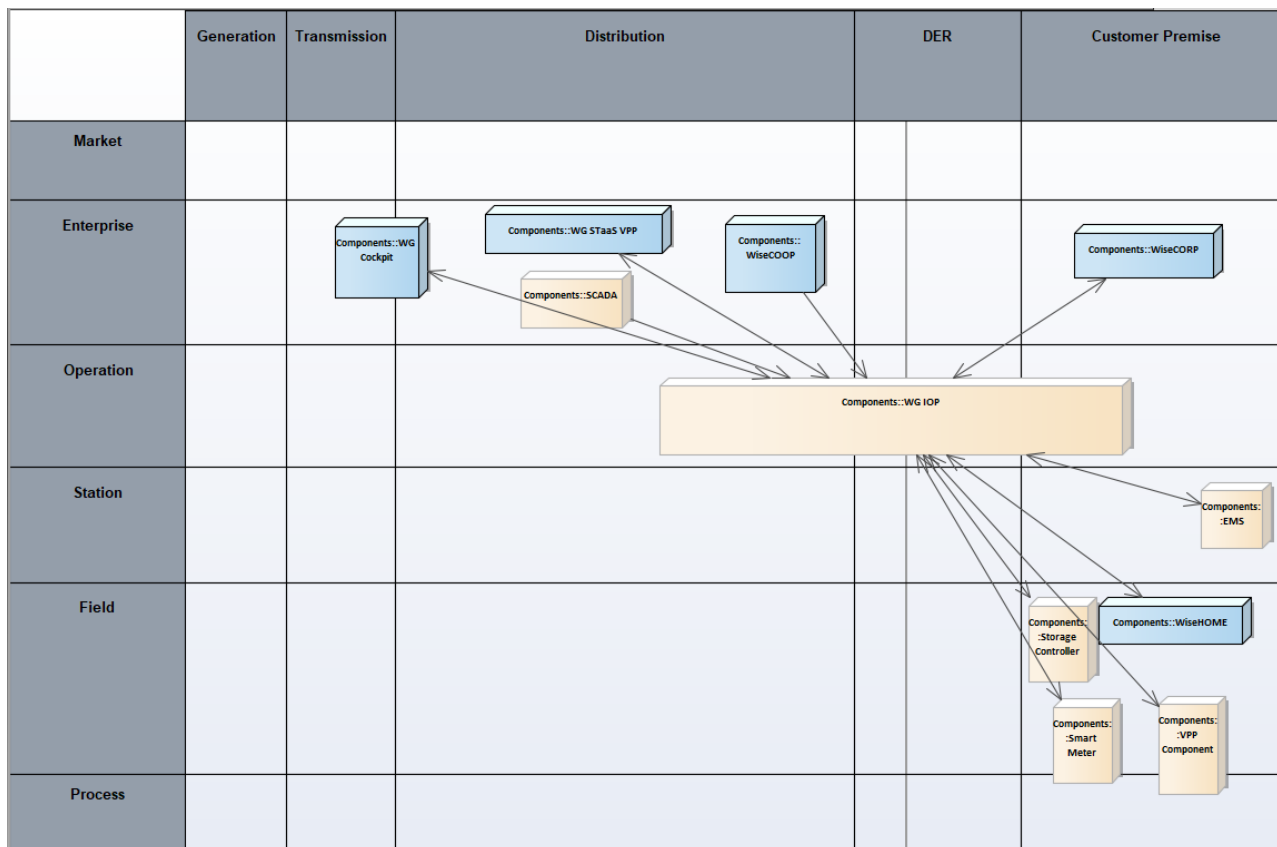


Figure 280 - SGAM Communication Layer

Communication Technology	Description
Modbus TCP/IP	
CAN	
IEC61850	
Web services	

Table 223 - List of Communication Technologies Involved

### 23.3.6 SGAM INFORMATION LAYER

The SGAM Information layer for this use case is illustrated below.

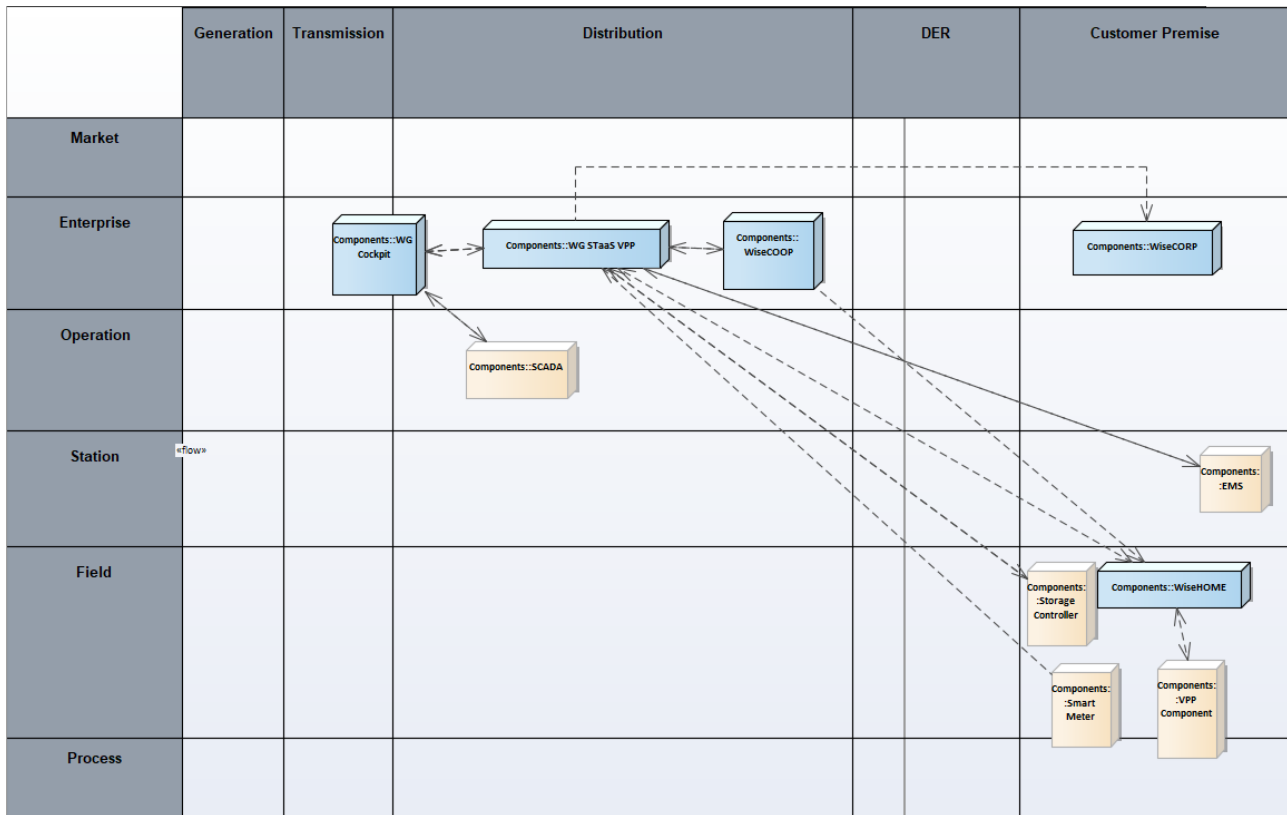


Figure 281 - SGAM Information Layer

### CANONICAL DATA MODEL

The following data models have been identified for modelling the information related to VPP Operation

Data Models
Flexibility data model
OpenADR
VPP schedule data models

Table 224 - List of Data Models

## STANDARDS AND INFORMATION OBJECT MAPPING

This secondary use case will leverage the following standards in order to align its outputs with ongoing activities by other parties so as to ensure replicability of the WiseGRID solution.

Data Standards
Flexibility data models
Schedule and set point data model
Storage data model

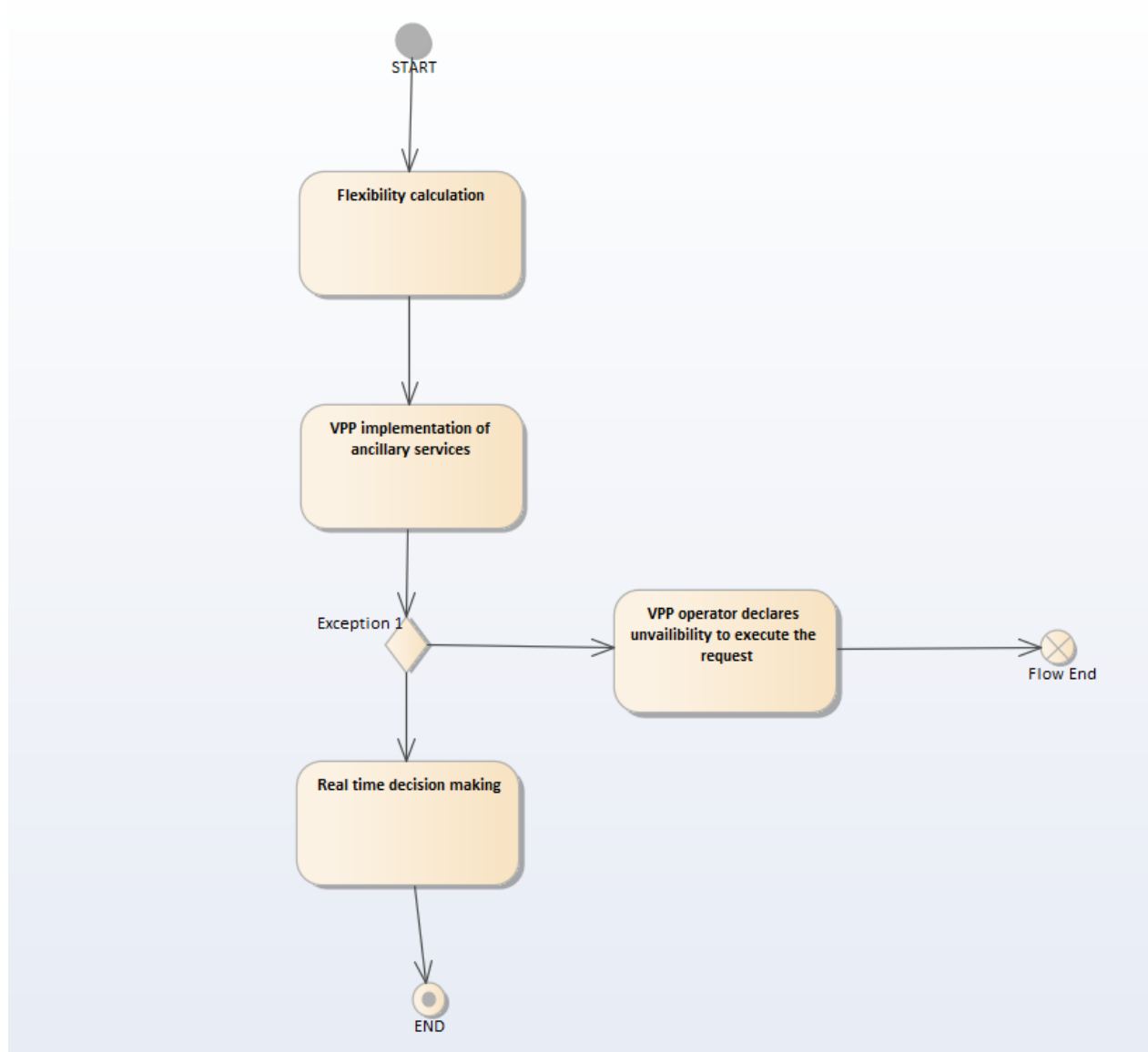
**Table 225 - List of Data Standards**

Information Objects	Data Model
Demand response request	Flexibility data model
Demand flexibility profile	Flexibility data model
Demand response	Flexibility data model
Flexibility offer	Flexibility data model
Flexibility request	Flexibility data model
Schedule data	Schedule and setpoint data model
Setpoint data	Schedule and setpoint data model

**Table 226 - List of Information Objects**

### 23.3.7 ACTIVITY DIAGRAM

The following diagram depicts the steps needed to operate ancillary services through VPP implementation



**Figure 282 - Primary Use Case Activity Diagram**

### 23.3.8 SEQUENCE DIAGRAM

The sequence diagram for this use case is depicted below.

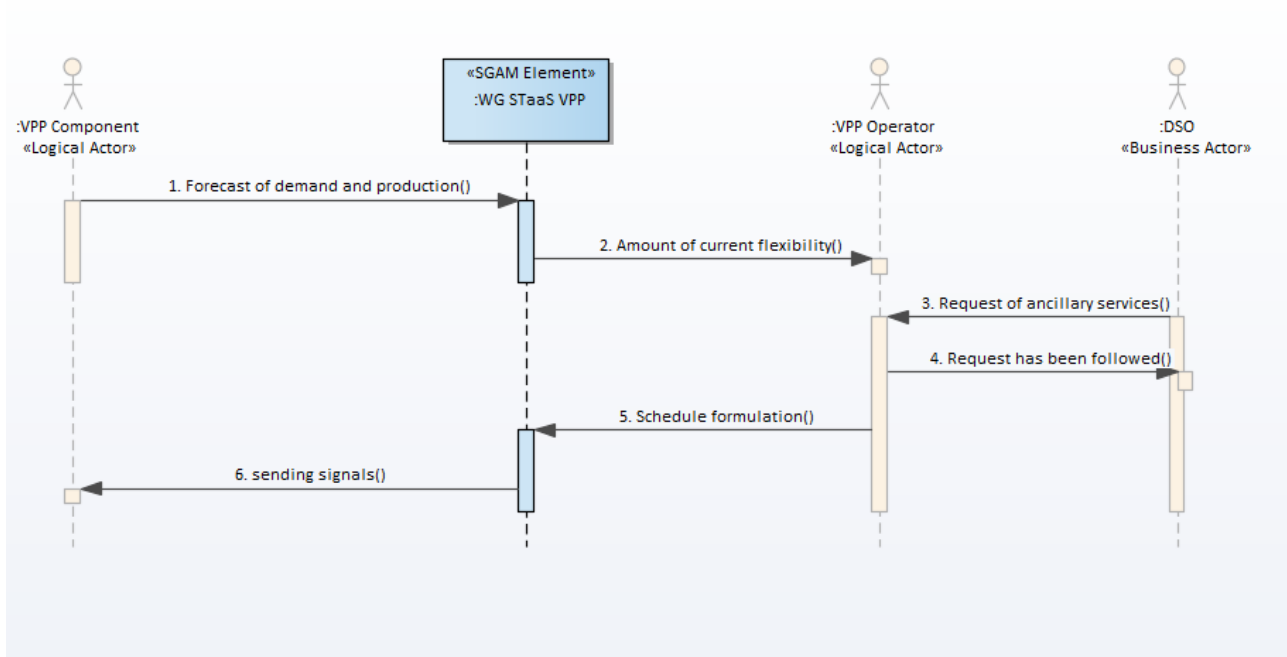


Figure 283 - Primary Use Case Sequence Diagram

## 23.4 HL-UC 6\_PUC\_4: VPP USERS RELATIONSHIP MANAGEMENT

### 23.4.1 PRIMARY USE CASE DESCRIPTION

This PUC is about the possibility to manage more efficiently the grid load avoiding peak by means of Demand Side Management (DSM) and Demand Response (DR) mechanisms, which push consumers (in an aggregated way) at VPP level to consume more or less RES according to the need of the grid. In this direction, this PUC describes the functionalities needed by the VPP Operator to manage the portfolio of VPP members. Such functionalities include: describes management of the contractual issues and Service Level Agreement (SLA) (HL-UC 6\_SUC\_4.1), management of member compensation (HL-UC 6\_SUC\_4.2) and DR actions (HL-UC 6\_SUC\_4.3)

### 23.4.2 SECONDARY USE CASE INTERACTIONS

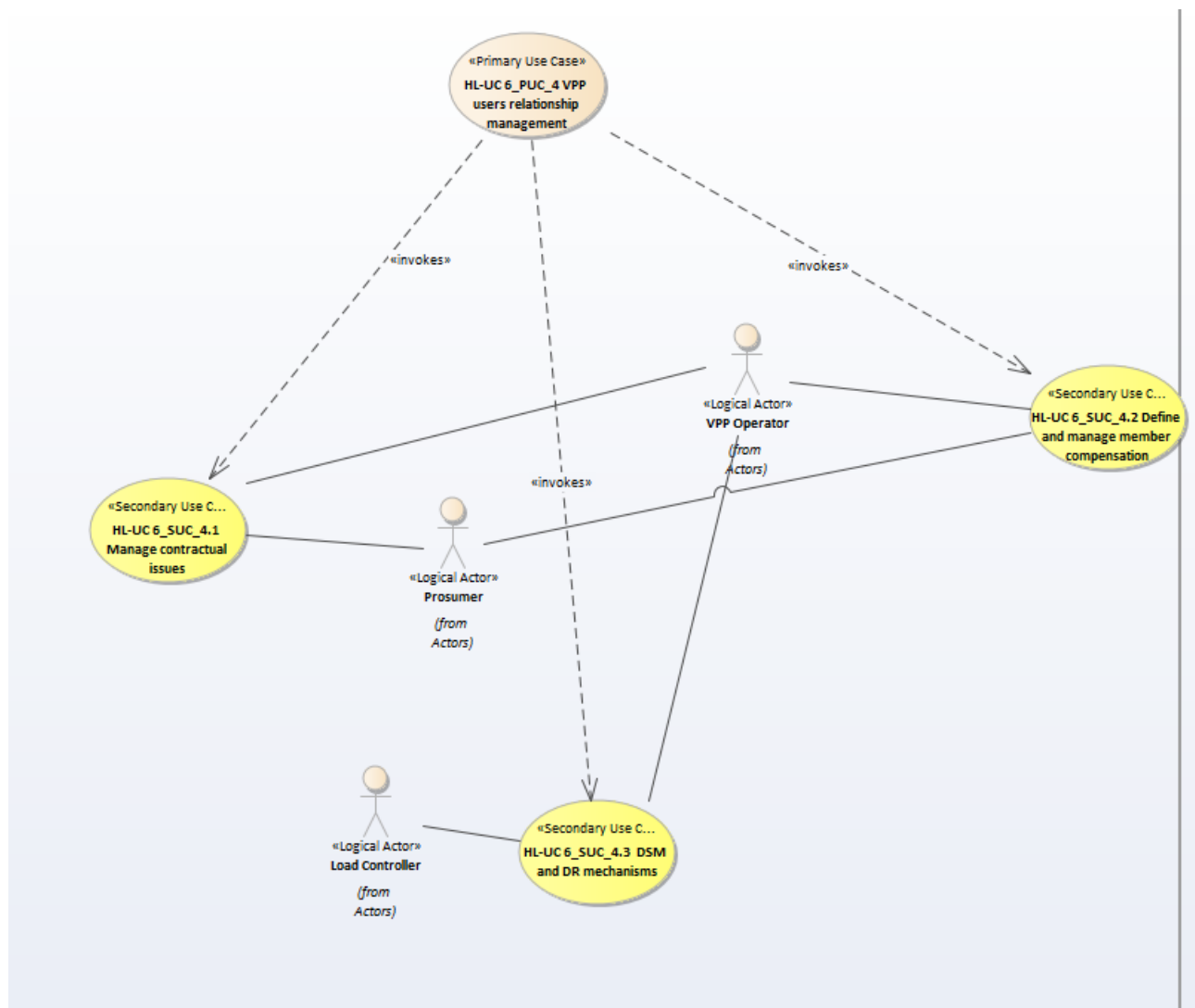


Figure 284 - SUCs Interactions Diagram



**Table 227 - Table of list of participating SUCs**

SUC Name	Description	Relation	PUC/SUC
Manage contractual issues	This SUC provides to the VPP the functions for managing contractual issues (e.g., define service level agreements -SLA- about energy dispatching) with the actors (Prosumers and Consumers) connected to the distribution grid that are (or can be) part of the VPP energy group. It is a contact point between VPP and VPP Components (Consumers, Producers and Prosumers).	Invokes	4.1
Define and manage member compensation	In order to manage energy selling, the VPP needs tools to help them define the energy price for compensating VPP members. It can be calculated taking into account: <ul style="list-style-type: none"> <li>- Incomes of the VPP from selling energy bids at the wholesale market</li> <li>- Incomes of the VPP from delivering ancillary services</li> </ul> Participation of individual VPP members in the processes described above	Invokes	4.2
DSM and DR mechanism	This SUC includes all the tools for enabling a VPP to communicate the Demand Side Management (DSM) or Demand Response (DR) mechanism to its customers (who sign a contract with the VPP).  VPP members offer their smart assets (controllable loads, batteries and RES) to the VPP Operator, which will operate them accordingly to the needs of the VPP. This SUC describes which information shall be shared with the VPP members to provide them an insight of the contribution of their assets to the overall operation of the VPP.	Invokes	4.3

### 23.4.3 SGAM FUNCTION LAYER

The SGAM Function layer for this use case is presented below.

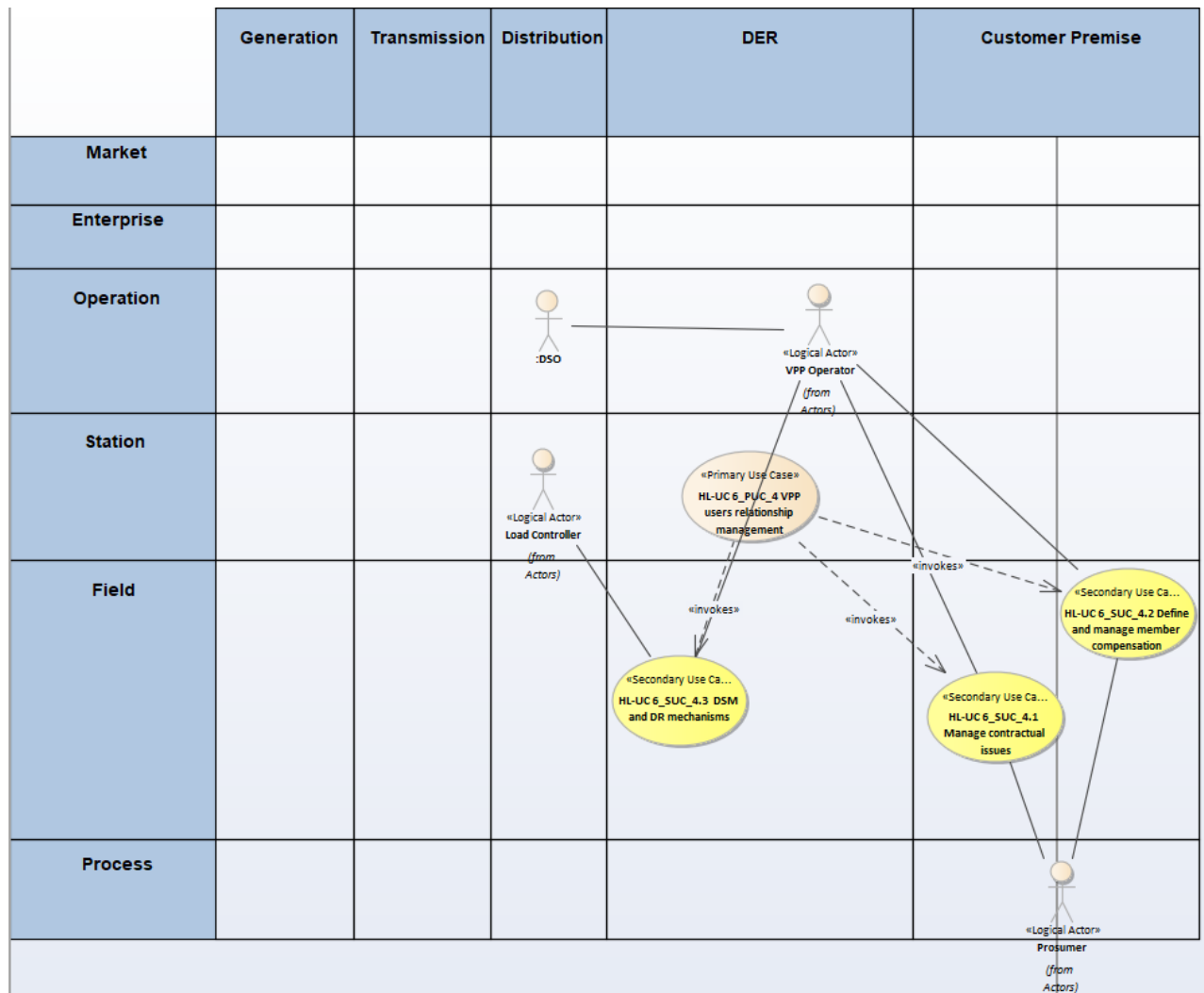


Figure 285 - SGAM Function Layer

Actor Name	Actor Type
Prosumer	Person
Load Controller	Device
VPP operator	Organisation
DSO	Organisation

Table 228 - List of Actors Involved

### 23.4.4 SGAM COMPONENT LAYER

The SGAM Component layer for this use case is presented below.

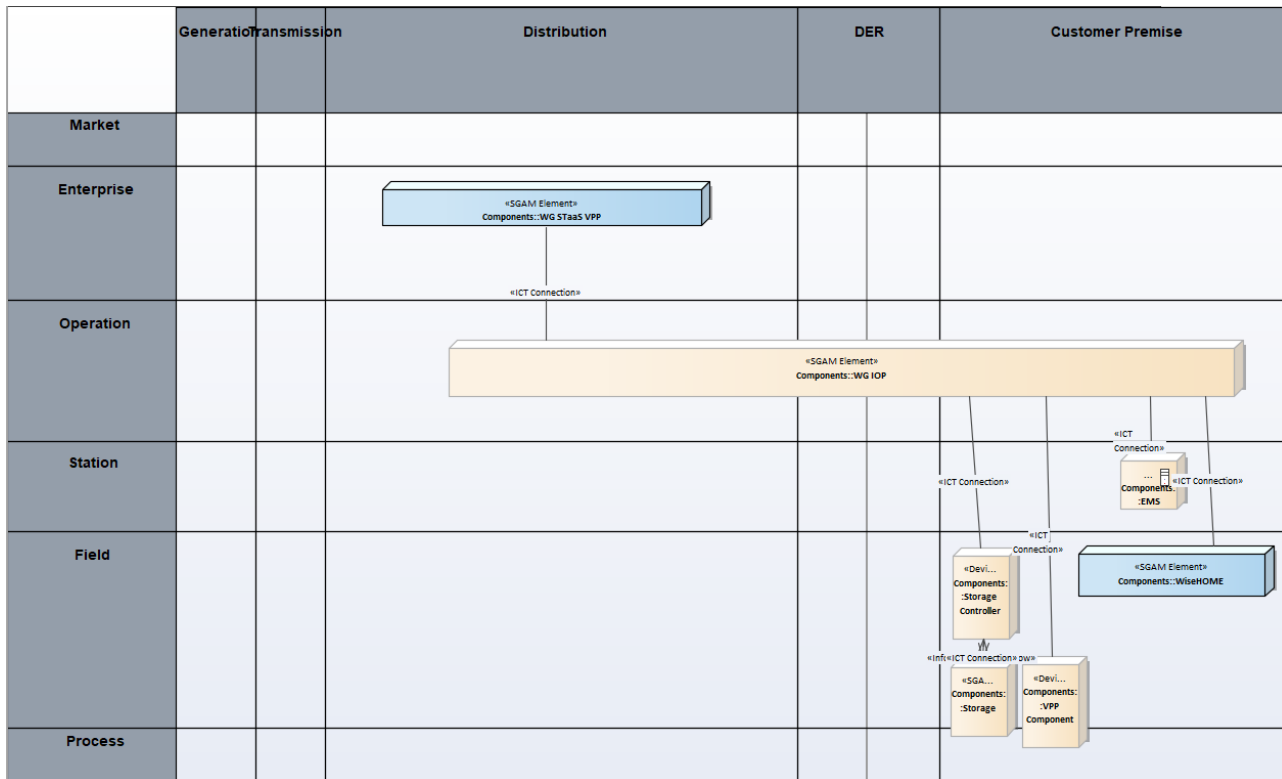


Figure 286 - SGAM Component Layer

Component	Component Type
VPP component	Device
Storage	Device
Storage controller	Device
EMS	Device
WiseHOME	SGAM element
WG IOP	SGAM element
WG Staas VPP	SGAM element

Table 229 - List of Components Participating in the Primary Use Case

## 23.4.5 SGAM COMMUNICATION LAYER

The SGAM Communication layer for this use case is presented below.

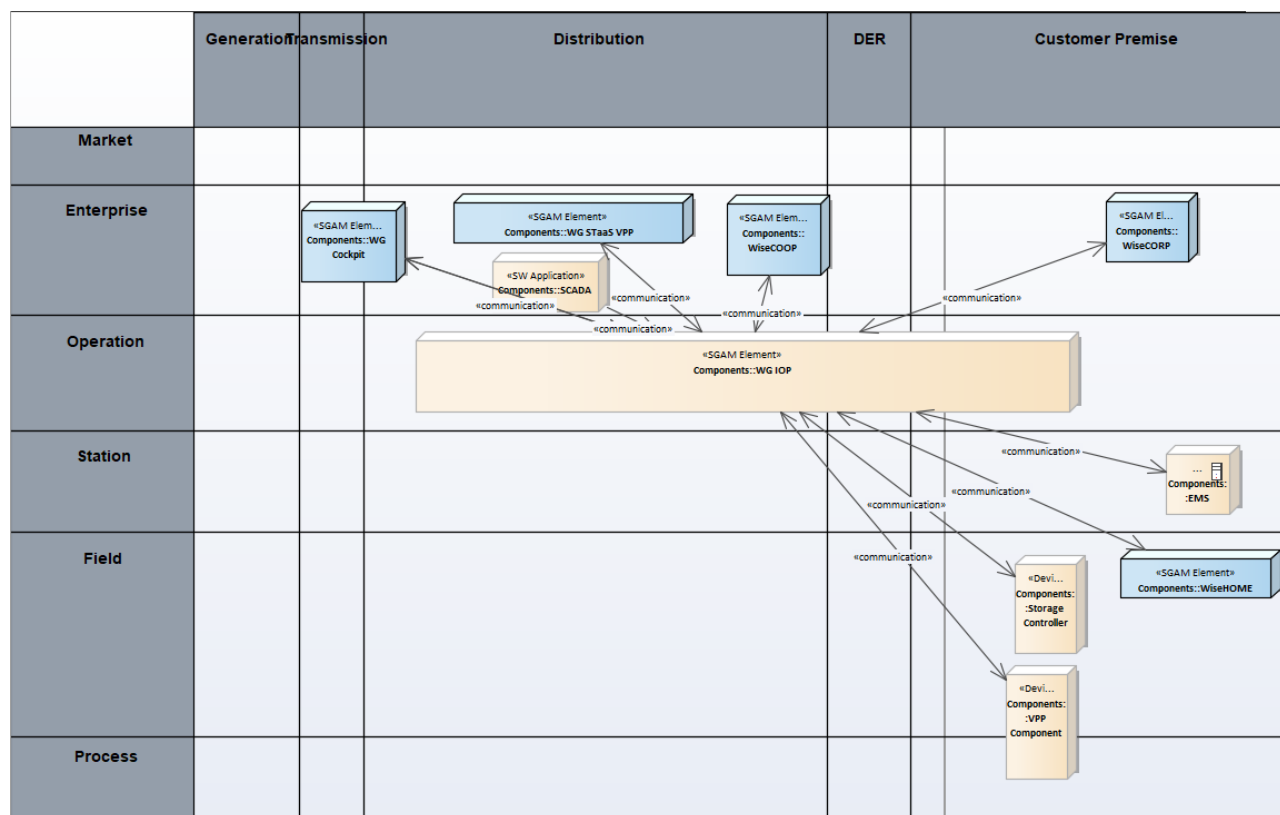


Figure 287 - SGAM Communication Layer

Communication Technology	Description
Modbus TCP/IP	
CAN	
IEC61850	
WebServices	

Table 230 - List of Communication Technologies Involved

### 23.4.6 SGAM INFORMATION LAYER

The SGAM Information layer for this use case is presented below.

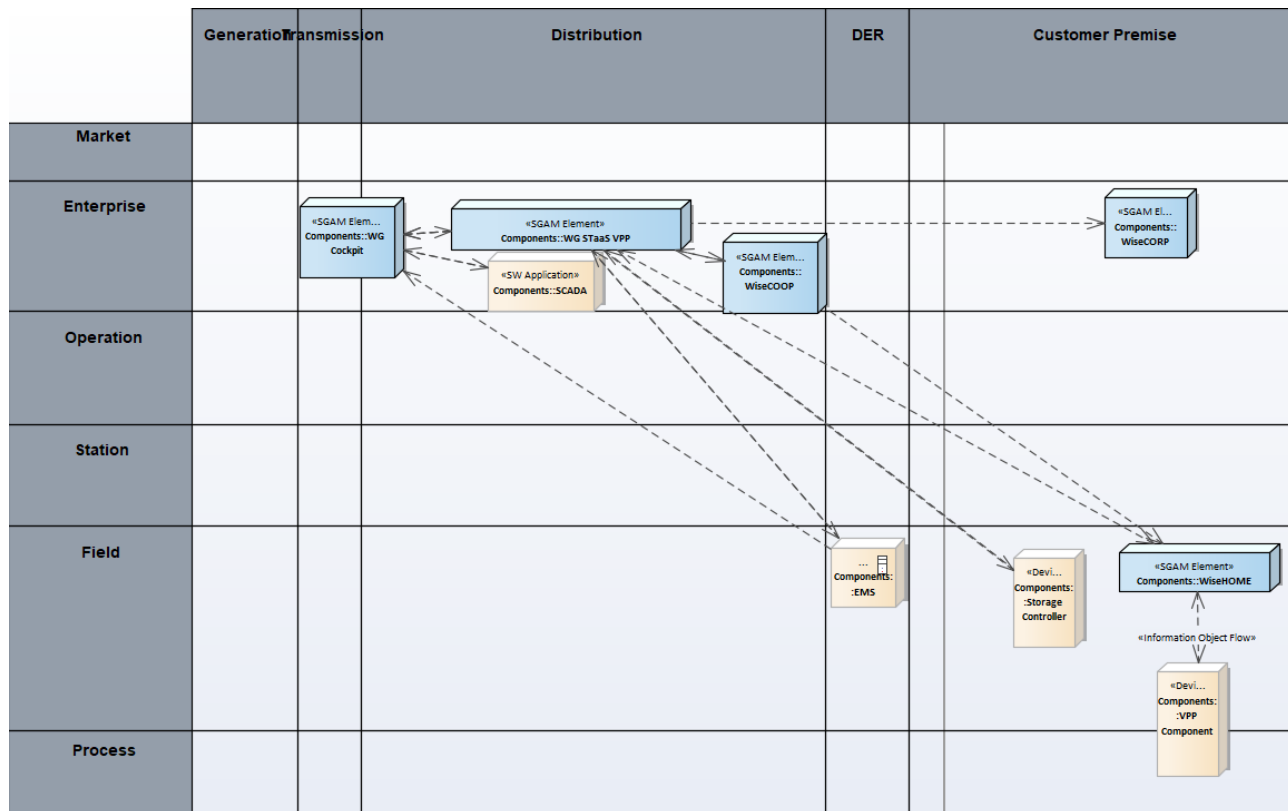


Figure 288 - SGAM Information Layer

### CANONICAL DATA MODEL

Data Models
Flexibility data model
OpenADR
VPP schedule data models

Table 231 - List of Data Models

### STANDARDS AND INFORMATION OBJECT MAPPING

Data Standards
Flexibility data models
Schedule and set point data model
Storage data model

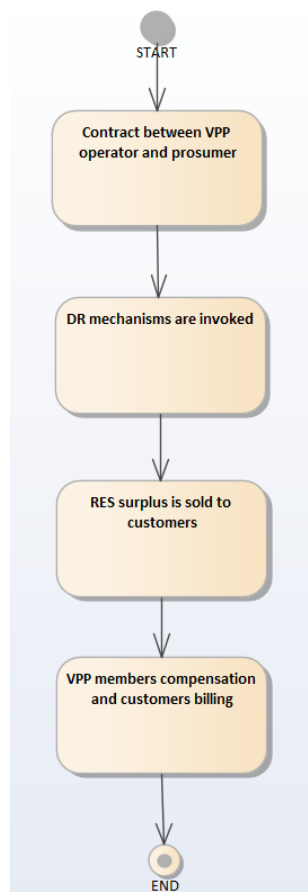
**Table 232 - List of Data Standards**

Information Objects	Data Model
Demand response request	Flexibility data model
Demand flexibility profile	Flexibility data model
Demand response	Flexibility data model
Flexibility offer	Flexibility data model
Flexibility request	Flexibility data model
Schedule data	Schedule and setpoint data model
Setpoint data	Schedule and setpoint data model

**Table 233 - List of Information Objects**

### 23.4.7 ACTIVITY DIAGRAM

The activity diagram for this use case is presented below.



**Figure 289 - Primary Use Case Activity Diagram**

### 23.4.8 SEQUENCE DIAGRAM

The sequence diagram for this use case is presented below.

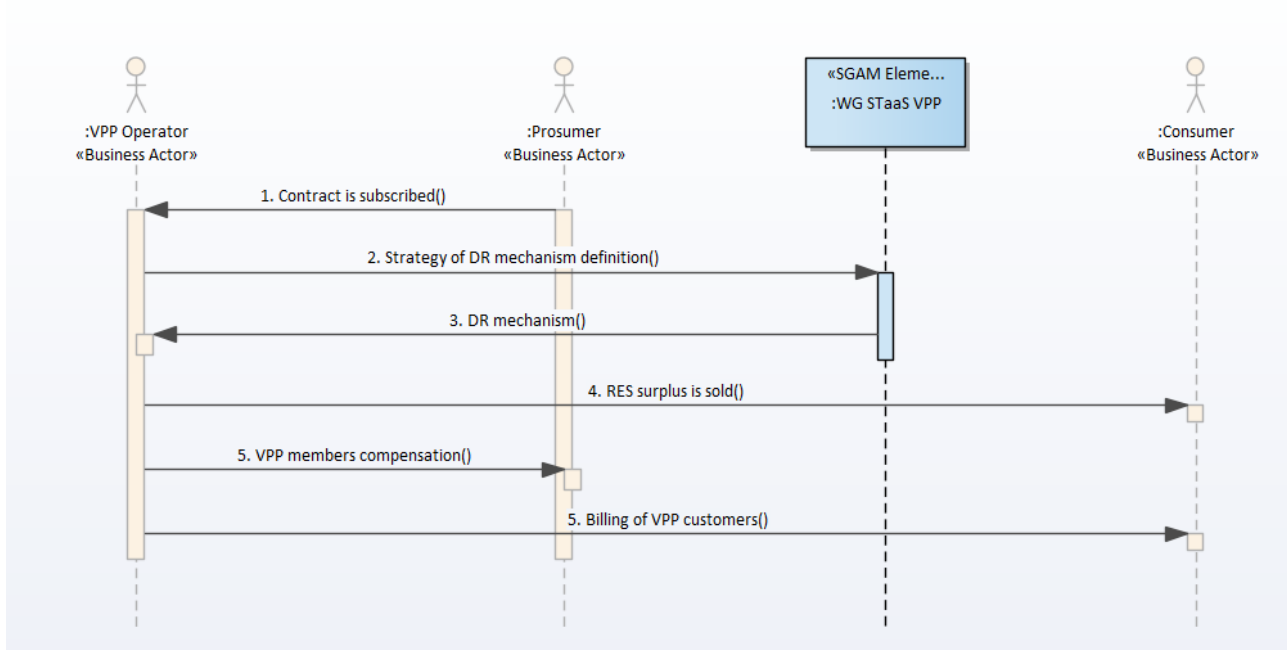


Figure 290 - Primary Use Case Sequence Diagram

## **24 APPENDIX G - ARCHITECTURE**

### **HL-UC 7: CITIZENS EMPOWERMENT IN ENERGY MARKET AND REDUCTION OF ENERGY POVERTY**



## **24.1 HL-UC 7\_PUC\_1: DYNAMIC MANAGEMENT OF DEMAND SIDE ASSETS IN TERTIARY SECTOR**

### **24.1.1 PRIMARY USE CASE DESCRIPTION**

To ensure the active engagement of businesses, industries, ESCOs, local communities and public facilities in energy markets and energy management initiatives, a corporate application tool should be available. This is a tool to facilitate the management of large infrastructures and promote the concept of smarter and responsible energy players by giving them more power and protection and also ownership, reducing their energy bill, supporting self-consumption by means of real-time data coming from all their energy devices and by means of demand response and load optimization schemes. To sum up, the goal of this PUC is to facilitate professionals (e.g. Facility Managers) on daily activities.

### 24.1.2 SECONDARY USE CASE INTERACTIONS

Under this PUC, several SUCs have been defined in order to consider different functionalities required by a facility manager.

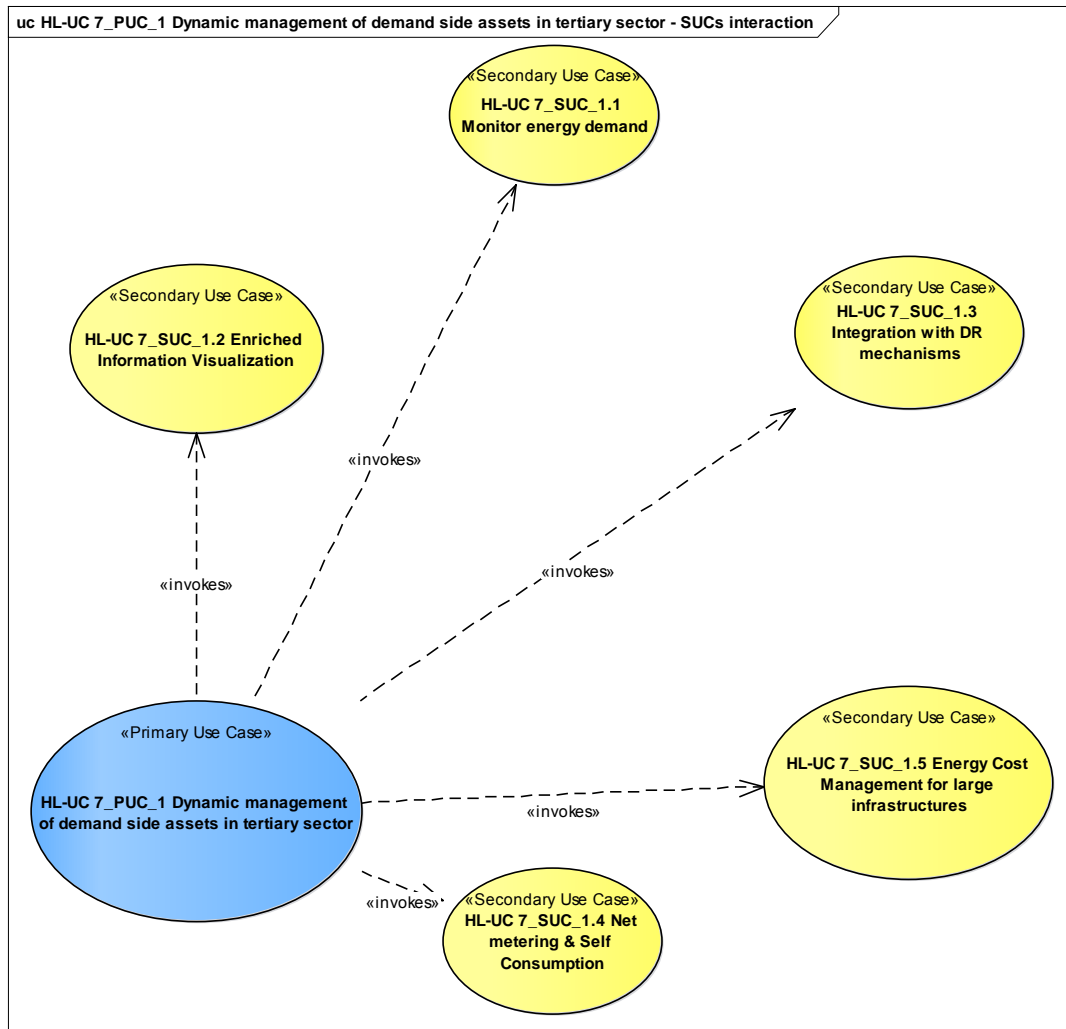


Figure 291 - SUCs Interactions Diagram

Table 234 - Table of list of participating SUCs

SUC Name	Description	Relation	PUC/SUC
HL-UC 7_SUC_1.1	Monitor energy demand		
HL-UC 7_SUC_1.2	Enriched information visualization		
HL-UC 7_SUC_1.3	Integration with DR mechanisms		
HL-UC 7_SUC_1.4	Net metering and self-consumption		
HL-UC 7_SUC_1.5	Energy cost management for large infra-structures		

### 24.1.3 SGAM FUNCTION LAYER

All features considered under this PUC fall under the *customer premise* domain. Several zones are covered:

- Field zone considers monitoring features
- Operation zone considers actions taken under demand-response campaigns
- Enterprise zone considers all features dealing with analysis of the energy usage and decision support

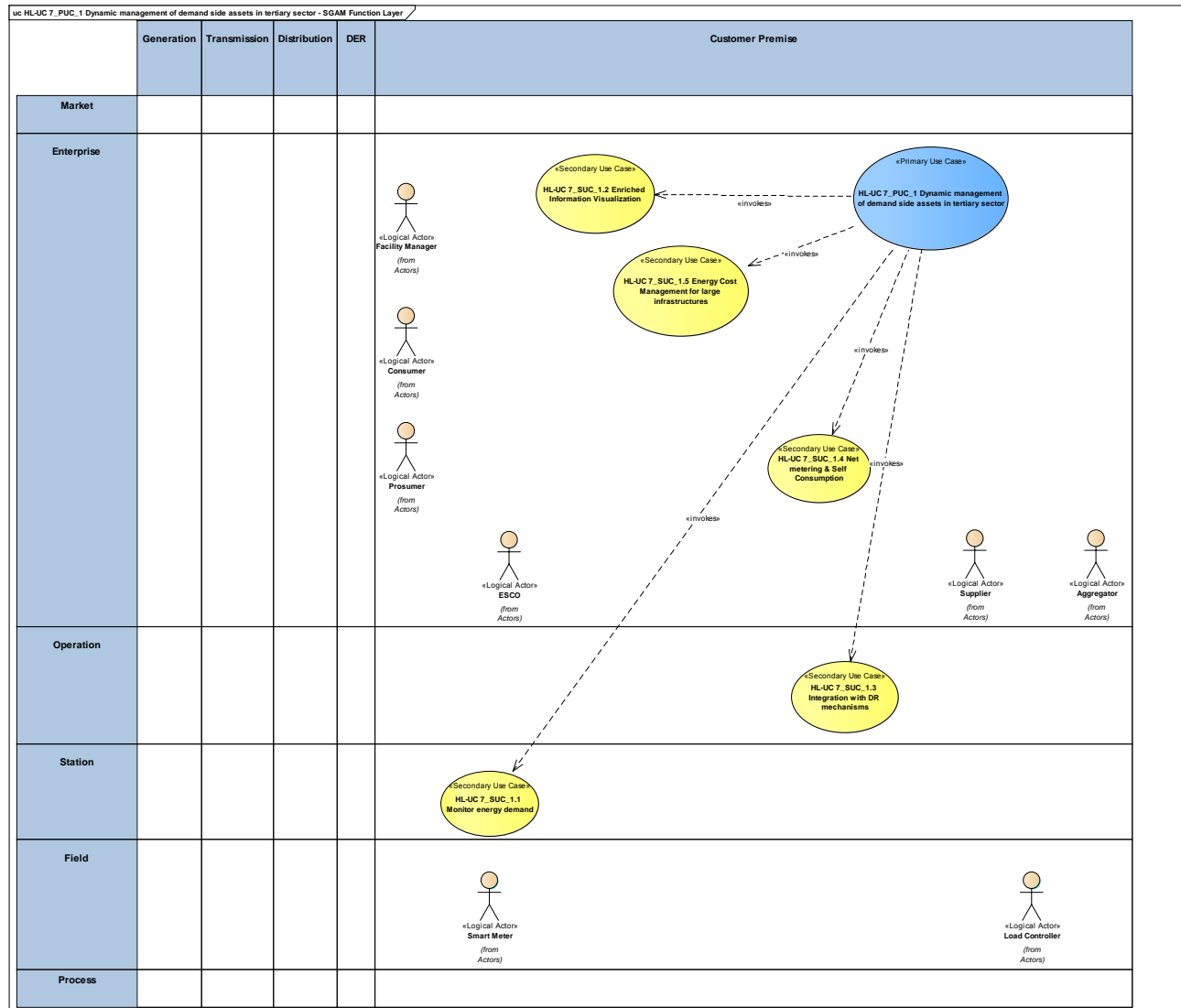


Figure 292 - SGAM Function Layer

**Table 235 - List of Actors Involved**

Actor Name	Actor Type
Prosumer	Person
RESCO	Organization
Sensor	Device
ESCO	Organization
Load controller	Device
Aggregator	Organization
Consumer	Person
Facility manager	Organization
Supplier	Organization
DSO	Organization

#### 24.1.4 SGAM COMPONENT LAYER

The main components identified under this PUC include:

- WiseCORP, which will be the core component implementing most features defined in the PUC
- Smart assets on the facility premises: including smart meters, sensors, RES controllers, storage, HVAC... These devices usually are locally controlled by a Building Management System, that provides a common interface to monitor and control those
- WiseCORP, which is the application for aggregators and will command the demand-response campaigns
- Auxiliary components, such as a tariff provider and forecast server, supporting some of the features to be implemented

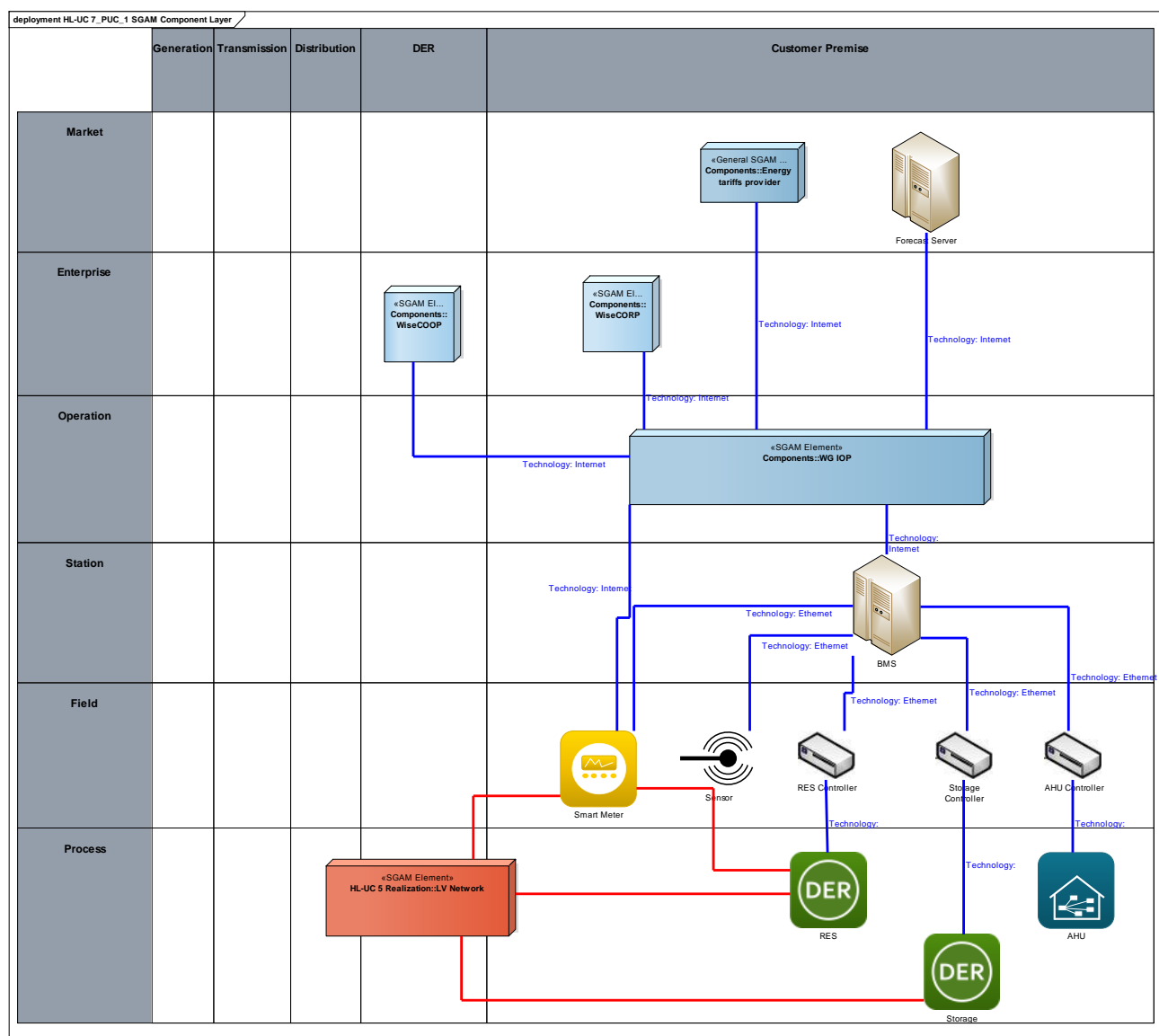


Figure 293 - SGAM Component Layer

Component	Component Type
Energy tariff provider	General SGAM Component
Forecast server	SGAM Element
WiseCOOP	SGAM Element
WiseCORP	SGAM Element
WG IOP	SGAM Element
BMS	SGAM Element
Smart meter	Smart meter
Sensor	Sensor
RES controller	Device
RES	SGAM Element
Storage controller	Device
Storage	SGAM Element
AHU controller	Device
AHU	SGAM Element
LV network	SGAM Element

**Table 236 - List of Components Participating in the Primary Use Case**

### 24.1.5 SGAM COMMUNICATION LAYER

Identified protocols of the communication layer can be classified into two groups:

- Smart appliance-related protocols for controlling the facility assets
- Communications with WiseGRID components: include the protocols considered to be enabled by the WG IOP

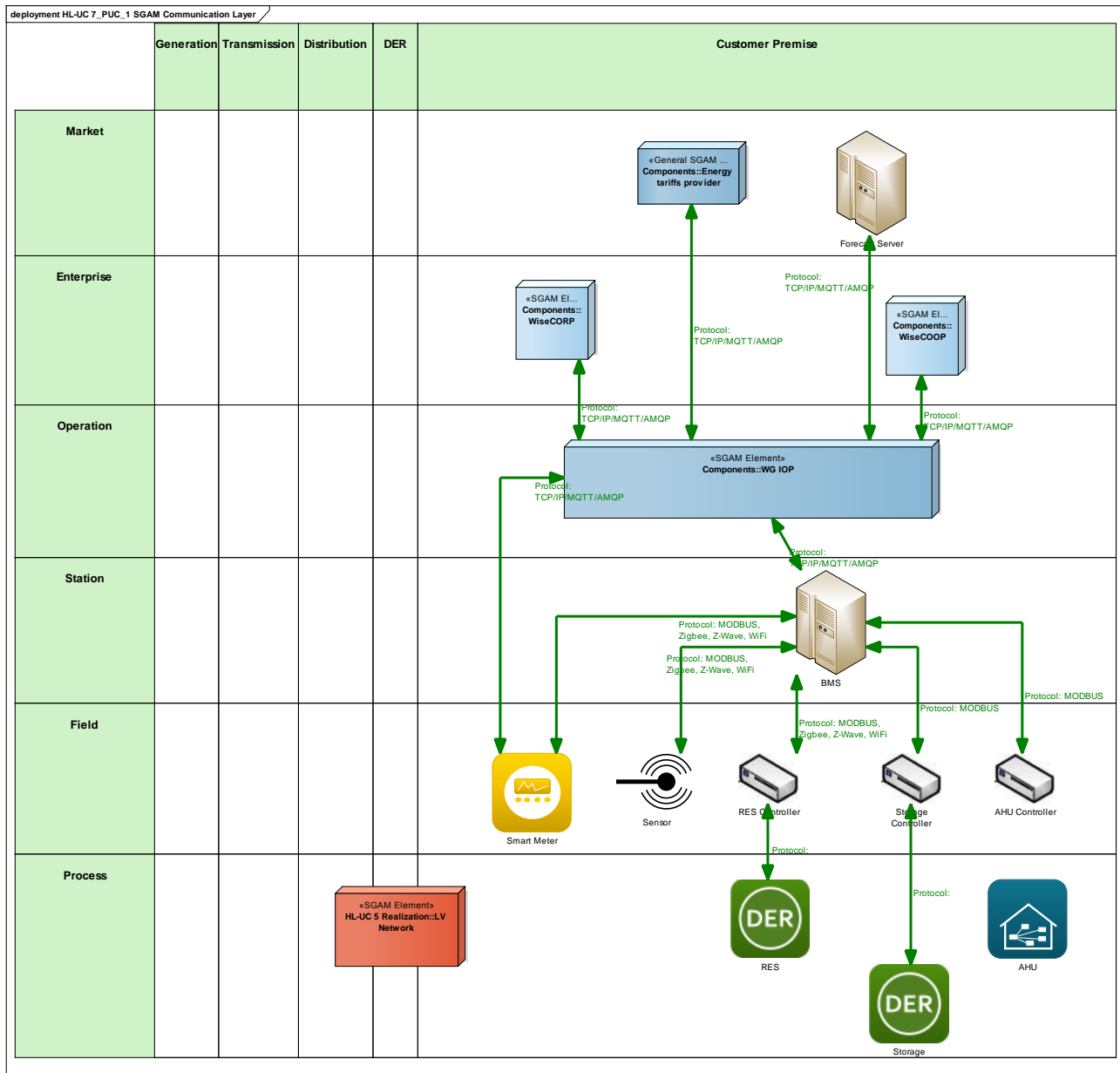


Figure 294 - SGAM Communication Layer

**Table 237 - List of Communication Technologies Involved**

Communication Technology	Description
TCP/IP	Group of protocols enabling communication between devices in a network up to the transport layer
AMQP	Open standard application layer protocol for message-oriented middleware, featuring message orientation, queuing, routing (including point-to-point and publish-and-subscribe), reliability and security
MQTT	ISO standard (ISO/IEC PRF 20922) publish-subscribe-based lightweight messaging protocol for use on top of the TCP/IP protocol
MODBUS	Serial communications protocol originally published for use with programmable logic controllers (PLCs). Simple and robust, it has become a de facto standard communication protocol and is now a commonly available means of connecting industrial electronic devices
Zigbee	IEEE 802.15.4-based specification for a suite of high-level communication protocols used to create personal area networks with small, low-power digital radios, such as for home automation, medical device data collection, and other low-power low-bandwidth needs, designed for small scale projects which need wireless connection
Z-Wave	Wireless communications protocol used primarily for home automation



This PUC needs of the retrieval of different information items from the facilities, namely:

- | deployment HL-UC 7_PUC_1 SGAM Information Layer |            |              |              |     |                  |  |  |  |  |
|---|------------|--------------|--------------|-----|------------------|--|--|--|--|
|   | Generation | Transmission | Distribution | DER | Customer Premise |  |  |  |  |
| Market  |            |              |              |     |                  |  |  |  |  |
| Enterprise                                      |            |              |              |     |                  |  |  |  |  |
| Operation                                       |            |              |              |     |                  |  |  |  |  |
| Station   |            |              |              |     |                  |  |  |  |  |
| Field   |            |              |              |     |                  |  |  |  |  |
| Process   |            |              |              |     |                  |  |  |  |  |

### D3.1 WiseGRID Architecture, Data Models, Standards and Data Protection (V1)

## CANONICAL DATA MODEL

The following data models are envisaged necessary to cover the different information items identified within this PUC

Data Models
Energy tariff
Forecast data model
Flexibility data model (USEF)
Building data model
DLMS/COSEM

Table 238 - List of Data Models

## STANDARDS AND INFORMATION OBJECT MAPPING

Table 239 - List of Data Standards

Data Standards
Energy tariff
Forecast data model
Flexibility data model (USEF)
Building data model
DLMS/COSEM

**Table 240 - List of Information Objects**

Information Objects	Data Model
Building data	Building data model
Building thermal model	Building data model
Energy metering	Building data model
Indoor environmental conditions	Building data model
Setpoint data	Building data model
Energy metering	DLMS/COSEM
Tariff definition	Energy tariff
Load/Production forecast	Forecast data model
Demand Response signal	Flexibility data model (USEF)
Demand flexibility profile	Flexibility data model (USEF)
Demand response request	Flexibility data model (USEF)
Flexibility offer	Flexibility data model (USEF)
Flexibility request	Flexibility data model (USEF)

### 24.1.7 ACTIVITY DIAGRAM

The following activity diagram summarizes the steps considered under this PUC to achieve a proper monitoring and optimization of the energy demand of the facilities under control.

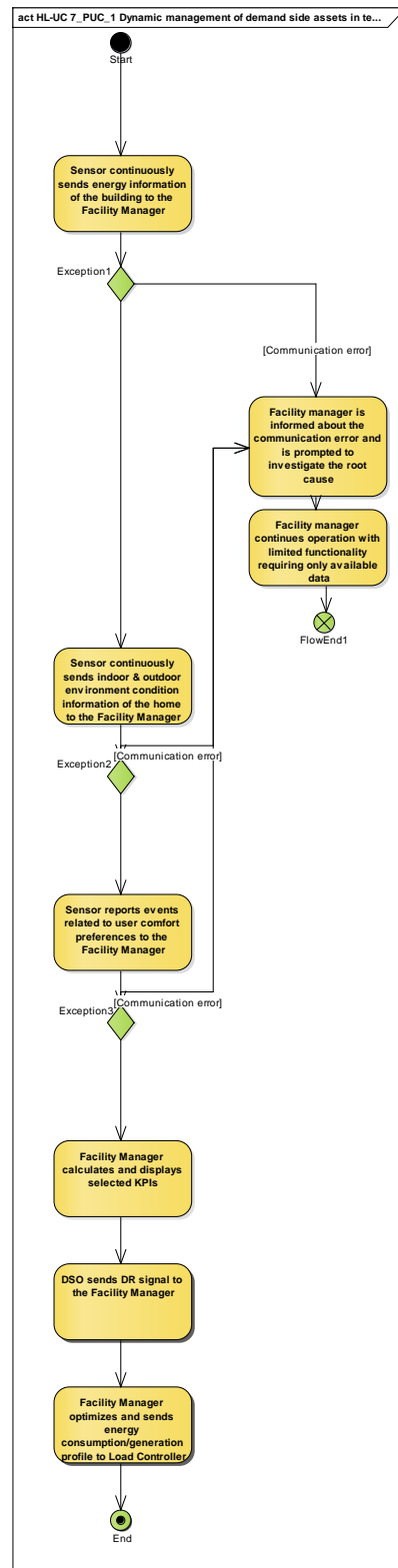


Figure 296 - Primary Use Case Activity Diagram

## 24.1.8 SEQUENCE DIAGRAM

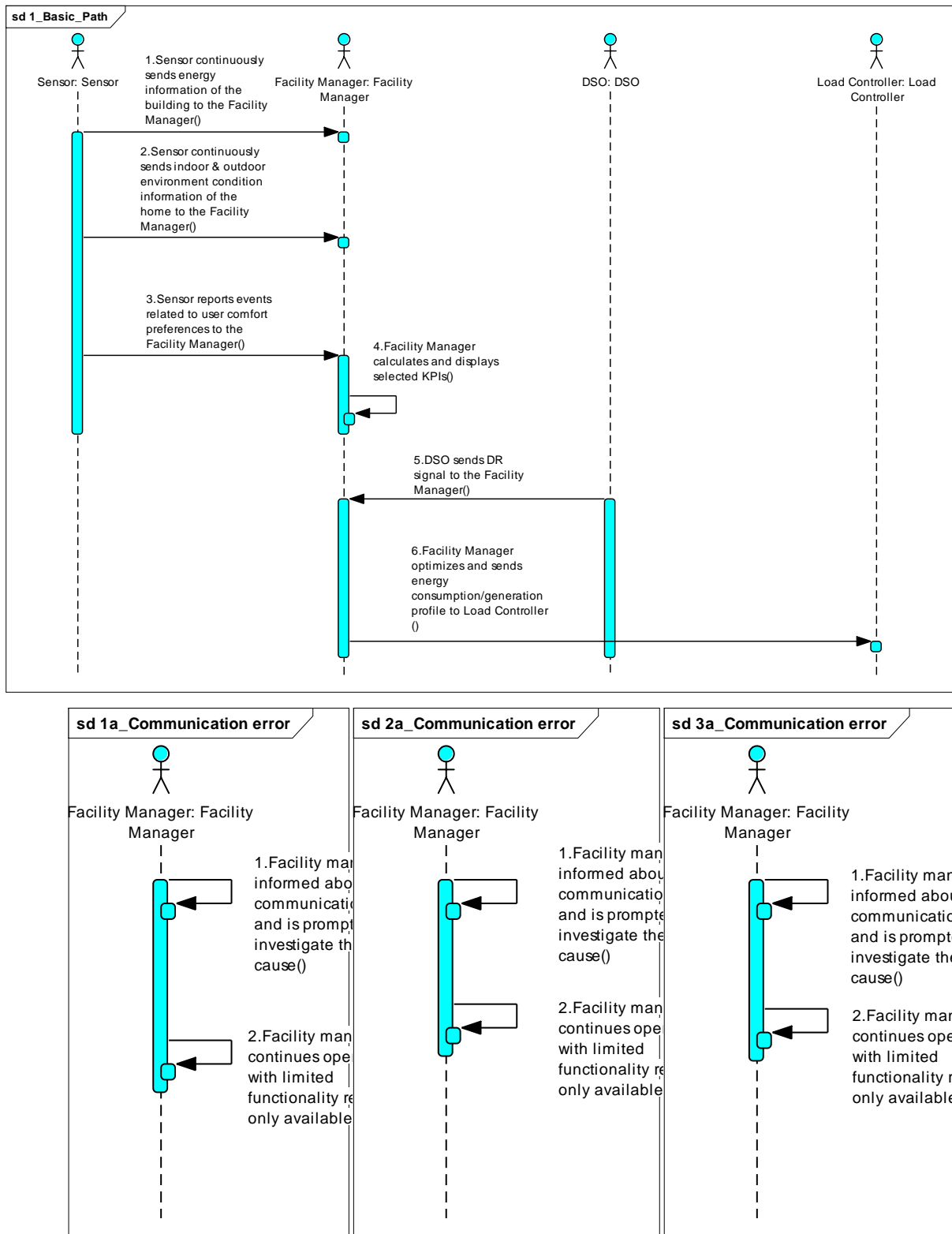


Figure 297 - Primary Use Case Sequence Diagram

## 24.2 HL-UC 7\_PUC\_2: DYNAMIC AGGREGATION OF DEMAND SIDE ASSETS AND ACTIVE PARTICIPATION INTO ENERGY MARKET

### 24.2.1 PRIMARY USE CASE DESCRIPTION

To support the active involvement of traditional (Suppliers) and new business (Aggregators, cooperatives) roles in energy markets a portfolio management tool will support the engagement of Consumers and Prosumers in emerging business models (e.g. real-time pricing, demand response).

The tool is an application for energy Suppliers, Aggregators, local communities and cooperatives of Consumers and Prosumers (and other intermediary companies) to help domestic and small businesses, Consumers and Prosumers achieve better energy deals: better services, prices and opportunities to participate in ancillary service markets will be offered to the final Consumers/Prosumers. This includes aggregation models such as VPP where the Aggregator (or other intermediate) gathers a portfolio and operates them as a unified and flexible resource on the energy market. In summary, the goal of this PUC is to provide the engine that facilitates energy stakeholders (Aggregators & Suppliers).

### 24.2.2 SECONDARY USE CASE INTERACTIONS

Under this PUC, several SUCs are defined to cover all functionalities needed by an aggregator or retailer managing a portfolio of prosumers with demand side management capabilities.

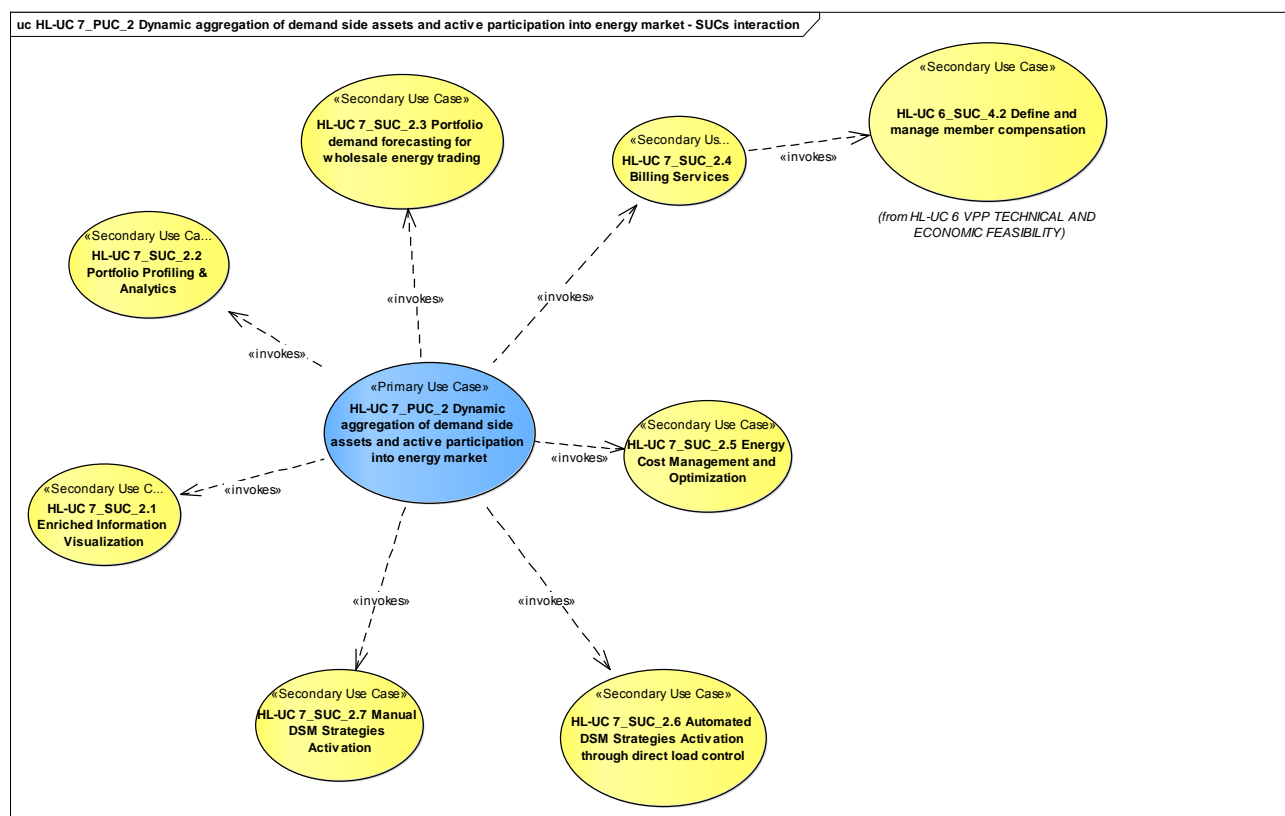


Figure 298 - SUCs Interactions Diagram

**Table 241 - Table of list of participating SUCs**

SUC Name	Description	Relation	PUC/SUC
HL-UC 7_SUC_2.1	Enriched information visualization		
HL-UC 7_SUC_2.2	Portfolio profiling and analytics		
HL-UC 7_SUC_2.3	Portfolio demand forecasting for wholesale energy trading		
HL-UC 7_SUC_2.4	Billing services	invokes	HL-UC 6_SUC_4.2 Define and manage member compensation
HL-UC 7_SUC_2.5	Energy cost management and optimization		
HL-UC 7_SUC_2.6	Automated DSM strategies activation through direct load control		
HL-UC 7_SUC_2.7	Manual DSM strategies activation		

### 24.2.3 SGAM FUNCTION LAYER

Due to the nature of the targeted actor (aggregators and suppliers), all SUCs fall under the *customer premise* domain. The considered functionalities fall both under the *enterprise* zone - mainly dealing with information analysis and operation optimization - and the *operation* zone - where SUCs that take actions to actually change the energy usage patterns are considered.

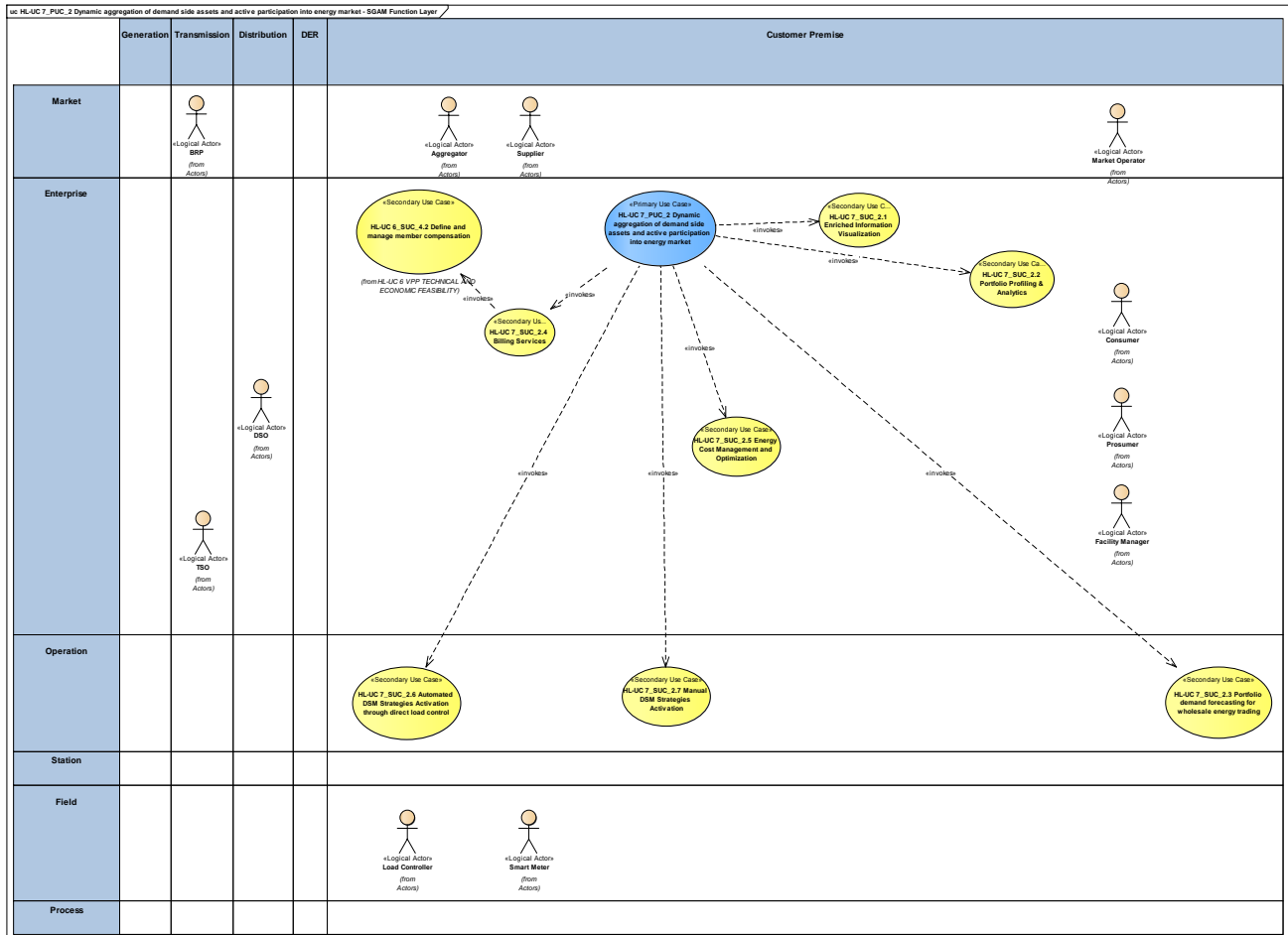


Figure 299 - SGAM Function Layer

Table 242 - List of Actors Involved

Actor Name	Actor Type
Consumer	Person
ESCO	Organization
Forecast provider	Organization
Facility manager	Organization
Smart meter	Device
Prosumer	Person
Load controller	Device
Sensor	Device



Actor Name	Actor Type
Supplier	Organization
Market operator	Organization
BRP	Organization

#### 24.2.4 SGAM COMPONENT LAYER

The identified components can be classified in the following categories:

- WiseCOOP, which is the core application implementing these features - targeting aggregators and retailers
- Field devices, providing energy metering information needed by the aggregator
- WiseHOME and WiseCORP, which represent the communication channel of the aggregator with the members of the portfolio
- WG Cockpit, which may trigger support mechanisms to the WiseCOOP - through the ancillary services market
- Other modules interacting or supporting the operations of the aggregator, such as the wholesale energy market, the weather forecast provider or the energy tariff provider

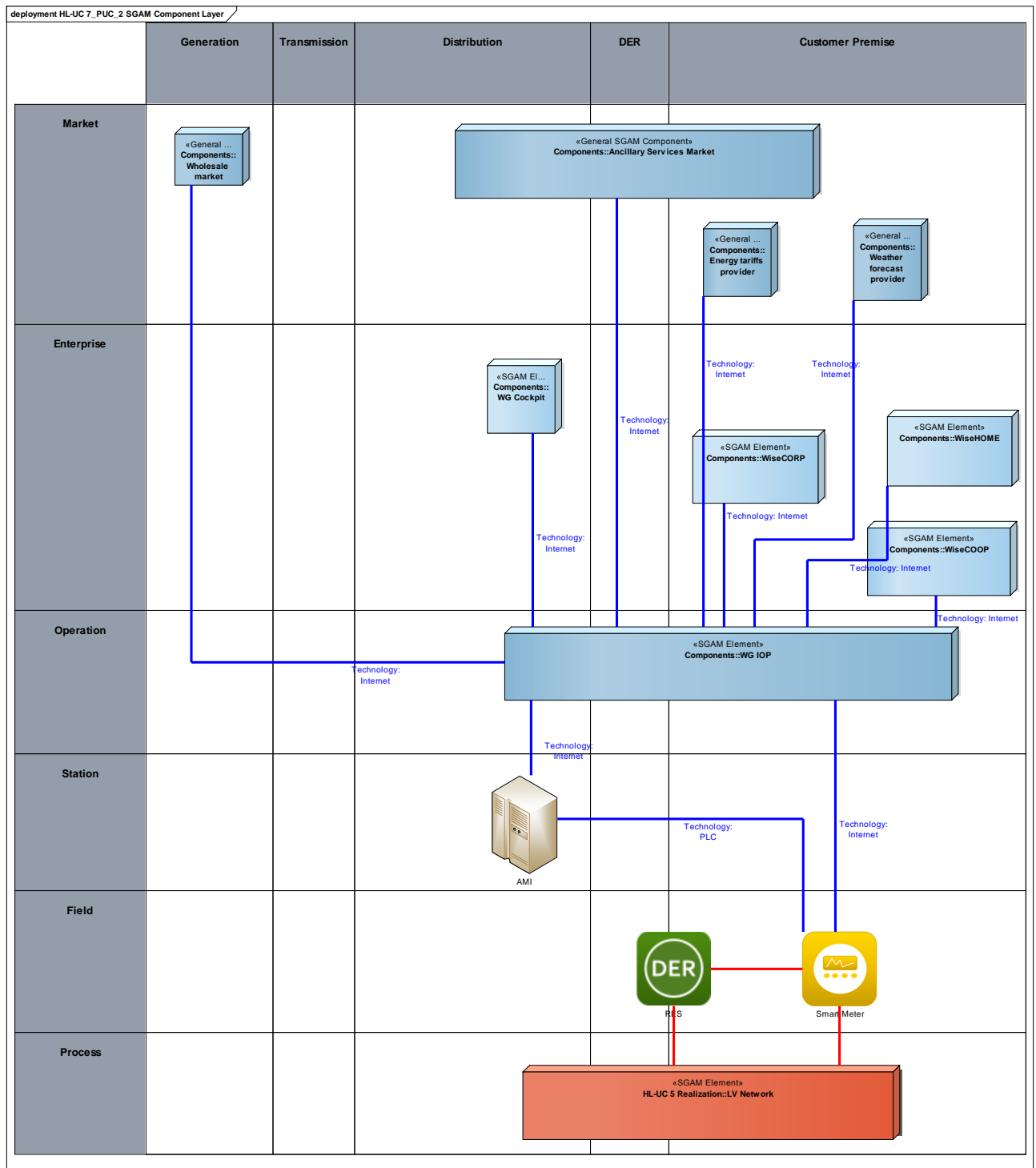


Figure 300 - SGAM Component Layer

**Table 243 - List of Components Participating in the Primary Use Case**

Component	Component Type
WiseCOOP	SGAM Element
WiseCORP	SGAM Element
WiseHOME	SGAM Element
WG Cockpit	SGAM Element
WG IOP	SGAM Element
Wholesale market	General SGAM Component
Ancillary services market	General SGAM Component
Energy tariffs provider	General SGAM Component
Weather forecast provider	General SGAM Component
AMI	SGAM Element
RES	Device
Smart meter	Smart meter
LV Network	SGAM Element

## 24.2.5 SGAM COMMUNICATION LAYER

Most communications foreseen under this PUC will be handled by the WG IOP, therefore enabled by the communication protocols supported by this component.

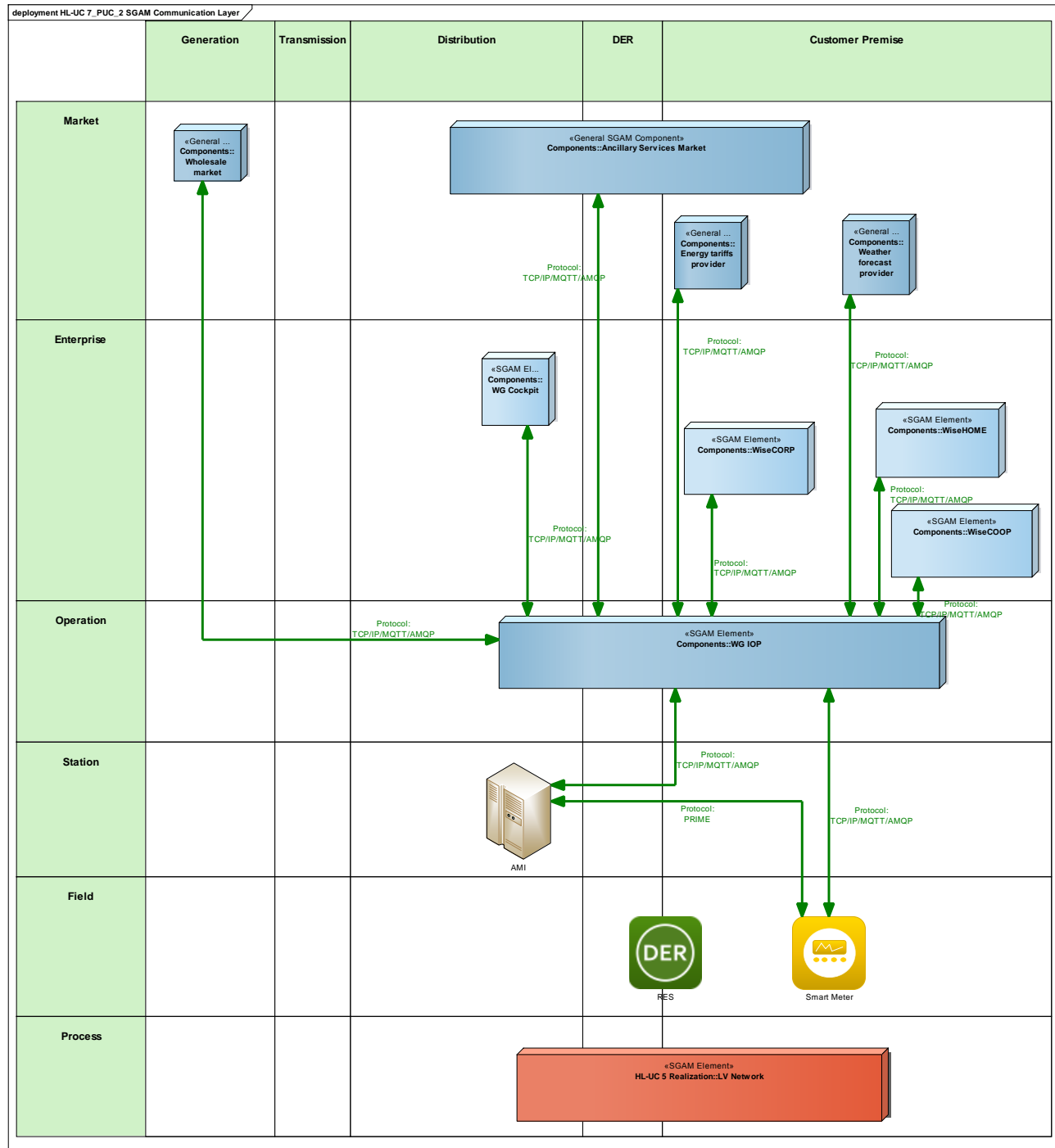


Figure 301 - SGAM Communication Layer

**Table 244 - List of Communication Technologies Involved**

Communication Technology	Description
TCP/IP	Group of protocols enabling communication between devices in a network up to the transport layer
MQTT	ISO standard (ISO/IEC PRF 20922) publish-subscribe-based lightweight messaging protocol for use on top of the TCP/IP protocol
AMQP	Open standard application layer protocol for message-oriented middleware, featuring message orientation, queuing, routing (including point-to-point and publish-and-subscribe), reliability and security
PRIME	Specification for narrow band powerline communication

## 24.2.6 SGAM INFORMATION LAYER

The main information items handled within this PUC include:

- Energy metering information
- Load and production forecasts
- Flexibility requests and offers for providing ancillary services
- Demand response-related messaging, including dynamic energy prices
- Wholesale market energy bids

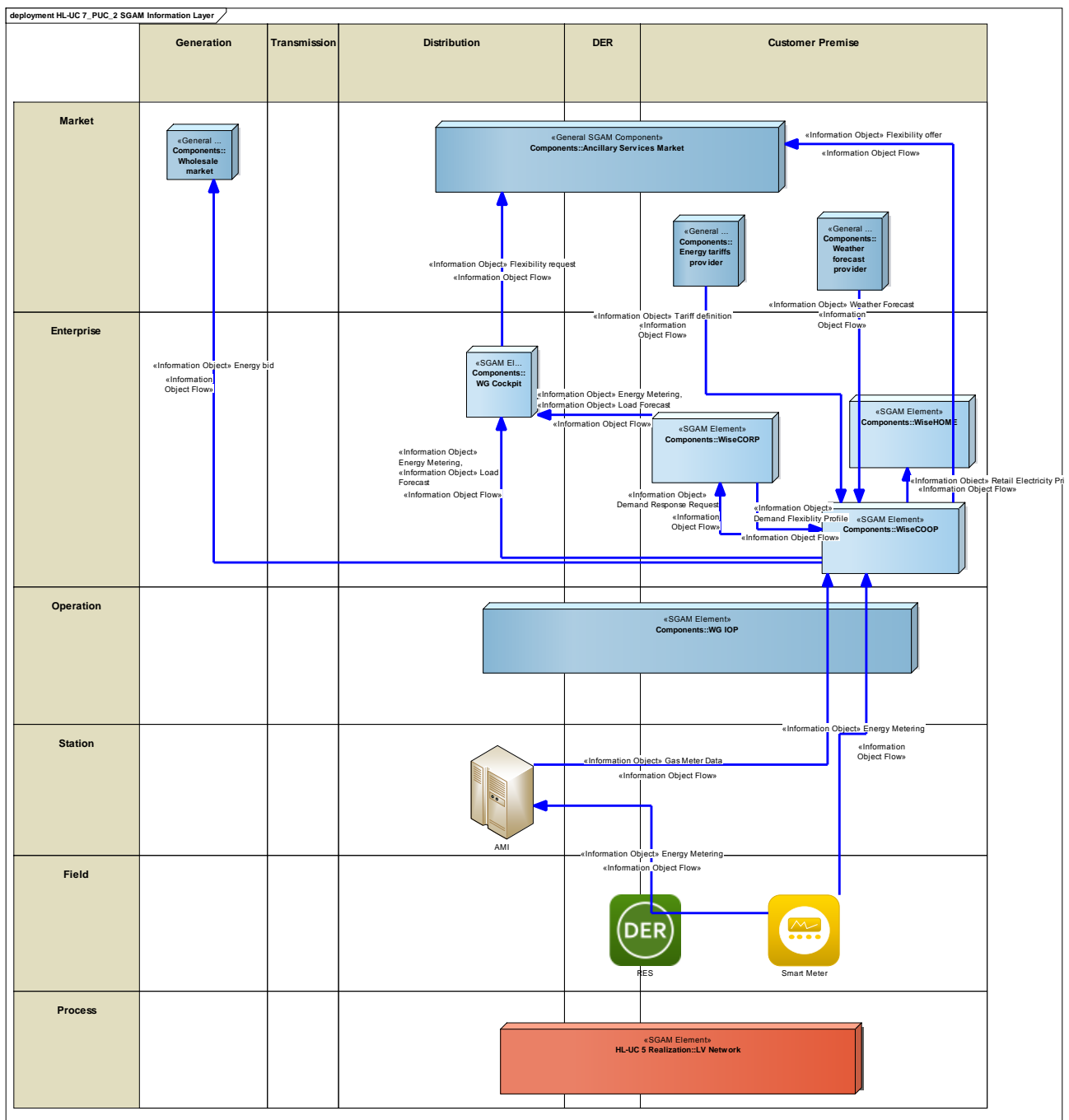


Figure 302 - SGAM Information Layer

## CANONICAL DATA MODEL

Canonical data models are needed for the identified information items, which are grouped in the following categories:

**Table 245 - List of Data Models**

Data Models
DLMS/COSEM
Weather forecast
Energy tariff
Flexibility Data Model (USEF)
Energy bids

## STANDARDS AND INFORMATION OBJECT MAPPING

The following standards have been identified related to the information items handled within this PUC:

**Table 246 - List of Data Standards**

Data Standards
DLMS/COSEM
CIM
Flexibility Data Model (USEF)

**Table 247 - List of Information Objects**

Information Objects	Data Model
Energy metering	DLMS/COSEM CIM
Weather forecasts	CIM
Demand flexibility	Flexibility Data Model (USEF)

### 24.2.7 ACTIVITY DIAGRAM

The following activity diagram shows the main actions taken by the aggregator in order to handle its portfolio of prosumers.

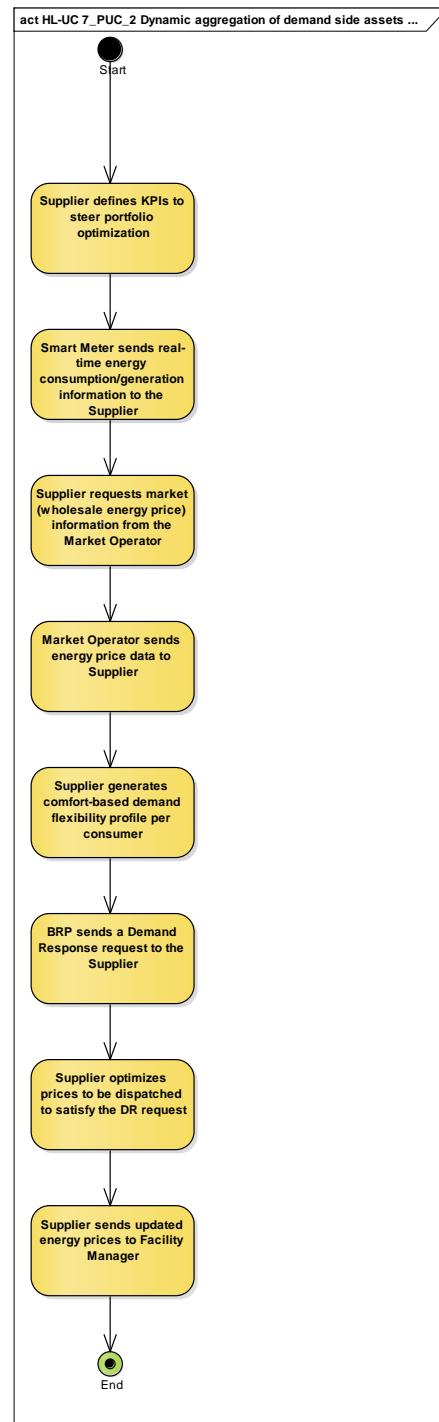


Figure 303 - Primary Use Case Activity Diagram



## 24.2.8 SEQUENCE DIAGRAM

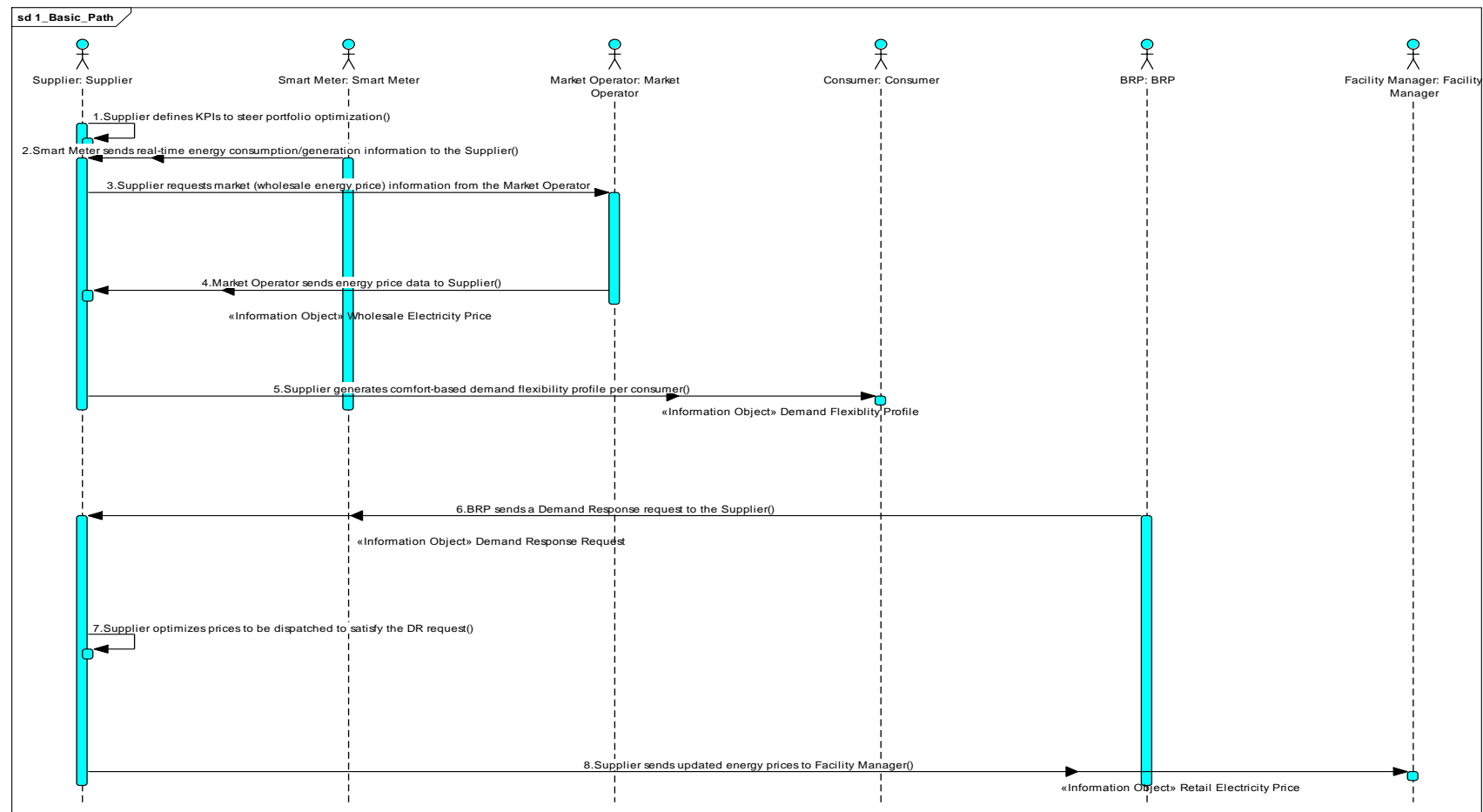


Figure 304 - Primary Use Case Sequence Diagram

## 24.3 HL-UC 7\_PUC\_3: CUSTOMERS ENGAGEMENT FOR ACTIVE MARKET PARTICIPATION

### 24.3.1 PRIMARY USE CASE DESCRIPTION

Towards citizen's empowerment in energy market and reduction of energy poverty, as the main objective of HL-UC 7, we have to ensure that even the small (residential) clients move from passive entities to active elements of the electricity grid. In order to ensure client participation, information about electricity usage and energy market (retail & ancillary services) operation should be available in an appealing but not intrusive way.

This can be done with a personalized application for individual domestic Consumers and Prosumers covering different types of functionalities like: real-time monitoring of consumption and production, participating in demand response programs (visualizing DR signals, e.g. price information), alerts, energy saving tips, etc.

This is actually the main objective of this PUC: to establish a dynamic channel of communication with the domestic Consumers and Prosumers, enabling their transformation to active grid elements.

### 24.3.2 SECONDARY USE CASE INTERACTIONS

This Secondary Use Case functionality-wise maps exactly to the functionalities of the WiseHOME tool, which is meant to be the single interface for citizens who want to engage in the energy markets through the Wise-GRID implementation.

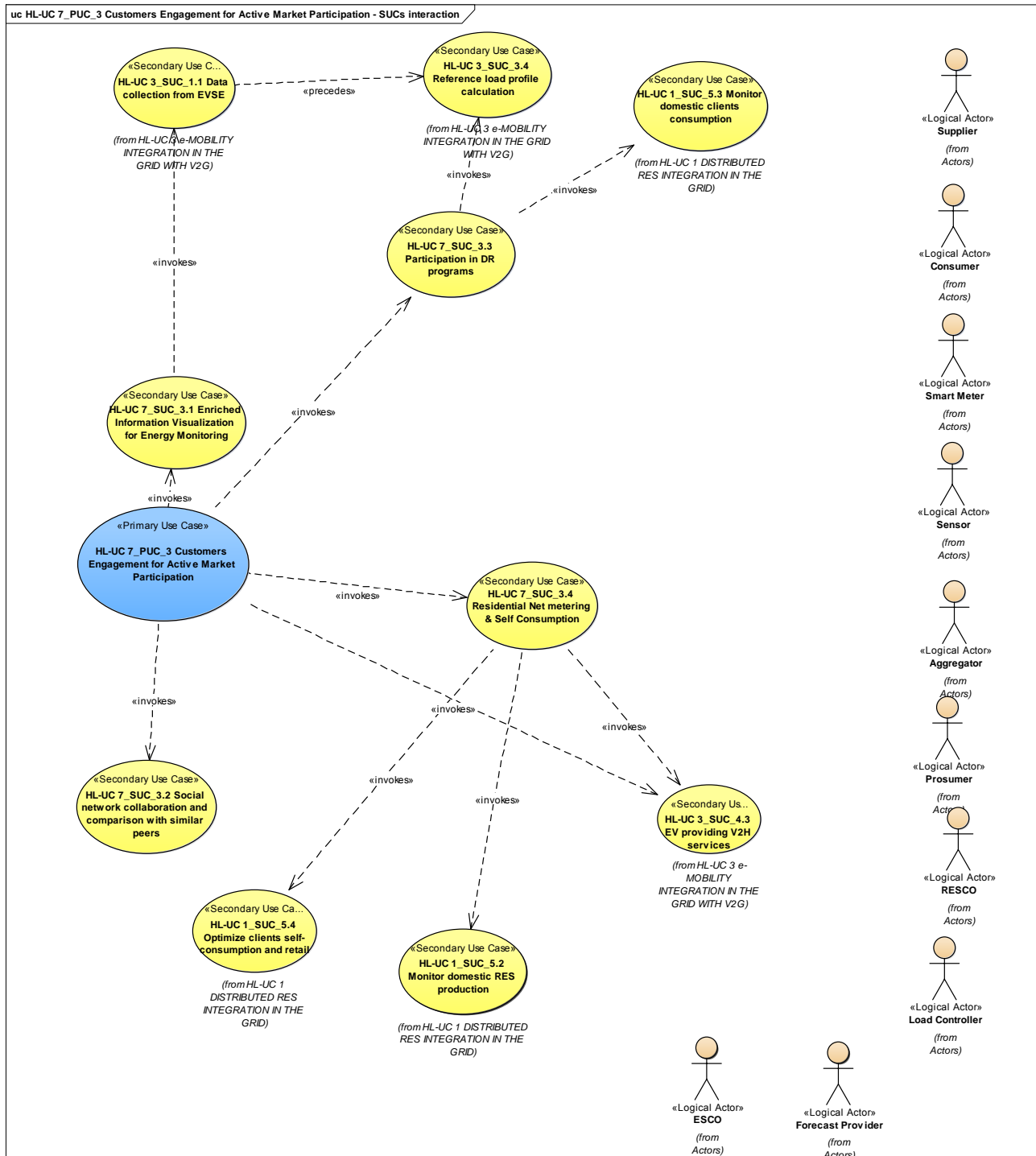


Figure 305 - SUCs Interactions Diagram

**Table 248 - Table of list of participating SUCs**

SUC Name	Description	Relation	PUC/SUC
Enriched Information Visualization for Energy Monitoring	This SUC provides an enriched visualisation tool for a better understanding of Pro/Consumers about their energy consumption.	Invokes	SUC_3.1
Social network collaboration and comparisons with peers	A primary purpose of this SUC and the tools that will implement it is to further develop the community (using open source software including sandbox modules that will enable the community members to extend its functionality or create new ones).	Invokes	SUC_3.2
Participation in DR programs	The main objective of this SUC is to develop and integrate advanced mechanisms for demand response that will enable final clients/Prosumers (household), individually or by means of third-party actors (retailers, Aggregators, etc.), to actively participate in the energy markets.	Invokes	SUC_3.3
Residential Net metering & Self Consumption	The main objective of this SUC is to allow the end-users of the application (residential clients) to participate in net metering & self-consumption concepts, promoting that way the idea of green, carbon-free living.	Invokes	SUC_3.4
Reference load profile calculation	This secondary use case describes how the Wise EVP calculates the reference load profile per regulation area.	Invokes	PUC3 SUC_3.4

deployment HL-UC 7\_PUC\_3 Customers Engagement for Active Market Participation - SGAM Function Layer



### Table 249 - List of Actors Involved

Actor Name	Actor Type
Aggregator	Organization
Supplier	Organization
RESCO	Organization
Prosumer	Person
Consumer	Person

Actor Name	Actor Type
Sensor	Device
Load Controller	Device
Smart Meter	Device

This section illustrates the main components that will play a role in the Demand Response framework as well as their associations, which will further on lead to the information flows.



**Table 250 - List of Components Participating in the Primary Use Case**

Component	Component Type
WiseCOOP	SGAM Element
WiseHOME	SGAM Element
WG IOP	SGAM Element
Sensor	Device
Electronic Meter	Device
HVAC Controller	Device
Load Controller	Device
CHP Controller	Device
EVSE	Device
Smart Meter	Device
EV	Device
RES	Device
HVAC	Device
Storage	Device
CHP	Device



### 24.3.5 SGAM COMMUNICATION LAYER

This section outlines the main communication technologies that will be utilised in the reference implementation of the WiseGRID project.

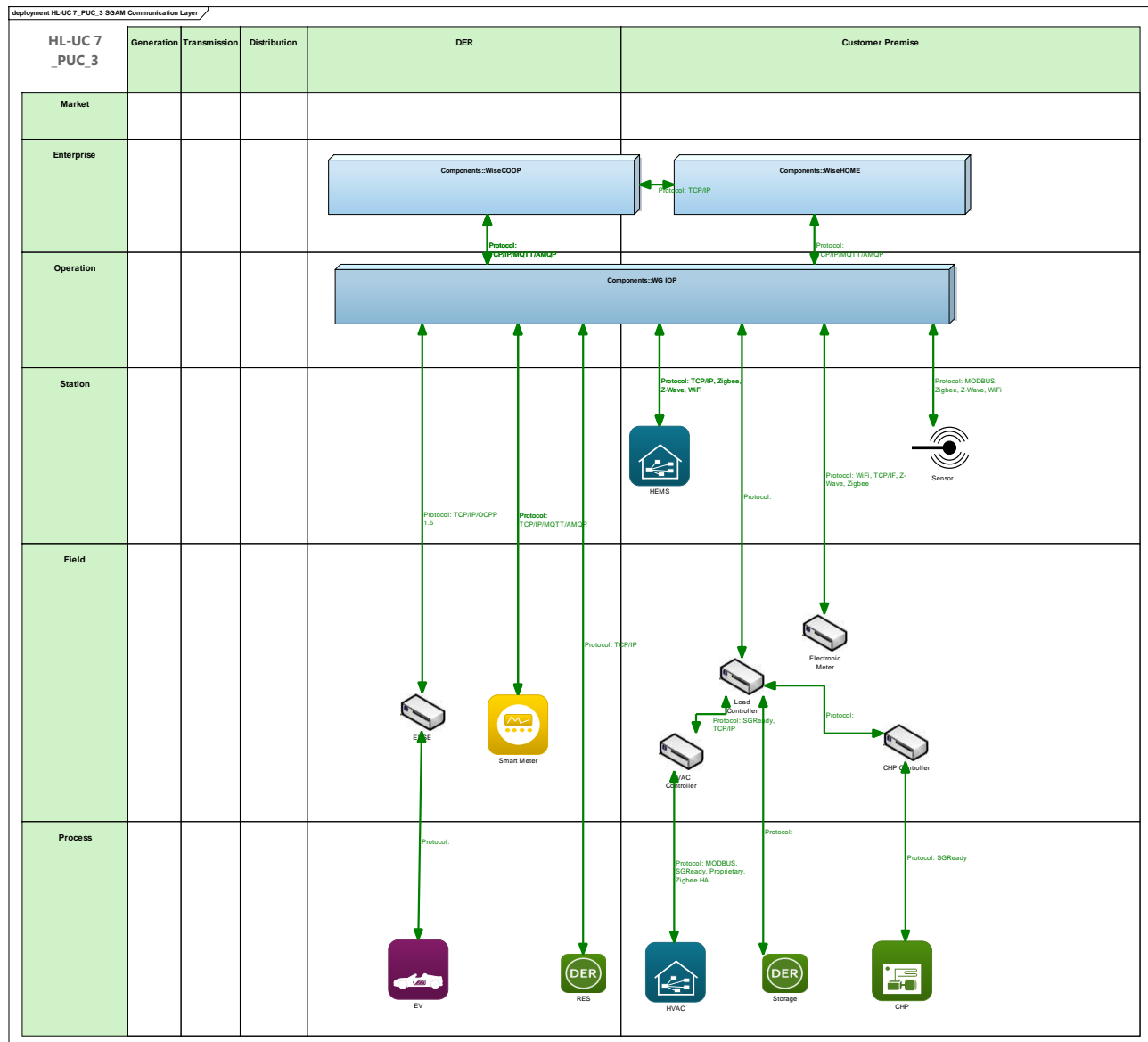


Figure 308 - SGAM Communication Layer

Table 251 - List of Communication Technologies Involved

Communication Technology	Description
TCP/IP	Group of protocols enabling communication between devices in a network up to the transport layer.
AMQT	Open standard application layer protocol for message-oriented middleware, featuring message orientation, queuing, routing (including point-to-point and publish-and-subscribe), reliability and security

Communication Technology	Description
MQTT	ISO standard (ISO/IEC PRF 20922) publish-subscribe-based lightweight messaging protocol for use on top of the TCP/IP protocol
OCPP1.5	The Open Charge Point Protocol is an open standard which describes a method enabling electrical vehicles to communicate with a central system.
Modbus	Serial communications protocol originally published for use with programmable logic controllers (PLCs). Simple and robust, it has become a de facto standard communication protocol and is now a commonly available means of connecting industrial electronic devices. Will probably be needed in WiseGRID for the interaction with RES or HVAC systems.
SGReady	Upcoming technology for the communication of smart grid ready devices. Its application will focus on HVAC and CHPs within WiseGRID.
Zigbee, Z-Wave, WiFi	Popular wireless communication technologies that may be employed for intra-building communications in order to collect sensor readings and send actuation commands. The final technology selection will depend on availability of infrastructure and choice of new equipment to install.

## 24.3.6 SGAM INFORMATION LAYER

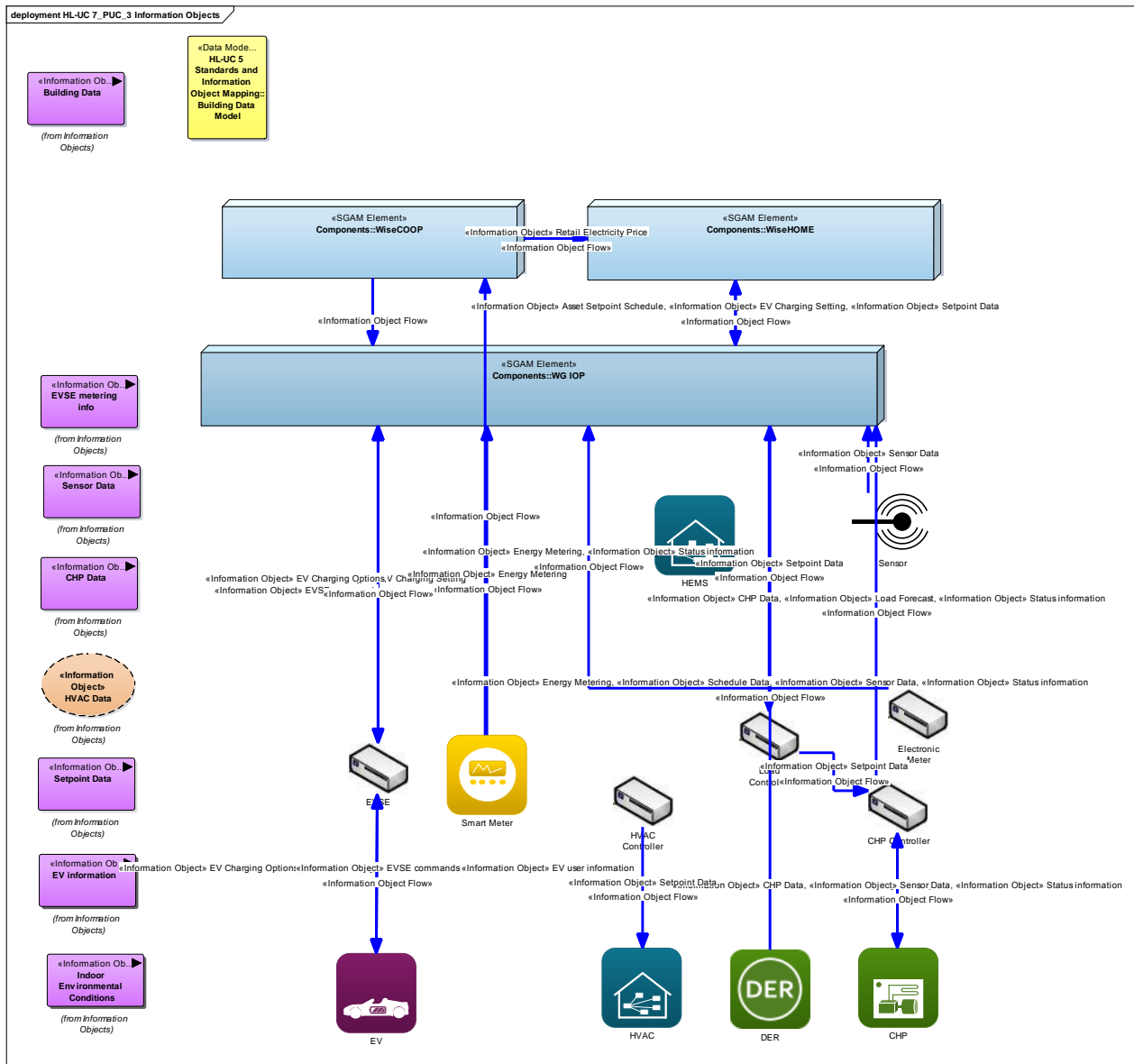


Figure 309 - SGAM Information Layer

## CANONICAL DATA MODELS

**Table 252 - List of Data Models**

Data Models
Building Information Model (BIM)
Universal Smart Energy Framework (USEF)
DLMS/COSEM
OpenADR
Energy asset/device operational status models
User preference models

## STANDARDS AND INFORMATION OBJECT MAPPING

This secondary use case will leverage the following standards in order to align its outputs with ongoing activities by other parties so as to ensure replicability of the WiseGRID solution.

**Table 253 - List of Data Standards**

Data Standards
Building Information Model (BIM)
Universal Smart Energy Framework (USEF)
DLMS/COSEM
OpenADR

The correspondence between the information objects of the previous models and the relevant standards is illustrated in the table below.

**Table 254: List of Information Objects**

Information Objects	Data Model
Asset Geolocation Data	BIM
Billing Data	OpenADR
Building Data	BIM
Demand Response Offer	USEF
Demand Response Request	USEF
Dynamic Storage Device Information	OpenADR
Energy Metering	DLMS/COSEM
Gas Meter Data	DLMS/COSEM
Indoor Environmental Conditions	BIM
Load Forecast	USEF
PV Forecast	USEF
PV Production Data	USEF
Retail Electricity Price	OpenADR
Tariff Definition	OpenADR

## 24.3.7 ACTIVITY DIAGRAM

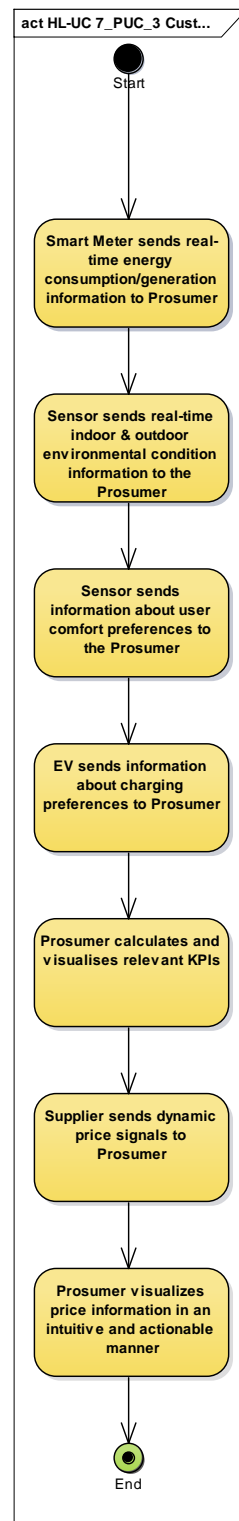


Figure 310 - Primary Use Case Activity Diagram

### 24.3.8 SEQUENCE DIAGRAM

The following sequence diagram depicts the fundamental process that needs to be followed in order for households to participate in the energy market via dynamic pricing tariff plans, either via manual response or through automated control of residential assets.

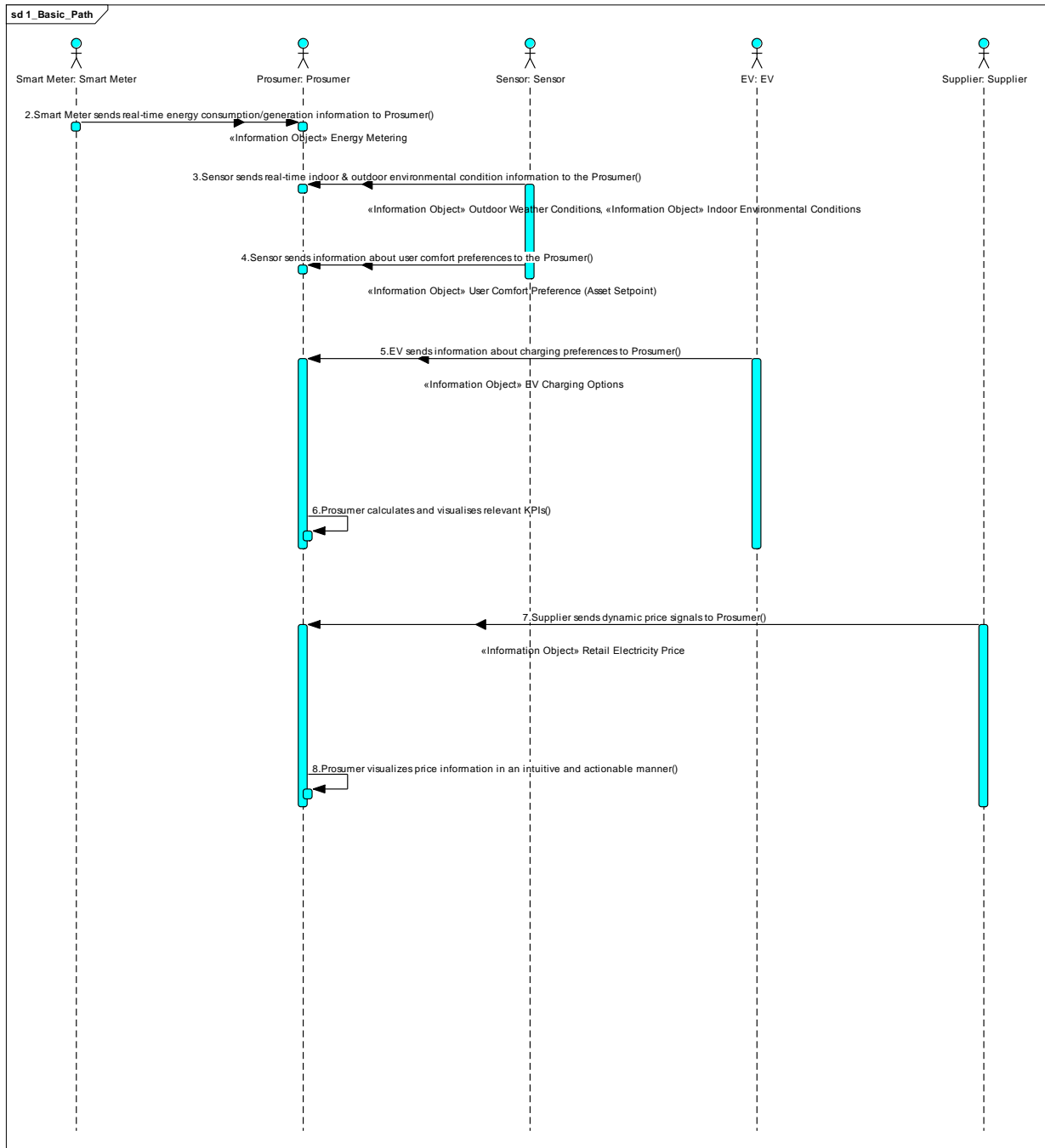


Figure 311 - Primary Use Case Sequence Diagram

## **25 APPENDIX H - PRIVACY & DATA PROTECTION LIST OF POSSIBLE CONTROLS**



## 25.1 POSSIBLE CONTROLS

### *Minimizing the amount of personal data*

*Objective:* to reduce the severity of risks by limiting the amount of personal data to what is strictly necessary to achieve a defined purpose.

### *Managing personal data retention periods*

*Objective:* to reduce the severity of risks by ensuring that personal data is not retained for longer than necessary.

### *Informing data subjects*

*Objective:* to ensure that the subjects are informed.

### *Obtaining the consent of data subjects*

*Objective:* to allow data subjects to make a free, specific and informed choice.

### *Managing persons within the organization who have legitimate access*

*Objective:* to reduce the risks associated with persons within the organization (employees, seconded subcontractors, interns and visitors) who have legitimate access to personal data.

### *Managing third parties with legitimate access to personal data*

*Objective:* to reduce the risk that legitimate access to personal data by third parties may pose to the data subjects' civil liberties and privacy.

### *Monitoring logical access controls*

*Objective:* to limit the risks that unauthorized persons will access personal data electronically.

### *Partitioning personal data*

*Objective:* to reduce the possibility that personal data can be correlated and that a breach of all personal data may occur.

### *Encrypting personal data*

*Objective:* to make personal data unintelligible to anyone without access authorization.

### *Anonymizing personal data*

*Objective:* to remove identifying characteristics from personal data.

### ***Protecting personal data archives***

*Objective:* to define all procedures for preserving and managing the electronic archives containing the personal data.

### ***Managing personal data violations***

*Objective:* to have an operational organization that can detect and treat incidents that may affect the data subjects' civil liberties and privacy.

### ***Tracing the activity on the IT system***

*Objective:* to allow early detection of incidents involving personal data and to have information that can be used to analyze them or provide proof in connection with investigations.

### ***Combating malicious codes***

*Objective:* to protect access to public (Internet) and uncontrolled (partner) networks, workstations and servers from malicious codes that could affect the security of personal data.

### ***Reducing software vulnerabilities***

*Objective:* to reduce the possibility to exploit software properties (operating systems, business applications, database management systems, office suites, protocols, configurations, etc.) to adversely affect personal data.

### ***Reducing hardware vulnerabilities***

*Objective:* to reduce the possibility to exploit hardware properties (servers, desktop computers, laptops, devices, communications relays, removable storage devices, etc.) to adversely affect personal data.

### ***Reducing the vulnerabilities of computer communications networks***

*Objective:* to reduce the possibility to exploit communications networks properties (wired networks, Wi-Fi, radio waves, fiber optics, etc.) to adversely affect personal data.

### ***Reducing the vulnerabilities of paper documents***

*Objective:* to reduce the possibility to exploit paper documents properties to adversely affect personal data.

### ***Reducing vulnerabilities related to the circulation of paper documents***

*Objective:* to reduce the possibility to exploit paper document circulation properties (within an organization, delivery by vehicle, mail delivery, etc.) to adversely affect personal data.

### ***Create procedures to address CoT and CoS***

*Objective:* To ensure that after such a change, no personal data is available

### ***Permitting the exercise of the right to object***

*Objective:* to ensure that individuals have the opportunity to object to the use of their personal data.

### ***Monitoring the integrity of personal data***

*Objective:* to be warned in the event of an unwanted modification or disappearance of personal data.

### ***Allowing the exercise of the right to correct***

*Objective:* to ensure that individuals may correct, add, update, block or delete their personal data.

### ***Permitting the exercise of the direct access right***

*Objective:* to ensure that individuals have an opportunity to know about their personal data.

### ***Reducing the vulnerabilities of individuals***

*Objective:* to reduce the possibility to exploit people (employees, individuals who are not part of an organization but are under its responsibility, etc.) by adversely affecting personal data.

### ***Non-collection of contentious data-items***

*Objective:* to avoid collection of data-items against client's wishes.

### ***No collection of identifiable information, only pseudonyms, or anonym data***

*Objective:* to prevent identification of the data subject through collected data.

### ***Purpose limitation, e.g. taking appropriate measures to ensure that personal data is only used for the purposes defined beforehand and not used for other related or unrelated purposes***

*Objective:* to ensure that personal data is only used for the purposes defined beforehand and not used for other related or unrelated purposes.

### ***Active measure to preclude the use of particular data-items in the making of particular decisions***

*Objective:* to ensure that decisions are made based only on due data-items.

### ***Limits on the use of information for a very specific purpose, with strong legal, organisational and technical safeguards preventing its application to any other purpose***

*Objective:* to ensure that information is used for the specified purpose and for nothing more than that.

### ***Active measures to preclude the disclosure of particular data-items***

*Objective:* to ensure that only required and permitted data-items are disclosed.

### ***Minimization of personal data retention by destroying it as soon as the transaction for which it is needed is completed***

*Objective:* to ensure compliance with legislation and to prevent misuse of personal data.

### ***Destruction schedules for personal information***

*Objective:* to ensure compliance with legislation and to prevent misuse of personal data.

***Use of mathematical methods without collecting and registration source data to reach goals***

*Objective:* to avoid collection of non-authorized data without prejudice to reach goals.

***Clear and consistent communication of purpose and goals of data collection***

*Objective:* to ensure that the client and other interested parties are clearly informed of purpose and goals of data collection.

***Make a privacy policy, code of conduct or certify the processing of the data to be more transparent***

*Objective:* to establish rights, responsibilities and boundaries in order to make data processing transparent to those involved.

***Not transferring the source data, but only the outcomes***

*Objective:* to avoid disclosure of undue data.

***Give the individual control over his data, for example by a secured website portal***

*Objective:* to ensure that the individual has control over his data according to his rights and responsibilities.

***Introduction automated controls on the data quality***

*Objective:* to ensure that data quality is monitored and maintained on a regular basis.

***Design, implementation and resourcing of a responsive complaints-handling system, backed by serious sanctions and enforcement powers***

*Objective:* to ensure that clients have a way of communicating their requests and complaints and to ensure that these are timely and adequately addressed.

***Audit***

*Objective:* this is a generic control to ensure that all implemented controls are in place.

## 26 APPENDIX I - ARCHITECTURE DEFINITIONS

## 26.1 LIST OF DEFINITIONS

### ***Controller***

The 'data controller' means, unless expressly designated by legislative or regulatory provisions relating to this processing, a person, public authority, department or any other organization who determines the purposes and means of the data processing.

### ***Data subject***

An identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. [Directive-1995-46]

### ***Feared event***

Incident that affects availability, integrity or confidentiality of the primary assets.

### ***Likelihood***

Estimation of the possibility that a risk occurs. It essentially depends on the level of exploitable vulnerabilities and on the level capabilities of the risk sources to exploit them.

### ***Measure (Control)***

Action to be taken to treat risks. It may be to avoid, modify/reduce, share/transfer or retain them.

### ***Personal data***

Information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. [Directive-1995-46].

### ***Personal data breach***

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community. [Directive-2009-136]

### ***Primary asset***

Process (those of the processing of personal data and those required by [Act-I&L]) or data (processed or used by legal process) whose availability, integrity or confidentiality has to be protected.

### ***Processing of personal data***

Mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction. [Directive-1995-46]

### ***Risk***

Scenario describing a feared event and all threats that make it possible. It is estimated in terms of severity and likelihood.

### ***Risk management***

Iterative process that allows to objectively manage the privacy risks on the data subjects concerned by a processing of personal data. It essentially consists in appreciating them (identification, estimation in terms of severity and likelihood, and evaluation for comparison), treating them (determining and implementing proportionate measures), accepting residual risks, communicating (stakeholder consultation, results presentation...), and monitoring changes over time (context, risk, measures...).

### ***Risk source***

Person or non-human source that can cause a risk, accidentally or deliberately.

### ***Severity (Impact)***

Estimation of the magnitude of potential impacts on the data subjects' privacy. It essentially depends on the level of identification of the personal data and prejudicial effect of the potential impacts.

### ***Supporting asset***

Asset on which some primary assets rely. It can be hardware, software, networks, people, paper or paper transmission channels.

### ***Threat***

Typical action used by risk sources that may cause a feared event.

### ***Vulnerability***

Characteristic of a supporting asset, that can be used by risk sources and allowing threats to occur.

## **27 APPENDIX J - STANDARDS AND INTEROPERABLE DATA MODELS STANDARDS**



## 27.1 LIST OF STANDARDS

In the table down below are listed the standard associated to the Smart Grids fields that are within this deliverable document.

SUBFIELD	APPLICABLE STANDARDS
AMI Backhaul Network	IEC 60870-5-101, IEC 60870-5-102, IEC 60870-5-103, IEC 60870-5-104, IEC 60904 series, IEC 61131, IEC 61158 series, IEC 61334-4-32, IEC 61334-4-41, IEC 61334-4-511, IEC 61334-4-512, IEC 61334-5-1, IEC 61334-61, IEC 61400-1, IEC 61400-2, IEC 61400-25-2, IEC 61400-25-3, IEC 61400-25-4, IEC 61400-3, IEC 61499, IEC 61724, IEC 61730, IEC 61784, IEC 61784-1, IEC 61836, IEC 61850-6, IEC 61850-7-1, IEC 61850-7-2, IEC 61850-7-3, IEC 61850-7-4, IEC 61850-7-410, IEC 61850-7-420, IEC 61850-80-4, IEC 61850-8-1, IEC 61850-8-2, IEC 61850-90-1, IEC 61850-90-10, IEC 61850-90-11, IEC 61850-90-12, IEC 61850-90-15, IEC 61850-90-2, IEC 61850-90-4, IEC 61850-90-5, IEC 61850-90-7, IEC 61850-90-9, IEC 61850-9-2, IEC 61968 series, IEC 61968-100, IEC 61970 series, IEC 62056-1-0, IEC 62056-31, IEC 62056-3-1, IEC 62056-3-2, IEC 62056-42, IEC 62056-46, IEC 62056-47, IEC 62056-4-7, IEC 62056-53, IEC 62056-5-3, IEC 62056-5-8, IEC 62056-6-1, IEC 62056-6-2, IEC 62056-6-9, IEC 62056-7-6, IEC 62056-8-3, IEC 62056-9-7, IEC 62282, IEC 62325 series, IEC 62351 series, IEC 62439, IEC 62488-1 (Formerly EN60663) - Part 1, IEC 62541 series, ISO 16484 series, ISO/IEC 12139-1, ISO/IEC 14543-3, ISO/IEC 14543-3 series, ISO/IEC 14908 series, ISO/IEC 14908-1, ISO/IEC 14908-2, ISO/IEC 14908-3, ISO/IEC 14908-4, ISO/IEC 15802 IEEE 802.1, ISO/IEC 7498-1, ISO/IEC 8802-3, ITU-T G.7041, ITU-T G.7042, ITU-T G.707, ITU-T G.709, ITU-T G.781, ITU-T G.783, ITU-T G.798, ITU-T G.803, ITU-T G.872, ITU-T G.983.1, ITU-T G.983.2, ITU-T G.983.3, ITU-T G.983.4, ITU-T G.983.5, ITU-T G.984.1, ITU-T G.984.2, ITU-T G.984.3, ITU-T G.984.4, ITU-T G.984.5, ITU-T G.984.6, ITU-T G.984.7, ITU-T G.987.1, ITU-T G.987.2, ITU-T G.987.3, ITU-T G.9901, ITU-T G.9902, ITU-T G.9903, ITU-T G.9904, ITU-T G.991.1, ITU-T G.991.2, ITU-T G.992.1, ITU-T G.992.2, ITU-T G.992.3, ITU-T G.992.4, ITU-T G.993.1, ITU-T G.993.2, ITU-T G.993.5, ITU-T G.994.1, ITU-T G.995.1, ITU-T G.996.1, ITU-T G.996.2, ITU-T G.9960 (PHY), ITU-T G.9961 (DLL), ITU-T G.9962 (MIMO), ITU-T G.9964 (PSD), ITU-T G.997.1, ITU-T G.998.1, ITU-T G.998.2, ITU-T G.998.3, ITU-T G.998.4, ITU-T G.999.1, ITU-T I.322
AMI Head End	IEC 60870-5-101, IEC 60870-5-104, IEC 60870-5-5, IEC 60904 series, IEC 61131, IEC 61158 series, IEC 61334-4-32, IEC 61334-4-41, IEC 61334-4-511, IEC 61334-4-512, IEC 61334-5-1, IEC 61334-61, IEC 61400-1, IEC 61400-2, IEC 61400-25, IEC 61400-25-2, IEC 61400-25-3, IEC 61400-25-4, IEC 61400-3, IEC 61499, IEC 61588 (IEEE 1588), IEC 61724, IEC 61730, IEC 61784-1, IEC 61836, IEC 61850 series, IEC 61850-6, IEC 61850-7-2, IEC 61850-7-3, IEC 61850-7-4, IEC 61850-7-410, IEC 61850-7-420, IEC 61850-80-4, IEC 61850-8-1, IEC 61850-8-2, IEC 61850-90-10, IEC 61850-90-11, IEC 61850-90-12, IEC 61850-90-15, IEC 61850-90-2, IEC 61850-90-4, IEC 61850-90-5, IEC 61850-90-7, IEC 61850-90-9, IEC 61968 series, IEC 61968-100, IEC 61970 series, IEC 62056 series, IEC 62056-1-0, IEC 62056-31, IEC 62056-3-1, IEC 62056-3-2, IEC 62056-42, IEC 62056-46, IEC 62056-47, IEC 62056-4-7, IEC 62056-53, IEC 62056-5-3, IEC 62056-5-8, IEC 62056-6-1, IEC 62056-6-2, IEC 62056-6-9, IEC 62056-7-6, IEC 62056-8-3, IEC 62056-9-7, IEC 62282, IEC 62325 series, IEC 62351 series, IEC 62351-1, IEC 62351-10, IEC 62351-11, IEC 62351-2, IEC 62351-3, IEC 62351-4, IEC 62351-5, IEC 62351-6, IEC 62351-7, IEC 62351-8, IEC 62351-9, IEC 62361 series, IEC 62361-102, IEC 62443 series, ISO 16484 series, ISO 8601, ISO/IEC 14543-3 series, ISO/IEC 14908 series, ISO/IEC 15118, ISO/IEC 27001, ISO/IEC 27002, ITU-T G.9901, ITU-T G.9902, ITU-T G.9903, ITU-T G.9904
Appliances	IEC 60364, IEC 60870 series, IEC 60870-5-101, IEC 60870-5-104, IEC 60904 series, IEC 61131, IEC 61158 series, IEC 61334-4-32, IEC 61334-4-41, IEC 61334-4-511, IEC 61334-4-512, IEC 61334-5-1, IEC 61334-61, IEC 61400-1, IEC 61400-2, IEC 61400-25-2, IEC 61400-25-3, IEC 61400-25-4, IEC 61400-3, IEC 61499, IEC 61724, IEC 61730, IEC 61784-1, IEC 61836, IEC 61850-6, IEC 61850-7-2, IEC 61850-7-3, IEC 61850-7-4, IEC 61850-7-410, IEC 61850-7-420, IEC 61850-80-4, IEC 61850-8-1, IEC 61850-8-2, IEC 61850-90-10, IEC 61850-90-11, IEC 61850-90-12, IEC 61850-90-15, IEC 61850-90-2, IEC 61850-90-7, IEC 61850-90-9, IEC 62056-1-0, IEC 62056-31, IEC 62056-3-1, IEC 62056-3-2, IEC 62056-42, IEC 62056-46, IEC 62056-47, IEC 62056-4-7, IEC 62056-53, IEC 62056-5-3, IEC

SUBFIELD	APPLICABLE STANDARDS
	62056-5-8, IEC 62056-6-1, IEC 62056-6-2, IEC 62056-6-9, IEC 62056-7-6, IEC 62056-8-3, IEC 62056-9-7, IEC 62282, IEC 62325 series, IEC 62351 series, IEC 62394, IEC 62457, IEC 62480, ISO 16484 series, ISO 17800, ISO/IEC 14543, ISO/IEC 14543-3 series, ISO/IEC 14543-4, ISO/IEC 14908 series, ISO/IEC 15045, ISO/IEC 15067-3, ISO/IEC 18012, ISO/IEC 24767, ITU-T G.9901, ITU-T G.9902, ITU-T G.9903, ITU-T G.9904
Asset Management	IEC 60076, IEC 60870-5-101, IEC 60870-5-104, IEC 61360, IEC 61400-25, IEC 61850 series, IEC 61850-80-1, IEC 61850-80-4, IEC 61850-8-1, IEC 61850-8-2, IEC 61850-90-2, IEC 61850-90-3, IEC 61897, IEC 61968 series, IEC 61968-100, IEC 61968-4, IEC 61968-6, IEC 61970 series, IEC 61970-1, IEC 61970-2, IEC 61970-301, IEC 61970-401, IEC 61970-452, IEC 61970-453, IEC 61970-456, IEC 61970-458, IEC 61970-501, IEC 61970-502-8, IEC 61970-552, IEC 62056 series, IEC 62056-6-9, IEC 62271-1x series, IEC 62271-2x series, IEC 62361 series, IEC 62361-102
Balance Scheduling	IEC 60870-5-101, IEC 60870-5-104, IEC 60904 series, IEC 61131, IEC 61158 series, IEC 61400-1, IEC 61400-2, IEC 61400-25-2, IEC 61400-25-3, IEC 61400-25-4, IEC 61400-3, IEC 61499, IEC 61724, IEC 61730, IEC 61784-1, IEC 61836, IEC 61850-6, IEC 61850-7-2, IEC 61850-7-3, IEC 61850-7-4, IEC 61850-7-410, IEC 61850-7-420, IEC 61850-8-1, IEC 61850-8-2, IEC 61850-90-10, IEC 61850-90-11, IEC 61850-90-12, IEC 61850-90-15, IEC 61850-90-2, IEC 61850-90-7, IEC 61850-90-9, IEC 61968 series, IEC 61968-100, IEC 61968-9, IEC 61970 series, IEC 61970-301, IEC 62282, IEC 62325 series, IEC 62325-301, IEC 62325-351, IEC 62325-450, IEC 62325-451-1, IEC 62325-451-2, IEC 62325-451-3, IEC 62325-503, IEC 62351 series, ISO 19142
Bay Controller	IEC 60255-24, IEC 60870-5-101, IEC 60870-5-103, IEC 60870-5-104, IEC 60870-5-5, IEC 60870-6, IEC 61158 series, IEC 61400-25, IEC 61588 (IEEE 1588), IEC 61850 series, IEC 61850-6, IEC 61850-7-2, IEC 61850-7-3, IEC 61850-7-4, IEC 61850-7-410, IEC 61850-80-1, IEC 61850-80-4, IEC 61850-8-1, IEC 61850-8-2, IEC 61850-90-1, IEC 61850-90-11, IEC 61850-90-12, IEC 61850-90-2, IEC 61850-90-3, IEC 61850-90-4, IEC 61850-90-5, IEC 61850-90-6, IEC 61850-90-7, IEC 61850-9-2, IEC 61869, IEC 62271-3, IEC 62325, IEC 62351 series, IEC 62351-1, IEC 62357, IEC 62361 series, IEC 62361-100, IEC 62439, ISO 8601
Billing	IEC 60870-5-101, IEC 60870-5-104, IEC 60904 series, IEC 61131, IEC 61158 series, IEC 61334-4-32, IEC 61334-4-41, IEC 61334-4-511, IEC 61334-4-512, IEC 61334-5-1, IEC 61334-61, IEC 61400-1, IEC 61400-2, IEC 61400-25-2, IEC 61400-25-3, IEC 61400-25-4, IEC 61400-3, IEC 61499, IEC 61724, IEC 61730, IEC 61784-1, IEC 61836, IEC 61850-6, IEC 61850-7-2, IEC 61850-7-3, IEC 61850-7-4, IEC 61850-7-410, IEC 61850-7-420, IEC 61850-80-4, IEC 61850-8-1, IEC 61850-8-2, IEC 61850-90-10, IEC 61850-90-11, IEC 61850-90-12, IEC 61850-90-15, IEC 61850-90-2, IEC 61850-90-7, IEC 61850-90-9, IEC 61968 series, IEC 61968-100, IEC 61968-9, IEC 61970 series, IEC 62056-1-0, IEC 62056-3-1, IEC 62056-3-2, IEC 62056-42, IEC 62056-46, IEC 62056-47, IEC 62056-4-7, IEC 62056-53, IEC 62056-5-3, IEC 62056-5-8, IEC 62056-6-1, IEC 62056-6-2, IEC 62056-6-9, IEC 62056-7-6, IEC 62056-8-3, IEC 62056-9-7, IEC 62282, IEC 62325 series, IEC 62351 series, IEC 62357, ISO 16484 series, ISO/IEC 14543-3 series, ISO/IEC 14908 series, ITU-T G.9901, ITU-T G.9902, ITU-T G.9903, ITU-T G.9904
Building Management System	IEC 60364, IEC 60870 series, IEC 61158 series, IEC 61334-4-32, IEC 61334-4-41, IEC 61334-4-511, IEC 61334-4-512, IEC 61334-5-1, IEC 61334-61, IEC 61400-25, IEC 61784, IEC 61850 series, IEC 61850-80-4, IEC 61850-90-5, IEC 62056 series, IEC 62056-1-0, IEC 62056-31, IEC 62056-3-1, IEC 62056-3-2, IEC 62056-42, IEC 62056-46, IEC 62056-47, IEC 62056-4-7, IEC 62056-53, IEC 62056-5-3, IEC 62056-5-8, IEC 62056-6-1, IEC 62056-6-2, IEC 62056-6-9, IEC 62056-7-6, IEC 62056-8-3, IEC 62056-9-7, IEC 62325 series, IEC 62351 series, IEC 62351-1, IEC 62351-10, IEC 62351-11, IEC 62351-2, IEC 62351-3, IEC 62351-4, IEC 62351-5, IEC 62351-6, IEC 62351-7, IEC 62351-8, IEC 62351-9, IEC 62394, IEC 62439, IEC 62443 series, IEC 62457, IEC 62480, IEC 62541 series, IEC 62872 Ed. 1.0, ISO 16484 series, ISO 17800, ISO/IEC 14543, ISO/IEC 14543-3 series, ISO/IEC 14543-4, ISO/IEC 14908 series, ISO/IEC 15045, ISO/IEC 15067-3, ISO/IEC 15118, ISO/IEC 18012, ISO/IEC 24767, ISO/IEC 27001, ISO/IEC 27002, ITU-T G.9901, ITU-T G.9902, ITU-T G.9903, ITU-T G.9904
Capacitor	IEC 60255-24, IEC 60870-5-101, IEC 60870-5-103, IEC 60870-5-104, IEC 60904 series, IEC 61131, IEC 61158 series, IEC 61400-1, IEC 61400-2, IEC 61400-25, IEC 61400-25-2, IEC 61400-25-3, IEC

SUBFIELD	APPLICABLE STANDARDS
	<p>61400-25-4, IEC 61400-3, IEC 61499, IEC 61724, IEC 61730, IEC 61784-1, IEC 61836, IEC 61850-6, IEC 61850-7-2, IEC 61850-7-3, IEC 61850-7-4, IEC 61850-7-410, IEC 61850-7-420, IEC 61850-80-1, IEC 61850-80-4, IEC 61850-8-1, IEC 61850-8-2, IEC 61850-90-1, IEC 61850-90-10, IEC 61850-90-11, IEC 61850-90-12, IEC 61850-90-15, IEC 61850-90-2, IEC 61850-90-3, IEC 61850-90-4, IEC 61850-90-5, IEC 61850-90-6, IEC 61850-90-7, IEC 61850-90-9, IEC 61850-9-2, IEC 61869, IEC 62271-3, IEC 62282, IEC 62351 series, IEC 62439, IEC 60255-24, IEC 60870-5-101, IEC 60870-5-103, IEC 60870-5-104, IEC 60904 series, IEC 61131, IEC 61158 series, IEC 61400-1, IEC 61400-2, IEC 61400-25, IEC 61400-25-2, IEC 61400-25-3, IEC 61400-25-4, IEC 61400-3, IEC 61499, IEC 61724, IEC 61730, IEC 61784-1, IEC 61836, IEC 61850-6, IEC 61850-7-2, IEC 61850-7-3, IEC 61850-7-4, IEC 61850-7-410, IEC 61850-7-420, IEC 61850-80-1, IEC 61850-80-4, IEC 61850-8-1, IEC 61850-8-2, IEC 61850-90-1, IEC 61850-90-10, IEC 61850-90-11, IEC 61850-90-12, IEC 61850-90-15, IEC 61850-90-2, IEC 61850-90-3, IEC 61850-90-4, IEC 61850-90-5, IEC 61850-90-6, IEC 61850-90-7, IEC 61850-90-9, IEC 61850-9-2, IEC 61869, IEC 62271-3, IEC 62282, IEC 62351 series, IEC 62439</p>
Charging Station	<p>IEC 60364, IEC 60364-4-41, IEC 60364-5-53, IEC 60364-5-55, IEC 60364-7-712, IEC 60364-7-722, IEC 60783, IEC 60784, IEC 60785, IEC 60786, IEC 61334-4-32, IEC 61334-4-41, IEC 61334-4-511, IEC 61334-4-512, IEC 61334-5-1, IEC 61334-61, IEC 61400-25, IEC 61850-80-4, IEC 61850-90-5, IEC 61850-90-8, IEC 61851 series, IEC 61851-1, IEC 61851-21, IEC 61851-22, IEC 61851-23, IEC 61851-24, IEC 61894, IEC 61968 series, IEC 61970 series, IEC 61980 series, IEC 61982 series, IEC 62056-1-0, IEC 62056-31, IEC 62056-3-1, IEC 62056-3-2, IEC 62056-42, IEC 62056-46, IEC 62056-47, IEC 62056-4-7, IEC 62056-53, IEC 62056-5-3, IEC 62056-5-8, IEC 62056-6-1, IEC 62056-6-2, IEC 62056-6-9, IEC 62056-7-6, IEC 62056-8-3, IEC 62056-9-7, IEC 62196, IEC 62351 series, IEC 62351-1, IEC 62351-10, IEC 62351-11, IEC 62351-2, IEC 62351-3, IEC 62351-4, IEC 62351-5, IEC 62351-6, IEC 62351-7, IEC 62351-8, IEC 62351-9, IEC 62443 series, ISO 6469, ISO 8713, ISO/IEC 14908 series, ISO/IEC 15118, ISO/IEC 15118 series, ISO/IEC 27001, ISO/IEC 27002, ITU-T G.9901, ITU-T G.9902, ITU-T G.9903, ITU-T G.9904</p>
CIS	<p>IEC 60870-5-101, IEC 60870-5-104, IEC 60904 series, IEC 61131, IEC 61158 series, IEC 61334-4-32, IEC 61334-4-41, IEC 61334-4-511, IEC 61334-4-512, IEC 61334-5-1, IEC 61334-61, IEC 61400-1, IEC 61400-2, IEC 61400-25-2, IEC 61400-25-3, IEC 61400-25-4, IEC 61400-3, IEC 61499, IEC 61724, IEC 61730, IEC 61784-1, IEC 61836, IEC 61850 series, IEC 61850-6, IEC 61850-7-2, IEC 61850-7-3, IEC 61850-7-4, IEC 61850-7-410, IEC 61850-7-420, IEC 61850-80-4, IEC 61850-8-1, IEC 61850-8-2, IEC 61850-90-10, IEC 61850-90-11, IEC 61850-90-12, IEC 61850-90-15, IEC 61850-90-2, IEC 61850-90-7, IEC 61850-90-9, IEC 61968 series, IEC 61968-1, IEC 61968-100, IEC 61968-11, IEC 61968-13, IEC 61968-2, IEC 61968-3, IEC 61968-4, IEC 61968-6, IEC 61968-8, IEC 61968-9, IEC 61970 series, IEC 61970-1, IEC 61970-2, IEC 61970-301, IEC 61970-401, IEC 61970-452, IEC 61970-453, IEC 61970-456, IEC 61970-458, IEC 61970-501, IEC 61970-502-8, IEC 61970-552, IEC 62056-1-0, IEC 62056-31, IEC 62056-3-1, IEC 62056-3-2, IEC 62056-42, IEC 62056-46, IEC 62056-47, IEC 62056-4-7, IEC 62056-53, IEC 62056-5-3, IEC 62056-5-8, IEC 62056-6-1, IEC 62056-6-2, IEC 62056-6-9, IEC 62056-7-6, IEC 62056-8-3, IEC 62056-9-7, IEC 62282, IEC 62325 series, IEC 62351 series, IEC 62351-1, IEC 62357, IEC 62361 series, IEC 62361-100, ISO 16484 series, ISO/IEC 14543-3 series, ISO/IEC 14908 series, ITU-T G.9901, ITU-T G.9902, ITU-T G.9903, ITU-T G.9904</p>
Conditioning Monitoring	<p>IEC 60076, IEC 60255-24, IEC 60870-5-101, IEC 60870-5-103, IEC 60870-5-104, IEC 61158 series, IEC 61360, IEC 61400-25, IEC 61850-6, IEC 61850-7-2, IEC 61850-7-3, IEC 61850-7-4, IEC 61850-7-410, IEC 61850-80-1, IEC 61850-80-4, IEC 61850-8-1, IEC 61850-8-2, IEC 61850-90-1, IEC 61850-90-11, IEC 61850-90-12, IEC 61850-90-2, IEC 61850-90-3, IEC 61850-90-4, IEC 61850-90-5, IEC 61850-90-6, IEC 61850-90-7, IEC 61850-9-2, IEC 61869, IEC 61897, IEC 61968 series, IEC 61968-1, IEC 61968-100, IEC 61968-11, IEC 61968-13, IEC 61968-2, IEC 61968-3, IEC 61968-4, IEC 61968-6, IEC 61968-8, IEC 61968-9, IEC 61970 series, IEC 61970-1, IEC 61970-2, IEC 61970-301, IEC 61970-401, IEC 61970-452, IEC 61970-453, IEC 61970-456, IEC 61970-458, IEC 61970-501, IEC 61970-502-8, IEC 61970-552, IEC 62271-1x series, IEC 62271-2x series, IEC 62271-3, IEC 62351 series, IEC 62439</p>

SUBFIELD	APPLICABLE STANDARDS
Customer Energy Management	IEC 60364, IEC 61158 series, IEC 61784, IEC 61850 series, IEC 61850-7-410, IEC 61850-8-2, IEC 61850-90-9, IEC 62056 series, IEC 62325 series, IEC 62351 series, IEC 62439, IEC 62443 series, IEC 62541 series, IEC 62872 Ed. 1.0
Customer Portal	IEC 60870-5-101, IEC 60870-5-104, IEC 60904 series, IEC 61131, IEC 61158 series, IEC 61334-4-32, IEC 61334-4-41, IEC 61334-4-511, IEC 61334-4-512, IEC 61334-5-1, IEC 61334-61, IEC 61400-1, IEC 61400-2, IEC 61400-25, IEC 61400-25-2, IEC 61400-25-3, IEC 61400-25-4, IEC 61400-3, IEC 61499, IEC 61724, IEC 61730, IEC 61784-1, IEC 61836, IEC 61850 series, IEC 61850-6, IEC 61850-7-2, IEC 61850-7-3, IEC 61850-7-4, IEC 61850-7-410, IEC 61850-7-420, IEC 61850-80-4, IEC 61850-8-1, IEC 61850-8-2, IEC 61850-90-10, IEC 61850-90-11, IEC 61850-90-12, IEC 61850-90-15, IEC 61850-90-2, IEC 61850-90-5, IEC 61850-90-7, IEC 61850-90-9, IEC 61968 series, IEC 61968-1, IEC 61968-100, IEC 61968-11, IEC 61968-13, IEC 61968-2, IEC 61968-3, IEC 61968-4, IEC 61968-6, IEC 61968-8, IEC 61968-9, IEC 61970 series, IEC 61970-1, IEC 61970-2, IEC 61970-301, IEC 61970-401, IEC 61970-452, IEC 61970-453, IEC 61970-456, IEC 61970-458, IEC 61970-501, IEC 61970-502-8, IEC 61970-552, IEC 62056-1-0, IEC 62056-31, IEC 62056-3-1, IEC 62056-3-2, IEC 62056-42, IEC 62056-46, IEC 62056-47, IEC 62056-4-7, IEC 62056-53, IEC 62056-5-3, IEC 62056-5-8, IEC 62056-6-1, IEC 62056-6-2, IEC 62056-6-9, IEC 62056-7-6, IEC 62056-8-3, IEC 62056-9-7, IEC 62282, IEC 62325 series, IEC 62351 series, IEC 62351-1, IEC 62351-10, IEC 62351-11, IEC 62351-2, IEC 62351-3, IEC 62351-4, IEC 62351-5, IEC 62351-6, IEC 62351-7, IEC 62351-8, IEC 62351-9, IEC 62357, IEC 62361 series, IEC 62361-100, IEC 62443 series, ISO 16484 series, ISO/IEC 14543-3 series, ISO/IEC 14908 series, ISO/IEC 15118, ISO/IEC 27001, ISO/IEC 27002, ITU-T G.9901, ITU-T G.9902, ITU-T G.9903, ITU-T G.9904
DER	IEC 60870-5-101, IEC 60870-5-104, IEC 60904 series, IEC 61131, IEC 61158 series, IEC 61400-1, IEC 61400-2, IEC 61400-25-2, IEC 61400-25-3, IEC 61400-25-4, IEC 61400-3, IEC 61499, IEC 61724, IEC 61730, IEC 61784-1, IEC 61836, IEC 61850-6, IEC 61850-7-2, IEC 61850-7-3, IEC 61850-7-4, IEC 61850-7-410, IEC 61850-7-420, IEC 61850-8-1, IEC 61850-8-2, IEC 61850-90-10, IEC 61850-90-11, IEC 61850-90-12, IEC 61850-90-15, IEC 61850-90-2, IEC 61850-90-7, IEC 61850-90-9, IEC 62282, IEC 62351 series
DER Control	IEC 60870-5-101, IEC 60870-5-104, IEC 60904 series, IEC 61000 Series, IEC 61000-2-12, IEC 61000-2-2, IEC 61000-3-13, IEC 61000-3-14, IEC 61000-3-15, IEC 61000-3-6, IEC 61000-3-7, IEC 61000-4-19, IEC 61000-4-30, IEC 61000-6-1, IEC 61000-6-2, IEC 61000-6-3, IEC 61000-6-4, IEC 61000-6-4, IEC 61000-6-5, IEC 61131, IEC 61158 series, IEC 61326, IEC 61400-1, IEC 61400-2, IEC 61400-25-2, IEC 61400-25-3, IEC 61400-25-4, IEC 61400-3, IEC 61499, IEC 61724, IEC 61730, IEC 61784-1, IEC 61836, IEC 61850-6, IEC 61850-7-2, IEC 61850-7-3, IEC 61850-7-4, IEC 61850-7-410, IEC 61850-7-420, IEC 61850-8-1, IEC 61850-8-2, IEC 61850-90-10, IEC 61850-90-11, IEC 61850-90-12, IEC 61850-90-15, IEC 61850-90-2, IEC 61850-90-7, IEC 61850-90-9, IEC 61968 series, IEC 61968-100, IEC 61970 series, IEC 62282, IEC 62351 series
Digital Sensors	IEC 60076, IEC 60255-24, IEC 60633, IEC 60700-1, IEC 60870-5-101, IEC 60870-5-103, IEC 60870-5-104, IEC 60870-5-5, IEC 60919, IEC 61158 series, IEC 61360, IEC 61400-25, IEC 61588 (IEEE 1588), IEC 61803, IEC 61850-6, IEC 61850-7-2, IEC 61850-7-3, IEC 61850-7-4, IEC 61850-7-410, IEC 61850-80-1, IEC 61850-80-4, IEC 61850-8-1, IEC 61850-8-2, IEC 61850-90-1, IEC 61850-90-11, IEC 61850-90-12, IEC 61850-90-14, IEC 61850-90-2, IEC 61850-90-3, IEC 61850-90-4, IEC 61850-90-5, IEC 61850-90-6, IEC 61850-90-7, IEC 61850-9-2, IEC 61869, IEC 61897, IEC 61954, IEC 62271-1x series, IEC 62271-2x series, IEC 62271-3, IEC 62351 series, IEC 62439, ISO 8601
DMS	IEC 60255-24, IEC 60870-5-101, IEC 60870-5-103, IEC 60870-5-104, IEC 60904 series, IEC 61131, IEC 61158 series, IEC 61334-4-32, IEC 61334-4-41, IEC 61334-4-511, IEC 61334-4-512, IEC 61334-5-1, IEC 61334-61, IEC 61400-1, IEC 61400-2, IEC 61400-25, IEC 61400-25-2, IEC 61400-25-3, IEC 61400-25-4, IEC 61400-3, IEC 61499, IEC 61724, IEC 61730, IEC 61784-1, IEC 61836, IEC 61850 series, IEC 61850-6, IEC 61850-7-2, IEC 61850-7-3, IEC 61850-7-4, IEC 61850-7-410, IEC 61850-7-420, IEC 61850-80-1, IEC 61850-80-4, IEC 61850-8-1, IEC 61850-8-2, IEC 61850-90-1, IEC 61850-90-10, IEC 61850-90-11, IEC 61850-90-12, IEC 61850-90-15, IEC 61850-90-2, IEC 61850-90-3, IEC 61850-90-4, IEC 61850-90-5, IEC 61850-90-6, IEC 61850-90-7, IEC 61850-90-9, IEC 61850-9-2, IEC

SUBFIELD	APPLICABLE STANDARDS
	61869, IEC 61968 series, IEC 61968-1, IEC 61968-100, IEC 61968-11, IEC 61968-13, IEC 61968-2, IEC 61968-3, IEC 61968-4, IEC 61968-6, IEC 61968-8, IEC 61968-9, IEC 61970 series, IEC 61970-1, IEC 61970-2, IEC 61970-301, IEC 61970-401, IEC 61970-452, IEC 61970-453, IEC 61970-456, IEC 61970-458, IEC 61970-501, IEC 61970-502-8, IEC 61970-552, IEC 62056 series, IEC 62056-1-0, IEC 62056-31, IEC 62056-3-1, IEC 62056-3-2, IEC 62056-42, IEC 62056-46, IEC 62056-47, IEC 62056-4-7, IEC 62056-53, IEC 62056-5-3, IEC 62056-5-8, IEC 62056-6-1, IEC 62056-6-2, IEC 62056-6-9, IEC 62056-7-6, IEC 62056-8-3, IEC 62056-9-7, IEC 62271-3, IEC 62282, IEC 62325 series, IEC 62351 series, IEC 62351-1, IEC 62357, IEC 62361 series, IEC 62361-100, IEC 62361-102, IEC 62439, ISO 16484 series, ISO 19142, ISO/IEC 14543-3 series, ISO/IEC 14908 series, ITU-T G.9901, ITU-T G.9902, ITU-T G.9903, ITU-T G.9904
DRMS	IEC 60870-5-101, IEC 60870-5-104, IEC 60904 series, IEC 61131, IEC 61158 series, IEC 61334-4-32, IEC 61334-4-41, IEC 61334-4-511, IEC 61334-4-512, IEC 61334-5-1, IEC 61334-61, IEC 61400-1, IEC 61400-2, IEC 61400-25-2, IEC 61400-25-3, IEC 61400-25-4, IEC 61400-3, IEC 61499, IEC 61724, IEC 61730, IEC 61784-1, IEC 61836, IEC 61850 series, IEC 61850-6, IEC 61850-7-2, IEC 61850-7-3, IEC 61850-7-4, IEC 61850-7-410, IEC 61850-7-420, IEC 61850-80-4, IEC 61850-8-1, IEC 61850-8-2, IEC 61850-90-10, IEC 61850-90-11, IEC 61850-90-12, IEC 61850-90-15, IEC 61850-90-2, IEC 61850-90-7, IEC 61850-90-9, IEC 61968 series, IEC 61968-1, IEC 61968-100, IEC 61968-11, IEC 61968-13, IEC 61968-2, IEC 61968-3, IEC 61968-4, IEC 61968-6, IEC 61968-8, IEC 61968-9, IEC 61970 series, IEC 61970-1, IEC 61970-2, IEC 61970-301, IEC 61970-401, IEC 61970-452, IEC 61970-453, IEC 61970-456, IEC 61970-458, IEC 61970-501, IEC 61970-502-8, IEC 61970-552, IEC 62056 series, IEC 62056-1-0, IEC 62056-31, IEC 62056-3-1, IEC 62056-3-2, IEC 62056-42, IEC 62056-46, IEC 62056-47, IEC 62056-4-7, IEC 62056-53, IEC 62056-5-3, IEC 62056-5-8, IEC 62056-6-1, IEC 62056-6-2, IEC 62056-6-9, IEC 62056-7-6, IEC 62056-8-3, IEC 62056-9-7, IEC 62282, IEC 62325 series, IEC 62351 series, IEC 62361 series, IEC 62361-102, ISO 16484 series, ISO 19142, ISO/IEC 14543-3 series, ISO/IEC 14908 series, ITU-T G.9901, ITU-T G.9902, ITU-T G.9903, ITU-T G.9904
EMS	IEC 60193, IEC 60255, IEC 60255-24, IEC 60870-5-101, IEC 60870-5-103, IEC 60870-5-104, IEC 60870-6, IEC 60904 series, IEC 61131, IEC 61158 series, IEC 61360, IEC 61400 series, IEC 61400-25, IEC 61400-25-2, IEC 61499, IEC 61512, IEC 61727, IEC 61784-1, IEC 61804, IEC 61850 series, IEC 61850-6, IEC 61850-7-2, IEC 61850-7-3, IEC 61850-7-4, IEC 61850-7-410, IEC 61850-80-1, IEC 61850-80-4, IEC 61850-8-1, IEC 61850-8-2, IEC 61850-90-1, IEC 61850-90-11, IEC 61850-90-12, IEC 61850-90-13, IEC 61850-90-2, IEC 61850-90-3, IEC 61850-90-4, IEC 61850-90-5, IEC 61850-90-6, IEC 61850-90-7, IEC 61850-9-2, IEC 61869, IEC 61968 series, IEC 61968-1, IEC 61968-100, IEC 61968-11, IEC 61968-2, IEC 61968-3, IEC 61968-4, IEC 61968-6, IEC 61968-9, IEC 61970 series, IEC 61970-1, IEC 61970-2, IEC 61970-301, IEC 61970-401, IEC 61970-452, IEC 61970-453, IEC 61970-456, IEC 61970-458, IEC 61970-501, IEC 61970-502-8, IEC 61970-552, IEC 61987, IEC 62056 series, IEC 62056-6-9, IEC 62264, IEC 62271-3, IEC 62282 series, IEC 62325, IEC 62325-301, IEC 62325-351, IEC 62325-450, IEC 62325-451-1, IEC 62325-451-2, IEC 62325-451-3, IEC 62351 series, IEC 62357, IEC 62361 series, IEC 62361-100, IEC 62361-101, IEC 62361-102, IEC 62439, IEC 62446, IEC 62541-1, IEC 62541-10, IEC 62541-2, IEC 62541-3, IEC 62541-4, IEC 62541-5, IEC 62541-6, IEC 62541-7, IEC 62541-8, IEC 62541-9, ISO 19142, ISO 81400
Energy Storage	IEC 60364, IEC 60870-5-101, IEC 60870-5-104, IEC 60904 series, IEC 61000 Series, IEC 61000-2-12, IEC 61000-2-2, IEC 61000-3-13, IEC 61000-3-14, IEC 61000-3-15, IEC 61000-3-6, IEC 61000-3-7, IEC 61000-4-19, IEC 61000-4-30, IEC 61000-6-1, IEC 61000-6-2, IEC 61000-6-3, IEC 61000-6-4, IEC 61000-6-5, IEC 61131, IEC 61158 series, IEC 61326, IEC 61400-1, IEC 61400-2, IEC 61400-25-2, IEC 61400-25-3, IEC 61400-25-4, IEC 61400-3, IEC 61499, IEC 61724, IEC 61730, IEC 61784-1, IEC 61836, IEC 61850-6, IEC 61850-7-2, IEC 61850-7-3, IEC 61850-7-4, IEC 61850-7-410, IEC 61850-7-420, IEC 61850-8-1, IEC 61850-8-2, IEC 61850-90-10, IEC 61850-90-11, IEC 61850-90-12, IEC 61850-90-15, IEC 61850-90-2, IEC 61850-90-7, IEC 61850-90-9, IEC 61968 series, IEC 61968-100, IEC 61970 series, IEC 62282, IEC 62325 series, IEC 62351 series, IEC 62439, IEC 62443 series, IEC 62541 series

SUBFIELD	APPLICABLE STANDARDS
Energy Trading Application	IEC 60870-5-101, IEC 60870-5-104, IEC 60904 series, IEC 61131, IEC 61158 series, IEC 61334-4-32, IEC 61334-4-41, IEC 61334-4-511, IEC 61334-4-512, IEC 61334-5-1, IEC 61334-61, IEC 61400-1, IEC 61400-2, IEC 61400-25-2, IEC 61400-25-3, IEC 61400-25-4, IEC 61400-3, IEC 61499, IEC 61724, IEC 61730, IEC 61784-1, IEC 61836, IEC 61850 series, IEC 61850-6, IEC 61850-7-2, IEC 61850-7-3, IEC 61850-7-4, IEC 61850-7-410, IEC 61850-7-420, IEC 61850-80-4, IEC 61850-8-1, IEC 61850-8-2, IEC 61850-90-10, IEC 61850-90-11, IEC 61850-90-12, IEC 61850-90-15, IEC 61850-90-2, IEC 61850-90-7, IEC 61850-90-9, IEC 61968 series, IEC 61968-100, IEC 61970 series, IEC 61970-301, IEC 62056 series, IEC 62056-1-0, IEC 62056-31, IEC 62056-3-1, IEC 62056-3-2, IEC 62056-42, IEC 62056-46, IEC 62056-47, IEC 62056-4-7, IEC 62056-53, IEC 62056-5-3, IEC 62056-5-8, IEC 62056-6-1, IEC 62056-6-2, IEC 62056-6-9, IEC 62056-7-6, IEC 62056-8-3, IEC 62056-9-7, IEC 62282, IEC 62325 series, IEC 62325-301, IEC 62325-351, IEC 62325-450, IEC 62325-451-1, IEC 62325-451-2, IEC 62325-451-3, IEC 62325-503, IEC 62351 series, IEC 62361 series, IEC 62361-102, ISO 16484 series, ISO/IEC 14543-3 series, ISO/IEC 14908 series, ITU-T G.9901, ITU-T G.9902, ITU-T G.9903, ITU-T G.9904
ERP	IEC 60076, IEC 60193, IEC 60255, IEC 60870-5-101, IEC 60870-5-103, IEC 60870-5-104, IEC 60870-6, IEC 60904 series, IEC 61131, IEC 61158 series, IEC 61360, IEC 61400 series, IEC 61400-25, IEC 61400-25-2, IEC 61499, IEC 61512, IEC 61727, IEC 61784-1, IEC 61804, IEC 61850 series, IEC 61850-7-2, IEC 61850-7-3, IEC 61850-7-4, IEC 61850-7-410, IEC 61850-80-1, IEC 61850-80-4, IEC 61850-8-1, IEC 61850-8-2, IEC 61850-90-1, IEC 61850-90-13, IEC 61850-90-2, IEC 61850-90-3, IEC 61850-90-4, IEC 61850-9-2, IEC 61897, IEC 61968 series, IEC 61968-1, IEC 61968-100, IEC 61968-11, IEC 61968-2, IEC 61968-3, IEC 61968-4, IEC 61968-6, IEC 61968-9, IEC 61970 series, IEC 61970-1, IEC 61970-2, IEC 61970-301, IEC 61970-401, IEC 61970-452, IEC 61970-453, IEC 61970-456, IEC 61970-458, IEC 61970-501, IEC 61970-502-8, IEC 61970-552, IEC 61987, IEC 62056 series, IEC 62056-1-0, IEC 62056-6-9, IEC 62264, IEC 62271-1x series, IEC 62271-2x series, IEC 62282 series, IEC 62325, IEC 62325 series, IEC 62325-301, IEC 62325-351, IEC 62325-450, IEC 62325-451-1, IEC 62325-451-2, IEC 62325-451-3, IEC 62325-503, IEC 62351 series, IEC 62357, IEC 62361 series, IEC 62361-100, IEC 62361-101, IEC 62361-102, IEC 62439, IEC 62446, IEC 62541-1, IEC 62541-10, IEC 62541-2, IEC 62541-3, IEC 62541-4, IEC 62541-5, IEC 62541-6, IEC 62541-7, IEC 62541-8, IEC 62541-9, ISO 19142, ISO 81400
FACTS	IEC 60255-24, IEC 60633, IEC 60700-1, IEC 60870-5-101, IEC 60870-5-103, IEC 60870-5-104, IEC 60919, IEC 61158 series, IEC 61400-25, IEC 61803, IEC 61850-6, IEC 61850-7-2, IEC 61850-7-3, IEC 61850-7-4, IEC 61850-7-410, IEC 61850-80-1, IEC 61850-80-4, IEC 61850-8-1, IEC 61850-8-2, IEC 61850-90-1, IEC 61850-90-11, IEC 61850-90-12, IEC 61850-90-14, IEC 61850-90-2, IEC 61850-90-3, IEC 61850-90-4, IEC 61850-90-5, IEC 61850-90-6, IEC 61850-90-7, IEC 61850-9-2, IEC 61869, IEC 61954, IEC 62271-3, IEC 62351 series, IEC 62439
FACTS Control	IEC 60255-24, IEC 60633, IEC 60700-1, IEC 60870-5-101, IEC 60870-5-103, IEC 60870-5-104, IEC 60870-5-5, IEC 60919, IEC 61158 series, IEC 61400-25, IEC 61588 (IEEE 1588), IEC 61803, IEC 61850-6, IEC 61850-7-2, IEC 61850-7-3, IEC 61850-7-4, IEC 61850-7-410, IEC 61850-80-1, IEC 61850-80-4, IEC 61850-8-1, IEC 61850-8-2, IEC 61850-90-1, IEC 61850-90-11, IEC 61850-90-12, IEC 61850-90-14, IEC 61850-90-2, IEC 61850-90-3, IEC 61850-90-4, IEC 61850-90-5, IEC 61850-90-6, IEC 61850-90-7, IEC 61850-9-2, IEC 61869, IEC 61954, IEC 62271-3, IEC 62351 series, IEC 62439, ISO 8601
Fault Detector	IEC 60255-24, IEC 60870-5-101, IEC 60870-5-103, IEC 60870-5-104, IEC 61158 series, IEC 61400-25, IEC 61850 series, IEC 61850-6, IEC 61850-7-2, IEC 61850-7-3, IEC 61850-7-4, IEC 61850-7-410, IEC 61850-7-420, IEC 61850-80-1, IEC 61850-80-4, IEC 61850-8-1, IEC 61850-8-2, IEC 61850-90-1, IEC 61850-90-11, IEC 61850-90-12, IEC 61850-90-2, IEC 61850-90-3, IEC 61850-90-4, IEC 61850-90-5, IEC 61850-90-6, IEC 61850-90-7, IEC 61850-9-2, IEC 61869, IEC 62271-3, IEC 62351 series, IEC 62351-1, IEC 62357, IEC 62361 series, IEC 62361-100, IEC 62439
GIS	IEC 60076, IEC 60870-5-101, IEC 60870-5-104, IEC 61360, IEC 61400-25, IEC 61850 series, IEC 61850-80-1, IEC 61850-80-4, IEC 61850-8-1, IEC 61850-8-2, IEC 61850-90-2, IEC 61850-90-3, IEC



SUBFIELD	APPLICABLE STANDARDS
	61897, IEC 61968 series, IEC 61968-1, IEC 61968-100, IEC 61968-11, IEC 61968-13, IEC 61968-2, IEC 61968-3, IEC 61968-4, IEC 61968-6, IEC 61968-8, IEC 61968-9, IEC 61970 series, IEC 61970-1, IEC 61970-2, IEC 61970-301, IEC 61970-401, IEC 61970-452, IEC 61970-453, IEC 61970-456, IEC 61970-458, IEC 61970-501, IEC 61970-502-8, IEC 61970-552, IEC 62056 series, IEC 62056-1-0, IEC 62056-6-9, IEC 62271-1x series, IEC 62271-2x series, IEC 62351 series, IEC 62351-1, IEC 62357, IEC 62361 series, IEC 62361-100, IEC 62361-102
Grid Meter	IEC 60255-24, IEC 60870-5-101, IEC 60870-5-103, IEC 60870-5-104, IEC 60904 series, IEC 61131, IEC 61158 series, IEC 61400-1, IEC 61400-2, IEC 61400-25, IEC 61400-25-2, IEC 61400-25-3, IEC 61400-25-4, IEC 61400-3, IEC 61499, IEC 61724, IEC 61730, IEC 61784-1, IEC 61836, IEC 61850-6, IEC 61850-7-2, IEC 61850-7-3, IEC 61850-7-4, IEC 61850-7-410, IEC 61850-7-420, IEC 61850-80-1, IEC 61850-80-4, IEC 61850-8-1, IEC 61850-8-2, IEC 61850-90-1, IEC 61850-90-10, IEC 61850-90-11, IEC 61850-90-12, IEC 61850-90-15, IEC 61850-90-2, IEC 61850-90-3, IEC 61850-90-4, IEC 61850-90-5, IEC 61850-90-6, IEC 61850-90-7, IEC 61850-90-9, IEC 61850-9-2, IEC 61869, IEC 62271-3, IEC 62282, IEC 62351 series, IEC 62439
HAN Gateway	IEC 60364, IEC 60870 series, IEC 60870-5-101, IEC 60870-5-102, IEC 60870-5-103, IEC 60870-5-104, IEC 60904 series, IEC 61131, IEC 61158 series, IEC 61334-4-32, IEC 61334-4-41, IEC 61334-4-511, IEC 61334-4-512, IEC 61334-5-1, IEC 61334-61, IEC 61400-1, IEC 61400-2, IEC 61400-25, IEC 61400-25-2, IEC 61400-25-3, IEC 61400-25-4, IEC 61400-3, IEC 61499, IEC 61724, IEC 61730, IEC 61784, IEC 61784-1, IEC 61836, IEC 61850-6, IEC 61850-7-1, IEC 61850-7-2, IEC 61850-7-3, IEC 61850-7-4, IEC 61850-7-410, IEC 61850-7-420, IEC 61850-80-4, IEC 61850-8-1, IEC 61850-8-2, IEC 61850-90-1, IEC 61850-90-10, IEC 61850-90-11, IEC 61850-90-12, IEC 61850-90-15, IEC 61850-90-2, IEC 61850-90-4, IEC 61850-90-5, IEC 61850-90-7, IEC 61850-90-9, IEC 61850-9-2, IEC 62056-1-0, IEC 62056-31, IEC 62056-3-1, IEC 62056-3-2, IEC 62056-42, IEC 62056-46, IEC 62056-47, IEC 62056-4-7, IEC 62056-53, IEC 62056-5-3, IEC 62056-5-8, IEC 62056-6-1, IEC 62056-6-2, IEC 62056-6-9, IEC 62056-7-6, IEC 62056-8-3, IEC 62056-9-7, IEC 62282, IEC 62325 series, IEC 62351 series, IEC 62351-1, IEC 62351-10, IEC 62351-11, IEC 62351-2, IEC 62351-3, IEC 62351-4, IEC 62351-5, IEC 62351-6, IEC 62351-7, IEC 62351-8, IEC 62351-9, IEC 62394, IEC 62439, IEC 62443 series, IEC 62457, IEC 62480, IEC 62488-1 (Formerly EN60663) - Part 1, IEC 62541 series, ISO 16484 series, ISO 17800, ISO/IEC 12139-1, ISO/IEC 14543, ISO/IEC 14543-3, ISO/IEC 14543-3 series, ISO/IEC 14543-4, ISO/IEC 14908 series, ISO/IEC 14908-1, ISO/IEC 14908-2, ISO/IEC 14908-3, ISO/IEC 14908-4, ISO/IEC 15045, ISO/IEC 15067-3, ISO/IEC 15118, ISO/IEC 15802 IEEE 802.1, ISO/IEC 18012, ISO/IEC 24767, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 7498-1, ISO/IEC 8802-3, ITU-T G.7041, ITU-T G.7042, ITU-T G.707, ITU-T G.709, ITU-T G.781, ITU-T G.783, ITU-T G.798, ITU-T G.803, ITU-T G.872, ITU-T G.983.1, ITU-T G.983.2, ITU-T G.983.3, ITU-T G.983.4, ITU-T G.983.5, ITU-T G.984.1, ITU-T G.984.2, ITU-T G.984.3, ITU-T G.984.4, ITU-T G.984.5, ITU-T G.984.6, ITU-T G.984.7, ITU-T G.987.1, ITU-T G.987.2, ITU-T G.987.3, ITU-T G.9901, ITU-T G.9902, ITU-T G.9903, ITU-T G.9904, ITU-T G.991.1, ITU-T G.991.2, ITU-T G.992.1, ITU-T G.992.2, ITU-T G.992.3, ITU-T G.992.4, ITU-T G.993.1, ITU-T G.993.2, ITU-T G.993.5, ITU-T G.994.1, ITU-T G.995.1, ITU-T G.996.1, ITU-T G.996.2, ITU-T G.9960 (PHY), ITU-T G.9961 (DLL), ITU-T G.9962 (MIMO), ITU-T G.9964 (PSD), ITU-T G.997.1, ITU-T G.998.1, ITU-T G.998.2, ITU-T G.998.3, ITU-T G.998.4, ITU-T G.999.1, ITU-T I.322
HVDC	IEC 60193, IEC 60255, IEC 60255-24, IEC 60870-5-101, IEC 60870-5-103, IEC 60870-5-104, IEC 60904 series, IEC 61131, IEC 61158 series, IEC 61360, IEC 61400 series, IEC 61400-25, IEC 61400-25-2, IEC 61499, IEC 61512, IEC 61727, IEC 61784-1, IEC 61804, IEC 61850-6, IEC 61850-7-2, IEC 61850-7-3, IEC 61850-7-4, IEC 61850-7-410, IEC 61850-80-1, IEC 61850-80-4, IEC 61850-8-1, IEC 61850-8-2, IEC 61850-90-1, IEC 61850-90-11, IEC 61850-90-12, IEC 61850-90-13, IEC 61850-90-2, IEC 61850-90-3, IEC 61850-90-4, IEC 61850-90-5, IEC 61850-90-6, IEC 61850-90-7, IEC 61850-9-2, IEC 61869, IEC 61987, IEC 62264, IEC 62271-3, IEC 62282 series, IEC 62325-301, IEC 62325-351, IEC 62325-450, IEC 62325-451-1, IEC 62325-451-2, IEC 62325-451-3, IEC 62351 series, IEC 62361-100, IEC 62361-101, IEC 62439, IEC 62446, IEC 62541-1, IEC 62541-10, IEC 62541-2, IEC 62541-3, IEC 62541-4, IEC 62541-5, IEC 62541-6, IEC 62541-7, IEC 62541-8, IEC 62541-9, ISO 81400
HVDC Control	IEC 60193, IEC 60255, IEC 60255-24, IEC 60870-5-101, IEC 60870-5-103, IEC 60870-5-104, IEC

SUBFIELD	APPLICABLE STANDARDS
	60870-5-5, IEC 60904 series, IEC 61131, IEC 61158 series, IEC 61360, IEC 61400 series, IEC 61400-25, IEC 61400-25-2, IEC 61499, IEC 61512, IEC 61588 (IEEE 1588), IEC 61727, IEC 61784-1, IEC 61804, IEC 61850-6, IEC 61850-7-2, IEC 61850-7-3, IEC 61850-7-4, IEC 61850-7-410, IEC 61850-80-1, IEC 61850-80-4, IEC 61850-8-1, IEC 61850-8-2, IEC 61850-90-1, IEC 61850-90-11, IEC 61850-90-12, IEC 61850-90-13, IEC 61850-90-2, IEC 61850-90-3, IEC 61850-90-4, IEC 61850-90-5, IEC 61850-90-6, IEC 61850-90-7, IEC 61850-9-2, IEC 61869, IEC 61987, IEC 62264, IEC 62271-3, IEC 62282 series, IEC 62325-301, IEC 62325-351, IEC 62325-450, IEC 62325-451-1, IEC 62325-451-2, IEC 62325-451-3, IEC 62351 series, IEC 62361-100, IEC 62361-101, IEC 62439, IEC 62446, IEC 62541-1, IEC 62541-10, IEC 62541-2, IEC 62541-3, IEC 62541-4, IEC 62541-5, IEC 62541-6, IEC 62541-7, IEC 62541-8, IEC 62541-9, ISO 81400, ISO 8601
Inter-Substation Network	IEC 60193, IEC 60255, IEC 60255-24, IEC 60633, IEC 60700-1, IEC 60870-5-101, IEC 60870-5-102, IEC 60870-5-103, IEC 60870-5-104, IEC 60904 series, IEC 60919, IEC 61000 Series, IEC 61000-2-12, IEC 61000-2-2, IEC 61000-3-13, IEC 61000-3-14, IEC 61000-3-15, IEC 61000-3-6, IEC 61000-3-7, IEC 61000-4-19, IEC 61000-4-30, IEC 61000-6-1, IEC 61000-6-2, IEC 61000-6-3, IEC 61000-6-4, IEC 61000-6-4, IEC 61000-6-5, IEC 61131, IEC 61158 series, IEC 61326, IEC 61360, IEC 61400 series, IEC 61400-1, IEC 61400-2, IEC 61400-25, IEC 61400-25-2, IEC 61400-25-3, IEC 61400-25-4, IEC 61400-3, IEC 61499, IEC 61512, IEC 61724, IEC 61727, IEC 61730, IEC 61784, IEC 61784-1, IEC 61803, IEC 61804, IEC 61836, IEC 61850 series, IEC 61850-6, IEC 61850-7-1, IEC 61850-7-2, IEC 61850-7-3, IEC 61850-7-4, IEC 61850-7-410, IEC 61850-7-420, IEC 61850-80-1, IEC 61850-80-4, IEC 61850-8-1, IEC 61850-8-2, IEC 61850-90-1, IEC 61850-90-10, IEC 61850-90-11, IEC 61850-90-12, IEC 61850-90-13, IEC 61850-90-14, IEC 61850-90-15, IEC 61850-90-2, IEC 61850-90-3, IEC 61850-90-4, IEC 61850-90-5, IEC 61850-90-6, IEC 61850-90-7, IEC 61850-90-9, IEC 61850-9-2, IEC 61869, IEC 61954, IEC 61968 series, IEC 61968-1, IEC 61968-100, IEC 61968-11, IEC 61968-13, IEC 61968-2, IEC 61968-3, IEC 61968-4, IEC 61968-6, IEC 61968-8, IEC 61968-9, IEC 61970 series, IEC 61970-1, IEC 61970-2, IEC 61970-301, IEC 61970-401, IEC 61970-452, IEC 61970-453, IEC 61970-456, IEC 61970-458, IEC 61970-501, IEC 61970-502-8, IEC 61970-552, IEC 61987, IEC 62264, IEC 62271-3, IEC 62282, IEC 62282 series, IEC 62325-301, IEC 62325-351, IEC 62325-450, IEC 62325-451-1, IEC 62325-451-2, IEC 62325-451-3, IEC 62351 series, IEC 62351-1, IEC 62357, IEC 62361 series, IEC 62361-100, IEC 62361-101, IEC 62439, IEC 62446, IEC 62488-1 (Formerly EN60663) - Part 1, IEC 62541 series, IEC 62541-1, IEC 62541-10, IEC 62541-2, IEC 62541-3, IEC 62541-4, IEC 62541-5, IEC 62541-6, IEC 62541-7, IEC 62541-8, IEC 62541-9, ISO 81400, ISO/IEC 12139-1, ISO/IEC 14543-3, ISO/IEC 14908-1, ISO/IEC 14908-2, ISO/IEC 14908-3, ISO/IEC 14908-4, ISO/IEC 15802 IEEE 802.1, ISO/IEC 7498-1, ISO/IEC 8802-3, ITU-T G.7041, ITU-T G.7042, ITU-T G.707, ITU-T G.709, ITU-T G.781, ITU-T G.783, ITU-T G.798, ITU-T G.803, ITU-T G.872, ITU-T G.983.1, ITU-T G.983.2, ITU-T G.983.3, ITU-T G.983.4, ITU-T G.983.5, ITU-T G.984.1, ITU-T G.984.2, ITU-T G.984.3, ITU-T G.984.4, ITU-T G.984.5, ITU-T G.984.6, ITU-T G.984.7, ITU-T G.987.1, ITU-T G.987.2, ITU-T G.987.3, ITU-T G.9901, ITU-T G.9902, ITU-T G.9903, ITU-T G.9904, ITU-T G.991.1, ITU-T G.991.2, ITU-T G.992.1, ITU-T G.992.2, ITU-T G.992.3, ITU-T G.992.4, ITU-T G.993.1, ITU-T G.993.2, ITU-T G.993.5, ITU-T G.994.1, ITU-T G.995.1, ITU-T G.996.1, ITU-T G.996.2, ITU-T G.9960 (PHY), ITU-T G.9961 (DLL), ITU-T G.9962 (MIMO), ITU-T G.9964 (PSD), ITU-T G.997.1, ITU-T G.998.1, ITU-T G.998.2, ITU-T G.998.3, ITU-T G.998.4, ITU-T G.999.1, ITU-T I.322
Laptop	IEC 60076, IEC 60870-5-101, IEC 60870-5-104, IEC 61360, IEC 61400-25, IEC 61850 series, IEC 61850-80-1, IEC 61850-8-1, IEC 61850-8-2, IEC 61850-90-2, IEC 61850-90-3, IEC 61897, IEC 61968 series, IEC 61968-1, IEC 61968-100, IEC 61968-11, IEC 61968-13, IEC 61968-2, IEC 61968-3, IEC 61968-4, IEC 61968-6, IEC 61968-8, IEC 61968-9, IEC 61970 series, IEC 62271-1x series, IEC 62271-2x series, IEC 62351 series, IEC 62351-1, IEC 62357, IEC 62361 series, IEC 62361-100
Load	IEC 60870-5-101, IEC 60870-5-104, IEC 60904 series, IEC 61131, IEC 61158 series, IEC 61334-4-32, IEC 61334-4-41, IEC 61334-4-511, IEC 61334-4-512, IEC 61334-5-1, IEC 61334-61, IEC 61400-1, IEC 61400-2, IEC 61400-25-2, IEC 61400-25-3, IEC 61400-25-4, IEC 61400-3, IEC 61499, IEC 61724, IEC 61730, IEC 61784-1, IEC 61836, IEC 61850-6, IEC 61850-7-2, IEC 61850-7-3, IEC 61850-7-4, IEC 61850-7-410, IEC 61850-7-420, IEC 61850-80-4, IEC 61850-8-1, IEC 61850-8-2, IEC 61850-90-10, IEC 61850-90-11, IEC 61850-90-12, IEC 61850-90-15, IEC 61850-90-2, IEC 61850-90-7, IEC 61850-



SUBFIELD	APPLICABLE STANDARDS
	90-9, IEC 62056-1-0, IEC 62056-31, IEC 62056-3-1, IEC 62056-3-2, IEC 62056-42, IEC 62056-46, IEC 62056-47, IEC 62056-4-7, IEC 62056-53, IEC 62056-5-3, IEC 62056-5-8, IEC 62056-6-1, IEC 62056-6-2, IEC 62056-6-9, IEC 62056-7-6, IEC 62056-8-3, IEC 62056-9-7, IEC 62282, IEC 62325 series, IEC 62351 series, ISO 16484 series, ISO/IEC 14543-3 series, ISO/IEC 14908 series, ITU-T G.9901, ITU-T G.9902, ITU-T G.9903, ITU-T G.9904
Load Control	IEC 60364, IEC 60870-5-101, IEC 60870-5-104, IEC 60904 series, IEC 61131, IEC 61158 series, IEC 61334-4-32, IEC 61334-4-41, IEC 61334-4-511, IEC 61334-4-512, IEC 61334-5-1, IEC 61334-61, IEC 61400-1, IEC 61400-2, IEC 61400-25-2, IEC 61400-25-3, IEC 61400-25-4, IEC 61400-3, IEC 61499, IEC 61724, IEC 61730, IEC 61784, IEC 61784-1, IEC 61836, IEC 61850 series, IEC 61850-6, IEC 61850-7-2, IEC 61850-7-3, IEC 61850-7-4, IEC 61850-7-410, IEC 61850-7-420, IEC 61850-80-4, IEC 61850-8-1, IEC 61850-8-2, IEC 61850-90-10, IEC 61850-90-11, IEC 61850-90-12, IEC 61850-90-15, IEC 61850-90-2, IEC 61850-90-7, IEC 61850-90-9, IEC 62056 series, IEC 62056-1-0, IEC 62056-31, IEC 62056-3-1, IEC 62056-3-2, IEC 62056-42, IEC 62056-46, IEC 62056-47, IEC 62056-4-7, IEC 62056-53, IEC 62056-5-3, IEC 62056-5-8, IEC 62056-6-1, IEC 62056-6-2, IEC 62056-6-9, IEC 62056-7-6, IEC 62056-8-3, IEC 62056-9-7, IEC 62282, IEC 62325 series, IEC 62351 series, IEC 62439, IEC 62443 series, IEC 62541 series, IEC 62872 Ed. 1.0, ISO 16484 series, ISO/IEC 14543-3 series, ISO/IEC 14908 series, ITU-T G.9901, ITU-T G.9902, ITU-T G.9903, ITU-T G.9904
Local Storage	IEC 60364, IEC 60870-5-101, IEC 60870-5-104, IEC 60904 series, IEC 61131, IEC 61158 series, IEC 61334-4-32, IEC 61334-4-41, IEC 61334-4-511, IEC 61334-4-512, IEC 61334-5-1, IEC 61334-61, IEC 61400-1, IEC 61400-2, IEC 61400-25-2, IEC 61400-25-3, IEC 61400-25-4, IEC 61400-3, IEC 61499, IEC 61724, IEC 61730, IEC 61784, IEC 61784-1, IEC 61836, IEC 61850 series, IEC 61850-6, IEC 61850-7-2, IEC 61850-7-3, IEC 61850-7-4, IEC 61850-7-410, IEC 61850-7-420, IEC 61850-80-4, IEC 61850-8-1, IEC 61850-8-2, IEC 61850-90-10, IEC 61850-90-11, IEC 61850-90-12, IEC 61850-90-15, IEC 61850-90-2, IEC 61850-90-7, IEC 61850-90-9, IEC 62056 series, IEC 62056-1-0, IEC 62056-31, IEC 62056-3-1, IEC 62056-3-2, IEC 62056-42, IEC 62056-46, IEC 62056-47, IEC 62056-4-7, IEC 62056-53, IEC 62056-5-3, IEC 62056-5-8, IEC 62056-6-1, IEC 62056-6-2, IEC 62056-6-9, IEC 62056-7-6, IEC 62056-8-3, IEC 62056-9-7, IEC 62282, IEC 62325 series, IEC 62351 series, IEC 62439, IEC 62443 series, IEC 62541 series, IEC 62872 Ed. 1.0, ISO 16484 series, ISO/IEC 14543-3 series, ISO/IEC 14908 series, ITU-T G.9901, ITU-T G.9902, ITU-T G.9903, ITU-T G.9904
MDMS	IEC 60870-5-101, IEC 60870-5-104, IEC 60904 series, IEC 61131, IEC 61158 series, IEC 61334-4-32, IEC 61334-4-41, IEC 61334-4-511, IEC 61334-4-512, IEC 61334-5-1, IEC 61334-61, IEC 61400-1, IEC 61400-2, IEC 61400-25-2, IEC 61400-25-3, IEC 61400-25-4, IEC 61400-3, IEC 61499, IEC 61724, IEC 61730, IEC 61784-1, IEC 61836, IEC 61850 series, IEC 61850-6, IEC 61850-7-2, IEC 61850-7-3, IEC 61850-7-4, IEC 61850-7-410, IEC 61850-7-420, IEC 61850-80-4, IEC 61850-8-1, IEC 61850-8-2, IEC 61850-90-10, IEC 61850-90-11, IEC 61850-90-12, IEC 61850-90-15, IEC 61850-90-2, IEC 61850-90-7, IEC 61850-90-9, IEC 61968 series, IEC 61968-100, IEC 61968-9, IEC 61970 series, IEC 62056 series, IEC 62056-1-0, IEC 62056-31, IEC 62056-3-1, IEC 62056-3-2, IEC 62056-42, IEC 62056-46, IEC 62056-47, IEC 62056-4-7, IEC 62056-53, IEC 62056-5-3, IEC 62056-5-8, IEC 62056-6-1, IEC 62056-6-2, IEC 62056-6-9, IEC 62056-7-6, IEC 62056-8-3, IEC 62056-9-7, IEC 62282, IEC 62325 series, IEC 62351 series, IEC 62357, IEC 62361 series, IEC 62361-102, ISO 16484 series, ISO/IEC 14543-3 series, ISO/IEC 14908 series, ITU-T G.9901, ITU-T G.9902, ITU-T G.9903, ITU-T G.9904
Meter Data Concentrator	IEC 60870-5-101, IEC 60870-5-104, IEC 60870-5-5, IEC 60904 series, IEC 61131, IEC 61158 series, IEC 61334-4-32, IEC 61334-4-41, IEC 61334-4-511, IEC 61334-4-512, IEC 61334-5-1, IEC 61334-61, IEC 61400-1, IEC 61400-2, IEC 61400-25-2, IEC 61400-25-3, IEC 61400-25-4, IEC 61400-3, IEC 61499, IEC 61588 (IEEE 1588), IEC 61724, IEC 61730, IEC 61784-1, IEC 61836, IEC 61850-6, IEC 61850-7-2, IEC 61850-7-3, IEC 61850-7-4, IEC 61850-7-410, IEC 61850-7-420, IEC 61850-80-4, IEC 61850-8-1, IEC 61850-8-2, IEC 61850-90-10, IEC 61850-90-11, IEC 61850-90-12, IEC 61850-90-15, IEC 61850-90-2, IEC 61850-90-4, IEC 61850-90-5, IEC 61850-90-7, IEC 61850-90-9, IEC 62056-1-0, IEC 62056-31, IEC 62056-3-1, IEC 62056-3-2, IEC 62056-42, IEC 62056-46, IEC 62056-47, IEC 62056-4-7, IEC 62056-53, IEC 62056-5-3, IEC 62056-5-8, IEC 62056-6-1, IEC 62056-6-2, IEC 62056-6-9, IEC 62056-7-6, IEC 62056-8-3, IEC 62056-9-7, IEC 62282, IEC 62325 series, IEC 62351 series,

SUBFIELD	APPLICABLE STANDARDS
	ISO 16484 series, ISO 8601, ISO/IEC 14543-3 series, ISO/IEC 14908 series, ITU-T G.9901, ITU-T G.9902, ITU-T G.9903, ITU-T G.9904
Mobile Device	IEC 60076, IEC 60870-5-101, IEC 60870-5-104, IEC 61360, IEC 61400-25, IEC 61850 series, IEC 61850-80-1, IEC 61850-8-1, IEC 61850-8-2, IEC 61850-90-2, IEC 61850-90-3, IEC 61897, IEC 61968 series, IEC 61968-1, IEC 61968-100, IEC 61968-11, IEC 61968-13, IEC 61968-2, IEC 61968-3, IEC 61968-4, IEC 61968-6, IEC 61968-8, IEC 61968-9, IEC 61970 series, IEC 62271-1x series, IEC 62271-2x series, IEC 62351 series, IEC 62351-1, IEC 62357, IEC 62361 series, IEC 62361-100
Neighborhood Network	IEC 60870-5-101, IEC 60870-5-102, IEC 60870-5-103, IEC 60870-5-104, IEC 60904 series, IEC 61131, IEC 61158 series, IEC 61334-4-32, IEC 61334-4-41, IEC 61334-4-511, IEC 61334-4-512, IEC 61334-5-1, IEC 61334-61, IEC 61400-1, IEC 61400-2, IEC 61400-25-2, IEC 61400-25-3, IEC 61400-25-4, IEC 61400-3, IEC 61499, IEC 61724, IEC 61730, IEC 61784, IEC 61784-1, IEC 61836, IEC 61850-6, IEC 61850-7-1, IEC 61850-7-2, IEC 61850-7-3, IEC 61850-7-4, IEC 61850-7-410, IEC 61850-7-420, IEC 61850-80-4, IEC 61850-8-1, IEC 61850-8-2, IEC 61850-90-1, IEC 61850-90-10, IEC 61850-90-11, IEC 61850-90-12, IEC 61850-90-15, IEC 61850-90-2, IEC 61850-90-4, IEC 61850-90-5, IEC 61850-90-7, IEC 61850-90-9, IEC 61850-9-2, IEC 61968 series, IEC 61968-100, IEC 61970 series, IEC 62056-1-0, IEC 62056-31, IEC 62056-3-1, IEC 62056-3-2, IEC 62056-42, IEC 62056-46, IEC 62056-47, IEC 62056-4-7, IEC 62056-53, IEC 62056-5-3, IEC 62056-5-8, IEC 62056-6-1, IEC 62056-6-2, IEC 62056-6-9, IEC 62056-7-6, IEC 62056-8-3, IEC 62056-9-7, IEC 62282, IEC 62325 series, IEC 62351 series, IEC 62439, IEC 62488-1 (Formerly EN60663) - Part 1, IEC 62541 series, ISO 16484 series, ISO/IEC 12139-1, ISO/IEC 14543-3, ISO/IEC 14543-3 series, ISO/IEC 14908 series, ISO/IEC 14908-1, ISO/IEC 14908-2, ISO/IEC 14908-3, ISO/IEC 14908-4, ISO/IEC 15802 IEEE 802.1, ISO/IEC 7498-1, ISO/IEC 8802-3, ITU-T G.7041, ITU-T G.7042, ITU-T G.707, ITU-T G.709, ITU-T G.781, ITU-T G.783, ITU-T G.798, ITU-T G.803, ITU-T G.872, ITU-T G.983.1, ITU-T G.983.2, ITU-T G.983.3, ITU-T G.983.4, ITU-T G.983.5, ITU-T G.984.1, ITU-T G.984.2, ITU-T G.984.3, ITU-T G.984.4, ITU-T G.984.5, ITU-T G.984.6, ITU-T G.984.7, ITU-T G.987.1, ITU-T G.987.2, ITU-T G.987.3, ITU-T G.9901, ITU-T G.9902, ITU-T G.9903, ITU-T G.9904, ITU-T G.991.1, ITU-T G.991.2, ITU-T G.992.1, ITU-T G.992.2, ITU-T G.992.3, ITU-T G.992.4, ITU-T G.993.1, ITU-T G.993.2, ITU-T G.993.5, ITU-T G.994.1, ITU-T G.995.1, ITU-T G.996.1, ITU-T G.996.2, ITU-T G.9960 (PHY), ITU-T G.9961 (DLL), ITU-T G.9962 (MIMO), ITU-T G.9964 (PSD), ITU-T G.997.1, ITU-T G.998.1, ITU-T G.998.2, ITU-T G.998.3, ITU-T G.998.4, ITU-T G.999.1, ITU-T I.322
Network Interface Controller	IEC 61400-25-2, IEC 61400-25-3, IEC 61400-25-4, IEC 61400-3, IEC 61499, IEC 61724, IEC 61730, IEC 61784, IEC 61784-1, IEC 61836, IEC 61850-6, IEC 61850-7-1, IEC 61850-7-2, IEC 61850-7-3, IEC 61850-7-4, IEC 61850-7-410, IEC 61850-7-420, IEC 61850-80-4, IEC 61850-8-1, IEC 61850-8-2, IEC 61850-90-1, IEC 61850-90-10, IEC 61850-90-11, IEC 61850-90-12, IEC 61850-90-15, IEC 61850-90-2, IEC 61850-90-4, IEC 61850-90-5, IEC 61850-90-7, IEC 61850-90-9, IEC 61850-9-2, IEC 62056-1-0, IEC 62056-31, IEC 62056-3-1, IEC 62056-3-2, IEC 62056-42, IEC 62056-46, IEC 62056-47, IEC 62056-4-7, IEC 62056-53, IEC 62056-5-3, IEC 62056-5-8, IEC 62056-6-1, IEC 62056-6-2, IEC 62056-6-9, IEC 62056-7-6, IEC 62056-8-3, IEC 62056-9-7, IEC 62282, IEC 62325 series, IEC 62351 series, IEC 62351-1, IEC 62351-10, IEC 62351-11, IEC 62351-2, IEC 62351-3, IEC 62351-4, IEC 62351-5, IEC 62351-6, IEC 62351-7, IEC 62351-8, IEC 62351-9, IEC 62439, IEC 62443 series, IEC 62488-1 (Formerly EN60663) - Part 1, IEC 62541 series, ITU-T G.991.1, ITU-T G.991.2, ITU-T G.992.1, ITU-T G.992.2, ITU-T G.992.3, ITU-T G.992.4, ITU-T G.993.1, ITU-T G.993.2, ITU-T G.993.5, ITU-T G.994.1, ITU-T G.995.1, ITU-T G.996.1, ITU-T G.996.2, ITU-T G.9960 (PHY), ITU-T G.9961 (DLL), ITU-T G.9962 (MIMO), ITU-T G.9964 (PSD), ITU-T G.997.1, ITU-T G.998.1, ITU-T G.998.2, ITU-T G.998.3, ITU-T G.998.4, ITU-T G.999.1, ITU-T I.322, ITU-T G.7041, ITU-T G.7042, ITU-T G.707, ITU-T G.709, ITU-T G.781, ITU-T G.783, ITU-T G.798, ITU-T G.803, ITU-T G.872, ITU-T G.983.1, ITU-T G.983.2, ITU-T G.983.3, ITU-T G.983.4, ITU-T G.983.5, ITU-T G.984.1, ITU-T G.984.2, ITU-T G.984.3, ITU-T G.984.4, ITU-T G.984.5, ITU-T G.984.6, ITU-T G.984.7, ITU-T G.987.1, ITU-T G.987.2, ITU-T G.987.3, ITU-T G.9901, ITU-T G.9902, ITU-T G.9903, ITU-T G.9904, IEC 60870-5-101, IEC 60870-5-102, IEC 60870-5-103, IEC 60870-5-104, IEC 60904 series, IEC 61131, IEC 61158 series, IEC 61334-4-32, IEC 61334-4-41, IEC 61334-4-511, IEC 61334-4-512, IEC 61334-5-1, IEC 61334-61, IEC 61400-1, IEC 61400-2, IEC 61400-25, ISO 16484 series, ISO/IEC 12139-1, ISO/IEC 14543-3, ISO/IEC 14543-3 series,

SUBFIELD	APPLICABLE STANDARDS
	ISO/IEC 14908 series, ISO/IEC 14908-1, ISO/IEC 14908-2, ISO/IEC 14908-3, ISO/IEC 14908-4, ISO/IEC 15118, ISO/IEC 15802 IEEE 802.1, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 7498-1, ISO/IEC 8802-3
OMS	IEC 60076, IEC 60870-5-101, IEC 60870-5-104, IEC 61360, IEC 61400-25, IEC 61850 series, IEC 61850-80-1, IEC 61850-80-4, IEC 61850-8-1, IEC 61850-8-2, IEC 61850-90-2, IEC 61850-90-3, IEC 61897, IEC 61968 series, IEC 61968-1, IEC 61968-100, IEC 61968-11, IEC 61968-13, IEC 61968-2, IEC 61968-3, IEC 61968-4, IEC 61968-6, IEC 61968-8, IEC 61968-9, IEC 61970 series, IEC 61970-1, IEC 61970-2, IEC 61970-301, IEC 61970-401, IEC 61970-452, IEC 61970-453, IEC 61970-456, IEC 61970-458, IEC 61970-501, IEC 61970-502-8, IEC 61970-552, IEC 62056 series, IEC 62056-6-9, IEC 62271-1x series, IEC 62271-2x series, IEC 62351 series, IEC 62351-1, IEC 62357, IEC 62361 series, IEC 62361-100, IEC 62361-102
OPER Backhaul Network	IEC 60076, IEC 60193, ITU-T G.7041, ITU-T G.7042, ITU-T G.707, ITU-T G.709, ITU-T G.781, ITU-T G.783, ITU-T G.798, ITU-T G.803, ITU-T G.872, ITU-T G.983.1, ITU-T G.983.2, ITU-T G.983.3, ITU-T G.983.4, ITU-T G.983.5, ITU-T G.984.1, ITU-T G.984.2, ITU-T G.984.3, ITU-T G.984.4, ITU-T G.984.5, ITU-T G.984.6, ITU-T G.984.7, ITU-T G.987.1, ITU-T G.987.2, ITU-T G.987.3, ITU-T G.9901, ITU-T G.9902, ITU-T G.9903, ITU-T G.9904, ITU-T G.991.1, ITU-T G.991.2, ITU-T G.992.1, ITU-T G.992.2, ITU-T G.992.3, ITU-T G.992.4, ITU-T G.993.1, ITU-T G.993.2, ITU-T G.993.5, ITU-T G.994.1, ITU-T G.995.1, ITU-T G.996.1, ITU-T G.996.2, ITU-T G.9960 (PHY), ITU-T G.9961 (DLL), ITU-T G.9962 (MIMO), ITU-T G.9964 (PSD), ITU-T G.997.1, ITU-T G.998.1, ITU-T G.998.2, ITU-T G.998.3, ITU-T G.998.4, ITU-T G.999.1, ITU-T I.322, IEC 60255, IEC 60255-24, IEC 60870-5-101, IEC 60870-5-102, IEC 60870-5-103, IEC 60870-5-104, IEC 60870-6, IEC 60904 series, IEC 61000 Series, IEC 61000-2-12, IEC 61000-2-2, IEC 61000-3-13, IEC 61000-3-14, IEC 61000-3-15, IEC 61000-3-6, IEC 61000-3-7, IEC 61000-4-19, IEC 61000-4-30, IEC 61000-6-1, IEC 61000-6-2, IEC 61000-6-3, IEC 61000-6-4, IEC 61000-6-4, IEC 61000-6-5, IEC 61131, IEC 61158 series, IEC 61326, IEC 61360, IEC 61400 series, IEC 61400-1, IEC 61400-2, IEC 61400-25, IEC 61400-25-2, IEC 61400-25-3, IEC 61400-25-4, IEC 61400-3, IEC 61499, IEC 61512, IEC 61588 (IEEE 1588), IEC 61724, IEC 61727, IEC 61730, IEC 61784, IEC 61784-1, IEC 61804, IEC 61836, IEC 61850 series, IEC 61850-6, IEC 61850-7-1, IEC 61850-7-2, IEC 61850-7-3, IEC 61850-7-4, IEC 61850-7-410, IEC 61850-7-420, IEC 61850-80-1, IEC 61850-80-4, IEC 61850-8-1, IEC 61850-8-2, IEC 61850-90-1, IEC 61850-90-10, IEC 61850-90-11, IEC 61850-90-12, IEC 61850-90-13, IEC 61850-90-15, IEC 61850-90-2, IEC 61850-90-3, IEC 61850-90-4, IEC 61850-90-5, IEC 61850-90-6, IEC 61850-90-7, IEC 61850-90-9, IEC 61850-9-2, IEC 61869, IEC 61897, IEC 61968 series, IEC 61968-1, IEC 61968-100, IEC 61968-11, IEC 61968-13, IEC 61968-2, IEC 61968-3, IEC 61968-4, IEC 61968-6, IEC 61968-8, IEC 61968-9, IEC 61970 series, IEC 61970-1, IEC 61970-2, IEC 61970-301, IEC 61970-401, IEC 61970-452, IEC 61970-453, IEC 61970-456, IEC 61970-458, IEC 61970-501, IEC 61970-502-8, IEC 61970-552, IEC 61987, IEC 62264, IEC 62271-1x series, IEC 62271-2x series, IEC 62271-3, IEC 62282, IEC 62282 series, IEC 62325, IEC 62325-301, IEC 62325-351, IEC 62325-450, IEC 62325-451-1, IEC 62325-451-2, IEC 62325-451-3, IEC 62351 series, IEC 62351-1, IEC 62357, IEC 62361 series, IEC 62361-100, IEC 62361-101, IEC 62439, IEC 62446, IEC 62488-1 (Formerly EN60663) - Part 1, IEC 62541 series, IEC 62541-1, IEC 62541-10, IEC 62541-2, IEC 62541-3, IEC 62541-4, IEC 62541-5, IEC 62541-6, IEC 62541-7, IEC 62541-8, IEC 62541-9, ISO 81400, ISO 8601 (IEC 28601), ISO/IEC 12139-1, ISO/IEC 14543-3, ISO/IEC 14908-1, ISO/IEC 14908-2, ISO/IEC 14908-3, ISO/IEC 14908-4, ISO/IEC 15802 IEEE 802.1, ISO/IEC 7498-1, ISO/IEC 8802-3
Operation Meter	IEC 60193, IEC 60255, IEC 60870-5-101, IEC 60870-5-103, IEC 60870-5-104, IEC 60904 series, IEC 61131, IEC 61158 series, IEC 61360, IEC 61400 series, IEC 61400-25-2, IEC 61499, IEC 61512, IEC 61727, IEC 61784-1, IEC 61804, IEC 61850-7-2, IEC 61850-7-3, IEC 61850-7-4, IEC 61850-7-410, IEC 61850-8-1, IEC 61850-8-2, IEC 61850-90-1, IEC 61850-90-13, IEC 61850-90-2, IEC 61850-90-4, IEC 61850-9-2, IEC 61968-1, IEC 61968-100, IEC 61968-11, IEC 61968-2, IEC 61968-3, IEC 61968-4, IEC 61968-6, IEC 61968-9, IEC 61970-1, IEC 61970-2, IEC 61970-301, IEC 61970-401, IEC 61970-452, IEC 61970-453, IEC 61970-456, IEC 61970-458, IEC 61970-501, IEC 61970-502-8, IEC 61970-552, IEC 61987, IEC 62264, IEC 62282 series, IEC 62325-301, IEC 62325-351, IEC 62325-450, IEC 62325-451-1, IEC 62325-451-2, IEC 62325-451-3, IEC 62351 series, IEC 62361-100, IEC 62361-101,

SUBFIELD	APPLICABLE STANDARDS
	IEC 62439, IEC 62446, IEC 62541-1, IEC 62541-10, IEC 62541-2, IEC 62541-3, IEC 62541-4, IEC 62541-5, IEC 62541-6, IEC 62541-7, IEC 62541-8, IEC 62541-9, ISO 81400
PEV	IEC 60364, IEC 60364-4-41, IEC 60364-5-53, IEC 60364-5-55, IEC 60364-7-712, IEC 60364-7-722, IEC 60783, IEC 60784, IEC 60785, IEC 60786, IEC 61850-90-8, IEC 61851 series, IEC 61851-1, IEC 61851-21, IEC 61851-22, IEC 61851-23, IEC 61851-24, IEC 61894, IEC 61980 series, IEC 61982 series, IEC 62196, IEC 62351 series, IEC 62443 series, ISO 6469, ISO 8713, ISO/IEC 15118 series
Phasor Data Concentrator	IEC 60870-5-101, IEC 60870-5-103, IEC 60870-5-104, IEC 60870-5-5, IEC 61588 (IEEE 1588), IEC 61850-6, IEC 61850-7-2, IEC 61850-7-3, IEC 61850-7-4, IEC 61850-80-1, IEC 61850-8-1, IEC 61850-8-2, IEC 61850-90-1, IEC 61850-90-2, IEC 61850-90-3, IEC 61850-90-4, IEC 61850-90-5, IEC 61850-9-2, IEC 61869, IEC 62351 series, ISO 8601, ISO 8601 (IEC 28601)
PMU	IEC 60870-5-101, IEC 60870-5-103, IEC 60870-5-104, IEC 60870-5-5, IEC 61588 (IEEE 1588), IEC 61850-6, IEC 61850-7-2, IEC 61850-7-3, IEC 61850-7-4, IEC 61850-80-1, IEC 61850-8-1, IEC 61850-8-2, IEC 61850-90-1, IEC 61850-90-2, IEC 61850-90-3, IEC 61850-90-4, IEC 61850-90-5, IEC 61850-9-2, IEC 61869, IEC 62351 series, ISO 8601
Power Scheduling	IEC 60193, IEC 60255, IEC 60870-5-101, IEC 60870-5-103, IEC 60870-5-104, IEC 60870-6, IEC 60904 series, IEC 61131, IEC 61158 series, IEC 61360, IEC 61400 series, IEC 61400-25-2, IEC 61499, IEC 61512, IEC 61727, IEC 61784-1, IEC 61804, IEC 61850 series, IEC 61850-7-2, IEC 61850-7-3, IEC 61850-7-4, IEC 61850-7-410, IEC 61850-8-1, IEC 61850-8-2, IEC 61850-90-1, IEC 61850-90-13, IEC 61850-90-2, IEC 61850-90-4, IEC 61850-9-2, IEC 61968-1, IEC 61968-100, IEC 61968-11, IEC 61968-2, IEC 61968-3, IEC 61968-4, IEC 61968-6, IEC 61968-9, IEC 61970-1, IEC 61970-2, IEC 61970-301, IEC 61970-401, IEC 61970-452, IEC 61970-453, IEC 61970-456, IEC 61970-458, IEC 61970-501, IEC 61970-502-8, IEC 61970-552, IEC 61987, IEC 62264, IEC 62282 series, IEC 62325, IEC 62325-301, IEC 62325-351, IEC 62325-450, IEC 62325-451-1, IEC 62325-451-2, IEC 62325-451-3, IEC 62351 series, IEC 62357, IEC 62361 series, IEC 62361-100, IEC 62361-101, IEC 62439, IEC 62446, IEC 62541-1, IEC 62541-10, IEC 62541-2, IEC 62541-3, IEC 62541-4, IEC 62541-5, IEC 62541-6, IEC 62541-7, IEC 62541-8, IEC 62541-9, ISO 19142, ISO 81400
Process Automation System	IEC 60364, IEC 60870-5-101, IEC 60870-5-104, IEC 60904 series, IEC 61131, IEC 61158 series, IEC 61334-4-32, IEC 61334-4-41, IEC 61334-4-511, IEC 61334-4-512, IEC 61334-5-1, IEC 61334-61, IEC 61400-1, IEC 61400-2, IEC 61400-25, IEC 61400-25-2, IEC 61400-25-3, IEC 61400-25-4, IEC 61400-3, IEC 61499, IEC 61724, IEC 61730, IEC 61784, IEC 61784-1, IEC 61836, IEC 61850 series, IEC 61850-6, IEC 61850-7-2, IEC 61850-7-3, IEC 61850-7-4, IEC 61850-7-410, IEC 61850-7-420, IEC 61850-80-4, IEC 61850-8-1, IEC 61850-8-2, IEC 61850-90-10, IEC 61850-90-11, IEC 61850-90-12, IEC 61850-90-15, IEC 61850-90-2, IEC 61850-90-5, IEC 61850-90-7, IEC 61850-90-9, IEC 62056 series, IEC 62056-1-0, IEC 62056-31, IEC 62056-3-1, IEC 62056-3-2, IEC 62056-42, IEC 62056-46, IEC 62056-47, IEC 62056-4-7, IEC 62056-53, IEC 62056-5-3, IEC 62056-5-8, IEC 62056-6-1, IEC 62056-6-2, IEC 62056-6-9, IEC 62056-7-6, IEC 62056-8-3, IEC 62056-9-7, IEC 62282, IEC 62325 series, IEC 62351 series, IEC 62351-1, IEC 62351-10, IEC 62351-11, IEC 62351-2, IEC 62351-3, IEC 62351-4, IEC 62351-5, IEC 62351-6, IEC 62351-7, IEC 62351-8, IEC 62351-9, IEC 62439, IEC 62443 series, IEC 62541 series, IEC 62872 Ed. 1.0, ISO 16484 series, ISO/IEC 14543-3 series, ISO/IEC 14908 series, ISO/IEC 15118, ISO/IEC 27001, ISO/IEC 27002, ITU-T G.9901, ITU-T G.9902, ITU-T G.9903, ITU-T G.9904
Relay	IEC 60193, IEC 60255, IEC 60255-24, IEC 60870-5-101, IEC 60870-5-103, IEC 60870-5-104, IEC 60870-5-5, IEC 60870-6, IEC 60904 series, IEC 61131, IEC 61158 series, IEC 61360, IEC 61400 series, IEC 61400-1, IEC 61400-2, IEC 61400-25, IEC 61400-25-2, IEC 61400-25-3, IEC 61400-25-4, IEC 61400-3, IEC 61499, IEC 61512, IEC 61588 (IEEE 1588), IEC 61724, IEC 61727, IEC 61730, IEC 61784-1, IEC 61804, IEC 61836, IEC 61850 series, IEC 61850-6, IEC 61850-7-2, IEC 61850-7-3, IEC 61850-7-4, IEC 61850-7-410, IEC 61850-7-420, IEC 61850-80-1, IEC 61850-80-4, IEC 61850-8-1, IEC 61850-8-2, IEC 61850-90-1, IEC 61850-90-10, IEC 61850-90-11, IEC 61850-90-12, IEC 61850-90-13, IEC 61850-90-15, IEC 61850-90-2, IEC 61850-90-3, IEC 61850-90-4, IEC 61850-90-5, IEC 61850-90-6, IEC 61850-90-7, IEC 61850-90-9, IEC 61850-9-2, IEC 61869, IEC 61987, IEC 62056-5-

SUBFIELD	APPLICABLE STANDARDS
	3, IEC 62264, IEC 62271-3, IEC 62282, IEC 62282 series, IEC 62325, IEC 62325-301, IEC 62325-351, IEC 62325-450, IEC 62325-451-1, IEC 62325-451-2, IEC 62325-451-3, IEC 62351 series, IEC 62351-1, IEC 62351-10, IEC 62351-11, IEC 62351-2, IEC 62351-3, IEC 62351-4, IEC 62351-5, IEC 62351-6, IEC 62351-7, IEC 62351-8, IEC 62351-9, IEC 62357, IEC 62361 series, IEC 62361-100, IEC 62361-101, IEC 62439, IEC 62443 series, IEC 62446, IEC 62541-1, IEC 62541-10, IEC 62541-2, IEC 62541-3, IEC 62541-4, IEC 62541-5, IEC 62541-6, IEC 62541-7, IEC 62541-8, IEC 62541-9, ISO 81400, ISO 8601, ISO/IEC 15118, ISO/IEC 27001, ISO/IEC 27002
Revenue Meter	IEC 61730, IEC 61784-1, IEC 61836, IEC 61850-6, IEC 61850-7-2, IEC 61850-7-3, IEC 61850-7-4, IEC 61850-7-410, IEC 61850-7-420, IEC 61850-80-4, IEC 61850-8-1, IEC 61850-8-2, IEC 61850-90-10, IEC 61850-90-11, IEC 61850-90-12, IEC 61850-90-15, IEC 61850-90-2, IEC 61850-90-4, IEC 61850-90-5, IEC 61850-90-7, IEC 61850-90-9, IEC 62056-1-0, IEC 62056-31, IEC 62056-3-1, IEC 62056-3-2, IEC 62056-42, IEC 62056-46, IEC 62056-47, IEC 62056-4-7, IEC 62056-53, IEC 62056-5-3, IEC 62056-5-8, IEC 62056-6-1, IEC 62056-6-2, IEC 62056-6-9, IEC 62056-7-6, IEC 62056-8-3, IEC 62056-9-7, IEC 62282, IEC 62325 series, IEC 62351 series, ISO 16484 series, ISO 8601, ISO/IEC 14543-3 series, ISO/IEC 14908 series, ITU-T G.9901, ITU-T G.9902, ITU-T G.9903, ITU-T G.9904, IEC 60870-5-101, IEC 60870-5-104, IEC 60870-5-5, IEC 60904 series, IEC 61131, IEC 61158 series, IEC 61334-4-32, IEC 61334-4-41, IEC 61334-4-511, IEC 61334-4-512, IEC 61334-5-1, IEC 61334-61, IEC 61400-1, IEC 61400-2, IEC 61400-25-2, IEC 61400-25-3, IEC 61400-25-4, IEC 61400-3, IEC 61499, IEC 61588 (IEEE 1588), IEC 61724
RTU	IEC 60870-5-101, IEC 60870-5-104, IEC 60870-5-5, IEC 60904 series, IEC 61000 Series, IEC 61000-2-12, IEC 61000-2-2, IEC 61000-3-13, IEC 61000-3-14, IEC 61000-3-15, IEC 61000-3-6, IEC 61000-3-7, IEC 61000-4-19, IEC 61000-4-30, IEC 61000-6-1, IEC 61000-6-2, IEC 61000-6-3, IEC 61000-6-4, IEC 61000-6-4, IEC 61000-6-5, IEC 61131, IEC 61158 series, IEC 61326, IEC 61400-1, IEC 61400-2, IEC 61400-25, IEC 61400-25-2, IEC 61400-25-3, IEC 61400-25-4, IEC 61400-3, IEC 61499, IEC 61588 (IEEE 1588), IEC 61724, IEC 61730, IEC 61784-1, IEC 61836, IEC 61850 series, IEC 61850-6, IEC 61850-7-2, IEC 61850-7-3, IEC 61850-7-4, IEC 61850-7-410, IEC 61850-7-420, IEC 61850-8-1, IEC 61850-8-2, IEC 61850-90-10, IEC 61850-90-11, IEC 61850-90-12, IEC 61850-90-15, IEC 61850-90-2, IEC 61850-90-4, IEC 61850-90-5, IEC 61850-90-7, IEC 61850-90-9, IEC 61968 series, IEC 61968-1, IEC 61968-100, IEC 61968-11, IEC 61968-13, IEC 61968-2, IEC 61968-3, IEC 61968-4, IEC 61968-6, IEC 61968-8, IEC 61968-9, IEC 61970 series, IEC 62056-5-3, IEC 62282, IEC 62351 series, IEC 62351-1, IEC 62351-10, IEC 62351-11, IEC 62351-2, IEC 62351-3, IEC 62351-4, IEC 62351-5, IEC 62351-6, IEC 62351-7, IEC 62351-8, IEC 62351-9, IEC 62357, IEC 62361 series, IEC 62361-100, IEC 62443 series, ISO 8601, ISO/IEC 15118, ISO/IEC 27001, ISO/IEC 27002
SCADA	IEC 61400-25, IEC 61850-90-5, IEC 61968 series, IEC 61970 series, IEC 61970-301, IEC 62056-5-3, IEC 62325 series, IEC 62325-301, IEC 62325-351, IEC 62325-450, IEC 62325-451-1, IEC 62325-451-2, IEC 62325-451-3, IEC 62325-503, IEC 62351 series, IEC 62351-1, IEC 62351-10, IEC 62351-11, IEC 62351-2, IEC 62351-3, IEC 62351-4, IEC 62351-5, IEC 62351-6, IEC 62351-7, IEC 62351-8, IEC 62351-9, IEC 62443 series, ISO/IEC 15118, ISO/IEC 27001, ISO/IEC 27002
Secondary Generation Control	IEC 60255-24, IEC 60870-5-101, IEC 60870-5-103, IEC 60870-5-104, IEC 60870-6, IEC 61158 series, IEC 61400-25, IEC 61850 series, IEC 61850-6, IEC 61850-7-2, IEC 61850-7-3, IEC 61850-7-4, IEC 61850-7-410, IEC 61850-80-1, IEC 61850-80-4, IEC 61850-8-1, IEC 61850-8-2, IEC 61850-90-1, IEC 61850-90-11, IEC 61850-90-12, IEC 61850-90-2, IEC 61850-90-3, IEC 61850-90-4, IEC 61850-90-5, IEC 61850-90-6, IEC 61850-90-7, IEC 61850-9-2, IEC 61869, IEC 61968 series, IEC 61970 series, IEC 61970-1, IEC 61970-2, IEC 61970-301, IEC 61970-401, IEC 61970-452, IEC 61970-453, IEC 61970-456, IEC 61970-458, IEC 61970-501, IEC 61970-502-8, IEC 61970-552, IEC 62271-3, IEC 62325, IEC 62351 series, IEC 62357, IEC 62361 series, IEC 62439
Smart Plug	IEC 60364, IEC 60870 series, IEC 60870-5-101, IEC 60870-5-104, IEC 60904 series, IEC 61131, IEC 61158 series, IEC 61334-4-32, IEC 61334-4-41, IEC 61334-4-511, IEC 61334-4-512, IEC 61334-5-1, IEC 61334-61, IEC 61400-1, IEC 61400-2, IEC 61400-25-2, IEC 61400-25-3, IEC 61400-25-4, IEC 61400-3, IEC 61499, IEC 61724, IEC 61730, IEC 61784-1, IEC 61836, IEC 61850-6, IEC 61850-7-2, IEC 61850-7-3, IEC 61850-7-4, IEC 61850-7-410, IEC 61850-7-420, IEC 61850-80-4, IEC 61850-8-1,



SUBFIELD	APPLICABLE STANDARDS
	IEC 61850-8-2, IEC 61850-90-10, IEC 61850-90-11, IEC 61850-90-12, IEC 61850-90-15, IEC 61850-90-2, IEC 61850-90-7, IEC 61850-90-9, IEC 62056-1-0, IEC 62056-31, IEC 62056-3-1, IEC 62056-3-2, IEC 62056-42, IEC 62056-46, IEC 62056-47, IEC 62056-4-7, IEC 62056-53, IEC 62056-5-3, IEC 62056-5-8, IEC 62056-6-1, IEC 62056-6-2, IEC 62056-6-9, IEC 62056-7-6, IEC 62056-8-3, IEC 62056-9-7, IEC 62282, IEC 62325 series, IEC 62351 series, IEC 62394, IEC 62457, IEC 62480, ISO 16484 series, ISO 17800, ISO/IEC 14543, ISO/IEC 14543-3 series, ISO/IEC 14543-4, ISO/IEC 14908 series, ISO/IEC 15045, ISO/IEC 15067-3, ISO/IEC 18012, ISO/IEC 24767, ITU-T G.9901, ITU-T G.9902, ITU-T G.9903, ITU-T G.9904
Station Controller	IEC 60193, IEC 60255, IEC 60255-24, IEC 60633, IEC 60700-1, IEC 60870-5-101, IEC 60870-5-103, IEC 60870-5-104, IEC 60870-5-5, IEC 60904 series, IEC 60919, IEC 61131, IEC 61158 series, IEC 61360, IEC 61400 series, IEC 61400-1, IEC 61400-2, IEC 61400-25, IEC 61400-25-2, IEC 61400-25-3, IEC 61400-25-4, IEC 61400-3, IEC 61499, IEC 61512, IEC 61588 (IEEE 1588), IEC 61724, IEC 61727, IEC 61730, IEC 61784-1, IEC 61803, IEC 61804, IEC 61836, IEC 61850 series, IEC 61850-6, IEC 61850-7-2, IEC 61850-7-3, IEC 61850-7-4, IEC 61850-7-410, IEC 61850-7-420, IEC 61850-80-1, IEC 61850-80-4, IEC 61850-8-1, IEC 61850-8-2, IEC 61850-90-1, IEC 61850-90-10, IEC 61850-90-11, IEC 61850-90-12, IEC 61850-90-13, IEC 61850-90-14, IEC 61850-90-15, IEC 61850-90-2, IEC 61850-90-3, IEC 61850-90-4, IEC 61850-90-5, IEC 61850-90-6, IEC 61850-90-7, IEC 61850-90-9, IEC 61850-9-2, IEC 61869, IEC 61954, IEC 61987, IEC 62056 series, IEC 62056-5-3, IEC 62056-6-9, IEC 62264, IEC 62271-3, IEC 62282, IEC 62282 series, IEC 62325-301, IEC 62325-351, IEC 62325-450, IEC 62325-451-1, IEC 62325-451-2, IEC 62325-451-3, IEC 62351 series, IEC 62351-1, IEC 62351-10, IEC 62351-11, IEC 62351-2, IEC 62351-3, IEC 62351-4, IEC 62351-5, IEC 62351-6, IEC 62351-7, IEC 62351-8, IEC 62351-9, IEC 62361 series, IEC 62361-100, IEC 62361-101, IEC 62361-102, IEC 62439, IEC 62443 series, IEC 62446, IEC 62541-1, IEC 62541-10, IEC 62541-2, IEC 62541-3, IEC 62541-4, IEC 62541-5, IEC 62541-6, IEC 62541-7, IEC 62541-8, IEC 62541-9, ISO 81400, ISO 8601, ISO/IEC 15118, ISO/IEC 27001, ISO/IEC 27002
Subscriber Access Network	IEC 60364, IEC 60870-5-101, IEC 60870-5-102, IEC 60870-5-103, IEC 60870-5-104, IEC 60904 series, IEC 61000 Series, IEC 61000-2-12, IEC 61000-2-2, IEC 61000-3-13, IEC 61000-3-14, IEC 61000-3-15, IEC 61000-3-6, IEC 61000-3-7, IEC 61000-4-19, IEC 61000-4-30, IEC 61000-6-1, IEC 61000-6-2, IEC 61000-6-3, IEC 61000-6-4, IEC 61000-6-4, IEC 61000-6-5, IEC 61131, IEC 61158 series, IEC 61326, IEC 61334-4-32, IEC 61334-4-41, IEC 61334-4-511, IEC 61334-4-512, IEC 61334-5-1, IEC 61334-61, IEC 61400-1, IEC 61400-2, IEC 61400-25-2, IEC 61400-25-3, IEC 61400-25-4, IEC 61400-3, IEC 61499, IEC 61724, IEC 61730, IEC 61784, IEC 61784-1, IEC 61836, IEC 61850 series, IEC 61850-6, IEC 61850-7-1, IEC 61850-7-2, IEC 61850-7-3, IEC 61850-7-4, IEC 61850-7-410, IEC 61850-7-420, IEC 61850-80-4, IEC 61850-8-1, IEC 61850-8-2, IEC 61850-90-1, IEC 61850-90-10, IEC 61850-90-11, IEC 61850-90-12, IEC 61850-90-15, IEC 61850-90-2, IEC 61850-90-4, IEC 61850-90-5, IEC 61850-90-7, IEC 61850-90-9, IEC 61850-9-2, IEC 61968 series, IEC 61968-1, IEC 61968-100, IEC 61968-11, IEC 61968-13, IEC 61968-2, IEC 61968-3, IEC 61968-4, IEC 61968-6, IEC 61968-8, IEC 61968-9, IEC 61970 series, IEC 62056 series, IEC 62056-1-0, IEC 62056-31, IEC 62056-3-1, IEC 62056-3-2, IEC 62056-42, IEC 62056-46, IEC 62056-47, IEC 62056-4-7, IEC 62056-53, IEC 62056-5-3, IEC 62056-5-8, IEC 62056-6-1, IEC 62056-6-2, IEC 62056-6-9, IEC 62056-7-6, IEC 62056-8-3, IEC 62056-9-7, IEC 62282, IEC 62325 series, IEC 62351 series, IEC 62351-1, IEC 62357, IEC 62361 series, IEC 62361-100, IEC 62439, IEC 62443 series, IEC 62488-1 (Formerly EN60663) - Part 1, IEC 62541 series, IEC 62872 Ed. 1.0, ISO 16484 series, ISO/IEC 12139-1, ISO/IEC 14543-3, ISO/IEC 14543-3 series, ISO/IEC 14908 series, ISO/IEC 14908-1, ISO/IEC 14908-2, ISO/IEC 14908-3, ISO/IEC 14908-4, ISO/IEC 15802 IEEE 802.1, ISO/IEC 7498-1, ISO/IEC 8802-3, ITU-T G.7041, ITU-T G.7042, ITU-T G.707, ITU-T G.709, ITU-T G.781, ITU-T G.783, ITU-T G.798, ITU-T G.803, ITU-T G.872, ITU-T G.983.1, ITU-T G.983.2, ITU-T G.983.3, ITU-T G.983.4, ITU-T G.983.5, ITU-T G.984.1, ITU-T G.984.2, ITU-T G.984.3, ITU-T G.984.4, ITU-T G.984.5, ITU-T G.984.6, ITU-T G.984.7, ITU-T G.987.1, ITU-T G.987.2, ITU-T G.987.3, ITU-T G.9901, ITU-T G.9902, ITU-T G.9903, ITU-T G.9904, ITU-T G.991.1, ITU-T G.991.2, ITU-T G.992.1, ITU-T G.992.2, ITU-T G.992.3, ITU-T G.992.4, ITU-T G.993.1, ITU-T G.993.2, ITU-T G.993.5, ITU-T G.994.1, ITU-T G.995.1, ITU-T G.996.1, ITU-T G.996.2, ITU-T G.9960 (PHY), ITU-T G.9961 (DLL), ITU-T G.9962 (MIMO), ITU-T G.9964 (PSD), ITU-T G.997.1,

SUBFIELD	APPLICABLE STANDARDS
	ITU-T G.998.1, ITU-T G.998.2, ITU-T G.998.3, ITU-T G.998.4, ITU-T G.999.1, ITU-T I.322
Switch Breaker	IEC 60255-24, IEC 60870-5-101, IEC 60870-5-103, IEC 60870-5-104, IEC 60904 series, IEC 61131, IEC 61158 series, IEC 61400-1, IEC 61400-2, IEC 61400-25, IEC 61400-25-2, IEC 61400-25-3, IEC 61400-25-4, IEC 61400-3, IEC 61499, IEC 61724, IEC 61730, IEC 61784-1, IEC 61836, IEC 61850-6, IEC 61850-7-2, IEC 61850-7-3, IEC 61850-7-4, IEC 61850-7-410, IEC 61850-7-420, IEC 61850-80-1, IEC 61850-80-4, IEC 61850-8-1, IEC 61850-8-2, IEC 61850-90-1, IEC 61850-90-10, IEC 61850-90-11, IEC 61850-90-12, IEC 61850-90-15, IEC 61850-90-2, IEC 61850-90-3, IEC 61850-90-4, IEC 61850-90-5, IEC 61850-90-6, IEC 61850-90-7, IEC 61850-90-9, IEC 61850-9-2, IEC 61869, IEC 62271-3, IEC 62282, IEC 62351 series, IEC 62439
Transformer	IEC 60255-24, IEC 60870-5-101, IEC 60870-5-103, IEC 60870-5-104, IEC 60904 series, IEC 61131, IEC 61158 series, IEC 61400-1, IEC 61400-2, IEC 61400-25, IEC 61400-25-2, IEC 61400-25-3, IEC 61400-25-4, IEC 61400-3, IEC 61499, IEC 61724, IEC 61730, IEC 61784-1, IEC 61836, IEC 61850-6, IEC 61850-7-2, IEC 61850-7-3, IEC 61850-7-4, IEC 61850-7-410, IEC 61850-7-420, IEC 61850-80-1, IEC 61850-80-4, IEC 61850-8-1, IEC 61850-8-2, IEC 61850-90-1, IEC 61850-90-10, IEC 61850-90-11, IEC 61850-90-12, IEC 61850-90-15, IEC 61850-90-2, IEC 61850-90-3, IEC 61850-90-4, IEC 61850-90-5, IEC 61850-90-6, IEC 61850-90-7, IEC 61850-90-9, IEC 61850-9-2, IEC 61869, IEC 62271-3, IEC 62282, IEC 62351 series, IEC 62439
Voltage-Regulator	IEC 60193, IEC 60255, IEC 60255-24, IEC 60870-5-101, IEC 60870-5-103, IEC 60870-5-104, IEC 60904 series, IEC 61131, IEC 61158 series, IEC 61360, IEC 61400 series, IEC 61400-1, IEC 61400-2, IEC 61400-25, IEC 61400-25-2, IEC 61400-25-3, IEC 61400-25-4, IEC 61400-3, IEC 61499, IEC 61512, IEC 61724, IEC 61727, IEC 61730, IEC 61784-1, IEC 61804, IEC 61836, IEC 61850-6, IEC 61850-7-2, IEC 61850-7-3, IEC 61850-7-4, IEC 61850-7-410, IEC 61850-7-420, IEC 61850-80-1, IEC 61850-80-4, IEC 61850-8-1, IEC 61850-8-2, IEC 61850-90-1, IEC 61850-90-10, IEC 61850-90-11, IEC 61850-90-12, IEC 61850-90-13, IEC 61850-90-15, IEC 61850-90-2, IEC 61850-90-3, IEC 61850-90-4, IEC 61850-90-5, IEC 61850-90-6, IEC 61850-90-7, IEC 61850-90-9, IEC 61850-9-2, IEC 61869, IEC 61987, IEC 62264, IEC 62271-3, IEC 62282, IEC 62282 series, IEC 62325-301, IEC 62325-351, IEC 62325-450, IEC 62325-451-1, IEC 62325-451-2, IEC 62325-451-3, IEC 62351 series, IEC 62361-100, IEC 62361-101, IEC 62439, IEC 62446, IEC 62541-1, IEC 62541-10, IEC 62541-2, IEC 62541-3, IEC 62541-4, IEC 62541-5, IEC 62541-6, IEC 62541-7, IEC 62541-8, IEC 62541-9, ISO 81400
WAMS	IEC 60870-5-101, IEC 60870-5-103, IEC 60870-5-104, IEC 60870-5-5, IEC 61588 (IEEE 1588), IEC 61850 series, IEC 61850-6, IEC 61850-7-2, IEC 61850-7-3, IEC 61850-7-4, IEC 61850-80-1, IEC 61850-80-4, IEC 61850-8-1, IEC 61850-8-2, IEC 61850-90-1, IEC 61850-90-2, IEC 61850-90-3, IEC 61850-90-4, IEC 61850-90-5, IEC 61850-9-2, IEC 61869, IEC 61968 series, IEC 61970 series, IEC 62056 series, IEC 62056-6-9, IEC 62351 series, IEC 62361 series, IEC 62361-102, ISO 8601, ISO 8601 (IEC 28601)

**Table 255 - List of available standards for WiseGRID [75].**

## **28 APPENDIX K - ARCHITECTURE COMMUNICATION INTERFACES**



## 28.1 OBTAINED INPUT DURING KYTHNOS WORKSHOP

This annex contains all the information obtained in the workshop celebrated in Kythnos. This workshop tried to identify the main communication interfaces among all the WiseGRID products. With this aim it is going to be listed for each product which other products are communicated with.

## 28.2 WG STAAS/VPP

WiseGRID Product	Communication	Type of information
WiseHOME	Bidirectional	VPP → Home : Billing information, status about service that is performed Home → VPP : Authorization
WiseCORP	Bidirectional	VPP → CORP : Billing information, status about services CORP → VPP : Authorization
WG Cockpit	Bidirectional	VPP → Cockpit : Aggregated information (available power, available capacity) Cockpit → VPP : Operator parameters, commands, Grid information
WiseCOOP	Bidirectional	VPP → COOP : Market availability information

Table 256 - Interfaces with WiseGRID products of WG STaaS/VPP.

Actor / Resource	Communication	Type of information
Aggregators (VPP managers)		
RESCos		
BRP		
Storage Unit		
Forecast Provider		
Smart Meter		
RES Unit		

Table 257 - Interfaces with actors and other resources of WG STaaS/VPP.

### 28.3 WISECORP

WiseGRID Product	Communication	Type of information
WiseRESCO	Bidirectional	Surplus production, forecast production Status and share of production of assets
WG STaaS/VPP	Bidirectional	
WiseCOOP	Bidirectional	WiseCORP → WiseCOOP : Real-time and forecast, generation and demand curves WiseCOOP → WiseCORP : Demand response, flexible availability, receiving commands for demand reduction/shifting

**Table 258 - Interfaces with WiseGRID products of WiseCORP.**

Actor / Resource	Communication	Type of information
Business	Bidirectional	Status of assets Flexibility analysis
Industries	Bidirectional	Result of local optimization
ESCOs	Bidirectional	Production/Consumption curves Integration with RESCO → Share of production
Public facilities	Bidirectional	Objectives of local optimization (e.g. price or CO2 emissions reduction, etc.)
BMS	Bidirectional	OPC - UA
HVAC systems	Bidirectional	Status, setpoint, commands
Battery Management System	Bidirectional	OPC - UA
Lighting	Bidirectional	
CHP	Bidirectional	Status, setpoint, commands
Forecast provider	Unidirectional	Demand / Production forecast
Price provider	Unidirectional	Energy price

**Table 259 - Interfaces with actors and other resources of WiseCORP.**

## 28.4 WISECOOP

WiseGRID Product	Communication	Type of information
WiseEVP	Bidirectional	Implicit demand response request
WG STaaS/VPP	Bidirectional	Contractual settlement information
WiseHOME	Bidirectional	Implicit demand response request
WiseCORP	Bidirectional	Implicit demand response request
WG Cockpit	Unidirectional	Grid status Dynamic grid tariff (if applicable) DSO as Market Operator

Table 260 - Interfaces with WiseGRID products of WiseCOOP.

## 28.5 WG FASTV2G

WiseGRID Product	Communication	Type of information
WiseEVP	Bidirectional	Authentication, metering data, charging session info, charging session orders
WiseHOME	Bidirectional	Availability Execution orders

Table 261 - Interfaces with WiseGRID products of WG FastV2G.

Actor / Resource	Communication	Type of information
EV	Bidirectional	

Table 262 - Interfaces with actors and other resource for WG FastV2G.

## 28.6 WISEEVP

WiseGRID Product	Communication	Type of information
WG FastV2G	Bidirectional	Authentication data Operational status
WG Cockpit	Unidirectional → Bidirectional →	Regulation area info Flexibility information and activation
WG StaaS/VPP *	Bidirectional	Flexibility information and activation

**Table 263 - Interfaces with WiseGRID products of WiseEVP.**

Actor / Resource	Communication	Type of information
Fleet managers	Unidirectional	SOC Charging session status Start/finish time of the charging session Geolocalization
EVSE operators	Unidirectional	Booking status EVSE status User profile
Car sharing cos.	Unidirectional	SOC Charging session status Start/finish time of the charging session Geolocalization EV booking info
Authentication totem or APP	Bidirectional	User ID EVSE ID Charging type and SOC Disconnection time

**Table 264 - Interfaces with actors and other resources of WiseEVP.**

## 28.7 WISEHOME

WiseGRID Product	Communication	Type of information
WG FastV2G	Bidirectional	SOC, available service, EV operating mode
WiseCOOP	Bidirectional	Energy prices, metering info, demand flexibility, forecast

**Table 265 - Interfaces with WiseGRID products of WiseHOME.**

Source: ITE.

Actor / Resource	Communication	Type of information
Domestic prosumers	Bidirectional	Consumption info Billing info State of Assets Instructions of use
Smart meter	Unidirectional	Metering data
Load controller	Bidirectional	Operation mode Status of operation Type of assets
Supplier	Bidirectional	

**Table 266 - Interfaces with actors and other resources of WiseHOME.**

## 28.8 WG RESCO

WiseGRID Product	Communication	Type of information
WiseHOME	Bidirectional	Personal data Energy monitoring Forecasting
WiseCORP	Bidirectional	

**Table 267 - Interfaces with WiseGRID products of WG RESCO.**

Actor / Resource	Communication	Type of information
RESOs		

**Table 268 - Interfaces with actors and other resources of WG RESCO.**

## 28.9 WG COCKPIT

**Table 269 - Interfaces with WiseGRID products of WG Cockpit.**

WiseGRID Product	Communication	Type of information
WiseEVP	Bidirectional	Flexibility (offer, demand, request) Voltage control support
WG StaaS/VPP	Bidirectional	Flexibility (offer, demand, request) Voltage control support
WiseCOOP	Bidirectional	Flexibility (offer, demand, request) Voltage control support
Wise CORP / Wise HOME	Unidirectional	Notifications, maintenance info, etc.

**Table 270 - Interfaces with actors and other resources of WG Cockpit.**

Actor / Resource	Communication	Type of information
DSOs	Unidirectional	DSO → WG Cockpit : Real-time topology data
Smart meters	Bidirectional	Metering data, commands and configuration
Grid assets, sensors	Bidirectional	Topology info (offline) Control and data acquisition

## **29 APPENDIX L - PRIVACY AND DATA PROTECTION QUESTIONS RELATED TO THE WISEGRID COMPONENTS**

***Is it possible to identify a natural person with the processed data (in itself or combined with other data) or are data anonymous? (Reason: If the data, recorded by the WiseGRID systems, relates to an identified or identifiable natural person it becomes personal data, thus data protection law becomes applicable).***

Connection with [2],

Chapter 2.1.1. Criterion 1 - Personal data involved

Annex II

List of possible controls: Partitioning personal data

Objective: to reduce the possibility that personal data can be correlated and that a breach of all personal data may occur

Connection with Data Protection Threats identification, chapter 3.4.1.1 - Threats that may jeopardize confidentiality. It is a question for guidance for a generic threat from losing confidentiality, in addition to this explained in [2],

Connection with [1]:

Annex 2 - Criteria for an acceptable DPIA:

When is a DPIA mandatory? Where a processing is “likely to result in a high risk”

*Possible answers:*

- a. Yes, it is
- b. No, it is not as long as .....
- c. Difficult to say.

*Hints:*

Within the project trials it will not be possible to identify natural persons through processed data, because there are used different types of anonymization in each system.

E.g.: At the level of systems (WiseCOOP, WiseCORP, WiseGRID cockpit, WiseGRID IOP etc.) processed data which labelled as sensitive will use an anonymized identification and the databases tables which reveal the identity is kept in other module of the system.

Sensitive data such as active power consumption reported with high time granularity (e.g. 1 minute or less) will be based either on natural person consent and will be used, where possible, as aggregated value from multiple consumption points, in order to hide personal behaviour.

Only in situations dealing with billing and payment of services like DR, the end-customer will be identified at the level of billing/services calculations

***Are special categories of personal data processed (such as data concerning health, biometric data, facial images, ideology, sexual habits, etc.)? (Reason: specific types of data fall under the scope of stricter rules as their processing results in a higher risk to the rights and freedoms of the data subjects).***

Connection with [2],



### Chapter 2.1.1. Criterion 1 - Personal data involved

*Possible answers:*

- a. Yes
- b. No

*Hints:*

In WiseGRID trials, there are personal data that will be processed. A distinction has been given between sensitive data and non-sensitive data

Particularly the active power consumed by natural persons are highlighted as special category of personal data processed, and a distinction is also made between the reporting rate of the sensitive data.

Load-profiles of energy at 15 minutes or one hour are considered as data necessary for billing, thus being subject of processed data needed for performing the service by the supplier, with the help of the distributor. Shorter reporting periods will be borne to energy service providers (usually ESCOs, but also aggregators - as providing special services), based on agreement from the natural persons which requested and agreed for receiving the service.

***Please list the types of data that you will collect when you use the system. See items A and B within the Workshop subchapters (tables). (Reason: If the data, recorded by the WiseGRID systems, relates to an identified or identifiable natural person it becomes personal data, thus data protection law becomes applicable).***

Connection with [1] Annex 2 - Criteria for an acceptable DPIA: A systematic description of the processing is provided ([3], Article 35(7)(a))

*Possible answers:*

*Data to be provided under table form (see items A and B within the workshop task 3.2 - file: 170608-WiseGRID-D3.1-T3.2\_WORKSHOP PREPARATORY DOCUMENT\_02, from redmine)*

*Hints:*

In WiseGRID trials, data used.

Each type of data is coupled with a specific WiseGRID system. The same type of data may be collected by several WiseGRID systems (data sent from source in a multi-actor environment), but each acts as independent and treats the data on its own responsibility

***Are the subjects well informed about the data which is collected from them? Is it well explained the purpose of the collected data, the retention time and the time granularity? Is it explained the legal basis for the collected data? Is it considered an option in case of denial of consent?***

Connection with [1] Annex 2 - Criteria for an acceptable DPIA: A systematic description of the processing is provided ([3], Article 35(7)(a))

Connection in [2] with Data Protection Threats identification, chapter 3.4.1.4 - Threats that may jeopardize personal data. It is a question for guidance for a generic threat for “Undeclared data collection” (3.4.1.4.4), “Invalidation of explicit consent” (3.4.1.4.6), “Non legally based personal data processing” (3.4.1.4.7) and “Lack of transparency” (3.4.1.4.8)

*Possible answers:*

*Hints:*

End-users are informed about the collected data and about which one is sensitive and need their approval. Moreover, the purpose for each data is also shared with the subjects. Personal (sensitive) data for which appears a denial of consent will be not collected, alternatives may be considered if they exist.

***Does WiseGRID process meta-data? If yes, what kind of meta-data and at what layer? (Reason: using meta-data would help the data controller to ensure compliance with the principles of data protection (e.g. data minimisation, data adequacy, etc.)).***

Connection with [1] Annex 2 - Criteria for an acceptable DPIA: A systematic description of the processing is provided ([3], Article 35(7)(a))

*Possible answers:*

- a. Yes. WiseGRID process meta data like .....within layer...
- b. No

*Hints:*

The following systems process meta-data.

***Please specify the format in which the data will be stored, and describe the devices and facilities where the data will be kept. (Reason: Description of processing operations fosters transparency of the system and help to build interoperability for the exercise to the data portability right).***

Connection with [1] Annex 2 - Criteria for an acceptable DPIA: A systematic description of the processing is

provided ([3], Article 35(7)(a))

*Hints:*

At the customer level, in the SMX part of USM / SLAM, data will be stored in CVS extended format. This data is stored in a trusted part, which is not accessible by external actors. External actors interact with SMX only through a sandboxed solution based on Docker and the communication with the trusted part is only by JSON messages, and not by direct connection to the trusted part. The Consortium will in the next future agree upon more interoperable format, i.e. XML or JSON.

In the WiseGRID systems (upper level), data will be stored as follows (description):

WiseCOOP, WiseCORP

WiseGRID cockpit

WiseGRID IOP

Etc.

***Are the processed data accurate and relevant? (Reason: the processed data should be relevant and accurate for the purposes of data processing. The WiseGRID systems should record and work with only those types of data which are necessary to reach the goal of the processing, furthermore the processed data must be accurate and kept up to date).***

Connection in [2] with Data Protection Threats identification, chapter 3.4.1.4 - Threats that may jeopardize personal data. It is a question for guidance for a generic threat for “collection exceeding purpose” (3.4.1.4.1),

*Possible answers:*

- a. Yes, they are accurate and relevant
- b. Yes, they are accurate
- c. Yes, they are relevant
- d. Rather not.

*Hints:*

This question is applicable where personal data processing, which is the case in the following project trials:

***The data controller is the person who has knowledge of and control over the means or the purpose(s) of the personal data processing operations. You are the data controller when you inter alia determine means and purposes when:***

- Collecting personal data and you store
- Transmitting the data

- Deleting the data
- Processing data using an algorithm

*Please explain in simple words when, at which point of the flow of data, you handle personal data. (Reason: The controller shall be held liable for the processing operation. In WiseGRID there are multiple parties with different degree of control over data. The roles of these controllers should be clarified).*

Connection with [1] Annex 2 - Criteria for an acceptable DPIA: A systematic description of the processing is provided ([3], Article 35(7)(a))

*Possible answers:*

- a. During data collection*
- b. During data process*
- c. During reporting*
- d. In most processes*
- e. In not any process*

*Hints:*

For personal data processing, data controllers should be specified.

*Please explain in simple words what is the role you play in the flow of personal data of end-users within the WISEGRID systems (Reason: the systematic description of the data processing operations is an indispensable element of the impact assessment).*

Connection with [1] Annex 2 - Criteria for an acceptable DPIA: A systematic description of the processing is provided (Article 35(7)(a))

*Possible answers:*

- a. Collecting*
- b. Verifying*
- c. Transmitting*
- d. Administrating*
- e. No role with personal data of end-users*

*Hints:*

During the trials, some personal data will be transferred or stored.

As for WISEGRID systems, after the end of the project, the DSO that will use WISEGRID Cockpit will use data

for billing purpose, payments, and network maintenance.

***How do you ensure the security of data? Please explain what you plan, intend or have decided to do in order to protect personal data when this is under your control. Are there parts of the infrastructure in which data are non-encrypted? In that part personal data are identifiable or pseudonymized? (Reason: appropriate technical and organisational measures should be applied to ensure a level of security appropriate to the potential risk, such as: safeguards against interception of wireless transmission; secured servers and clouds where information is stored; passwords; encryption; etc.)***

Connection with [1] Annex 2 - Criteria for an acceptable DPIA: A systematic description of the processing is provided ([3], Article 35(7)(a))

Connection in [2] with Data Protection Threats identification, chapter 3.4.1.1 - Threats that may jeopardize confidentiality. It is a question for guidance for a generic threat for "hardware loss" (3.4.1.4.5), but also for any access to hardware.

*Possible answers:*

- a. *There are not non-encrypted parts within the system.*
- b. *There are parts of the infrastructure in which data are non-encrypted. In that part; personal data are identifiable.*
- c. *There are parts of the infrastructure in which data are non-encrypted. In that part; personal data are pseudonymized.*

*Hints:*

For the protection of personal data security, WISEGRID systems.

***If personal data are transmitted, please describe the network and the connections between the devices that are used. Is this network isolated from public networks or nodes? In any case, but specifically if it is about public networks, is the data encrypted during the communication process? (Reason: To determine the level of adequacy of the applied security measures, every determining factor should be taken into consideration whereas the means of communication is a pivotal element).***

Connection in [2] with Data Protection Threats identification, chapter 3.4.1.1 - Threats that may jeopardize confidentiality. It is a question for guidance for a generic threat for "Eavesdropping of computer channels" (3.4.1.4.5). Also, Man-in-the-middle attack via computer channels (3.4.1.2.3), related to threats identification, chapter 3.4.1.2 - Threats that may jeopardize integrity

*Possible answers:*

- a. The network used is public
- b. The network used is private
- c. The network used is mixed

*Hints:*

In the Trials, some personal data are transmitted.

For the WiseGRID all data communications are secure and encrypted.

The credentials are kept and distributed according to the following procedures (see annex)

***Are the processing operations documented? How is the documentation of the processing operations maintained? Are there considered for instance logs to memorize these operations? (Reason: The documentation will help in the identification of risks both for the controller and for the supervisory authority. Furthermore, the maintenance of the record of the activities could be advantageous in multiple cases.)***

Connection in [2] with Data Protection Threats identification, chapter 3.4.1.2 - Threats that may jeopardize integrity. It is a question for guidance for a generic threat for "Abnormal use of software"

(3.4.1.2.20).

*Possible answers:*

- a. Processing operations are documented and logs are used to memorise operations
- b. Processing operations are documented.
- c. Processing operations are partly documented.

*Hints:*

The WISEGRID systems are designed in order to use log file to trace actions.

***Do you maintain logs to track authorised (or unauthorised) access to personal data for a specific time period? (Reason: Breaches of security should be tracked). Which is the period for keeping the logs? Is it made a penetration test for the system?***

Connection in [2] with Data Protection Threats identification, chapter 3.4.1.2 - Threats that may jeopardize integrity. It is a question for guidance for a generic threat for "Abnormal use of software"

(3.4.1.2.20) and Insufficient access control procedures (3.4.1.2.6) and Insufficient logging mechanism (3.4.1.2.8), Breach in security implementation (3.4.1.2.9)

*Possible answers:*

- a. Yes, few maintain logs for all accessing activities
- b. Only in some cases
- c. Not necessarily

*Hints:*

In the trials, there will be personal data processing.

In WISEGRID system, at SMX level the personal data access will be authorized and tracked through the RBAC System of SMX.

At WiseGRID upper level systems the following solutions will be developed:

***Do you have a “personal data breach reaction plan” and “reporting protocol”? Or is there a designated data protection officer? (Reason: In case of the occurrence of a personal data breach, countermeasures should be applied immediately. Re. the reporting protocol, in case of the occurrence of a personal data breach, the supervisory authorities and affected parties (if needed) should be notified immediately.)***

Connection with [1] Annex 2 - Criteria for an acceptable DPIA: *Risks to the rights and freedoms of data subjects are managed (Article 35(7)(c)):*

*- measures envisaged to treat those risks are determined (Article 35(7)(d) and recital 90)*

Connection in [2] with Data Protection Threats identification, chapter 3.4.1.3 - Threats that may jeopardize availability. It is a question for guidance for a generic threat for Denial of service (3.4.1.3.3)

*Possible answers:*

- a. Yes, there is an alert and report protocol and also a reaction procedure for such “data breach”.
- b. We only have an alert system
- c. Nothing is implemented for such case

*Hints:*

In WISEGRID trials, there will be personal data processing.

For WISEGRID systems, the responsibility to develop a data breach plan will be the obligation of each actor, e.g. of DSO.

***How do you inform the data subjects (clients, end-users) about the intended data processing operations? Please describe methods that you use to provide information to the data subjects. (Reason: when personal data is processed, the data subjects shall be informed prior to the processing. This means that when individuals stand or walk in front of a device, they must know that they might be recorded. The right of the data subject to be informed about processing operations regarding him or her shall be guaranteed.)***

Connection with [1] Annex 2 - Criteria for an acceptable DPIA:

A systematic description of the processing is provided ([3], Article 35(7)(a))

Connection in [2] with Data Protection Threats identification, chapter 3.4.1.2 - Threats that may jeopardize integrity. It is a question for guidance for a generic threat for Incomplete information (3.4.1.2.13)

*Possible answers:*

- a. *We send an email (or SMS) with short description of data usage.*
- b. *We send a hard copy letter with short description of data usage.*
- c. *We use different communication form (as .....).*
- d. *We do not inform about such activities.*

*Hints:*

The type of data processing ....

***Are there some unpredictable purposes in the final architecture of WISEGRID? Please enlist all possible purposes that personal data processing can have within WISEGRID Architecture. (Reason: to increase transparency and to be compliant with right to information: all purposes must be declared to the data subject before data processing starts. For new undeclared purposes, we need another request for consent to users).***

Connection with [1] Annex 2 - Criteria for an acceptable DPIA: A systematic description of the processing is provided ([3], Article 35(7)(a))

*Possible answers:*

- a. *Yes, there are unpredictable purposes in the final architecture of WISEGRID. For such cases a new consent will be considered.*
- b. *Yes, there are unpredictable purposes in the final architecture of WISEGRID. Such cases are possible and do not need special attention.*
- c. *No, there are not unpredictable purposes in the final architecture of WISEGRID. Possible purposes are .....*

*Hints:*

The project architecture considers security and privacy by design,

The architecture is extensible to incorporate new functionality, which we cannot predict. However, the architecture is predictable in its operation.

DSOs have their own handling of personal data, which WISEGRID does not influence.



***If the processing of personal data is based on the consent of the data subject, how do you guarantee that it was informed, specific and freely given? (Reason: Providing sufficient information regarding the data processing operation of the WISEGRID systems might raise obstacles).***

Connection in [2] with Data Protection Threats identification, chapter 3.4.1.2 - Threats that may jeopardize integrity. It is a question for guidance for a generic threat for “Abnormal use of software” (3.4.1.2.20).

*Possible answers:*

- a. We defined an “acknowledge form” that will be signed by data subject and then stored.*
- b. We have an electronic dialog (email or SMS) asking and getting answer related to such consent.*
- c. We get a verbal confirmation by phone call.*
- d. This is not a specific issue to be considered.*

*Hints:*

In WISEGRID Trials, there will be personal data processing.

For WISEGRID systems, the different actors, such as DSO-user (after the end of the project) will have the responsibility to inform appropriately end-users through letters, etc.

For the “privacy” informed consent it should be prepared a sample.

***Is the end date of the processing period set (how long is the personal data retained)? What will happen with the personal data afterwards? Would it be possible that you as operator could reuse these data or transmit them to others (e.g. data brokers)? (Reason: the processing of personal shall have an end date. Data afterwards should be deleted or anonymised).***

Connection in [2] with Data Protection Threats identification, chapter 3.4.1.2 - Threats that may jeopardize personal data. It is a question for guidance for a generic threat for “Missing erasure policies or mechanisms; excessive retention periods” (3.4.1.4.3).

*Possible answers:*

- a. The period to retain personal data is predefined and fixed within the application. Further on, data are deleted or anonymised with no recovery possibility.*
- b. The period to retain personal data is predefined and fixed within the application. Further on, data are stored in secured conditions and recovery is possible.*
- c. The period to retain personal data is configurable based on project evolution. Data subject is permanently aware about this. Further on, data are deleted or anonymised with no recovery possibility.*
- d. The period to retain personal data is configurable based on project evolution. Data subject is not aware about this.*

- e. *Personal data are available after processing period and can be further reused.*

*Hints:*

In WISEGRID trials, there is personal data processing.

For WISEGRID systems, the different actors, such as DSOs, will have the responsibility to clarify duration of the data storage.

However, this aspect depends also on national regulations.

***How do you ensure data subjects (data owners) are able to use their rights (such as right to access to data related to them, the right to erase data related to them, rectify such data, restrict or block the processing)? Is there a platform they can use (i.e. a website, a user-friendly interface, etc.) or a responsible person they can turn to (i.e. data protection officer, data controller, responsible consortium member, etc.)? (Reason: a platform should be established where data subjects can practice their rights. Proper documentation should make it possible to find the information the data subject seeks.)***

Connection in [2] with Data Protection Threats identification, chapter 3.4.1.2 - Threats that may jeopardize personal data. It is a question for guidance for a generic threat for “Missing erasure policies or mechanisms; excessive retention periods” (3.4.1.4.3).

*Possible answers:*

- a. *There is a user interface that facilitates data subject to access and update such data accordingly.*
- b. *There is a data protection officer, permanently available to contact data subject on such matters.*
- c. *These data are not accessible for the data subjects.*
- d. *Other*

*Hints:*

In WISEGRID trials, there is personal data processing.

It will be the responsibility of the user (through its legal office, after the end of the project) to ensure the full exercise of all rights.

***Are any data fully automatically processed? In such case, you must communicate the user meaningful information about the LOGIC under the algorithm, including the reason for combining it with other data. How would you explain such logic? (Reason: the new right to access under GDPR has a wider scope)***

Connection in [2] with Data Protection Threats identification, chapter 3.4.1.2 - Threats that may jeopardize integrity and personal data. It is a question for guidance for a generic threat for integrity “A lack of transparency for automated individual decisions” (3.4.1.2.16) and personal data “Combination exceeding purpose” (3.4.1.4.2).

*Possible answers:*

- a. *Yes, data are fully automatically processed. The logic is presented under separate tool (i.e. help menu...)*
- b. *Data are not fully automatically processed.*

*Hints:*

Yes, personal data may be involved.

Component descriptions will present the logic of our processing, and the documentation will be publicly available.

***Does the system provide data subjects with the option to exercise the right to data portability (i.e. to have a copy of personal data related to personal users in a machine-readable format and, if technically feasible, transmit them to another data controller)? (Reason: WISEGRID must guarantee that also the right to data portability can be exercised, especially in case of change of supply)***

Connection in [2] with Data Protection Threats identification, chapter 3.4.1.2 - Threats that may jeopardize integrity. It is a question for guidance for a generic threat for "Access to data that was not intended (not necessary for the purpose of collection)" (3.4.1.2.10).

*Possible answers:*

- a. *Yes, the system provides data subjects with the option to exercise the right to data portability (i.e. to have a copy of personal data related to personal users in a machine-readable format and, if technically feasible, transmit them to another data controller).*
- b. *No, the system does not provide data subjects with the option to exercise the right to data portability.*

*Hints:*

Yes, accessible through the User Interface, it will be developed in the project.

***What is the interplay of "personal data breach" definition with Threat definitions under WISEGRID? (personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed. (GDPR, Article 4(12))***

Connection with [1], Annex 2 - Criteria for an acceptable DPIA:

Risks to the rights and freedoms of data subjects are managed ([3], Article 35(7)(c)):

- threats that could lead to illegitimate access, undesired modification and disappearance of data are identified;

Connection in [2] with Data Protection Threats identification, chapter 3.4.1.2 - Threats that may jeopardize integrity. It is a question for guidance for a generic threat for “Insufficient information security controls” (3.4.1.2.7).

*Possible answers:*

- a. *There is no interplay.*
- b. *The interplay is according GDPR Art 4(12)*

*Hints:*

Personal data breach is considered to be a threat, so there is a correspondence between the legal definition of personal data breach and threat definitions.

***What measures of interoperability of format exist for providing personal data to users? (Reason: Under GDPR “controllers are encouraged to develop interoperability of formats” in which they process data and this is also aimed at a full exercise of the right to data portability).***

Connection with preamble of [3] “Whereas (68)”, pag.13. text: “Data controllers should be encouraged to develop interoperable formats that enable data portability”.

*Possible answers:*

- a. *The level of interoperability of format is high*
- b. *The level of interoperability is not significant.*
- c. *This issue is not considered by controllers.*

*Example of text for starting the answer:*

Interoperability of data used after the end of the project by actors, e.g. DSO, will be ensured through compatible format for the processing of data, for instance XML or JSON formats.

***Is it applied a digital signature process for getting the acceptance of certain data processing? Please describe the process involving both natural person which accepts the terms and the actor which ask for the agreement which involved acceptance of the personal data processing.***

Connection in [4] with “Privacy techniques” and “Privacy preserving computations”.

*Possible answers:*

- a. *Yes, it is applied a digital signature process for getting the acceptance of certain data processing.*  
*Short description:*

- b. *No, it is not applied a digital signature process for getting the acceptance of certain data processing.*

*Hints:*

For making more effective the process of acquiring or retreating from a certain service, a mechanism based on electronic signatures will be implemented. The process will involve clear description of the data to be processed and the acceptance at natural person level by signing electronically the contract will involve automatic or semi-automatic reprogramming of RBAC systems at the level of natural persons (SLAM with RBAC system) and at level of WiseGRID systems.

***Is it applied a set of measures to avoid or detect software alteration, such that changes can be detected in due time in order not to alter data integrity and confidentiality?***

Connection in [2] with Data Protection Threats identification, chapter 3.4.1.2 - Threats that may jeopardize integrity. It is a question for guidance for a generic threat for "Software alteration" (3.4.1.2.1)

***Is it applied a Role based Access Control at different levels of data storage (at meter level, at IOP, big data and WiseGRID Apps level)?***

Connection in [2] with Data Protection Threats identification, chapter 3.4.1.2 - Threats that may jeopardize integrity. It is a question for guidance for a generic threat for "Insufficient access control procedures" (3.4.1.2.6)

***Is it considered the protection of data for not being transmitted outside the European Economic Area?***

Connection in [2] with Data Protection Threats identification, chapter 3.4.1.2 - Threats that may jeopardize integrity. It is a question for guidance for a generic threat for "The protection of data is compromised outside the European Economic Area (EEA)". (3.4.1.2.11)

*Possible answer:*

*Databases, clouds and servers are working only in the EEA. The design is made such that data cannot be transmitted or stored outside EEA.*

***Will be considered measures for hardware loss (e.g. theft, physical intrusion) and loss of power (leading***

*e.g. to system unavailability)?*

Connection in [2] with Data Protection Threats identification, chapter 3.4.1.2 - Threats that may jeopardize availability. It is a question for guidance for a generic threat for "Hardware loss (3.4.1.3.1) and Loss of Power (3.4.1.3.2)

*Possible answers:*

- a. Data in the hardware is encrypted.*
- b. For vital information systems there are uninterruptible power supplies in place.*

***Is unavailability due to attacks leading to Denial of service considered? Please explain measures.***

Connection in [2] with Data Protection Threats identification, chapter 3.4.1.2 - Threats that may jeopardize availability. It is a question for guidance for a generic threat for "Denial of service" - DoS (3.4.1.3.3)

*Possible answer:*

*Attack scenarios are analyzed and measures to detect and stop DoS are considered. One important measure is the fact that all actors have communication through VPNs allocated to that functionality, thus reducing substantially attacks from unknown actors.*

## **29.1 QUESTIONNAIRE REFERENCES**

[1] Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, Adopted on 4 April 2017, Article 29 Data Protection Working Party

[2] Expert Group 2: Regulatory Recommendations for Privacy, Data Protection and Cyber-Security in the Smart Grid Environment - Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems

[3] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

[4] Privacy and Data Protection by Design - from policy to engineering, December 2014, ENISA - European Union Agency for Network and Information Security

## 29.2 EXTRAS

### ARTICLE 29 DATA PROTECTION WORKING PARTY

Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679, Adopted on 4 April 2017, Article 29 Data Protection Working Party

The WP29 proposes the following criteria which data controllers can use to assess whether or not a DPIA, or a methodology to carry out a DPIA, is sufficiently comprehensive to comply with the GDPR:

- 1. A systematic description of the processing is provided (Article 35(7)(a)):**
  - 1.1. nature, scope, context and purposes of the processing are taken into account (recital 90)
  - 1.2. personal data, recipients and period for which the personal data will be stored are recorded
  - 1.3. a functional description of the processing operation is provided;
  - 1.4. the assets on which personal data rely (ma, software, networks, people, paper or paper transmission channels) are identified
  - 1.5. compliance with approved codes of conduct is taken into account (Article 35(8));
- 2. Necessity and proportionality are assessed (Article 35(7)(b)): measures envisaged to comply with the Regulation are determined (Article 35(7)(d) and recital 90), taking into account:**
  - 2.1. measures contributing to the proportionality and the necessity of the processing on the basis of:
    - 2.2.1. specified, explicit and legitimate purpose(s) (Article 5(1)(b));
    - 2.2.2. lawfulness of processing (Article 6);
    - 2.2.3. adequate, relevant and limited to what is necessary data (Article 5(1)(c));
  - 2.3. measures contributing to the rights of the data subjects:
    - 2.3.1. information provided to the data subject (Articles 12, 13 and 14);
    - 2.3.2. right of access and portability (Articles 15 and 20);
    - 2.3.3. right to rectify, erase, object, restriction of processing (Article 16 to 19 and 21)
    - 2.3.4. recipients
    - 2.3.5. processor(s) (Article 28);
    - 2.3.6. safeguards surrounding international transfer(s) (Chapter V);
    - 2.3.7. prior consultation (Article 36)
- 3. Risks to the rights and freedoms of data subjects are managed (Article 35(7)(c)):**
  - 3.1. origin, nature, particularity and severity of the risks are appreciated (cf. recital 84) or, more specifically, for each risk (illegitimate access, undesired modification, and disappearance of data) from the perspective of the data subjects:
    - 3.1.1. risks sources are taken into account (recital 90);
    - 3.1.2. potential impacts to the rights and freedoms of data subjects are identified in case of illegitimate access, undesired modification and disappearance of data;

- 3.1.3. threats that could lead to illegitimate access, undesired modification and disappearance of data are identified;
- 3.1.4. likelihood and severity are estimated (recital 90);
- 3.2. measures envisaged to treat those risks are determined (Article 35(7)(d) and recital 90);

#### **4. Interested parties are involved:**

- 4.1. the advice of the DPO is sought (Article 35(2));
  - 4.2. the views of data subjects or their representatives are sought (Article 35(9))
- 

### **Data Protection Threat identification [2], Step 4 of the proposed Questionnaire**

In order to facilitate the identification of threats, a non-exhaustive list of generic threats is provided in [2]. They are grouped according to their impact on confidentiality, integrity and availability of the data.

#### **3.2.1.1 Threats that may jeopardize confidentiality (9 generic threats)**

The following table presents the generic threats that can lead to:

- Illegitimate access to personal data,
- Compromise of processing (if this feared event is considered).

#### **3.2.1.2 Threats that may jeopardize integrity (20 generic threats)**

The following table presents the generic threats that can lead to:

- Changes in processing,
- Unwanted changes of personal data,
- Alterations to legal processes if this feared event is considered).

#### **3.2.1.3 Threats that may jeopardize availability (3 generic threats)**

The following table presents the generic threats that can lead to:

- Unavailability of legal processes,
- Disappearance of personal data,
- Unavailability of processing (if this feared event is considered).

#### **3.2.1.4 Threats that may jeopardize personal data (8 generic threats)**

The following table presents the generic threats that can lead to:

- Breaches of legal processes,
- Breach of use of personal data



## **30      APPENDIX M - PRIVACY & DATA PROTECTION - DATA SOURCES FOR DSO**

**Table 271 - PRIVACY & DATA PROTECTION - DATA SOURCES FOR DSO**

No.	Data type (focus on your use-case specific data)	Actor who needs (DSO, suppl, ESCO, aggr. etc.)	Source of data (device or entity)	Time series data granularity (TSG), data accuracy	Why is needed the data	Privacy status
1	Flexibility request	Aggregator	DSO	TSG: 15 minutes	DSO sends flexibility request to aggregator in order to find out if capacities are available for grid management/ balancing	Private
2	Demand response request	Aggregator	DSO	TSG: 15 minutes	DSO sends request to aggregator in order to find out if demand response capacities are available for grid congestion management/ balancing	Private
3	Schedule data	DSO	Aggregator	Daily/15 min?	Schedule data is necessary for the operation of the VPP	Private
4	Flexibility offer	DSO	Aggregator	TSG: 15 minutes	Aggregator offers flexibility/free capacities that ist VPP can currently provide	Private
5	Demand response offer	DSO	Aggregator	TSG: 15 minutes	Aggregator offers demand response capacities that ist VPP can currently provide	Private

## **31 APPENDIX N - PRIVACY & DATA PROTECTION - DATA SOURCES FOR NON-DSO**

**Table 272 - PRIVACY & DATA PROTECTION - DATA SOURCES FOR NON-DSO**

No.	Data type (focus on your use-case specific data)	Actor who needs (DSO, suppl, ESCO, aggr. etc.)	Source of data (device or entity)	Time series data granularity (TSG), data accuracy	Why is needed the data	Privacy status
1	Metadata of the organization (name, address, description, contact info...)	WGStaaS/VPP	User of the application (Aggregator)	Upon registration	User management	Private
2	Metadata of portfolio members (name/alias, address, Universal Supply Point Code)	Aggregator	Portfolio members, Owner of VPP assets	Upon registration in the organization	Portfolio management, binding energy measurements to a particular customer	Private
3	Energy metering (production/demand)	Aggregator	Smart meter	TSG: 15 minutes	Billing, basis for portfolio profiling and flexibility estimation	Private
4	Static Storage/VPP Unit data	Aggregator	Storage/VPP Unit	Upon registration	Portfolio management and	Private
5	Dynamic Storage/VPP Unit data	Aggregator, Prosumer, Storage Operator (visualization via WiseHOME and WiseCORP)	Storage/VPP Unit	TSG: 1 s	Billing, basis for portfolio profiling, flexibility estimation and Storage/VPP Unit control	Private
6	Schedule data	Storage/VPP Unit	Aggregator	Daily (15 min)?	Storage/VPP Unit control	Private
7	Setpoint data	Storage/VPP Unit	Aggregator	TSG: 1 s	Storage/VPP Unit control	Private
8	Energy flexibility models	Aggregator	Aggregator/retailer/cooperative (through portfolio profiling and analysis)	TSG: 1 hour	Flexibility models are used to estimate the amount of VPP capacity that can be used for	Private

No.	Data type (focus on your use-case specific data)	Actor who needs (DSO, suppl, ESCO, aggr. etc.)	Source of data (device or entity)	Time series data granularity (TSG), data accuracy	Why is needed the data	Privacy status
					providing services	
9	Bid offer	Market Operator	Aggregator	TSG: 15 min (bid is triggered depending on available capacity)	VPP capacity is offered to the energy market in order to reach additional income	Private
10	Bid acceptance/acknowledgement	Aggregator	Market Operator	TSG: 15 min (bid is triggered depending on available capacity)	Billing, Scheduling of Storage/VPP units	Private
11	Energy tariffs	Aggregator	Retailers	Upon changes in the tariffs (yearly) or a dynamic price scheme (15 minutes)	necessary for flexibility estimation and Storage/VPP Unit control	Private
12	Demand forecasts	Aggregator	Aggregator (through portfolio profiling and analysis)	Daily (15 min)	necessary for flexibility estimation and Storage/VPP Unit control	Private
13	Production forecasts	Aggregator	Aggregator (through portfolio profiling and analysis), Market data	Daily (15 min)	necessary for flexibility estimation and Storage/VPP Unit control	Private
14	Weather forecasts	Aggregator	Weather forecast provider	Daily (hourly or even 15 min?)	Input für unit selection and scheduling algorithms	Public