

Deliverable 7.3
Actions initiated
with standardization organizations

—
2 0 1 9

Document Information

Programme	Horizon 2020 – Cooperation / Energy
Project acronym	FutureFlow
Grant agreement number	691777
Number of the Deliverable	D7.3
WP/Task related	[WP7 / T7.3.4]
Type	(distribution level)
Confidential:	Public
Date of delivery	[23.10.2019]
Status and Version	Version 2.0
Number of pages	26 pages
Document Responsible	Gemalto

Versioning:

Version	Date	Author(s)	Notes	Status
1.0	27.07.2018	GEMALTO	Initial document	draft
1.1	14.05.2019	GEMALTO	WP6	draft
1.2	27.05.2019	GEMALTO	Updates after 27.05.2019 conference call	draft
1.3	27 06 2019	GEMALTO/EIMV	Updates after 13 06 2019 conference call, Cybergrid comments. Contribution on chapters 1 and 2.2	draft
1.4	08.10.2019	EIMV	Updates related to the activities with standardisation organisations	draft
1.5	15.10.2019	GEMALTO	Added Conclusion	Final draft
1.6	16.10.2019	EIMV	Minor corrections	Final draft
2.0	23.10.2019	GEMALTO	Final version	Final

Executive summary

This deliverable focuses on the interactions established by the FutureFlow project stakeholders and standardization organization:

- to identify relevant applicable standards that can be relied upon within the project
- to enhance applicable existing standards, as assessed during the course of the project
- to develop new standards or expand existing ones to fill any identified gaps where standards for interoperability would be beneficial.

It starts by providing a general overview of the reference architecture and applicable standards, and details for each of these their applicability in the project and further enhancements or gaps filling that may be needed. Different sections detail the standards for different application areas (TSO domain, ICT domain, DR/DG level...). The deliverable also reports about the presentation of standardization related findings to the standardization body.

Contents

1	Reference architecture	7
1.1	Reference architecture according to IEC.....	7
1.2	European reference architecture.....	8
1.3	Mapping of FutureFlow use case to SGAM.....	12
2	General ICT and IoT standards applicable to the context	14
2.1	oneM2M	14
2.2	MQTT	19
3	Overview of energy standards	19
3.1	HV-DC grid architecture	19
3.2	Auxiliary Power System Standardization	20
3.3	aFRR regulation.....	20
3.4	Energy Management harmonized data model for industry and power grid	20
3.5	Data modelling for Micro Grid Management	21
3.6	Interoperable identification and (sub)billing (using the AMI) capabilities in Smart Grid	21
3.7	System management of T&D systems, DER and Micro-grid systems connected	22
4	Conclusion on FutureFlow standardization findings	23
5	Presentation of FutureFlow standardization related findings to the Slovenian Institute for Standardization – a full member of IEC, CEN, CENELEC and ETSI	23
6	Bibliography	25
6.1	Energy Cybersecurity	25

1 Reference architecture

Smart grid solutions are in general complex systems consisting of many components. Integration of these components and solutions is practically not possible without an appropriate standardization framework. The creation of a standardization framework requires a systematic approach supported by an appropriate methodology as well as a reference architecture. The first attempt in doing so has been undertaken by NIST¹ that issued the first version of the standardization framework [1], which was then later also used by IECs' ² Technical Committee TC57 which comprehensively defined the reference architecture for information exchange within the electrical power grid system [1].

1.1 Reference architecture according to IEC

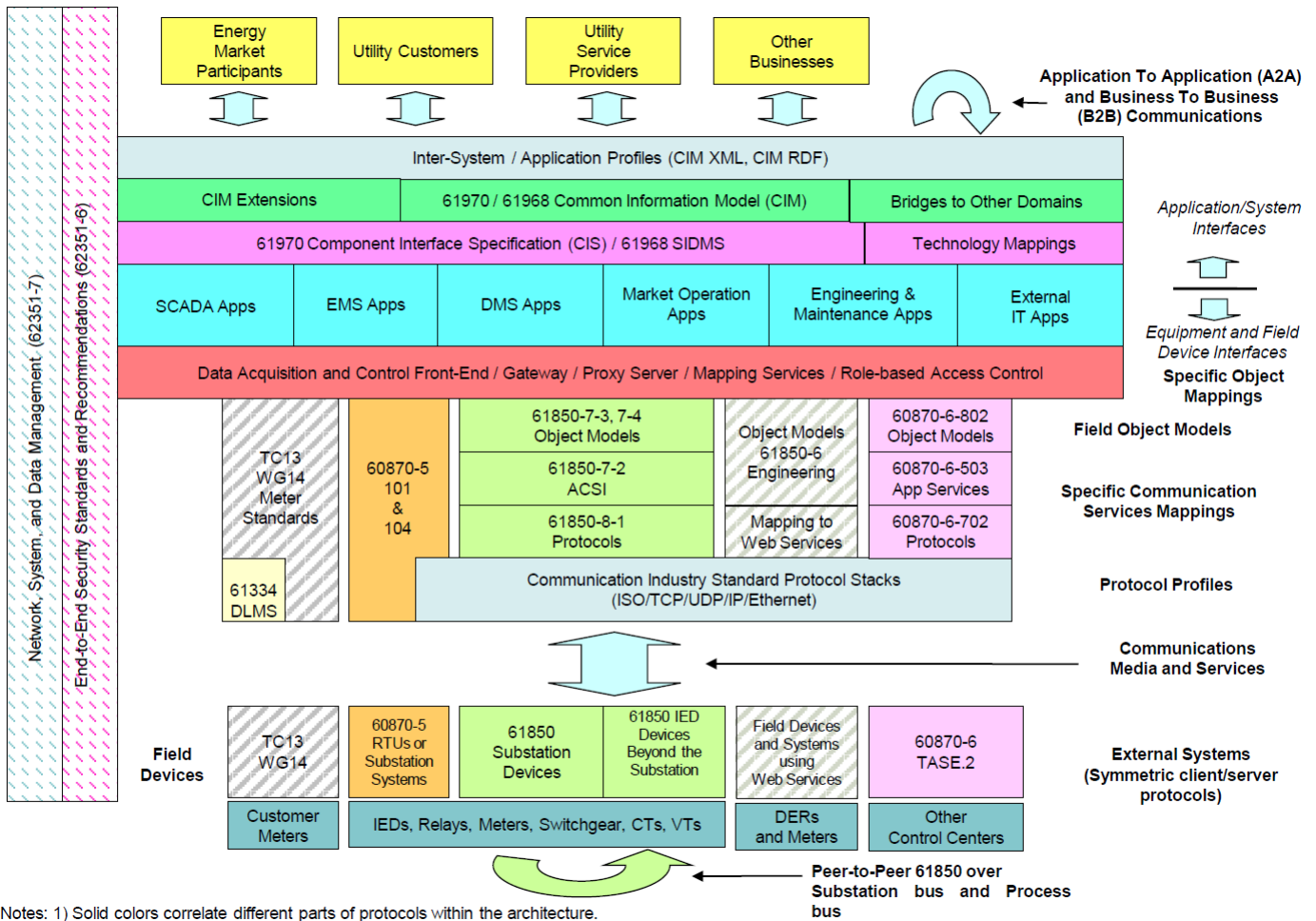
Figure 1.1 states the reference architecture for integrating devices, systems and applications of the electrical power system within the TC57 technical committee framework under IEC [1]. It predominately focuses into the fields of operations and management of the electrical power system, including network automation and advanced metering infrastructure.

The most important families of standards prescribed by the IEC reference architecture are:

- IEC 61850 for the field of grid automatization,
- IEC 61334 for the field of advanced metering infrastructure (AMI),
- IEC 60870-5 for real-time data exchange between remotely controllable devices (Remote Terminal Units - RTU) and their supervision systems,
- IEC 60870-6 for data exchange between centres of operation,
- IEC 61968 in 61970 for the field of modelling the electrical power system as well as IT/OT system integration,
- IEC 62351 for the field of information security and ICT network and system management.

¹ National Institute of Standards and Technology

² International Electrotechnical Commission



*Notes: 1) Solid colors correlate different parts of protocols within the architecture.
 2) Non-solid patterns represent areas that are future work, or work in progress, or related work provided by another IEC TC.

Figure 1.1: Reference architecture according to IEC [1]

1.2 European reference architecture

The European standardization (CEN, CENELEC and ETSI) summarizes the IEC standards and even further upgrades the architecture, and places it into the context of European specifications in yet even more detail. This standardization was created following the initiative of the European Commissions' M/490 mandate to set up a standardization framework for European smart grids [5]. It was prepared by the CEN-CENELEC-ETSI Smart Grid Coordination Group and is now covered within the following documents:

- Reference Architecture - RA - Reference Architecture [6],
- Set of standards- FSS - First set of Standards [7],
- Sustainable standardization process and associated tools for team work - SP - Sustainable Processes [8] and
- Recommendations for information security - SGIS - Smart-grid Information Security [9].

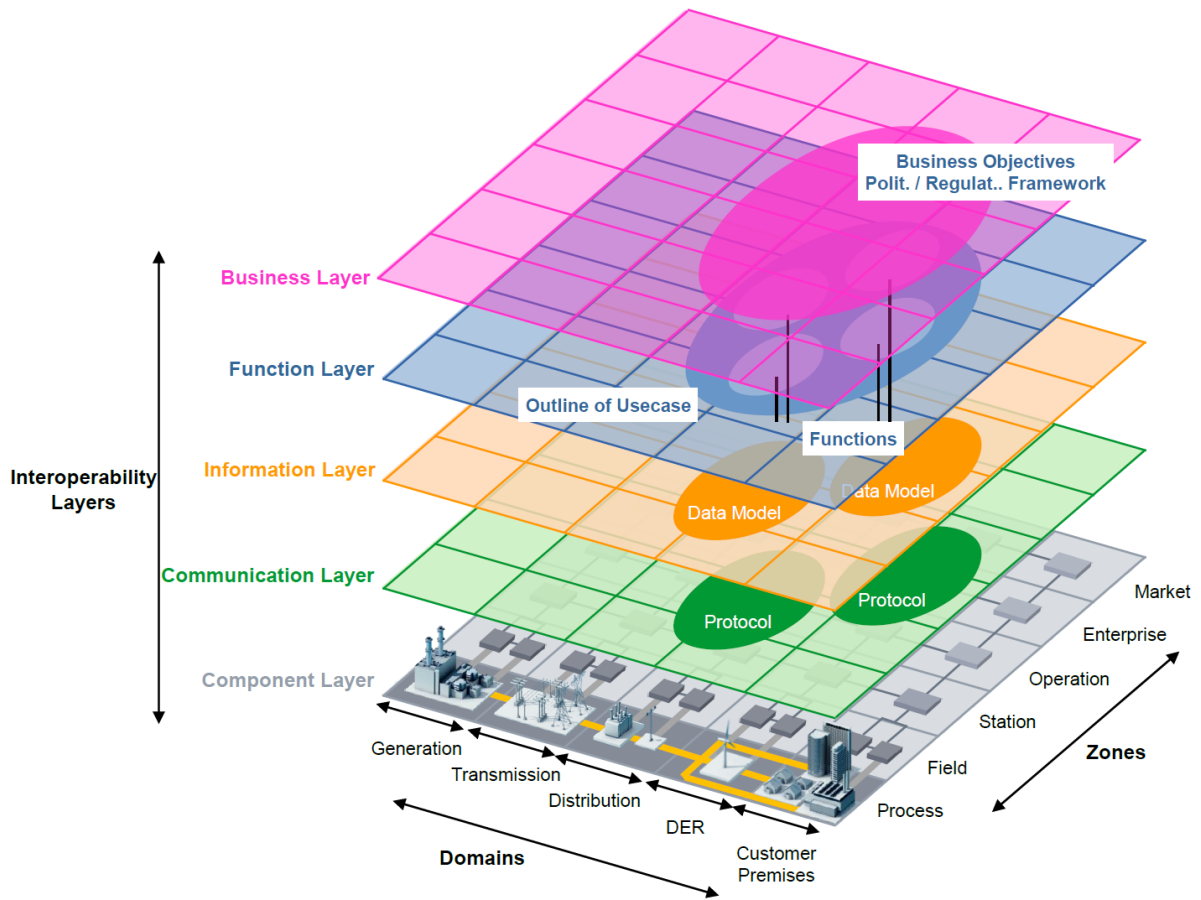


Figure 1.2: Smart-grid Architectural Model (SGAM) [2]

Within [6] the architectural framework of the European smart-grid networks - *Smart-grids Architecture Model (SGAM) Framework* (Figure 1.2) is defined. The basis of this model is the smart-grid information plane, which is represented by a Cartesian plane composed of five domains of one group as well as six zones of the other group.

The domains are the following ones:

- (Bulk) Generation
- Transmission
- Distribution
- Distributed energy resources
- Customer premises

And the zones are:

- Process (basic processes running within a domain)
- Field (devices in the field, eg. protection relays, etc.)
- Station (control and management at the substation level)
- Operation (on the level of control centers, SCADA/DMS/EMS)

- Enterprise (IT systems in the company)
- Market (IT support for the energy market)

Each interoperability layer is divided as described above. The layers are arranged one above the other (Figure 1.2). For each layer, the relevant standards are defined within the set of standards, which are selected according to their position in the information plane (see example below, Figures 1.3, 1.4 and 1.5). It is also worth mentioning that certain areas vertically intersect all layers (*cross-cutting issues*) - for example, the field of information security.

The purpose of SGAM is to give a systematic setting of standards that can be considered for a particular use case. The procedure can be summarized as follows:

- we start from a given use-case example,
- the components of a particular use-case are mapped on to the smart-grid information plane - the component layer - into cartesian products of domains and zones that concern them,
- In the Set of standards, we then find which standards are relevant for a given layer within interoperability layers.

Let's take an example – for example using the integration of distribution system operators' systems that deal with the power network. These are operations and planning support systems (SCADA / DMS, outage management system (OMS), network planning), the asset management system (EAM - Enterprise Asset Management) and other systems, such as the geographic information system (GIS).

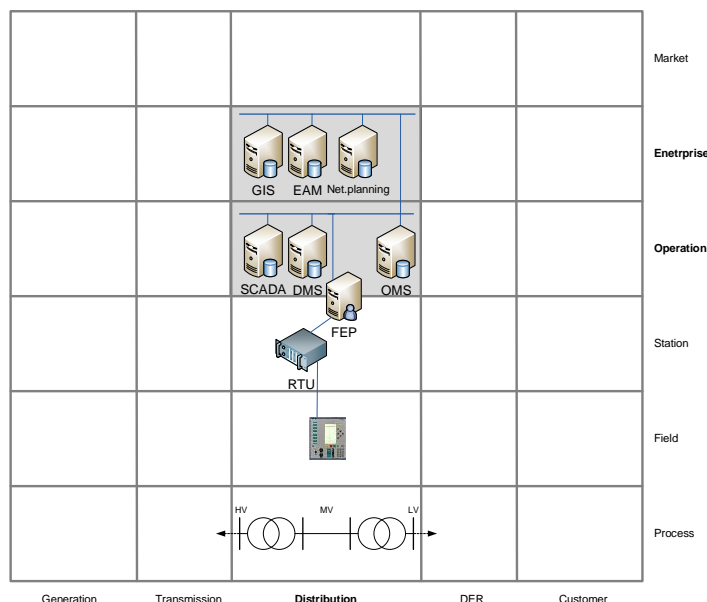


Figure 1.3: Example: Mapping into SGAM – component layer

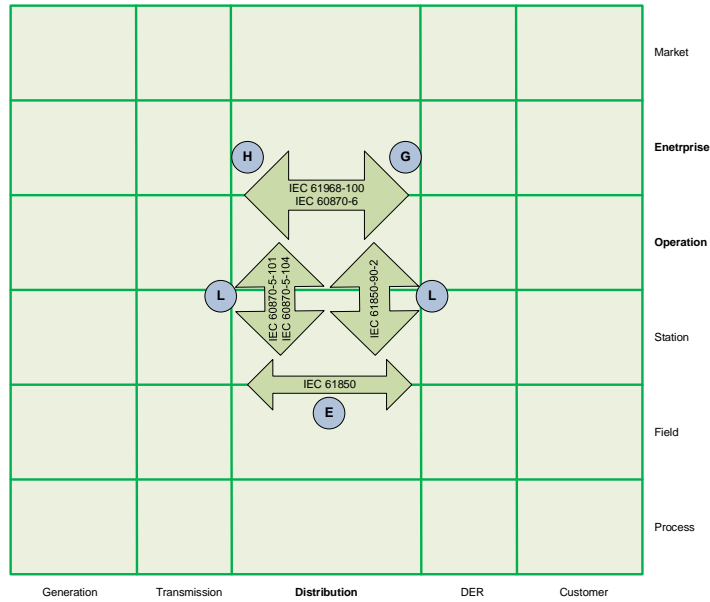


Figure 1.4: Example: Communication layer

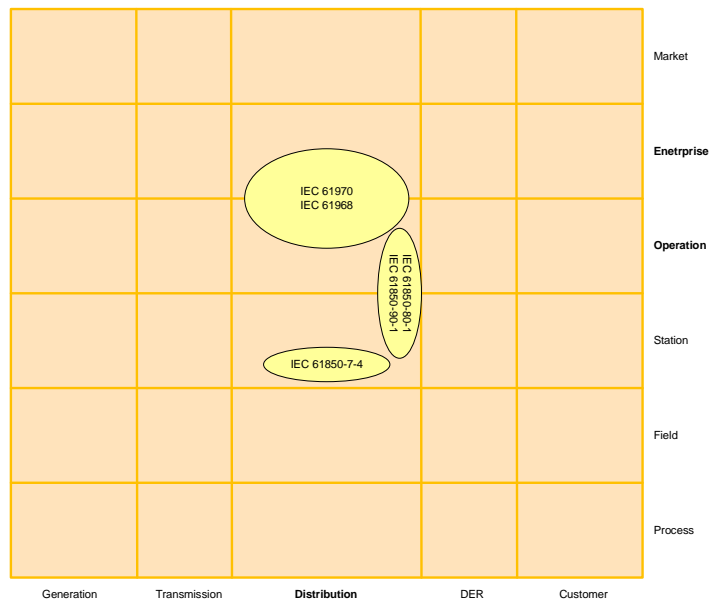


Figure 1.5: Example: Information layer

Figure 1.3 shows the mapping of these systems to the information plane of the component layer. The systems are divided into the domain of *distribution* within the *enterprise* and *operation* zones. Some systems can also be installed at the borders of zones and/or domains such as for example the FEP (Front End Processor), which serves to exchange

data between SCADA and the RTU (Remote Terminal Unit).

According to Figure 1.3, we need to find relevant standards within the set of standards for individual interoperability layers.

Figure 1.4 shows the relevant standards of the communication layer. Letters in circles represent the type of network for which we have a list of relevant standards for network compatibility within the set of standards (Table 77 in [7]), while the arrows contain standards that provide syntactic compatibility.

In Figure 1.5, relevant standards of the information layer are provided within the yellow ellipses, which allow semantic compatibility and place it into a certain business context.

The current version of the set of standards predominately addresses the standards of the communication and information layer of the interoperability fund.

Let's have a look at the most important layers within the Integration Fund, which can be used in the integration process of these systems.

1.2.1 Communication layer

For the integration of information systems in the zones of *operation* and *company* the reference architecture foresees the use of an H type network (*enterprise smart-grid sub-network*) and standards that allow IPv4 or IPv6 network connectivity. At the higher layer it specifies the IEC 61968-100 standard which defines the interfaces and methods of transmitting messages between systems within a Service Oriented Architecture (SOA).

1.2.2 Information layer

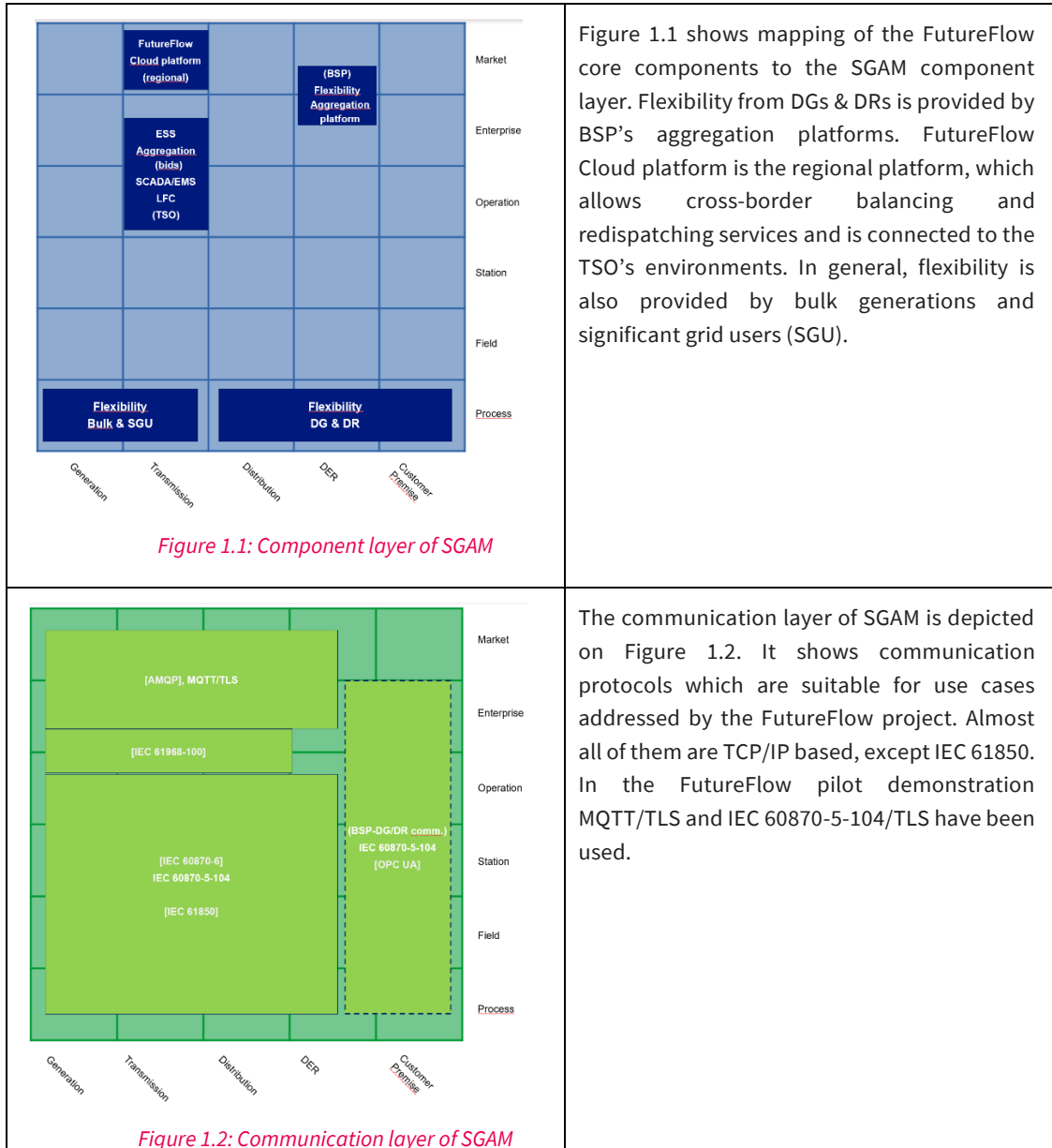
The information layer is one of the key layers that enables the implementation of smart grids. Without this layer it is not possible to perform an efficient system integration within a complex system such as the smart grid.

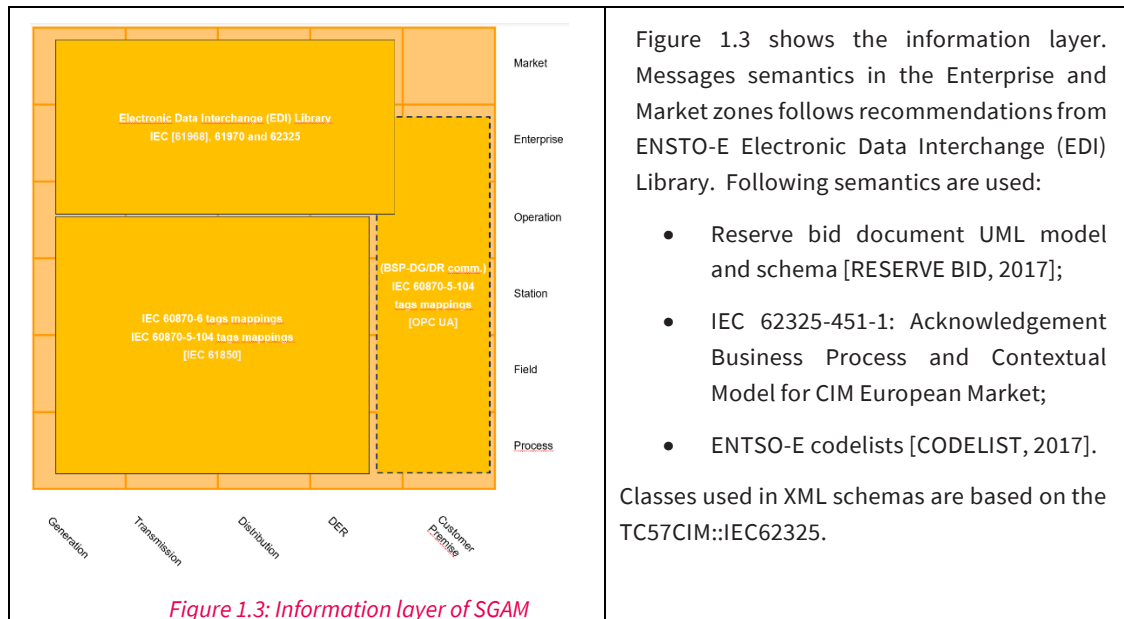
The key part of the information layer are data models. Modern data models are based on objects and relations among them. They enable the description and presentation of knowledge from a specific field of application or the specification of conceptualization, which is also called ontology. These are semantic models that allow computer recognition of the meaning of information.

The reference architecture for smart grids is determined by the CIM model (Common Information Model) as the basic semantic model for modeling the electric power system within the zones of *operations*, *company* and *the market* and the interaction of these zones.

1.3 Mapping of FutureFlow use case to SGAM

In the table below mapping of the FutureFlows' components to the SGAM is presented.





2 General ICT and IoT standards applicable to the context

2.1 oneM2M

2.1.1 Overview

The oneM2M Standardization partnership between accredited regional Telecom Standardization Development organizations across the globe (Europe: ETSI; North America: TIA, ATIS; Japan: TTC, ARIB; Korea: TTC; China: CCSA; India: TSDSI) is a structure similar to 3GPP aiming to specify a Service Layer exposing a common API for information exchanges to IoT applications, covering needs specific to IoT environments such as Subscription / Notification and Store and Forward. This service layer consists of middleware distributed across a communication infrastructure and gateways/devices, abstracting the complexity of underlying layers in a technology agnostic way while relying on capabilities exposed by the specific transport layers being used (e.g. wired Internet protocol, 3GPP, LPWAN etc) to meet requested QoS. Besides being agnostic to transport technologies and encompassing existing device management technologies (OMA DM or LwM2M for cellular and BBF TR-069 for wireline), the oneM2M layer acts as an interworking platform to integrate proprietary device protocols (e.g. supporting LwM2M, Home Appliance Information Model, AllJoyn/OIC/OCF devices, OPC-UA etc.), supports semantics information to enable interpretation across applications with different data models, and is being enriched to support translation across ontologies.

See www.onem2m.org for further details on oneM2M.

The oneM2M core specifications (based on Release 2A) were adopted for official publication as ITU-T recommendations, according to the agreement between the oneM2M Partners and ITU-T SG20. This includes System Architecture (TS-0001), Device Management (TS-0005 for OMA DM + LwM2M and TS-0006 for BBF TR-069), Field

Device Configuration (TS-0022), Protocols (TS-0004), bindings to CoAP (TS-0008), HTTP (TS-0009), MQTT (TS-0010) and Websockets (TS-0020), LwM2M Interworking (TS-0014), and other specifications related to interop testing, Home Appliance Information Models and Base Ontology.

Gemalto chaired the security Working Group of this organization during the course of the project, until July 2018. As a result, many security features elaborated in oneM2M were designed with the FutureFlow context in mind.

- *The core security specification in oneM2M, TS-0003, describe flexible security frameworks to provide the following services:*
 - *Remote Security Provisioning framework (RSPF): relies on either symmetric PSK, PK/Certificates, or third party assistance (e.g. 3GPP GBA/MEF)*
 - *Security Association Establishment Framework (SAEF): supports Security associations between adjacent nodes (TLS or DTLS based), or End-to-end security services through MAF*
 - *Authorization and Access Control: initially based on Access Control Lists associated to resources, now enriched with support of dynamic authorization schemes (e.g. OAuth tokens), roles and contextual attributes.*
 - *Privacy Policy Management: Uses a “Terms and Conditions mark-up language” to facilitate user management of privacy preferences across multiple applications and integrate local or sectorial regulatory constraints into resulting Access Control Policies.*

It also comprises several annexes, including Annex J specifying a UICC application (based on ETSI TS 102 221) to support the above frameworks.

The latest “point release” 2A completes the initial Release 2 published early 2017 and contains the following additional security related specifications:

- **TS-0022 “Field Device Configuration”:** This specification addresses the provisioning and configuration of field devices, including security bootstrapping for enrolment with a Service Provider, and maintenance during operation with a service provider using Device Management.
- **TS-0032 “MAF (M2M Authentication Function) and MEF (M2M Enrolment Function) interfaces”:** This specification defines adaptations of the service-oriented API enabling M2M nodes (which could be infrastructure servers, Gateways or field devices) to interact with a Trust-enabling infrastructure used to provision security credentials. The trust infrastructure is assumed to be operated by a party trusted by all stakeholders (including multiple applications), and therefore differentiates between an M2M Enrolment Function (MEF) trusted by the Enrolment ecosystem (from manufacturing until association for operation with a Service Provider) and handling the security bootstrapping, and an M2M Authentication Function (MAF) trusted by the ecosystem for operational usage with a service provider, and able to provision credentials in the various nodes that need to communicate securely (including credentials used to provide end-to-end security at the application level).

Release 3 finalization: This new release expected to be published early Q2 2018 will integrate the following new features:

- **New Normative Annex L to TS-0003:** This annex specifies a GlobalPlatform inspired **framework to support cryptographic services (including support of PK, AEAD and elliptic curves) in an embedded secure element.** In order to facilitate implementation as a JavaCard applet, it does not rely on UICC specific features such as a standardized file system. It may therefore supersede the previous Annex J defining UICC based security services, which was never deployed.
- **TS-0016 “Secure Environment Abstraction”:** This specification extends the oneM2M RESTful device API to enable easy access from application developers to cryptographic services provided by a “Secure Environment”, such as specified in Annex L in the case of embedded Secure Elements. The “Secure Environment” concept intends to provide abstraction of different security implementation such as eSE, TEE, maybe TPM tomorrow, and White-box cryptographic software.
- In Release 3, the **access control API** has been enhanced to support management of distributed configuration involving separation of Policy Decision Point and Policy Enforcement Point.
- TR-0038, a **“Developers Guide for implementing security”**, is also being finalized (thanks to Qualcomm) as part of the “Developers Guides” series intended to facilitate adoption of the oneM2M API by IoT developers.

Features in discussion for Release 4: Release 4 timing should extend through 2018 to early 2019. The following security extensions are being discussed:

- **TR-0041 “Decentralized authentication”:** Initiated by Huawei, a Technical Report, TR-0041, has been drafted, which suggests to extend the TS-0003 RSPF and SAEF frameworks to accommodate an Identity Based cryptographic scheme, where the public key of an entity can be derived from its identity Id while the corresponding secret key is generated by a trusted authority. The main benefit of IBC is that the public key does not have to be certified since its authenticity can be checked by simply re-generating it from the identity. Its main drawback is that it needs a trusted entity who generates (and so has access to) all the entities’ secret keys. The proposed Key generation process is a combination of the Schnorr’s signature with the Diffie-Hellman key exchange protocol.
- **TR-0048 “App-ID Registry Functions”:** The current oneM2M specifications support the concept of an application database, the “App-ID registry”, where application versions can optionally be registered to obtain a unique identifier valid across multiple service providers. Iconectiv (an Ericsson subsidiary), currently mandated by ATIS to operate this registry, is proposing to enrich the registry with security features which could facilitate, for example, the barring of all entities of a rogue application without reconfiguring the access control currently assigned individually to each entity.
- **TR-0050 “Attribute-Based access control policy”:** The aim of this work item is to consolidate and extend the access control mechanisms already defined in previous releases in a more homogeneous manner.

- **TR-0040 “Trust Management in oneM2M”:** This work item aims at enhancing trust management in IoT ecosystems.
- **TS-00XX (not assigned yet) “GlobalPlatform Interworking”:** The aim of this work item initiated by Gemalto and GlobalPlatform (as an industry partner of oneM2M) is to fully integrate GlobalPlatform secure management capabilities in the oneM2M service layer, in a way that complements the existing Device Management technologies.

Overview of relevant work in other Working Groups:

- **Conformance Program:** Currently TTA (the Korean partner) is still the only certification authority, however it is expected that the GCF (Global Certification Forum) will also be accredited to act in this role soon. Currently TTA only addresses Interoperability but intends to enlarge its scope to cover Compliance testing as well. *The list of already certified products (available at http://www.onem2mcert.com/sub/sub04_01.php) is getting longer and richer, including e-IoT Energy Platform and Gateways from Korean electric supplier KEPCO, Universal IoT Gateway from ModaCom, Infrastructure servers from 6 different sources, and several other end products and software components.*
- **Test Working Group: TS-0031 “oneM2M Features catalog”** (currently mostly based on Release 1) will be part of release 3, which is used as the basis for the **“Definition of Product Profiles”** in TS-0025. As the current profiles focus solely on the API level, exclusively of any configuration features, they only consider Access Control in terms of security. The specifications developed by the TST WG (currently for Rel-1) always serve as the basis for the conformance program.
- **Other technical Working Groups:** Many deliverables are being finalized for release 2A or 3, or progressing for later releases (“TR” are non-normative reports while “TS” are normative specifications and other “WI” produce changes to existing specifications). The following may be of interest:
 - o General:
 - TR-0044 Heterogeneous identification in oneM2M system
 - TR-0051 oneM2M API Guide (Rel-4)
 - o Interworking:
 - TS-0033 Proximal IoT Interworking framework
 - TS-0026 3GPP Interworking
 - WI-0029 OPC-UA Interworking
 - TR-0031 OMA LwM2M Device Management and Interworking enhancements
 - TR-0042 W3C Web of Things Interworking
 - TR-0043 Modbus Interworking
 - TR-0027 DDS Usage in oneM2M
 - o Information domain translation, semantics and ontologies:
 - TR-0033 Study on enhanced semantic enablement
 - TS-0030 Ontology Based Interworking
 - TR-0049 Industrial Domain information model mapping and semantic support (Rel-4)

2.1.2 Analysis in the FutureFlow perspective

The use of a standard IoT framework in FutureFlow would ensure interoperability across components from different origins and would facilitate application development via the use of a standardized API. But mostly, this standards integrate advanced capabilities for end device management including software updates, as well as a complete set of advanced security features including authentication and authorization / Access Control. In addition, oneM2M would provide a semantic layer facilitating interworking between components using different data models, including the concept of ontologies.

We remark that the FutureFlow architecture is based on exactly the same layers that oneM2M relies upon in its standard framework:

- use of TCP/IP (and TLS for security)
- use of the HTTP and MQTT protocols for information dissemination
- Use of OAuth for security
- REST based application programming interface.

In this context, it seems that the main impact on the FutureFlow architecture to migrate to oneM2M, beyond alignment on the oneM2M Management and security mechanisms, would mostly impact the API level. Though oneM2M technology was not used in the FF demo platform, mostly because of lack of maturity at the time where the project started, it could therefore be recommended that later, larger scale deployment of AFRR balancing platforms consider adopting the oneM2M Standards to ensure broader service layer interoperability. In addition to integrating all security mechanisms developed in the current project, this would provide homogeneity and reinforced security for access control and authorization and optionally facilitate remote DRDG, TEMS and WAMS management through the inclusion of technologies already widely deployed in underlying ICT networks.

Analyzing the suitability of oneM2M to fit the constraints of FutureFlow, we remark that real-time constraints are not well taken into account in the current oneM2M releases. The applicability of the standard to Smart Grid use cases was already demonstrated by KoreaGrid, but they already mentioned that this point had to be improved, and such work is under way for oneM2M Release 4 which might be published around end 2019.

An important part of oneM2M is the inclusion of semantic interoperability between multiple data models. This is a problem frequently encountered in smart grid applications including in the FutureFlow Use Cases. In this context, oneM2M developed a Reference Ontology based on the European SAREF (Smart Appliance Reference Ontology) which is already suitable for the DR/DG level. This ontology is currently extended to address many other domains by ETSI TC SmartM2M. However the inclusion of Energy Transmission Data Models such as CIM might not yet be one of their current priority. Therefore, we recommend that the project stakeholders who are members of ETSI or oneM2M promote the extension of the oneM2M Reference Ontology to the wider Energy Distribution and Transmission domain as a strong priority.

2.2 MQTT

2.2.1 Overview

MQTT is a machine-to-machine (M2M)/"Internet of Things" connectivity protocol defined at OASIS and ISO. It was designed as an extremely 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.

See <http://mqtt.org/> and <https://docs.oasis-open.org/mqtt/mqtt/v5.0/mqtt-v5.0.html> for further details on MQTT standard.

2.2.2 Analysis in the FutureFlow perspective

Some high end equipments may benefit from full fledged processing power and connectivity, allowing them to participate directly into advanced and complex exchange systems like the blockchain illustrated in FutureFlow project. But most decentralized energy production devices like solar panels or wind turbines fall under the "IoT" classification, including constrained execution environment and limited connectivity. Nevertheless they also need to send production information and occasionally receive some configuration commands or updates remotely, and MQTT fits perfectly for these devices as they will delegate the more advanced processing, like blockchain access, to a trusted central gateway.

MQTT can be deployed in a straightforward model, just requiring an online and public MQTT server address, but it offers many optional advanced security mechanisms to better control accesses and enhance trust. Of course, for the energy domain, MQTT clients must be required to prove their identity based on certificates, communication must be encrypted and some quality of service must be ensured e.g. by using dedicated MQTT server.

In the context of this project, MQTT was also used as a standard exchange protocol to propagate energy production events published on the central blockchain to partners monitoring system.

3 Overview of energy standards

"In areas of converging technologies, experts who have developed IT security standards are now being faced with the need to work closer with users of IT applications. They also need to realize that, in many areas, functional safety and IT security can no longer be considered separately. IT security must be seen as a "business facilitator" and not as a cost factor." (G20 declaration, 2016).

Among the SmartGrid standardization gaps identified in 2016 by the ETSI/CEN/CENELEC Smart Energy Coordination Group (SGCG) of the M/490 European SmartGrid Standardization Mandate, the following seem the most relevant in the FutureFlow Context:

3.1 HV-DC grid architecture

Description: With the development of off-shore grids, there is a need for coordination, coherence and interoperability for equipment (converters, circuit-breakers, protection,...) as well as for grid topology (grid design, voltage level, grid code,...) in the High Voltage DC domain. The ESO standardization should take into account the work done in the German committee context.

System: HV-DC systems

Involved domains: Transmission (mainly)

Impacted layers: Component (mainly),

Impacted zones: Process/Field

Related use cases: to be determined

TCs/WGs to be involved: IEC TC8, TC8X, TC22

3.2 Auxiliary Power System Standardization

Description: Develop standardization for auxiliary power systems (low voltage DC networks): AC/DC converters, DC management systems, DC protection

System: DER, Storage, PV, EV, Power Quality

Involved domains: Distribution, DER, Customer premises

Impacted layers: Component (mainly), communication and information

Impacted zones: Process/Field

Related use cases: to be determined

TCs/WGs to be involved: TC 22, TC 77, CISPR, CLC/TC 205, TC 57, TC 13

Affected standards/work items: (IEC and other SDOs)

3.3 aFRR regulation

Description: TSO-BSP communication for providing aFRR signals, metering and validation data exchange by using IEC 60870-5-104. Additionally using the regulation towards the DER.

System: TSO, BSP, DER, Storage, PV, EV, Power Quality

Involved domains: TSO, Distribution, DER, Customer premises

Impacted layers: Component (mainly), communication and information

Impacted zones: Process/Field

Related use cases: aFRR regulation and validation

Affected standards/work items: (IEC and other SDOs): IEC 60870-5-104.

3.4 Energy Management harmonized data model for industry and power grid

Description: An energy management system can be stand-alone or can be part of the process automation system. This applies to industrial processes, electrical components linked to the processes and auxiliary equipment. In many cases, the same technology is used on the power utility supply side (substation automation technology) and demand side. In order to facilitate energy management, all the equipment related to the process, to the electrical installation and to the auxiliary services should be able to communicate together. Because of many existing industrial processes, an important consideration is the ability to upgrade on-site energy systems to enable integration with smart grid signals such as dynamic pricing and curtailment demand response. **Harmonized data model for industry and power grid:** Too many data models already exist without mapping between them. We recommend harmonizing the data model related to energy management between Industry and Electricity (EN 61158, EN 61850)

System: EMS, DMS, HEM, BEM

Involved domains: Transmission, Distribution, DER, Customer premises

Impacted layers: Component, Communication and Information

Impacted zones: Process/Field, station, operation, enterprise

Related use cases: to be determined

TCs/WGs to be involved: CLC/TC 205, TC 65 and TC 57

Affected standards/work items: (IEC and other SDOs) EN 61158 and EN 61850

3.5 Data modelling for Micro Grid Management

Description: Provide data model to enable remote monitoring and controlling a micro-grid and especially to manage its status related to its connection to the grid (islanding detection, islanding modes, connection, disconnection, reconnection, these modes are not fully covered today)

System: Micro-grid systems, Distribution management systems, DER operation systems, Industrial automation systems, Building Automation systems, Home Automation systems

Involved domains: DER, Customer premises, Distribution

Impacted layers: information layer

Impacted zones: from process to operation

Related use cases: refer to the FSS Report

TCs/WGs to be involved: CLC TC8X, IEC TC8 IEC TC57 WG14, WG17, WG10, WG21 IEC PC118 IEC TC64 (safety and security)

Affected standards/work items: (IEC and other SDOs) IEC 61850 series, IEC 61968 series

Already engaged work: (existing work items in IEC and other SDOs; similar to point above) IEC TC57 – IEC 61850-90-15, IEC 62746

We note that in the context of adoption of oneM2M as a reference service layer standard for future deployments, the above 2 gaps could be easily addressed by extending the oneM2M Reference Ontology to cover these data models, as suggested above.

3.6 Interoperable identification and (sub)billing (using the AMI) capabilities in Smart Grid

Description: Some Smart Grid use cases such as E-mobility, involving billing of customers for using EV-charging infrastructure, require convenient means for seamless customer identification and authentication and secure transaction between the infrastructure and a customer or EV-equipment. Some standards exist in the telecommunication sector that could easily be extended or adapted to enable interoperable deployments in Smart Grid applications. These standards are about using smart cards that may be combined with contactless technology. This concerns the standardization of identification mechanism, question is how is the metrology is covered

System: Security, Telecommunication, Authentication authorization accounting system, E-mobility system, Trading system, DER operation system

Involved domains: Potentially all, particular impact on customer premises and DER.

Impacted layers: All, but major impact on component and communication layer

Impacted zones: All, major impact on Operation and Field and it will have impact on market and enterprise

Related use cases: Clusters such as Access control, Billing, market settlement, DER operation and management, E-665 mobility

TCs/WGs to be involved: ETSI TC SCP, ETSI SAGE, SGIS (support is needed for this proposition), TC57, JWG M468/M490 on E-mobility communication

Affected standards/work items: Standards related to secure identification and transactions using IEC62351 series, IEC 62746 DR standard (in progress), NFC (Near Field Communication) technology such as ETSI TS 102 221, TS 102 613, TS 102 622 and related API specification

3.7 System management of T&D systems, DER and Micro-grid systems connected

Description: Provide a standard way to manage in security the different steps of a smart grid system, with dynamic reconfiguration and remote access features, from start-up to a secured energized and operational stage, and to keep these operational capabilities all along its life cycle, still with the same level of security.

System: Substation automation, Feeder Automation system, Power Quality distributed management system, Distribution management systems, Transmission management systems, DER operation systems, Micro-grid systems

Involved domains: All,

Impacted layers: communication, information layer,

Impacted zones: from process to enterprise

Related use cases: to be retrieved from the FSS Report

TCs/WGs to be involved: CLC TC8X, IEC TC8, 751 IEC TC57 WG14, WG17, WG10, WG21, WG15

IEC TC88, IEC TC69

IEC TC13

Affected standards/work items: IEC 61850 series, IEC 61968 series, IEC 61970 series

Already engaged work: existing work items in IEC and other SDOs; IEC TC57 – some preliminary work already started there (CIM (WG21) or IEC 61850 based (WG10/17)) in strong relationship with TC57 WG15 (security)

4 Conclusion on FutureFlow standardization findings

- In the scope of the FutureFlow project, the MQTT protocol was used and successfully tested, as well for the real-time data (measurements & control), as also for the market-related data (bidding, cross-zonal capacities, acknowledgement business process, etc.). It can also be well secured (by TLS), as was also proven in the FutureFlow project. It is standardized (ISO/IEC 20922:2016), but hasn't been considered for usage for such kind of applications. Thus, it was recommended, that the MQTT (with CIM based semantics) is considered as an option for applications in the electric power system domain and that it is added to the list of available protocols in the scope of Smart Grid Reference Architecture. ICT and IoT standards, as well as energy related standards are quite complete and mature and allow interoperable and secure deployment of Smart Grid solutions. Members should continue monitoring and influencing identified standards to preserve FutureFlow project investments.

5 Presentation of FutureFlow standardization related findings to the Slovenian Institute for Standardization – a full member of IEC, CEN, CENELEC and ETSI

On October 8th 2019 the FutureFlow findings and results regarding the standardization were presented to the Slovenian IEC TC57's mirror committee – SISI TC/PSE. The committee is within the SIST - the Slovenian Institute for Standardization (SIST), which is recognized as the national standards body in the Republic of Slovenia. SIST develops, adopts and maintains Slovenian standards, and participates in the work of international (ISO, IEC, ITU-T) and European Standardisation Organisations (CEN, CENELEC, ETSI).³

The meeting's agenda was as follows:

1. Approval of the proposed agenda
2. Approval of the minutes of the previous ordinary meeting and review of the conclusions of the correspondence meetings
3. Review of the work of related European and international committees
4. Report on Current Trends in the IEC TC57 (Souvent)
5. **Presentation of FutureFlow's findings on standardization and proposals for amendments to the SGRA (reference architecture) (Souvent)**
6. SIST TC/PSE 2020 Plan

The presentation was focused on:

- Deliverable 1.3: Data needed to implement the common activation function - two use cases were described in accordance with IEC 62559:
 - Use case description for aFRR (crossborder – TSO-TSO model)

³ Ref <http://www.sist.si/en>

- The use case or redispatch actions in TSO-TSO cross border market model

Analysing the deliverables of the CEN-CENELEC-ETSI Smart Grid Coordination Group in the context of the EU M/490 standardization mandate group, especially the “SGCG/M490/G_Smart Grid Set of Standards” and “SG-CG/M490/L_Flexibility Management”, it was found, that there are no use cases related to cross-border balancing and redispatching. Consequently, the semantics for the data exchange is not defined for all the data which needed to be exchanged.



5.1: FutureFlow presentation for the Slovenian Institute for Standardization – full member of IEC and CENELEC

The FutureFlow’s related meeting’s conclusion was that both use case descriptions, which were made in accordance to the IEC 62559 use case description methodology and template will be contributed to the IEC smart grids use cases repository through the IEC National Committee of Slovenia represented by SIST. The same applies to the proposal to add the MQTT to the list of relevant protocols for use cases related to the data exchange in the scope of the Smart Grid Reference Architecture. The proposal will be sent to the CEN-CENELEC-ETSI Smart Grid Coordination Group through the SIST.

6 Bibliography

6.1 Energy Cybersecurity

General EU references:

1. Cyber Security & Privacy report, 12/2016, CEN-CENELEC-ETSI Smart Energy Grid Coordination Group (SEG-CG)
2. Smart Grid Set of Standards, version 4.1 draft, 01/2017, CEN-CENELEC-ETSI Smart Energy Grid Coordination Group (SEG-CG)
3. “Best Available Techniques reference document for the cyber security and privacy of the ten minimum functional requirements of the Smart Metering systems”, DG ENER Task Force EG2, 2016

German BSI Smart Metering requirements:

Complete set of Technical guidelines (gateway including security modules, PKI etc.) for smart meter gateways:
https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03109/index_hm.html

Overview and access to documentation - Protection profiles, technical guidelines and cryptographic recommendations:

https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/SmartMeter/UebersichtSP-TR/uebersicht_node.html

UK Smart Metering Implementation Plan:

1. Comms Hub Technical Spec (CHTS):
<https://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0ahUKEwip8MbtwbXRAhVGahoKHW9OA3QQFggI MAE&url=https%3A%2F%2Fwww.smartenergycodecompany.co.uk%2Fdocs%2Fdefault-source%2Fsec-documents%2Fdeveloping-sec%2Fbaselined-sec-subsiary-documents%2Fchts-v1-47-final.docx%3Fsvrsn%3D2&usg=AFQjCNGhitjPC8tudtaX5JTyVGVDcDERtw&sig2=nd4TYxvnFUMwwA4ejbQug&bvm=bv.142059868,d.d2s>
2. Great Britain Companion Specifications:
<https://www.gov.uk/government/consultations/smart-metering-implementation-programme-great-britain-companion-specification-version-08>
3. Smart Metering V2 spec:
<https://www.gov.uk/government/consultations/smart-metering-equipment-technical-specifications-second-version>
4. SG-CG/M490/H_Smart Grid Information Security (Phase 1)
<ftp://ftp.cen.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/Security.pdf>
5. SG-CG/M490/H_Smart Grid Information Security (Phase 2)
ftp://ftp.cenelec.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/SGCG_SGIS_Report.pdf

ENISA References:

1. <http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering>

2. <http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/sgtl/smart-grid-threat-landscape-and-good-practice-guide>
3. <http://www.enisa.europa.eu/activities/Resilience-and-CIIP/workshops-1/2014/eg2>
4. <http://www.enisa.europa.eu/activities/Resilience-and-CIIP/workshops-1/2012/smart-grid-certification-components>
5. <http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/information-sharing-exchange/good-practice-guide>

[1] 'IEC 62357-1:2012 Power systems management and associated information exchange - Part 1: Reference architecture'. IEC, 2012.

[2] 'Smart Grids Reference Architecture'. CEN-CENELEC-ETSI Smart Grid Coordination Group, Nov-2012.