STARGRID

FP7 - 318782

D5.1 – Preliminary Project Report

Version	V1.0	Status	final
Work Package	WP5	Preparation Date	2014-10-30
Due Date	M24	Submission Date	
Main Author(s)	Giorgio Franchioni (RSE) David Nestle (IWES) Marco Portula (IWES) Christoph Nölle (IWES) Mihai Calin (DERlab) Doina Dragomir (ASRO)		
Contributors	Speranta Stomff (ASRO) J. Emilio Rodríguez (Tecnalia) Ainhoa Ascarza (Tecnalia) Diana Craciun (DERlab)		
Dissemination Level	PU	Nature	R
Keywords	Smart Grid, Standardisation, Recommendations		

Version History

Version	Date	Author(s)	Comments
v0.1	2014-06-13	David Nestle (IWES), Marco Portula (IWES)	Initial Version for adding contributions by partners
v0.2	2014-07-08	Giorgio Franchioni (RSE)	Content added
v0.3	2014-07-18	Marco Portula (IWES)	Restructuring
v0.4	2014-10-20	Christoph Nölle (IWES), David Nestle (IWES), Giorgio Franchioni (RSE), Mihai Calin (DERlab), Doina Dragomir (ASRO), Speranta Stomff (ASRO), Emilio Rodríguez (Tecnalia)	Integration of stand-alone documents by partners
V1.0	2014-10-30	Giorgio Franchioni (RSE), Emilio Rodríguez (Tecnalia), Christoph Nölle (IWES), David Nestle (IWES)	Overall revision
V1.1			
V1.2			

Table of Contents

Executive summary

This deliverable proposes and discusses preliminarily the STARGRID Recommendations relevant to the Smart Grid Standardisation framework. It provides six main Recommendations, respectively concerning:

- The alignment of standards with national/local regulations.
- System interfaces among Smart Grid stakeholders.
- Interoperability issues.
- Security and Privacy.
- The Standardisation process.
- Distributed Energy Resources integration rules and specifications.

The Recommendations are mainly addressed to Policy Makers (the EC within them), Standardisation Bodies and Regulation Authorities. However, one may easily recognize that the document targets the stakeholders of the Smart Grid value chain as well.

Along with the above Recommendations, the deliverable proposes a number of "corollary" recommendations as well. Whenever suitable, it highlights good practices of implementation, coming from defined experiences in the European context, e.g. from EU funded projects.

For each topic, the document explains the motivations subtended by the relevant recommendations and discusses the possible impact of their implementation on the electric system and on the main impacted stakeholders.

Finally, the deliverable gives some indications on possible implementation ways and associates to each Recommendation priority and urgency suggestions.

The deliverable thus synthesizes the work carried out by STARGRID with the analysis of the current Smart Grid Standardisation framework and of the related initiatives either from Standardisation Bodies and Industry stakeholders. The provided Recommendations also refer to the specific survey done by STARGRID on industry representatives through suitable questionnaires and workshops. The results of the mentioned analysis and of the survey as well are publicly available in the STARGRID web site.

The present document has to be considered, as said, preliminary. Indeed, the document is intended for distribution to sector experts for comments and early feedback.

The results of this further survey will converge in the final Deliverable of STARGRID D6.2, which will be published in January 2015.

R1 Enrich an obligate core with modular elements fitting national/local regulation

Addressed at Standardisation Bodies and Regulation Authorities

Summary

Typically there is a trade-off in Standardisation between the level of details specified, the extent of applications and the geographical acceptance for which consensus can be reached in a certain time. Many standards on IEC level can be applied to a relatively wide set of applications (like the IEC 61850 family) and they are applicable to products and services world-wide. On the other hand specific national or even regional standards are oftentimes developed strongly focused on the specific regulatory and other conditions (e.g. for DER control and smart metering). These standards are not necessarily compliant or conformant with relevant IEC standards, but development is performed much more quickly due to the limited scope. Furthermore such standards in some cases are more specific about mandatory requirements for full interoperability. This leads to the unfavourable situation that the strong base and the quality represented by IEC standards is not used in many smart grid related cases because the necessary adaptation to country-specific regulation cannot be performed in the short time required or the process seems to be too difficult and for this reason independent local standards are developed and made mandatory by regulation.

Main Recommendations

1. Provide core standards based on core use cases that can be extended and profiled in order to fit national regulation. The core should cover:
    a. System Interfaces (see R2 Obligatory standards for System Interfaces).
    b. Security and Privacy (see R4 Security and Privacy).
    c. DER-Grid Connection Rules (see R6).
2. Set up a collaboration framework between Regulation Authorities and Standardisation Bodies, in particular at national level.
3. Foresee possibility of national extensions to International/European standards.
4. Extend core standards out of variety of national extensions.

Explanation

A) Standardisation must adopt use cases from political and regulatory authorities and evolve them over time (time modularity)

Use Cases of functionalities and applications should be the references of any Standardisation initiative. Definition of Use Cases of functionalities and applications, at least for the most complex operations, is deemed essential as a pre-requisite of the Standardisation in the smart grids complex context.

Smart grids and smart metering depend heavily on regulation and legal frameworks (like grid operation and electricity markets in general). They are and will most likely remain within the next years diverse between Member States of the EU. Also other national differences regarding grid structure, customer behaviour, security concerns, etc. lead to very different situations and developments. For this reason, collaborative mechanisms between Regulation Authorities and Standardisation organizations should be set up that make sure Standardisation committees react quickly on regulatory requirements and to make sure that regulators understand the opportunity of making adapted international standards mandatory for the interaction of the stakeholders affected by a certain regulation. Such collaboration should especially ensure that very specific use cases defined by regulation are covered by the respective standards.

To increase interoperability the content of core standards should at least cover an EU harmonised minimum set of supported use cases within a certain field of application (e.g. smart metering). In areas of national regulatory competence this indicates a minimum of national regulation. This could be achieved by an EU Directive or probably by EC recommendations.

A good example is the set of recommendations provided by the EC on basic use cases for smart metering: European Commission Recommendation 2012/148/EU on preparations for the roll-out of smart metering systems. They should be even more precise and should be provided also for the other system interfaces (see R2 Obligatory standards for System Interfaces). Relevant Standardisation committees should check whether these requirements are met by the current standards (instead of inventing their own use cases). Another example is the tariff application cases defined by the German technical guideline TR-03109.

Many discussions are focussed on questions what kind of use cases is to be expected in the future. As there is no reliable prediction possible, this can lead to significant delay even for the Standardisation of clearly needed use cases. It should be ensured to make standards available that reflecting the current situation. The aim to enable envisioned use cases of the future should be taken into account, but discussion on that should not postpone an initial version for now. A later extension of the standard to cover new use cases should ensure backward compatibility.

B) Member States as source of evolution (area modularity)

A (temporary) diversity of standards and regulation in Europe based on a common core could be seen as an opportunity. As described before regulatory conditions regarding smart grids are and will most likely remain within the next years diverse between Member States of the EU.

This imposes a major challenge to the development of smart grid standards, as standards have to serve the use cases that are relevant to each market and grid regulation situation. Usually regulation and legal frameworks will not adapt to standards, but standards have to support the regulatory and legal situation. It is a good approach to aim at the development of standards that are flexible regarding this. It is also a fact, though, that regulators and markets tend to prefer standards that specifically reflect the requirements of the current situation as these usually are simpler to implement and implications on the market position are easier to understand. Especially the system

interfaces (see R2), which may need to be adopted by regulation and made mandatory for certain applications/devices will need to be specific to national requirements.

Using the same core it should become much easier to transfer regulatory concepts from one Member State, but this should also help to compare regulations and to make efficient use of the experiences gained in each Member State.

C) Require national uniformity

As explained before on one hand the specifications should not be too fragmented. On the other hand national diversity regarding this Standardisation is probably necessary to gain relevance (see Section before). For this reason at least Member States should be required to adopt binding rules for certain applications (in particular system interfaces between independent actors, security and data protection, interconnection rules for distributed energy resources). Smaller Member States may choose to cooperate with others to generate a substantial market based on common standards.

National standards should demonstrate that they reflect current regulatory and legal national framework to enable the development of smart grids under the respective conditions. They should go beyond the current situation, though (e.g. reflect variable tariffs).

It could be an option to provide European standards that would become mandatory for all Member States not having provided own system interface standards by a certain date.

Implementation

This recommendation is addressed to Standardisation organizations as well as to regulators. A stronger collaboration between Standardisation organisations and regulators is considered crucial by the authors to enable markets for core smart grid functions.

Main impacted stakeholders

Regulation Authorities;
Standardisation Bodies

Some recent developments indicate a tendency in the proposed direction already, like the interaction between European grid codes, national grid codes, and Standardisation (e.g. the ENTSO-E Requirements for Generators code, and the European standards/specifications EN 50438:2013 and CLC/FprTS 50549), or the European Smart Metering Directives 2009/72/EC and 2009/73/EC, which demand national legislative actions for the Smart Meter rollout. The latter have been supported by a recommendations on the functionalities to be covered (EC Recommendation European Commission Recommendation 2012/148/EU), which ask for the implementation of standardised interfaces, in particular regarding customer access to meter data (§42a).

R2 Obligatory standards for System Interfaces

Addressed at Policy Makers, Regulation Authorities (EU and national), and Standardisation Bodies

Summary

In this document "system interface" refers to interfaces where different major stakeholder roles of the smart grid communicate with each other and therefore the interfaces could impact on the sphere of different actors. That is exactly the point where interoperability is needed. A list of proposed system interfaces is given at the end of the recommendation description. The recommendation aims to introduce a set of mandatory system interface specifications based on International standards, in order to allow for full market participation of distributed energy resources, demand response providers, aggregators and other innovative energy services providers. The lack of commonly agreed upon communication standards is a major stumbling block for the Smart Grid development, and prevents many new effective solutions for the grid operation to proceed from the research stage to actual implementation. Based on the findings of the STARGRID project, we present a list of system interfaces, which are urgently lacking such a common denominator, and propose a development process, which includes both the European and national levels.

Main Recommendation

1. Interoperability on system interfaces should be ensured by Standardisation and regulation; for this purpose, regulation authorities shall define obligatory standards that are uniform at least on national level.

Corollary Recommendations

- Implement a European framework that specifies a set of system interfaces requiring national regulatory provisions, to ensure interoperability at least on a national level. Foster voluntary cooperation between Member States to develop harmonised solutions, without slowing down the process excessively.
- Technical specifications imposed by regulatory means should be based on International standards, wherever possible, and must define test procedures and certification requirements. (R3 Prioritize interoperability test specifications for all Smart Grid standards).
- Take security seriously: standardised solutions require a high level of security measures, to prevent devastating effects of large scale attacks. (R4 Security and Privacy).
- Find a balance between market and standards approach.

Explanation

One of the main barriers for market introduction of Smart Grid technologies involving distributed energy resources, and end customers in general, is the coordination of the interaction of smart grid stakeholders. The legal and regulatory conditions in many cases are flexible for business cases involving several stakeholders such as energy traders, energy service companies, operators of flexible load and generation, smart meter owners, etc. (even though market conditions in many cases do not provide the necessary incentives at the moment). In contrast to this the lack of clearly defined

interfaces of the relevant systems is a major blocker for the development of new smart grid-based services. If a company wants to offer smart grid-relevant services to other stakeholder it needs a common interface allowing to connect to potential customers and business partners.

Although to a great extend standards covering the system interfaces are available or in preparation, they do not immediately guarantee interoperability, due to choices that need to be made (profiling), and overlapping scope of different standards. In order to overcome this problem, we recommend that regulation is put in place which enforces the specification of the relevant system interfaces. Especially such interfaces that are controlled by regulation should be uniform at least within each Member State (as explained in R1, Section D national uniformity is considered a realistic short-term perspective compared to European-wide common system interfaces).

The set of interfaces and the basic requirements should be defined at European level, whereas the actual technical specifications could be developed at national level. Although a harmonised European framework would be desirable from the point of view of the common market, both the electricity grids and markets are currently quite diverse between Member States, and it might prove difficult and time-consuming to agree on a single solution for all of them.

In order to allow for full interoperability system interfaces should also be specified in a more extensive way than other communication: they need specifications regarding authentication, access permissions, and data models. They should be publicly and freely available, and they need rules for testing as well as for certification. Clearly defined system interfaces are essential for the development of smart grid and smart metering services in market competition. Too many different flavours or even different standards for one system interface would shatter the market into tiny fragments, not inviting any business cases. An extreme example would be each metering service provider defining its own interface or each manufacturer defining its own interface. For this reason, it should be aimed at having at least mandatory national standards, promising a market size suitable for successful business cases.

There is a tension area seen between market based evolution and obligatory standards. On the one hand, the market based approach provides initially most freedom of choice. Interoperability will be achieved after one or a few systems succeed over others. Even if this state is reached, it will take some time and stranded costs for the

Good practice 1: Smart Metering

Germany has issued a clear regulation for Smart Metering*, prescribing among others strong security and data protection measures, as well as the data format for message exchanges. The latter is based on the COSEM data model, defined in IEC 62056. The framework explicitly takes into account services beyond metering itself, such as remote load control, or data access for service providers other than the metering operator. Communication between meters and external parties must be routed through a Smart Meter Gateway (the Local Network Access Point), separating the customer's premises from the WAN. Furthermore, the Smart Meter Gateway provides interfaces for local data access and load control.

Inevitably, the required security level will lead to increased costs for the meter rollout, which is a great concern for many stakeholders.

*https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03109/index_htm.html (in German)

combed out. On the other hand, obligatory standards provide secured interoperability from the start but at the cost of strict regulation without choice and competition on the best solution. For this reason the approach of mandatory system interface specifications should be limited to system interfaces that are installed under regulation such as smart metering systems, interfaces of grid operators to other stakeholder and regulated control interfaces of DER units.

Smart metering is an example where a process was started similar to the one proposed here. The European Directive 2009/72/EC[1] demands Member States to implement measures for a Smart Meter rollout, provided a positive outcome of a cost-benefit analysis. System interfaces relevant for Smart Metering are 2a, 2b, 2c, in Fig. 1. Since the Directive does not require national regulators to specify the system interfaces, this has been left open by most national roll-out directives, and hence each grid operator or metering operator can specify their own solution. An exception is the German solution, which demands not only strong security and data protection measures, but also defines the communication methods (see box).

System interfaces

A possible list of system interfaces is as follows (excluding interfaces that are already well specified, like grid-grid communication), see also Figure 1:

1) Grid Operator – Local Controller
2) Metering interfaces:
    a. SMG – Local Controller
    b. SMG – Authorised External Entity
    c. Metering Operator – other Authorised External Entity
3) Authorised External Market Entity – Local Controller

SMG is the Smart Meter Gateway, which provides the Local Network Access Point (LNAP). A local controller could be a DER controller, a Customer Energy Management System (CEMS), a charging controller, or the like. The local controller may also be integrated into the Smart Meter Gateway.

Interface 1: Grid operator – Local controller

This is required to send control commands to the local controller in the case of grid instabilities (based on prior agreements), and to report status information to the grid operator.

An example could be feed-in management for DERs. In times of excessive generation from renewable generators, the grid operator may send a shut-down signal to connected generators (either to those obliged to shut down by law or connection requirements, or those with a dedicated contract). The specification of this interface is currently mostly left to the grid operator, which is a feasible approach on the one hand, but has some problematic effects for the DER operator, who is restricted in his or her choice of controller, to one that supports the interface defined by the grid operator.

[1] http://eur-lex.europa.eu/legal-content/EN/ALL/;ELX_SESSIONID=ktnLJ2rLKmwhGLH0N7zkDFzCyqt8ZFv1nLHB8J4kMBGjTJhm57nX!1835060013?uri=CELEX:32009L0072

Interface 2a: SMG – Local controller

This interface allows end users, and e.g. DER operators, to access meter data and use them for monitoring or control strategies.

Interface 2b: SMG – Authorised External Entity

Exchange of meter and tariff data between the gateway and an external party, like the metering operator.

Interface 2c: Metering operator – Authorised External Entity

An alternative to direct communication between SMG and external parties is the forwarding of meter data by the metering operator.

Interface 3: **Authorised External Market Entity – Local Controller**

This interface is relevant e.g. for virtual power plants and other energy services. Information exchanged includes incentives, control signals, status information, and the like. In general, this interface may not fall into the realm of regulation, but there may be special cases where it does, like market platforms for local energy services.

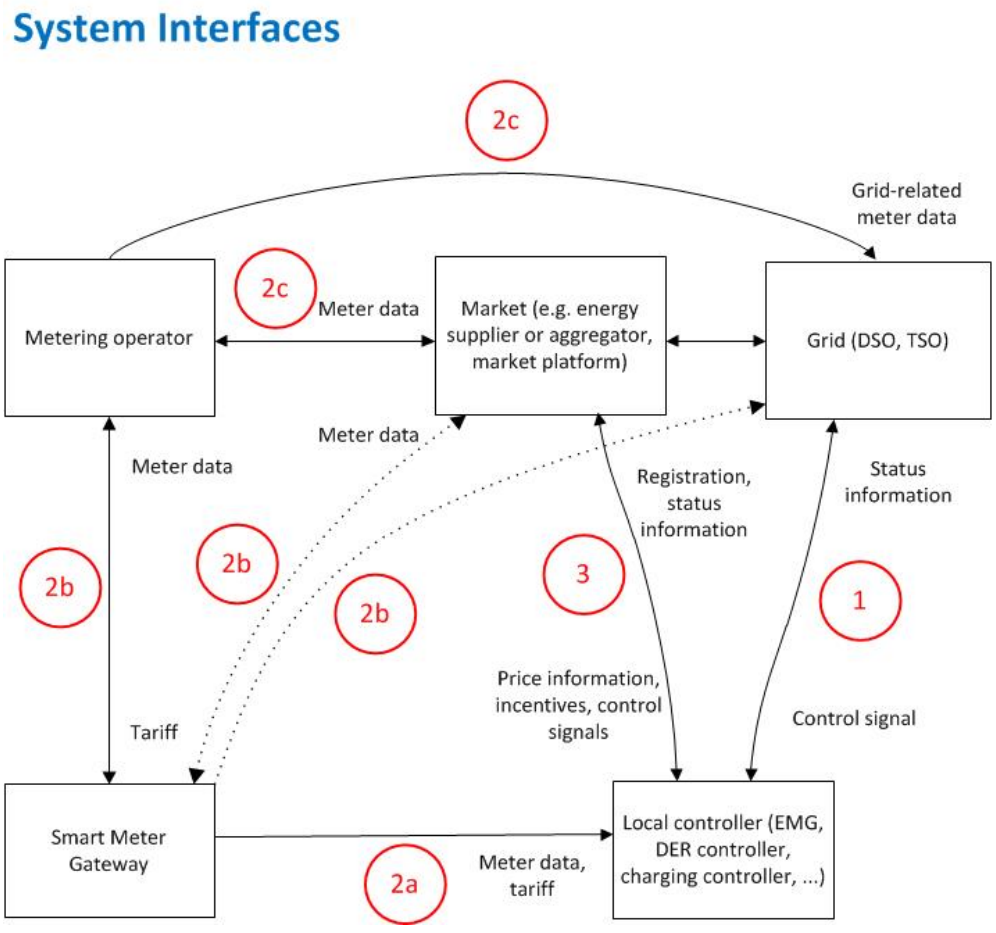


Figure 1: Proposed system interfaces

Impact

- Secured interoperability.
- Increased market competition due to standardised interfaces; commercial feasibility of innovative energy services; accelerated market development due to reduced connection costs.
- Reduced risk of vendor lock-in for grid operators, DER operators, etc.
- Increased end customer participation in energy markets; demand response implementations.
- Competition for the best communication solution cut-off or reduced.

Main impacted stakeholders

Regulators.

Also: Grid operators, DER operators, end customers, energy services providers.

Implementation

This recommendation is addressed to legislation first of all. They should aim to establish regulations suitable to ensure interoperability. The technical specifications should be based on International standards, and the development process may well include a cooperation between regulators and (national) Standardisation bodies, which could define national profiles (and extensions where required) of International standards.

Harmonised European specifications are desirable, and a process involving the definition of system interfaces and basic requirements at EU level could initiate the national legislatory processes. Cooperation of Member States should be encouraged.

Priority and Urgency

Many Smart Grid technologies have been extensively tested in field tests and demonstration projects, but products rolled out often either lack the required communication capabilities for full Smart Grid functionality, or rely on legacy or proprietary solutions. Some innovative business cases expected to play a role in the future electricity market are not feasible in current setting, partly due to the lack of system interface specifications. We believe that this is one of the major obstacles for Smart Grid implementation, and urge the regulators to take immediate action. A prioritisation of interfaces will have to be performed, and presumably the process will last several years. Therefore, we consider it a short- to medium-term objective (2015-2018).

R3 Prioritize interoperability test specifications for all Smart Grid standards

Addressed at Standardisation Bodies and Industry

Summary

Smart Grid operation, relying on the strong interaction of different infrastructures, domains, players, applications and functions, technologies, etc., requires interoperability between devices and systems for all application functions. Standard conformance is a pre-requisite for interoperability and is necessary, but not sufficient condition to guarantee the system interoperability. Specific interoperability tests are necessary, at least for the most critical functions and systems (Use Cases).

The importance of test procedures regarding interoperability, compliance and conformance has been highlighted e.g. in the report of the working group Interoperability of the SGCG (to be published). Their investigation also shows that today most standards contain no such testing specifications or only some relevant aspects/domains are covered. The specification of sufficient test procedures within the usual Standardisation process is quite difficult as this requires not only knowledge in the respective Standardisation domain, but also experience in the development of testing procedures, test coverage etc. The development of such procedures usually requires a consistent development process governed by a specialized institution and cannot be solely covered by a group of experts delegated by different companies. For this reason also financing of the development of such a testing specification which in many cases should be accompanied by testing machines or reference hardware is a typical task of a standard's user group or industry initiative that organises the process and carries out the testing of the test specification and setup. EU funded projects could also provide a suitable framework the development and validation of testing procedures for specific applications, in particular for standards that lack a dedicated users group.

The compliance to interoperability requirements through tests should be certified and a certification system relying on the availability of qualified testing infrastructures should be established.

Main Recommendation

1. Prioritize the development and adoption of interoperability test specifications to validate interoperability of components and systems for Smart Grid applications.
2. Develop a process to increase the involvement of testing and certification organisations in the Standardisation process, in particular regarding the development of test specifications.

Corollary Recommendations

- Identify and define critical Use Cases, where interoperability tests are most urgent. Whenever necessary for these critical situations, develop missing use cases.
- Regulatory actions could be necessary to share the costs of development and performance of interoperability tests among the stakeholders.

- Foster cooperation between players of the Smart Grid value chain (especially Energy and Communication operators) to develop smart grid solutions based on standardised approaches to enhance the interoperability of components and systems (e.g. user groups for specific standards).
- Support the coordinating activities of the SGCG concerning the identification of critical Use Cases and the development of methods and tools for the implementation of interoperability tests.
- The implementation of Interoperability tests requires the availability of qualified testing infrastructures, able to create the system validation framework, and agreed test procedures.
- Take advantage of EU funded projects to develop interoperability tests specifications.

Explanation

A) Interoperability Requirements

Interoperability represents the ability of system/sub-systems/intelligent devices to exchange information and use them in order to perform required functions. The risk of non-interoperability increases with the complexity of the system. This is especially true when considering the evolution of the energy system toward the Smart Grid paradigm, whose operation relies on the strong interaction of different infrastructures (the energy and the ICT one), different domains, players, applications and functions, technologies, etc. Moreover, the Smart Grid shall be interoperable with related infrastructures (e.g. the intelligent transport, smart cities, etc.) in order to sustain the development of the Energy market.

Interoperability not only concerns communication and energy operation aspects, but has a broader impact across related sectors: organisation, regulation, market, social. Standardisation plays a crucial role in achieving interoperability goals, provided that it may ensure total internal consistency, robustness and efficiency.

Standard conformance is a pre-requisite for interoperability and so it is necessary, but it is not a sufficient condition to guarantee the system interoperability: standards often cover a broad range of use cases, so that a specific profile needs to be developed for each implementation. Besides, standard implementation can vary due to national specifications (for example, the DLMS standard and the different companion specifications required by DSOs in different countries). As a consequence, a product conforming to a standard does not automatically ensure its correct operation when included in a complex system.

Therefore, in order to demonstrate the interoperability of any equipment/device integrated in the Smart Grid, specific interoperability tests are necessary. The Use Cases related to an application define the information exchange between systems at an abstract level. The mapping of this information on ICT standards, both at information and communication levels, defines a set of rules that should be checked through interoperability tests.

B) Interoperability Test Overview

Interoperability tests are "systemic", whilst standard conformance tests are "unit" tests. This means that performing interoperability tests requests the univocal definition of the system environment (the configuration to be reproduced) and conditions (the reference system state), as well as the definition and description of the specific case (Use Case).

Therefore, performing interoperability tests may be a highly complex and fruitful task.

To guarantee their repeatability and reproducibility, interoperability test methods have to be developed, agreed and standardised.

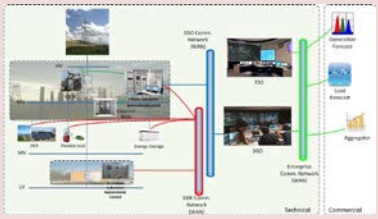
Of course, this implies an agreement on the rules for the interoperability performance of devices in the Smart Grid system.

C) Proposals for organization and financing

In the perspective of the Standardisation of the interoperability tests, the SG stakeholders have the task to clearly identify and define the Use Cases where the interoperability of a product/system has to be validated and work to include interoperability provisions into the related standard. The development of testing and certification specifications requires special knowledge not usually required by committee members. It should also be accompanied by the development of a reference implementation and the set-up of an initial testing environment, tasks that go far beyond the committee work of standards drafting. A possible solution to this could be that the committee in charge issues a mandate to a particular testing and certification organisation, or an industry initiative / user group to develop the specification. A voting could then be performed on the delivered draft. The question how to remunerate the service of the testing organisation remains to be solved. Possibly, the latter could then serve as a root certification institute that authorises other laboratories to certify compliant products. In some cases, the competitive advantage of being able to perform tests and certifications before their competitors may even be motivation enough for an organisation to invest in the development of a specification. But these are only suggestions; it is in the responsibility of the Standardisation Bodies to develop a suitable process, preferably in close collaboration with testing laboratories.

Good practice 2: Take advantage from EU funded projects to develop interoperability tests Use Cases and specifications.

A good reference is the Use Case of "Voltage Control in Medium Voltage Grid" developed within the project SmartC2Net



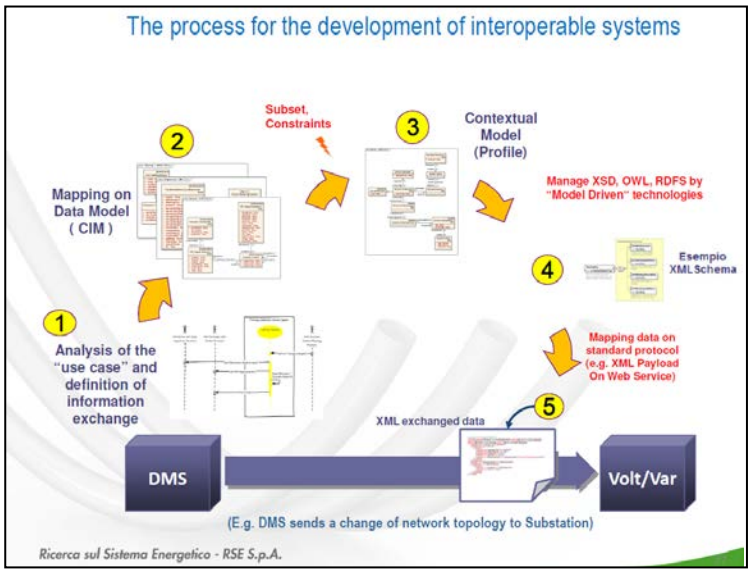
http://smartc2net.eu/SmartC2Net_UC_VoltageControl-Medium%20Voltage%20Grid.pdf

See also the EU-FP7 Project: COTEVOS – Concepts, capacities and Methods for Testing EV Systems and their Interoperability within the Smart Grids (www.cotevos.eu)

EU funded projects could be a suitable context to validate interoperability tests specifications. Good reference examples are, for instance, the projects SmartC2Net and Cotevos. They could possibly also target the actual development of specifications, ensuring the due consideration of interoperability aspects already since the concept phase (interoperability by-design).

Some stakeholders (e.g. manufacturers and system integrators) complain that requirements for Interoperability tests may affect the costs of equipment and the market penetration capacity. This aspect must be taken due account of when elaborating the related Standards. A specific Cost-Benefit Analysis should support the decisions. Efforts should be dedicated to select the Use Cases where the interoperability should be validated to tests and to limit the requirement to the most critical conditions. Furthermore, in certain cases it may be sensible that regulatory bodies foster specific actions so as to share the costs of interoperability tests among the stakeholders. For instance, manufacturers and system integrators could access specific funds or incentives for the certification of the interoperability tests. Suitable testing infrastructures could be supported to provide assistance to manufacturers and to carry out interoperability tests. Tests procedures should be optimised (e.g. automated) to the cost reduction extent.

D) Data models



Since a Smart Grid may incorporate many different types of physical networks, interoperability specifications should not restrict the choice of physical communication layer; instead, interoperability must be ensured mainly in the "upper" communication layers, like the data model. For the Smart Grid there are three relevant data models. The so-called Common Information Model (CIM) covers the "Operation", "Enterprise", and "Market" zones, whereas the other two reference data models covering "Process", "Field" and "Station" zones are IEC 61850 (for "Generation", "Transmission", "Distribution" and "DER" domains), and COSEM (for smart metering: "DER" and "Customer premises" domains). Harmonization of the three data models is paramount. The STARGRID survey has evidenced the strong interest of Smart Grid stakeholders and mainly of ICT and Telecommunication representatives to the works for the harmonisation and integration of different data models to cover the complete set of Smart Grid functionalities.

The concept of a profile, which specifies in a defined context which standards (parts) are used and how, represents a suitable tool to achieve interoperability between systems.

The concept of "Basic Application Profile (BAP)" (e.g. a profile for the interlock function) is aimed at this approach. Groups of BAPs provide functionality at higher level. Granularity of profiles and guidelines for the definition of BAPs and for their generation are deemed urgent matters of discussion. Apart from Standardisation, interoperability conditions may be supported by operation agreements inside the value chain: this is the objective of initiatives like ISGIS (Italian Smart Grid Industrial System).

Good practice 3: Foster agreements on standards adoption inside the value chain

With the objective to create a network of national operators able to develop smart grid solutions based on Standardisstandardised approaches, the "Italian Smart Grid Industry System" has been recently established in Italy.

Formed by Industry and research representatives, with the active participation of Standardisation bodies and with the support of the Economic Development Ministry and of the energy Authority, the network aims at ensuring a competitive advantage in the Italian industrial system and putting it in a position to offer to the market modular, integrated, interoperable, and rational applications.

http://www.rse-web.it/eventi/Smart-gridl-rsquoItalia-vuole-fare-Sistema.page

Expected Impact

The cost of executing interoperability tests might increase the costs of equipment and system providers. However, they may constitute a "quality label", leading to an "interoperability certification" of products, which could facilitate the procurement phases and the value for money of the validated products. In the end, this may reduce cost for technology integration and the interoperability validation is expected to ensure the security of the supply by the network operators, reduce their vendor-dependence, and is expected to lead to lower costs at the system level.

Main impacted stakeholders

Smart Grid stakeholders will only invest into fully interoperable systems. They have the Task to identify and define critical Use Cases for interoperability tests.

ICT providers and telecom operators should contribute to define the proper conditions (protocols and data exchange models) for the interoperability validation.

Equipment manufacturers and System integrators would mainly support the costs of requirements for interoperability tests and this will affect their competitiveness.

It is also worth considering that, in general, interoperability requirements are pertinent with the information security ones.

Interoperability tests validate step-by-step the Use Case: this allows, among the rest, validating early implementation of standardised technologies and providing feedbacks to Standardisation bodies for the validation of the standards themselves.

Interoperability tests require the availability of qualified testing infrastructures, able to reproduce the system validation environment, to perform the tests according with agreed procedures and quality system and to guarantee a transparent approach.

Implementation of the recommendations

The basis of the implementation of the interoperability tests is the definition of the Use cases referred to. This is especially a task of Smart Grids stakeholders in their specific context, as said, in cooperation with ICT and telecommunication operators.

This first step is already partially in progress within the activities of the SGCG. A first definition of generic high level Use Cases is already available[2].

Common efforts of Smart Grids stakeholders participating in the Standardisation committees should be addressed to select "interoperability critical" Use Cases and, for this latter, to further specify requirements coming to Interoperability Test Cases. The creation of a repository of such Interoperability Test Cases will ensure a common understanding and approach.

Standardisation Bodies, strongly supported by the concerned Industry, should mainly have in charge the preparation and maintenance of relevant standards in order to facilitate the implementation of the recommendations.

The direct participation of SMEs and sector Associations is strongly recommended, for sake of transparency and to supervise aspects like the cost-benefit issues.

Standardisation Bodies need to implement a suitable process for the development of testing and certification specifications, involving in particular the relevant laboratories.

Priority and Urgency

Interoperability, that is the pre-requisite for the implementation of the Smart Grid, is one of the highest ranked gaps identified in the STARGRID survey. Standardisation of a methodology for interoperability tests is therefore a priority.

Considering the timing of the evolution of the Smart Grid system, interoperability testing Standardisation is deemed a medium-term objective (2020).

[2] http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/xpert_group1_sustainable_processes.pdf

R4 Security and Privacy

Addressed at Policy Makers and Regulation Authorities (EU and national)

Summary

Smart Grid is intrinsically a system highly sensitive to information security problems. The overall operation of the electric/energy infrastructure, strictly relying on the interaction with communication infrastructures, exposes the entire system to risks of malicious attacks (physical and cyber). Moreover, the complexity of the entire system and the huge number of different players and deployed technologies (e.g. the monitoring network) dramatically increase the number of vulnerabilities that can be exploited. Traditional security solutions may be ineffective against aimed attacks to the Smart Grid operation and information system. A new scheme is necessary based on the anti-intrusion rules. Security is a global issue, requesting an overall approach to face new vulnerabilities and risks. Currently, a number of important Standardisation works on security are in progress at EU level, under the outlook of the SGIS (Smart Grid Information Security) experts group. The efforts to cover the gaps of Standardisation on security should be strongly supported and the coordination among the initiatives should be enforced. In general, the legal framework supporting security Standardisation is feeble across Europe, with negative peaks in some countries. There is no sufficient fostering by the utilities and the sensitivity of the end users is not developed too much. It is essentially a cultural issue. Policies at EU and country level should be developed and implemented to overcome these barriers. Furthermore, considering the coverage of the Smart Grid evolution the security/privacy/data protection law framework should be harmonized at EU level.

Main Recommendation

Develop a standards framework for security against physical and information attacks and data protection encompassing the requirements of Smart Grids with a coordinated and systemic approach.

Corollary Recommendations

- Stakeholders should clarify and agree the requirements on information security and data privacy. Cooperation of the operators of the involved networks is essential to this extent.
- Stakeholders should use standardised formats, language and models for the specification of requirements on security/privacy.
- Approach the security Standardisation through a security-by-design concept based on a thorough Use Case definition and associated risk analysis. Standardise the approach methodology.
- Take advantage of EU funded projects to develop security Use Cases and specifications.
- Coordinate Security and Interoperability analysis approaches.
- Develop a harmonised legal framework across Europe, ensuring security of the energy system and the protection of data.

- Collect the minimum amount of personal information needed without compromising the quality of the provided services. Anonymize individual identity.
- Transparency: inform the customer about the collection, use and disclosure of the personal details and accept his preferences. Always obtain the express consent before disclosing personal information to third parties. Allow consumer to access his personal data and make corrections.
- Enhance awareness and provide clear instructions on information privacy and protection to utilities and consumers using Smart Grid services. Policies at EU and country level should be implemented to overcome cultural barriers to privacy and data protection.

Explanation

Smart Grid is intrinsically a system highly sensitive to information security problems. The overall operation of the electric/energy infrastructure, strictly relying on the interaction with communication infrastructures (in many cases involving public networks), exposes the entire system to risks of malicious attacks (physical and cyber). Moreover, the required availability, the complexity of the entire system and the huge number of different players and deployed technologies (e.g. the monitoring network) dramatically increase the number of vulnerabilities that can be exploited. Security must be considered for the operation of the Smart Grid and also for the user acceptance (for example, data privacy of smart meters as detected during STARGRID assessment).

Communications networks for the Smart Grid

Depending on the Smart Grid target applications, different types of communication networks and also collections of communication networks using different transmission technologies may be selected in order to transmit and deliver Smart Grid data. The following network types could be defined for the Smart Grids

a) Subscriber Access Network
b) Neighborhood network
c) Field Area Network
d) Low-end intra-substation network
e) Intra-substation network
f) Inter substation network
g) Intra-Control Centre / Intra-Data Centre network
h) Enterprise Network
i) Balancing Network
j) Interchange network
k) Trans-Regional / Trans-National network
l) Wide and Metropolitan Area network
m) Industrial Fieldbus Area Network

CEN-CENELEC-ETSI Smart Grid Coordination Group
First Set of Standards
http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/xpert_group1_first_set_of_standards.pdf

The same issues directly impact the operational security. This latter is not specifically addressed by this recommendation: the topic is treated in the dedicated ENTSO-E Network Code "aiming at setting out clear and objective requirements for TSOs, DSOs and significant grid users in order to contribute to non-discrimination, effective competition and the efficient functioning of the Internal Electricity Market and to ensure system security"[3].

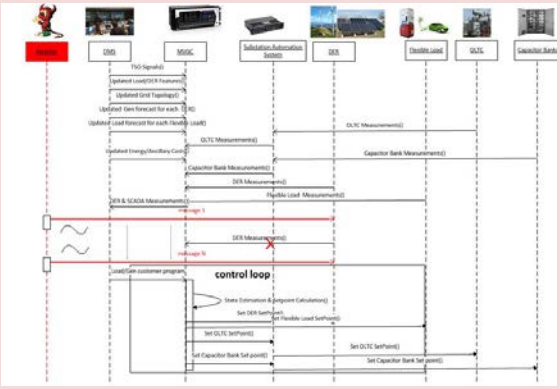
[3] https://www.entsoe.eu/fileadmin/user_upload/_library/resources/OS_NC/130924-AS-NC_OS_2nd_Edition_final.pdf

However, the correlation of information security and operational security is obvious. It is enough to consider, in the best case, the latency effects that may be caused by the slowing down of the communication process because of the information security needs. In general, operational security requires an accurate, timely and adequate exchange of relevant data and information: no barriers between the different actors involved in should exist, especially those caused by malicious actions.

Along with this, consumer privacy must not be sacrificed when exploiting the benefits of the Smart Grid. Smart meters and smart appliances will provoke a data explosion of private details of daily life (consumer behaviour and characteristics) and it is not clear who will have access to this information in addition to the utility without consent of the customer.

Good practice 4: Take advantage from EU funded projects to develop security Use Cases and specifications.

The project SoES (www.soes-project.eu) has developed reference Security analysis for fundamental Use Cases: "Voltage Control in Medium Voltage Grid"; "Photovoltaic Storage and Generation"; "Load reduction programs" and "Smart Meter Configuration ".



No consensus exists on privacy implications of the Smart Grid, and there is a lack of standards and procedures to deal with this issue. Comprehensive definitions of personally identifiable information and execution of privacy impact assessments (PIAs) become crucial in the utility industry.

Traditional security solutions may be ineffective against aimed attacks to the Smart Grid operation and information system. A new scheme is necessary based on the anti-intrusion rules. It has been suggested that the same approach as for critical infrastructures should be adopted and tailored to the energy conversion chain, including among the rest: asset identification; security control; perimeters security; physical security; personnel & training; recovery management.

Security is a global issue, requesting an overall approach to face new vulnerabilities and risks (e.g. use of public network instead of private and segregated one; physical security of smart meters).

Expected Impact

To face security issues according to such an approach is difficult and expensive to implement, due to the complexity of the problem and the huge number of players and technologies involved. In fact, each node (player/technology) may introduce vulnerabilities in the system.

The approach requires the thorough definition of the Use Cases of security, especially for the distribution grid. This is a very demanding job, needing investigations, which may be carried out through specific R&D works. Functional Use Cases defined according to the security requirements are still missing, although they are being developed within some EU funded projects (e.g. SoES "Security of Energy Systems" http://www.soes-project.eu). The elaboration of the use cases done by the SGCG-FSS maps connections, protocols and standards on the SGAM, but does not enter into details

of the specification of the security risks and requirements. EU funded projects may be the ideal context to develop an effective security framework for a systemic approach, produce tools and guidelines, as well as identify best practices.

A risk analysis applied to each Use Case should be done, to identify threats and vulnerabilities and propose countermeasures. The risk analysis associated with the Use Case, combined, whenever necessary, with a related cost-benefit assessment would lead to the selection of the most critical Use Cases.

Main impacted stakeholders

Network operators (energy and communication) are responsible for the security (physical and information) of the operated infrastructures and have to univocally define the requirements for their protection. They are also concerned with the associated costs.

End Users are mainly impacted by privacy and data protection issues.

Utilities are concerned with the costs (not only for security, but, in general, of Smart Grid implementation) and different attitudes against the issue may rise country-by-country, depending on their business dimensions and on the country regulations. In this line, the results of the EU FP7 project ESCORTS (European Network for the Security of Control and Real Time Systems, www.escortsproject.eu), which assessed the vulnerabilities of computer networks and SCADA architectures in the energy domain, should be considered.

Implementation of the recommendations

An approach similar to the one proposed for the Standardisation of an interoperability testing methodology (see R3 Prioritize interoperability test specifications for all Smart Grid standards) could be adopted also for the Security issue, at least for the selection and definition of the related Use Cases, that have several aspects in common: definition of the actors and their interfaces; type of information exchanged; data models and protocols used, etc. On the other hand, the solution of interoperability issues in the different domains is a pre-requisite of all aspects of the security, e.g. Standardisation/harmonisation of protocols and unified information models.

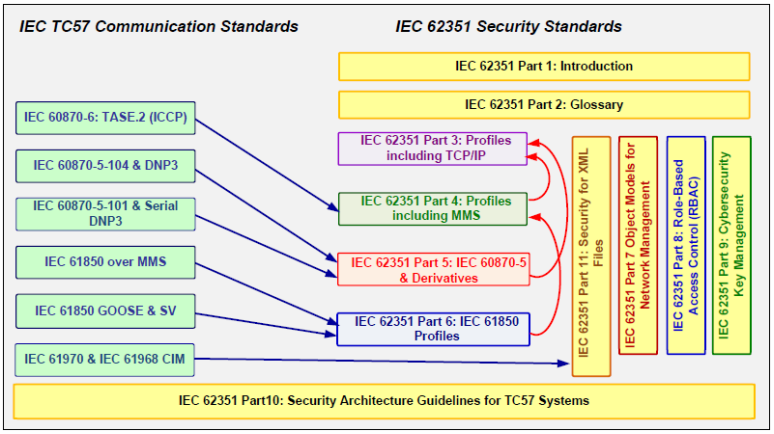
Requirements on security/privacy are not clear and agreed enough and this is one of the reasons why Use Cases for security of Smart Grids functionalities are still poorly defined. Standards for expressing such requirements are needed as well as cooperation among operators of electric and telecommunication networks in reaching common understandings based on those standards.

Currently, a number of important Standardisation works on security are in progress at EU level, under the outlook of the SGIS (Smart Grid Information Security) experts working group under the European Commission Smart Grid Mandate M/490 to European Standardisation Organizations (ESOs).

ISO/IEC is working on the series 27000, mostly related to governance aspects (risk assessment, industrial processes, policies) but touching also some technical aspects. Of especial relevance is ISO/IEC TR 27019 (Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry).

At the level of IEC committees, IEC TC65 is working on industrial networks (ref IEC 62443,-i.e. ISA 99-) information security in industrial automation, and IEC TC57 WG15 is specifically related to Power Systems (ref: IEC 62351).

Since some aspects are in common, there is a clear request for harmonization. Collaboration agreements between committees are in place, normally formalized in IEC as "liaison actions".



The works in progress on IEC 62351 series have especially high relevance and reflect the complexity of a critical subject like security in the Smart Grid. IEC 62351 specifies the end-to-end security of the IEC/TR 62357-1 reference architecture (communication infrastructure of energy management systems). It covers most of the IEC TC57 communication protocols but does not cover information security management issues (included in other standards like IEC 62443 and ISO/IEC 27000 series).

In practice, specific Standardisation of smart grid security does not exist yet. At present, Parts 7 and 8 of IEC 62351 are not standards, yet, but only Technical Reports. Different Parts of the standard series have to be developed iteratively as linked to each other. Aspects like roles and certification are not yet standardised for Smart Grids, although already well developed in other contexts. Part 7 is anyhow important, because it refers to the monitoring, which allows investigating new threats not yet covered.

The IEC 62351 standard assigns a great significance to the certification process, which is important indeed. However, certification it is not enough per se: security should be built since the Smart Grid conceptualisation and design according with the "security-by-design concept". In the USA, Canada and part of Mexico, the NERC CIP standards family (North American Electric Reliability Corporation – Critical Infrastructure Protection programme) is mandatory for the operation of the grid and generating plants. The NERC CIP parts are certified by the Federal Energy Regulatory Commission to provide a cyber-security framework: identification of the criticalities and vulnerabilities of the network assets, personnel training, electronic security perimeter, physical security, systems security management, incident reporting, recovery plans, etc.

In addition to the already mentioned initiative of ENTSO-e, also ENISA's (http://www.enisa.europa.eu: European Union Agency for Network and Information Security) works are important, related in general to security and resilience of the critical infrastructures, mainly Power and Transport.

Among the conclusions of the mentioned ESCORTS project, there was emphasized the need to increase awareness of potential cyber-attacks, and to encourage best practices jointly between

manufacturers and end users. ESCORTS also recommended to reduce the divergence between current Standardisation efforts on process control and power system control, and to develop test platforms for cyber-security assessment and testing.

The efforts to cover the gaps of Standardisation on security in Smart Grids should be strongly supported and the coordination among European and national initiatives should be enforced.

The role of SGIS, to make gaps analysis and provide guidance and recommendations, is deemed essential. The use of the SGIS Framework (formerly known as "SGIS Toolbox") is highly recommended to perform risk assessments. It can also be used to guide through the election and implementation of cyber security measures for the different Use Cases.

Besides, Smart Grid security standards should include the adequate security metrics to allow the quantification of the implemented security measures. These metrics should be continuously monitored to support the risk management and decision taking.

In general, the legal framework supporting security Standardisation is feeble across Europe, with negative peaks in some countries. There is no sufficient fostering by the utilities and the sensitivity of the end users is not developed enough. It is essentially a cultural issue. Policies at EU and country level should be developed and implemented to overcome these barriers. Furthermore, considering the coverage of the Smart Grid evolution the security/privacy/data protection law framework should be harmonised at EU level.

Consumers/customers data protection is the pre-requisite for their participation in the business and the realisation of forecast benefits. Therefore, a wider sensitivity on data protection and privacy issues should be strongly fostered at EU level. At present, there are big differences country-by-country. Legal provisions on data protection in ICT technologies are not yet adequate/harmonised in EU countries. Standards for use of sensible energy data are still missing in EU, in spite of the Commission 2012/148 recommendation. It is expected that the upcoming European Commission data protection regulation will mitigate this situation (GDPR, "General Data Protection Regulation") when applied to the Smart Grid ecosystem.

Privacy protection measures must be embedded in the smart grid design ("privacy by design" and "privacy by default") to appropriately manage the personal information held by involved stakeholders. Consumers must have the control of their electricity consumption and their private information to generate needed confidence for the active participation in the Smart Grid (for example, in demand response programmes).

Mature and emerging privacy protection technologies must be adapted and applied to Smart Grid Use Cases requiring personal information (mainly in smart metering, but in the near future also smart appliances and electric vehicles). From this point, the transfer to Standardisation of the validated mechanisms complying with the relevant requirements should be accomplished.

SGIS is working on the definition of the framework for privacy and data protection, but we are still far from any Standardisation initiative, which is not, of course, within the direct duty of the security experts group.

Priority and Urgency

Security in Smart Grids is one of the highest ranked gaps identified in the STARGRID survey. Issuing the Standardisation framework for security is therefore a priority.

Considering the timing of the evolution of the Smart Grid system, and the complexity of the topic Smart Grid security Standardisation is deemed a medium-term objective (2020).

R5 Enlarge participation to the Standardisation process

Addressed at Standardisation Bodies

Summary

Main Recommendation

Implement mechanisms and tools ensuring transparency and the largest participation in the Standardisation process of all stakeholders' representatives, especially SMEs and end users. Enhance the role and foster the participation of sector associations.

Corollary Recommendations

- Simplify the access to standards and related metadata by providing publicly available information through a user-friendly online platform.
- Enable harmonisation of the Standardisation process through a better coordination at European and national levels.
- Enhance visibility of working documents and the participation of stakeholders in the Standardisation process by enabling public consultations and including Standardisation activities in publicly funded projects.
- Increase the participation of sector associations and SMEs in the Standardisation process.
- Cooperation frameworks among Standardisation Bodies, like SGCG, SMCG, eMCG, should be maintained and supported beyond the end of the respective Mandates.
- Also cooperation with industry initiatives performing pre-Standardisation activities and developing own specifications on certain smart grid aspects should be fostered.
- Foster pre-normative actions in EU-funded projects.
- Promote the Smart Grid Architecture Model as the central classification scheme for Smart Grid standards.

Basis for the recommendations

A) Dissemination

European Standardisation Organisations (ESOs: CEN, CENELEC and ETSI), as well as the International Standardisation Organisations (for instance, IEC and ISO) provide a lot of information in their websites about Standardisation work, listing publications and projects for all technical committees and subcommittees. The national "mirror" committees to the European/International technical committees are expected to participate to the Standardisation process, to ensure the formulation of coherent national positions through directly involvement of all categories of stakeholders. Organisations represented in national committees (known as members of technical committees) are expected to liaise closely with their nominated representatives so that their interests are pursued effectively.

National Standards Bodies (NSBs), as members of ESOs and International Standardisation Organisations, are expected to have in place a suitable mechanism to disseminate information on the work program of their national "mirror" technical committees (including at least the titles of the projects of national, European and international standards at the public consultation stage), for general public review. This approach shall ensure that the standards reflect the opinion of most of their users. However, for many stakeholders, the Standardisation process is currently not easily accessible, and related activities are not easy to follow up due to the limited communication channels and related information access. Increased dissemination activities, such as the provision of online information (see for instance boxes "Good practice 5 & 7"), regular newsletters and open workshops, could enhance stakeholders' involvement in the process and increase the outreach of Standardisation.

Good practice 5: DIN drafts library

The German standardisation organisation DIN offers free access to draft standards via its online standardisation library (https://www.entwuerfe.normenbibliothek.de/; in German). All drafts are visible during their public enquiry stage. This enables a simple access to drafts and the possibility to comment for stakeholders who could not participate in the committee itself. A notification can be setup for particular standard series.

In order to decide on whether a Standardisation project is relevant to them, stakeholders could greatly benefit from user-friendly online platforms to find relevant information about the reasons of why a new project has been started and the expected outcome, for instance what kind of changes are foreseen for the revision of a standard. Such information is important both from the point of view of standards implementation and participation in the process, but currently does not seem to be readily available outside the respective committees. A short summary of the motivation to launch a new work item and, in the case of a revision, the expected major changes with respective to the current version could be included on the web page.

Good practice 6: IEC Smart Grid Standards Map

The mapping tool of the IEC provides a user-friendly graphical overview on standards related to the Smart Grid, including also non-IEC standards:
http://smartgridstandardsmap.com

Furthermore, it allows to search for standards applicable to particular components of the grid (graphically and text-based).

The STARGRID consortium is likewise creating a database on Smart Grid standards. It lacks the graphical representation of the IEC tool, but aims to allow for more fine-grained selection of standards, based on additional categories like publication date, issuing organisation, etc. Publication is targeted for end of 2014.

Already a central access to the database of current projects, besides access via the web page of individual committees, could improve the visibility of Standardisation projects. An elegant solution could be the inclusion of a current projects list in an online library, such as the one described in the box "Good practice 5", which also enables public access to drafts in the enquiry stage.

The STARGRID survey analysis[4] outcome shows that the industry representatives have a rather scarce awareness of the Standardisation initiatives

[4] STARGRID: "Smart Grid Industry Initiatives Documentation Map" – 2014 (http://stargrid.eu/downloads/2013/07/STARGRID_Industry_Initiatives_Documentation_Map_v1.0.pdf)

in progress, although they attribute high relevance to the discussions on specific problems within the Standardisation Bodies and other initiatives promoters. This evidence should be taken into due consideration by the concerned institutions as it indicates lack of information and perhaps poor participation of stakeholders (especially SMEs).

B) Cooperation frameworks

Cooperation among Standardisation Bodies is essential for the harmonic development of the Standardisation framework intended to a multidisciplinary system like the Smart Grid one. Frameworks like SGCG, SMCG, eMCG should be maintained and supported beyond the end of the respective Mandates, and the system architecture(s) developed by these groups should be promoted.

The concept of the "Committee System" (similar to the legislation development by the European Union Committee System) should be fostered for the supervision of different technical committees' work. The coordination of the different actions among different players is a matter of regulation (which may fix roles and priority) and of Standardisation (which fixthe nature of the action and the way to carry it out). This should also include industry initiatives active in smart grid Standardisation via mechanisms that should be developed together by Standardisation bodies and these initiatives. Industry alliances are often more agile for developing Standardised specifications and this mechanism can be an efficient route towards the formulation of a final standard.

Good practice 7: ISGIS

An example of good practice is the ISGIS: Italian Smart Grid Industry System*, whose aims are:

- to agree operative solutions within the Italian Smart Grid value chain;
- to disseminate Standardisstandardised architectures for Smart Grids
- to promote the participation of Italian SMEs in the Standardisstandardised design, giving them the opportunity to offer in the overall EU market interoperable solutions.

_____

*http://www.solarexpo.com/files/convegni/convegni-e-seminari/2014/ISGIS_Italian%20Smart%20Grid%20In

Generally, Standardisation Bodies have an excellent overview of the work within their own technical areas; however, they are sometimes not aware of the developments of other technical areas. Therefore, the knowledge should be made publicly available from all sides.

C) Contributions from publicly funded projects

Another option for involving more stakeholders in the Standardisation process is to include Standardisation in publicly funded projects. We therefore support the CEN/CENELEC recommendation[5] of including specific Standardisation Sessions in the structure of the publicly funded projects. Recommendation to this task should be included in the H2020 and other research/innovation work programs. It is a fact that "Standardisation can help bridge the gap

[5] CEN/CENELEC: "Integrating Standards in your Horizon 2020 project" – 2014 (http://www.cencenelec.eu/news/publications/Publications/Standards_Horizon2020.pdf)

between research and market, by enabling the fast and easy transfer of research results to the European and International market".

Innovation projects constitute the ideal environment for the development, validation and assessment of new standards. Benefiting from the involvement of the whole value chain, innovation projects ensure development beyond the state of the art and share and promote the project outcomes among the stakeholders.

Good practice 8: EU projects

Among the EC funded projects, the development of the Voltage Control Use Case within the activities of FP7 project SmartC2Net http://smartc2net.eu/ is a good example.
Other examples to be mentioned are Green e-Motion (www.greenemotion-project.eu) and Grid4EU (www.grid4eu.eu).

The publicly funded environment would guarantee standards applicability related to different technologies, thus contributing to a Standardisation framework, which is directly in line with the technological developments.

Publicly funded projects may complement the necessary resources allocated for the implementation and validation of the reference use cases to be included in standards.

The inclusion of Standardisation in innovation projects would represent an effective way to ensure the involvement of SMEs in the process and to increase their competitiveness on the market.

Expected Impact

- Bringing together ideas and experience in products, materials, processes or services of companies, academic experts, researchers, SMEs, consumers and regulators will lead to higher quality standards.
- Involving all relevant parties will lead to high acceptability of standards.
- Involving SMEs and end-users will ensure consensus in Standardisation activities.
- Involving all affected stakeholders in the development of standards will lead to a better applicability of the latter.
- Introducing standards development into innovation projects would represent an effective way to involve SMEs in the process and to increase their competitiveness on the market.
- Introducing standards development into innovation projects will also ensure development beyond the state of the art and sharing and promoting project outcomes among stakeholders.

Main impacted stakeholders

Standardisation Bodies are, of course, the major impacted actors of the recommendation.

However Policy Makers (EC and national governments) and national authorities have the responsibility to foster the harmonized and transparent Standardisstandardisation process

Users are impacted/affected by the recommendation as future standards will consider their needs.

Implementation of the recommendations

The implementation of guidelines for stakeholders to be involved in Standardisation must be implemented by the Standardisation Bodies. Funding agencies should promote Standardisation contributions in innovation projects.

R6 Harmonise the Regulation and Standardisation framework for DER interconnection rules

Addressed at Policy makers, Regulation Authorities and Standardisation Bodies

Summary

STARGRID fosters the coherent harmonization of the Regulation/Standardisation framework ensuring effective, transparent and economically fair integration of DERs in the electric grid. The massive penetration of DERs into the grid requires effective regulation to avoid risks for the stability and security of the electric system. In some countries the availability of a coherent regulation/Standardisation framework to manage the related problems is urgent. At EU level, on the regulation front, ENTSO-E is working on the set Network Codes (NC), some of which are currently at the comitology stage. In parallel, on the Standardisation front, CENELEC has upgraded standards and technical specifications that receive the NC provisions on DERs integration with the aim of becoming reference for national implementations. In the meantime, national regulators, network operators and Standardisation Bodies are elaborating the local framework. This work, developed in parallel and to some extent with independent views, may generate inconsistencies in the provisions and country-by-country discrepancies without a coherent and harmonized approach. Stakeholders of DER integration, mainly DER producers and system integrators and designers, warn for possible impacts on costs, competitiveness, effectiveness of integration procedures and transparency. A strong coordination at national and European levels (and between the levels) of the activities of the different committees working on the Standardisation of Smart grid is an urgent need to avoid overlapping and confusion.

Main Recommendation

Foster the coherent harmonisation of the Regulations/Standards framework ensuring effective, transparent and economically fair integration of DER in Smart Grids.

Corollary Recommendations

- Tendency to national Standardisation before consolidating the EU interconnection rules may negatively impact the industry competitiveness.
- The use of European standards will be crucial in providing guidance for a progressive alignment of the national legal frameworks avoiding product variance and facilitating further deployment of DER.
- The level of requirements should be proportioned to the power of the equipment and some thresholds to their implementation should be fixed.
- Upgrade the Standardisation process so as to allow a more deep and extended consultation of the involved stakeholders and to guarantee transparency and non-discriminatory conditions, against unilateral and non-motivated decisions driven by more influent stakeholders.

- A mutual acknowledgment system for conformance testing would promote competitiveness of industry and enhance the quality of products.

Explanation

The massive penetration of DERs into the grid, especially from non-programmable energy sources, is increasingly posing challenges regarding stability and security of the electric networks, which require effective control and management rules. This fact is well acknowledged, in general, by all stakeholders (mainly Regulation Authorities, Network operators; DER operators and producers) and there is as well an increasing interest of the public on the matter.

ACER, under solicitation of EC, has entrusted ENTSO-E for the issuing of regulations at EU level, ruling the connection of generators to the grid. This led, in March 2013, to the delivery of the ENTSO-E RfG Network Code, approved by the ACER, and currently in the comitology phase, before becoming part, as EU regulation, of the EU laws body. From the final entry into force of the Code, prevailing over any local regulations, a transition period of three years will allow the national implementation processes to adequate their national codes accordingly. With the aim of giving guidance for national implementation of the RfG NC, ENTSO-E has also issued a dedicated implementation guideline (Oct 2013).

In the meantime, at EU level, Standardisation organisations have worked to produce technical standards (e.g. EN 50438:2013 “Requirements for micro-generating plants to be connected in parallel with public low-voltage distribution networks”) and technical specifications (CLC/FprTS 50549 “Requirements for generating plants to be connected in parallel with distribution networks - Part 1: Connection to a LV distribution network and above 16A; Part 2: Connection to a MV distribution network”, both currently at the approval stage) receiving the provisions of the code, with the objective of constituting reference, at national implementation, for further specifications of values and ranges of non-exhaustive requirements contained in the code itself.

At national level, in parallel, a number of initiatives are in progress with the aim of providing information or parameters additional to the ones provided by the RfG NC and issued by the relevant Network Operators or the relevant TSO. In the meantime, national standards provide technical provisions specifying, for the local area, requirements for the connection of generators to the grid.

For instance, in Italy, already in 2012, i.e. largely before the final approval of the mentioned RfG code, the relevant TSO – TERNA - has produced the so-called Allegato 70: “Technical regulation of system requirements for distributed generation”, whilst the national Standardisation Body issued the standards CEI 0-16:2012 and CEI 0-21:2012, dealing with the connection of generators respectively to the MV and LV networks. As a cascade effect, the Italian Distribution Network Operator imposed to the energy producers connected to the grid mandatory connection/disconnection rules and thresholds, with an urging span time for the implementation.

These running initiatives clearly reflect the hurry to pose a quick remedy to the dramatic penetration of the energy resources and to the connected potential stability risks for the entire energy system.

On the contrary, in some countries, national codes are still missing and therefore no local standards have been produced yet.

Expected Impact

Harmonisation and coordination of Regulations/Standardisation initiatives will solve some inner difficulties of the impacted stakeholders and hampers to the implementation of the initiatives themselves.

There is a certain concern from stakeholders, mainly generator producers, about a number of issues, which could raise from a non-sufficiently harmonised Regulations/Standards framework at EU level concerning the integration of DER.

The tendency to implement national regulation before consolidating the EU interconnection rules created country-by-country discrepancies, which may impact the industry competitiveness.

New versions, variants, explanation guidelines following one another may generate confusion as well, even if they are justified by the need of alignments made necessary to remove inconsistencies of documents with delivering time gaps, as already seen. For instance, comments on the version of FprTS 50549 1-2 submitted for final approval put in evidence important discrepancies: requirements not compatible with current technologies; requirements beyond current standard values and beyond ENTSO-E RfG current and future; requirements unjustified (not supported by a CBA, deemed necessary); operations not required leading to oversize components; missing compliance procedures and security aspects that may hamper the use of some standard elements.

At the level of regulations, rigid provisions can be accepted, provided that they may guarantee transparency and non-discriminatory conditions, against unilateral and non-motivated decisions driven by more influent stakeholders.

Lack of harmonisation may also cause higher costs for some stakeholder's categories. It is a fact that the RfG code does not imply the full harmonisation of the rules across EU, and important country-by-country differences may still be. Of course, as explicitly mentioned by the RfG implementation guidelines, characteristics of networks and topologies may vary across Europe, causing different inertia in the system. However, other less urgent aspects may impact. Some technical capabilities set in the Network Codes can have a general negative impact on DER deployment as they can lead to increased equipment costs and to lengthier connection procedures. Just as an example, small generators (< 1 kW) are potentially covered by the RfG, but in Italy they are not considered in the connection standards. This fact may result in oversized solutions covering the requirements of different countries and therefore in higher costs.

Some stakeholders suggest that the level of requirements should be proportioned to the power of the equipment and some thresholds to their implementation should be fixed. Moreover, coherently with an EU harmonisation policy, compliance procedures should be defined with a European Standardisation approach, in order to avoid additional burden especially with low-size generators (third party product certificates should be allowed). A mutual acknowledgment system for conformance testing is needed, such as certification got in one country could be extended to other

countries; this would reduce costs and promote competitiveness of industry and enhance the quality of products.

Concerns could come to manufacturers and DER operators for existing equipment in the case retrofitting will be necessary for their integration in the grid according with the new rules. A cost analysis should before demonstrate the real benefits. However, this could not be a big problem, requesting, in most cases, just adaptation of the equipment governing software. In case prescribed capabilities are not technically implementable in a short time period, the NC may give rise to delays in the erection of DERs.

The survey of STARGRID with the stakeholders and the analysis of specific standards, somehow related with integration issues, evidenced other aspects, more tied to the consistency of the documents with the real application conditions, but in a way also to be considered in a harmonisation process. Just to mention a case, compliance tests have high relevance in the RfG code. It happens that some functional test specifications are not clear or detailed enough in the corresponding standards and this may generate incongruent provisions for conformance tests with respect to the laboratory capacity. Designers and laboratory operators are the players mostly concerned with this aspect.

Implementation of the recommendations

Harmonisation of the standards framework in the case of Smart Grid requests a large sharing of and agreement on the options, considering the complexity of the system itself and of the stakeholders involved, often with conflicting interests. This could lead to consider the upgrading of the Standardisation process, with modifications that allow a stricter and more frequent consultation of the stakeholders.

Main impacted stakeholders

Network (Transmission and Distribution) Operators are responsible of ensuring the security and the quality of the energy supply.

DER operators need clear integration rules supporting their business in a transparent way.

DER manufacturers and system integrators are concerned with the potentially higher costs and procurement hampers caused by disharmonic rules and country-by-country different approaches.

Designers and urge well-defined and coherent technical specifications.

For instance, Industry sector Associations should have an essential role in supporting the conformance of provision requirements with the product specifications and the certification capacity.

Although considering the above reserves, there is, in general, the need of speeding up the completion of the standards framework, both at EU and national level. For instance, monitoring the state of the system is a pre-requisite for the management of the DER integration and is becoming more and more complex. Difficulties are already at MV level, but will come to an explosion when the monitoring needs will be extended to the LV (in Italy there are about 500.000 secondary stations!): physical location of the instruments and their connection to the communication infrastructure is still a problem to be faced with impact on standards.

The use of European standards will be crucial in providing guidance for a progressive alignment of the national legal frameworks avoiding product variance and facilitating further deployment of DER by a better use/understanding of DER capabilities. Some stakeholders suggest that the evolution of 50549 1-2 Technical Specifications towards full EU standards should be fostered and sped up as it will trigger harmonisation and will facilitate further DG deployment. This could be of great benefit especially for designers and constructors.

The concept of System Committees, which is growing e.g. in IEC (http://www.iec.ch/about/activities/systemswork.htm), aimed at elaborating upper level models (i.e. definition of system architectures) is deemed a good basis of an effective coordination of Standardisation works in complex systems like Smart Grid.

The activity of the Smart Grid Coordination Group is fully in line with the harmonisation and coordination objectives.

Priority and Urgency

The harmonisation and coordination at National and European levels (and between the levels) of the Regulations/Standards framework for DER integration is an urgent need to avoid overlapping and confusion.

Considering the timing of the evolution of the framework, implementation and reinforcement of harmonisation procedures should be established as a short-term objective (2015).