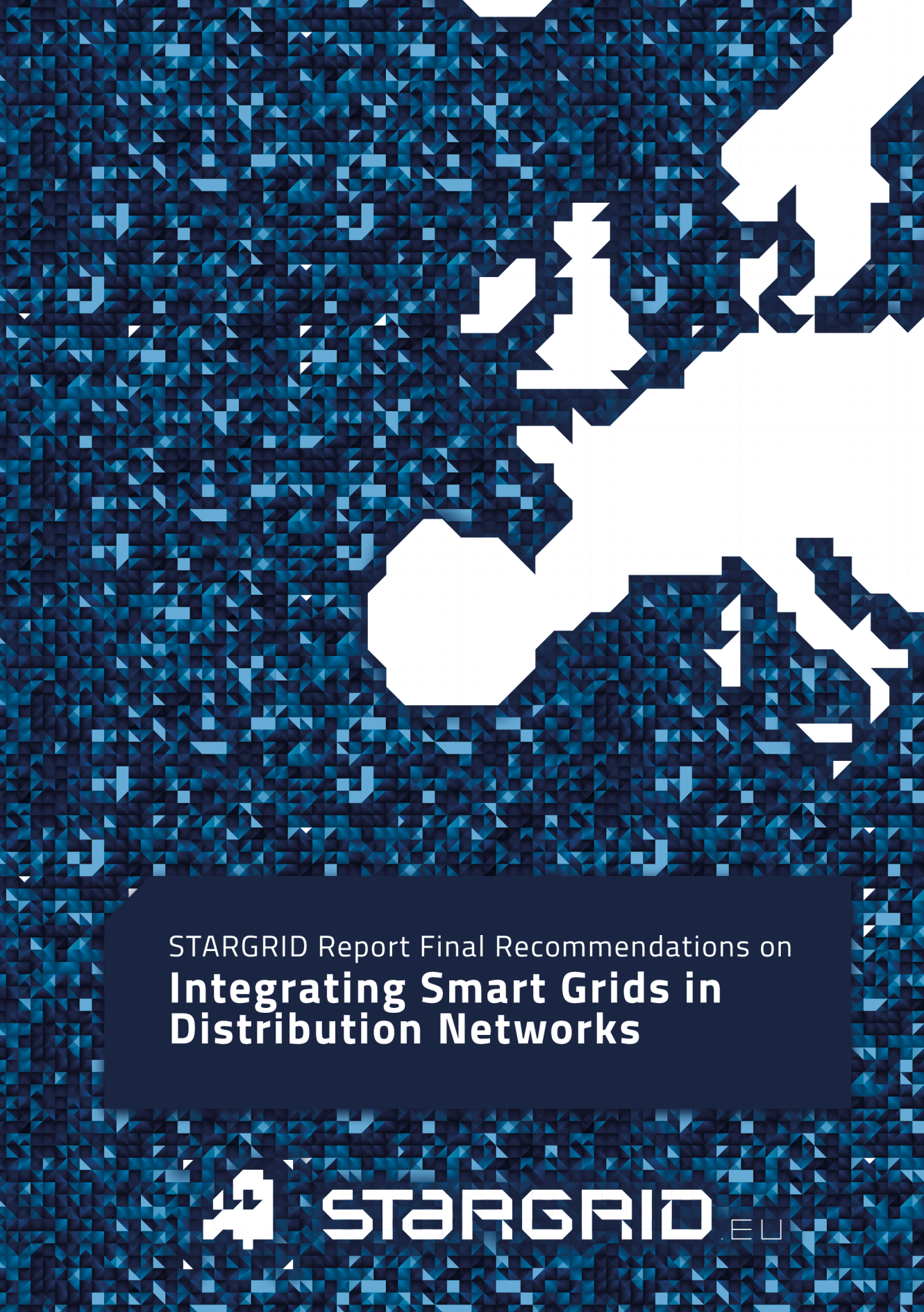

STARGRID Report Final Recommendations on

Integrating Smart Grids in Distribution Networks

STARGRID.EU

STARGRID

FP7 – 318782

RECOMMENDATIONS FOR SMARTER DISTRIBUTION NETWORKS

Christoph Nölle (Fraunhofer IWES), David Nestle (Fraunhofer IWES), Giorgio Franchioni (RSE), Mihai Calin (DERlab), Doina Dragomir (ASRO), J. Emilio Rodríguez (Tecnalia)

Fraunhofer IWES, Königstor 59, D-34119 Kassel, Germany
Phone (49) 561 7294-492, Fax (49) 561 7294-100
E-mail: Christoph.noelle@iwes.fraunhofer.de

STARGRID has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement No 318782.

TABLE OF CONTENTS

1. Executive summary 1

2. R1: Provision of harmonised core regulations at national / local level 4

2.1. Summary 4
2.2. Main recommendations 4
2.3. Explanation 5
2.4. Implementation 8

3. R2: Preparation of new standards and regulations for system integration 9

3.1. Summary 9
3.2. Main recommendation 9
3.3. Corollary recommendations 9
3.4. Explanation 10
3.4.1. System interfaces 11
3.5. Expected impact 13
3.6. Implementation 13
3.7. Priority and urgency 13
3.8. Good practices 14
3.8.1. Smart metering 14

4. R3: Prioritisation of interoperability tests specifications in Smart Grid standards 15

4.1. Summary 15
4.2. Main recommendations 15
4.3. Corollary recommendations 16
4.4. Explanation 16
4.5. Expected impact 21
4.6. Implementation of the recommendations 22
4.7. Priority and urgency 23
4.8. Good practices 23
4.8.1. Take advantage of EU funded projects to develop interoperability test use cases and specifications 23
4.8.2. Foster agreements on standards adoption inside the value chain 24

5. R4: Augmentation of information and communication security and privacy. 25

5.1. Summary 25
5.2. Main recommendation 25
5.3. Corollary recommendations 26
5.4. Explanation 26
5.4.1. Communications networks for the Smart Grid 28
5.5. Expected impact 28

5.6. Implementation of the recommendations 29
5.7. Priority and urgency 33
5.8. Good practices 33
5.8.1. Take advantage of EU funded projects to develop security use cases and specifications. 33

6. R5: Augmentation of the stakeholders' participation in the standardisation process 34

6.1. Summary 34
6.2. Main recommendation 35
6.3. Corollary recommendations 35
6.4. Explanation 35
6.5. Expected impact 38
6.6. Implementation of the recommendations 38
6.7. Good practices 39
6.7.1. VDE Verlag drafts library 39
6.7.2. IEC Smart Grid Standards Map 39
6.7.3. ISGIS 39
6.7.4. EU projects 39

7. R6: Harmonisation of the regulation and standardisation framework for DER interconnection rules 40

7.1. Summary 40
7.2. Main recommendation 40
7.3. Corollary recommendations 40
7.4. Explanation 41
7.5. Expected impact 43
7.6. Implementation of the recommendations 46
7.7. Priority and urgency 48

Acknowledgements 49

1. Executive summary

This report provides a set of six recommendations with respect to Smart Grid standardisation and regulation, addressed to standardisation bodies, policy makers, regulatory authorities and Smart Grid stakeholders, such as manufacturers and grid operators, generation operators, prosumers, energy services providers, etc. Furthermore, it aims to lay down the most relevant obstacles to a large scale deployment of Smart Grid technologies related to standardisation and regulation, and indicates possible approaches to overcome these problems.

A recurrent theme of the recommendations is the question how to ensure interoperability between the multitude of subsystems and actors involved in the Smart Grid, and how to achieve fair market conditions for all involved players.

Along with the abovementioned recommendations, the report proposes a number of "corollary" recommendations as well. For each topic, the document explains the motivations underlying the relevant recommendations and discusses the possible impact of their implementation on the electric power system and on the main impacted stakeholders. Finally, it shows possible ways of implementation and gives suggestions regarding priority and urgency issues. It thus synthesises the work carried out by the STARGRID project with the analysis of the current Smart Grid standardisation framework and the related initiatives from both standardisation bodies and industry stakeholders. Discussions of a preliminary version of the report with selected experts from the Smart Grid ecosystem have been used to validate and update the recommendations in the report.

The aforementioned recommendations are briefly listed and described below. A complete description is given in chapters 2 to 7.

R1: Provision of harmonised core regulations at national / local level

R2: Preparation of new standards and regulations for system integration

R3: Prioritisation of interoperability tests specifications in Smart Grids standards

R4: Augmentation of information and communication security and privacy

R5: Augmentation of the stakeholders' participation in the standardisation processes

R6: Harmonisation of the regulation and standardisation framework for DER interconnection rules.

In R1 we offer arguments for requiring a better alignment between regulation and standardisation. The need for this alignment arises from the fact that the Smart Grid involves both highly competitive and strongly regulated areas. Whenever regulation prescribes technical provisions, it should refer to international standards and involve the affected stakeholders in the drafting process.

The New Legislative Framework is a good and proven approach on how standards can support legislation, but its applicability is limited when it comes to system

interfaces with strong interoperability requirements. Recommendation R2 considers this topic. The communication channels between regulated actors and market actors should be specified in detail by the regulator, and needs to be harmonised at national level. Stakeholders should strive to agree on standardised interfaces regarding the communication among market actors. A list of system interfaces demanding urgent action that we consider as a major success factor for the Smart Grid development is proposed.

R3 deals with interoperability testing and certification. A recent analysis by the Smart Grid Coordination Group has shown that many important standards are still lacking testing provisions. In addition, for a complex system involving a multitude of device types and communication channels, the usual conformance testing for individual standards is not sufficient. Instead, an integrated approach is needed on top of that, involving tests in a realistic application environment. Standards' user groups should play an important role in the development of the testing and certification specifications and an extended laboratory infrastructure will be needed.

Subject of R4 are information security and data privacy, which are of primordial importance for the Smart Grid, whose new communication channels and increased number of actors make it vulnerable to attacks on the electric power system, abuse of data, etc. Current activities concerning this topic are being listed and arguments for a coordinated approach towards information security standardisation are being provided. The "privacy by design and by default" principle helps to protect consumers and generates trust in Smart Grid technologies and should be strongly promoted.

R5 deals with the standardisation process - its transparency and related received contributions. Since different topics relevant for the Smart Grid are distributed over multiple committees and even within different standardisation organisations, it becomes more and more challenging for stakeholders to keep track of the developments. The STARGRID survey has shown that most of the ongoing standardisation initiatives are hardly known outside the respective committees. It is therefore essential that standardisation organisations intensify their dissemination efforts. Finally, we provide some proposals for improvements, along with examples of good practice.

In R6 we take up the topic of interconnection rules for distributed energy resources (DER). Currently, a harmonisation of the EU member states' provisions is taking place, with the Requirements for Generators grid code entering the comitology phase, and new European standards and specifications being under development. We sketch the current status and emphasise the critical issues for a successful harmonisation.

Recommendations R2 (system interfaces), R4 (security and data privacy), and R6 (DER interconnection rules) are examples where strong interaction between regulation and standardisation is required, as explained in more general terms in R1. The proposed process of R1 involves the development of a uniform national

framework in the first step, possibly supported by European framework legislation, followed by the European harmonisation process where feasible. Whereas the system interfaces considered here can mostly be found in the first phase, national rules for DER interconnections are quite advanced in many cases and the harmonisation process has already taken off. Experiences from national implementations have been taken into account in the development of an EU-wide grid code and related European standards and we envision a similar process for the system interfaces.

2. R1: Provision of harmonised core regulations at national / local level

This recommendation is addressed to regulatory authorities and standardisation bodies.

2.1. Summary

The Smart Grid increasingly involves interactions between strongly regulated actors, like grid operators or metering operators, with other free market players, like energy services companies or DER operators. Legislation, regulatory authorities and standardisation bodies should collaborate closely in order to develop a consistent framework of technical regulations and standardisation. Regulatory provisions, either at EU or national level, should be based on international standards and the relevant standardisation bodies may support the regulators in the profiling process.

Given the differences in grid structure, security concerns, technologies, etc., between the EU member states, it may not be feasible to implement a pan-European Smart Grid regulation. A European legislative framework giving details about the national implementations can be a viable approach. A harmonised regulation is required at the very least on a national level in order to avoid market fragmentation, i.e. the implementation details for system interfaces (see also R2) and aspects of security and data privacy as well as interconnection rules should be specified by the regulator. The regulatory provisions can be seen as a mandatory core of specifications which have to be extended by standard profiles for interactions between free market actors in order to create a full interoperability framework. Standardisation committees and other dedicated stakeholder working groups should develop solutions in form of profiles or possibly extensions to existing international standards, taking into account the core of applicable technical regulations and other national characteristics.

2.2. Main recommendations

1. Set up a collaboration framework between regulatory authorities and standardisation bodies, in particular at a national level. National technical regulations should be based on international standards wherever possible.

2. Provide a core of Smart Grid regulations and standardisations for the following core applications:

a) System Interfaces (see R2)

b) Security and Privacy (see R3)

c) DER-Grid Connection Rules (see R6)

2.3. Explanation

A) Enhance the collaboration framework between regulation and standardisation

While many of today's Smart Grid actors are heavily regulated, such as grid operators, the uptake of distributed energy resources (DER) and the coupling of information networks and electricity grids means that new opportunities open up for real market-based energy services, including for instance aggregation of DERs in a virtual power plant, or new energy services for end customers based on modern monitoring capabilities. The interaction between regulated actors and the free market raises new challenges: it can be a big obstacle for energy service companies if they require access to their customers' meter data, but each metering operator uses their own data format and different procedures for data transmission. Similarly, if grid operators require different interfaces for DER control even within a single country, this leads to high costs and impedes the development of innovative add-on solutions.

It is unlikely that standardisation alone will be able to solve this problem. Standardisation is useful for harmonising technical solutions between different market actors, since they all may expect to profit from an improved market development due to harmonisation. Fully regulated actors, on the other hand, have little incentive to engage in the harmonisation of their interfaces. It is therefore essential that at least the national regulator enforce common interfaces wherever interaction between regulated actors and market actors takes place.

This implies that regulators must become active in a field that has so far belonged to the realm of standardisation, namely the provision of technical specifications for certain interfaces. On the other hand, international standardisation organisations like IEC (International Electrotechnical Commission) may have already developed solutions for these interfaces and it is absolutely mandatory to make use of this work. However, this does not imply that all the work is already done. International standards tend to be very generic and require additional profiling before standards can actually be applied to specific use cases (see the "Interoperability report" for a good explanation[1]). This remains a task for the regulators. On the other hand, it could make sense for them to delegate this task to a national standardisation committee since the standardisation bodies already have a process for participation of the affected actors in place, and the committees encompass many competences. For this purpose, a mandate could be issued by the regulator to the standardisation body which would then set up a special committee dedicated to the development of the profile.

Note how this proposal deviates from the process currently in use. The usual interaction between regulation and standardisation bodies involves the so-called New Legislative Framework[2]: the regulator imposes certain functional requirements on products, which can be satisfied either by adopting a so-called

[1] http://www.cencenelec.eu/standards/Sectors/SustainableEnergy/SmartGrids/Pages/default.aspx
[2] http://ec.europa.eu/growth/single-market/goods/new-legislative-framework/index_en.htm

Harmonised Standard[3], in which case it is assumed without further verification that the requirements are satisfied; or through a partly or completely independent solution, in which case compliance with the regulations must be verified explicitly.

This approach has proven very successful in areas of application like health and safety and it has been proposed by several stakeholders in the STARGRID stakeholder survey to follow this approach for Smart Grids as well. We do support this proposal where functional requirements are concerned, but argue that interoperability at system interfaces (see also R2) requires a more restrictive approach with regulation involving detailed technical specifications instead of just functional requirements. For instance, it is not sufficient that each metering operator provides an interface for authorised external market participants (or the end customers themselves) to access smart metering data, but for an efficient development it is essential to have a uniform interface across different metering operators. It is not sufficient that each grid operator specifies exactly their interface for feed-in management of distributed energy resources, but this interface must be uniform at least on a national level in order to create reasonable market sizes for single products.

Stakeholders have brought forward two main concerns regarding this proposal. Firstly, many argue that international solutions are preferable over national ones, so at least EU-wide solutions should be aimed at. This is a valid point, but given the current situation, even national harmonisation would be a great step forward for some areas. Where an EU-wide harmonisation would lead to severe delays, a pragmatic modus operandi has to be found. An approach recently adopted at EU level concerning smart metering regulation (3rd Energy Package) and the ACER/ENTSO-E grid codes, may be a viable compromise, because both set a common European reference frame for specific national implementations.

Secondly, the translation of regulations into technical aspects has so far been the sole responsibility of standardisation. As explained above, we believe that this step is necessary where interfaces between regulated and non-regulated actors are concerned. On the other hand, it makes sense to demand that international standards should be the basis for the technical regulations. The latter should preferably be developed as profiles of available standards and it may be required that in EU directives for instance, deviations from this rule in national implementations have to be explicitly justified.

Necessarily, there is a trade-off between free market development and strict regulation. Regulation in one area may foster the market development in other areas by removing blockers and ensuring equal opportunities for all involved actors. However, regulation can slow down innovation, especially if it imposes a particular technical solution as proposed for the system interfaces. A potential way

[3] http://ec.europa.eu/growth/single-market/european-standards/harmonised-standards/index_en.htm

to diminish this risk is to allow for other solutions besides the mandatory one – regulated actors will be enforced to provide a particular common interface, but may offer alternative ones in addition.

B) Standardisation to reflect and extend the regulatory framework

In heavily regulated market domains like electricity grids, standardisation has to interact with the regulatory framework. Whereas regulation should always be restricted to a minimum set of necessary use cases, the specification of obligatory technical rules by a regulatory authority may create new possibilities for standardisation as well, which could include adjacent market-driven use cases and profiles extending the original specification. For instance, if the regulator prescribes a certain communication protocol and data model for the remote control of distributed energy resources, then the same interface may be used and extended for the integration of DERs into a virtual power plant. Ideally, if the regulatory provisions are based on international standards, then the extended standardisation may be developed as a more comprehensive profile of the same set of standards. This work could either be done in (typically national) standardisation committees or in other dedicated stakeholder working groups.

On the other hand, if technical regulations are to be based on standards, the availability of standards covering the relevant use cases must be ensured. If extensions to existing standards or new developments are required, the regulator should try to avoid stand-alone solutions, but rather issue a mandate to the relevant standardisation body for the development of a standard that suits its purpose and fits into the general standardisation framework. This step should preferably be done at EU level. We have already argued above that the second step of developing a profile of an international standard to be used in a technical regulation may then take place at the national level, if a common European setting is not feasible (see also the next item).

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

A (temporary) diversity of standards and regulations in Europe may be seen as an opportunity. Regulatory conditions regarding Smart Grids are and will most likely remain diverse between member states of the EU within the next years, and the development of necessary rules should not be hampered too much by a tedious search for a commonly acceptable compromise. It therefore makes sense in certain domains to impose a common European framework, which then has to be cast into specific national implementations by the respective regulators. As mentioned above, this is exactly the approach that has been taken for the ACER/ENTSO-E grid codes and the smart metering provisions included in the 3rd Energy Package, hence this part of the recommendation is fully in line with current practice. Experiences from the national implementations may then be taken as guidelines for a later harmonisation of the rules.

As an example for such a harmonisation process one can mention the interconnection rules for DER, where several countries with a high DER

penetration have developed strong regulations over the past years, which were then used as a basis for the Requirements for Generators grid code at EU level. The latter still allows for a certain degree of flexibility for the national implementations, though it has been argued that an even higher level of harmonisation would be even more of use (see R6).

D) Require national uniformity

We have argued above that a certain level of regional variation regarding technical regulation in Smart Grids is acceptable and even required due to national differences regarding grid structure, customer behaviour, security concerns, etc. Nonetheless, the specifications should not be too fragmented, so inefficiencies resulting from the diversity of requirements can be reduced. For this reason, at least member states should be required to adopt binding rules for certain applications (in particular system interfaces involving regulated actors, security and data protection, and interconnection rules for distributed energy resources). Smaller member states may choose to cooperate with others to generate a substantial market based on common standards. It could be an option to provide a European sample specification that becomes mandatory for all member states which cannot provide their own specifications by a certain date.

2.4. Implementation

This recommendation is addressed mainly to politics and regulators, but also affects the standardisation bodies. A stronger collaboration between standardisation organisations and regulators is considered crucial by the authors to enable markets for core Smart Grid functions. In particular, national technical regulations shall be based on European/international standards (adopted as national standards). This requires in turn that standards covering the relevant use cases are available or at least are in the development process.

Some recent developments have followed this direction, like the development of European grid codes, national grid codes, and standardisation related to DER interconnection rules (e.g. the ENTSO-E Requirements for Generators grid code, and the European standards/specifications EN 50438:2013 and CLC/TS 50549), or the European smart metering provisions included in Directives 2009/72/EC and 2009/73/EC, which demand national legislative actions for intelligent metering systems and associated infrastructure.

The latter have been supported by recommendations on the covering of functionalities (EC Recommendation European Commission Recommendation 2012/148/EU), which ask for the implementation of standardised interfaces, in particular those regarding customer access to meter data (§42a).

3. R2: Preparation of new standards and regulations for system integration

This recommendation is addressed to policy makers, regulatory authorities (EU and national), and standardisation bodies.

3.1. Summary

This recommendation details the general approach described in R1 for the system interfaces. The concept of "system interfaces" refers to the communication across Smart Grid (sub-) system boundaries or between different actors. This is exactly why interoperability is needed most urgently. The recommendation proposes to introduce a set of mandatory system interface specifications based on international standards in cases where interaction between regulated actors and the free market is required, in order to allow for full market participation of distributed energy resources, demand response providers, aggregators and other innovative energy services providers. When only free market interaction is concerned, standards or profiles should be developed by the relevant stakeholders to accelerate the market development.

The lack of commonly agreed communication standards is a major stumbling block for the Smart Grid development and inhibits 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 should be addressed either by legislation or the relevant standardisation committees.

3.2. Main recommendation

The interoperability of system interfaces should be ensured by standardisation and regulation. For this purpose, regulatory authorities shall define obligatory specifications that are uniform at least on a national level. Voluntary standards complement the framework by specifying the system interfaces between market actors.

3.3. 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.

- Take security seriously: standardised solutions require a high level of security measures to prevent devastating effects of large scale attacks.

- System interfaces beyond the realm of regulation should be addressed by standardisation committees or other dedicated stakeholder working groups.

3.4. Explanation

One of the main barriers for market introduction of Smart Grid technologies involving distributed energy resources and end customers in general is the availability of standardised interfaces among 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, or smart meter owners (even though market conditions do not necessarily provide sufficient incentives at the moment). In contrast to this, the lack of clearly defined interfaces between the relevant systems is a major obstacle for the development of new Smart Grid based services.

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 where interfaces to regulated actors are concerned. Interfaces covered by regulation should be uniform at least within each member state (as explained in R1, national uniformity is considered a realistic short-term perspective compared to European-wide common system interfaces).

In order to allow full interoperability, system inter-faces should also be specified in a more extensive way than other communication systems: they need specifications regarding authentication, access permissions and data models. Regulatory provisions should be publicly and freely available and they need rules for testing as well as for certification. Clearly defined system inter-faces are essential for the development of Smart Grid and smart metering services in market competition. Too many 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 meter manufacturer defining its own interface. For this reason, it should be aimed at having at least mandatory national specifications in order to guarantee a market size suitable for successful business cases.

There seems to be an area of tension between market-based evolution and obligatory standards. On one hand, the market-based approach provides most freedom of choice. Interoperability will be achieved after one or a few systems succeed over others. On the other hand, obligatory specifications provide secured interoperability from the start but at the cost of strict regulation without choice and competition for 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 of a process that is in line with this recommendation. The European Directive 2009/72/EC[4] 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 all the way down to the communication protocol, 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 3.8.1. Smart Metering).

3.4.1. 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:

- Grid Operator – Local Controller (regulated)
- Metering Interfaces: (regulated)
    a) SMG – Local Controller
    b) SMG – Authorised External Entity
    c) Metering Operator – other Authorised External Entity
- Authorised External Market Entity – Local Controller (unregulated)

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) or Home Automation gateway, a charging controller, or the like. The local controller may also be integrated into the Smart Meter Gateway.

Interface 1: Grid operator – Local controller

The requirement is to send control commands to the local controller, for instance in the case of grid instabilities 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 at the moment mostly left to the grid operator.

[4] 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 for control strategies.

Interface 2b: SMG – Authorised External Entity

In this case, the exchange of meter and tariff data is carried out between the gateway and an external party, comparable to 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 aggregators and other energy services providers. Information exchanged includes incentives, control signals, status information and the like. In general, this interface does not fall into the realm of regulation, but there may be special cases where it does, like market platforms for local energy services.

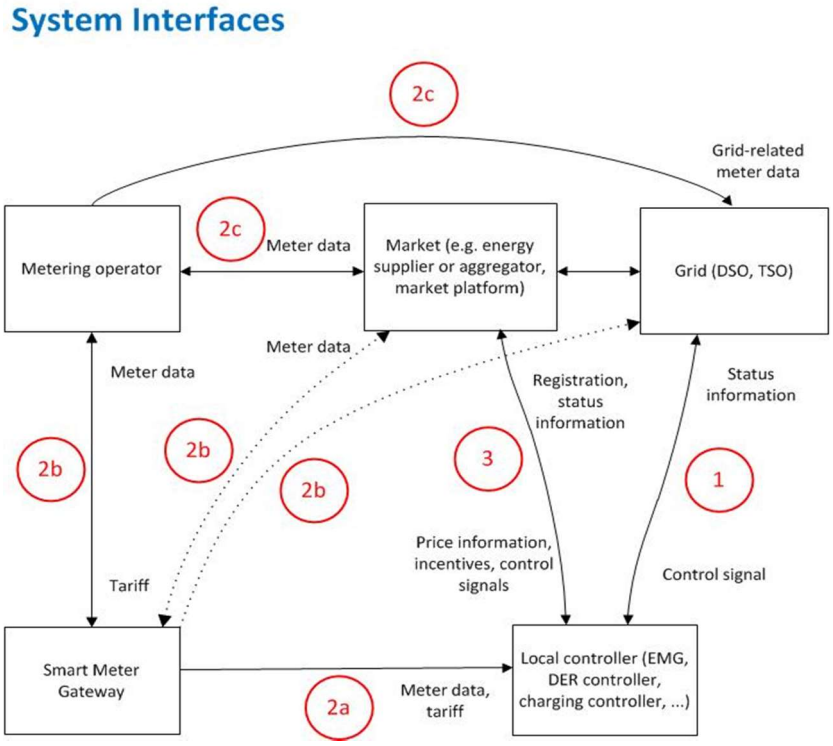

Figure 1: ***Proposed system interfaces***

3.5. Expected 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

3.6. Implementation

This recommendation is addressed to legislation and standardisation bodies. They should aim to establish regulations/standards suitable to ensure interoperability. The technical specifications should be based on European/international standards and the development process of the regulations may include a co-operation between regulators and (national) standardisation bodies, as proposed in recommendation R1.

Harmonised European specifications are desirable and a process involving the definition of system interfaces and basic requirements at EU level could initiate the national legislative processes. Cooperation of member states and the use of international standards should be encouraged.

Main stakeholders impacted by this recommendation are regulators and standardisation bodies, as well as grid operators, DER operators, end customers, and energy services providers.

3.7. Priority and urgency

Many Smart Grid technologies have been extensively tested in field tests and demonstration projects, but very often the rolled out products either lack the required communication capabilities for full Smart Grid functionality or rely on legacy or proprietary solutions. Some innovative business cases which were expected to play a role in the future electricity market are not feasible in the 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 in particular the regulators/legislation to take immediate action. A prioritisation of interfaces will have to be performed and the process will presumably last several years. Therefore, we consider it a short- to medium-term objective (2015-2018).

3.8. Good practices

3.8.1. Smart metering

Germany has issued a clear regulation for smart metering[5], 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 as 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.

[5] https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03109/index_htm.html in German

4. R3: Prioritisation of interoperability tests specifications in Smart Grid standards

This recommendation is addressed to standardisation bodies and industry.

4.1. Summary

Smart Grid operations rely on the strong interaction between different infrastructures, domains, players, applications and functions, technologies, etc., and thus require interoperability between the devices and systems for all application functions. Standard conformance is a prerequisite for interoperability and is a 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[6]. Their investigation also shows that today most standards contain no such testing specifications or cover only some relevant aspects/domains. The establishment of suitable technical specifications for interoperability tests requires a seamless coordination between the involved technical committees to implement the systemic approach methodology developed recently. Moreover, good knowledge and experience in the development of testing procedures, test coverage etc. given by relevant specialised organisations is absolutely necessary. As a consequence, the development of interoperability test procedures cannot be solely covered by a group of experts delegated by different companies, as in a standardisation committee. For this reason, the standard's user group or industry initiative that organises the process and carries out the testing of the test specification and setup is typically also involved in financing the development of such a testing specification, which, in many cases, should be accompanied by testing machines or reference hardware. EU funded projects could also provide a suitable framework for the development and validation of testing procedures for specific applications, in particular for standards that lack a dedicated user 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.

4.2. Main recommendations

1. Prioritise the development and adoption of interoperability test specifications to validate interoperability of components and systems for Smart Grid applications.

---

[6] ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/SGCG_Interoperability_Report.pdf

2. A coordinating entity should be installed to establish and maintain a "certification system" for the interoperability of Smart Grid devices and systems and to define what use cases should be covered by such a certification system.

4.3. Corollary recommendations

- Identify and define those critical use cases where interoperability tests are most urgent. Whenever necessary for these critical situations, develop missing use cases.

- Support the appointment of a coordinating entity (steering committee) with the aim of defining the basic criteria for the selection and/or preparation of relevant use cases; refine the methodology; assure maintenance of available testing specifications, and develop a work programme in close collaboration with the affected stakeholders.

- Develop a process to increase the support of testing and certification organisations as consultants in the definition of interoperability test specifications.

- 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).

- The implementation of interoperability tests requires the availability of qualified testing infrastructures, the ability to create the system validation framework and an agreement on test procedures.

- Take advantage of EU funded projects to develop interoperability tests specifications. Specific networking actions should be addressed by targeted calls (e.g. within H2020).

- In the elaboration/revision process of SG standards, include the verification that interoperability testing provisions are covered.

4.4. Explanation

Interoperability overview and requirements

Interoperability represents the ability of systems, sub-systems or intelligent devices to exchange information and use them in order to perform required functions. The risk of non-interoperability increases as the complexity of the system grows. This is especially true when considering the evolution of the energy system towards 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. intelligent

transport, smart cities, etc.) in order to sustain the development of the energy market.

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

Standard conformance is a prerequisite for interoperability, 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 (e.g. 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 shall be carried out. 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.

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 and which level of interoperability is needed.

Use Cases Selection

Besides the dedicated standards user groups, which perform the actual development of detailed use case and testing specifications, a coordinating entity would be of great benefit, which could define the basic criteria for the selection of use cases, refine the methodology, maintain an overview of available testing specifications, and develop a roadmap for the development work in close collaboration with the affected stakeholders. This role is similar to the one taken

on by the Smart Grid coordination group for the development of actual standards, or a systems committee at IEC level. Indeed, the coordination group could be operated by the ESOs and benefit from their well-established participation and communication processes.

Where regulatory provisions are concerned, the task of defining the use cases is the regulator's responsibility. Moreover, it might make sense for the regulators to delegate the task to a user group or industry association by issuing a formal mandate. A close collaboration between regulation and standardisation is highly desirable in any case. The user group has the task to select, 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. Use cases could be extensions of the high level use cases identified within SGCG. With regard to the identification and definition of the use cases, user groups should also take specific national situations (e.g. information flows could vary country-by-country, depending on internal regulations) into consideration. Technical committees, when drafting/revising standards, should evaluate whether the interoperability testing topic is covered by a related user group. If not, actions should be taken. The interoperability tool proposed by the working group interoperability of the SGCG is a helpful instrument for this analysis, also when considering a methodological point of view. The development of testing and certification specifications should also be accompanied by the definition of a reference layout and the set-up of an initial testing environment. Therefore, the participation in this process of testing/certification organisations is important. Product manufacturers should sustain part of the costs. In some cases, the competitive advantage of being able to perform tests and certifications before their competitors may be even motivation enough for an organisation to invest in the development of those specifications.

Data models

Since a Smart Grid may incorporate many different types of physical networks, the interoperability specifications should not restrict the choice of physical communication layer. Interoperability must rather 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 the areas "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). Harmonisation of the three data models is paramount. The STARGRID survey has evidenced the strong interest of Smart Grid stakeholders and ICT and telecommunication representatives in the harmonisation and integration of different data models to cover the complete set of Smart Grid functionalities.

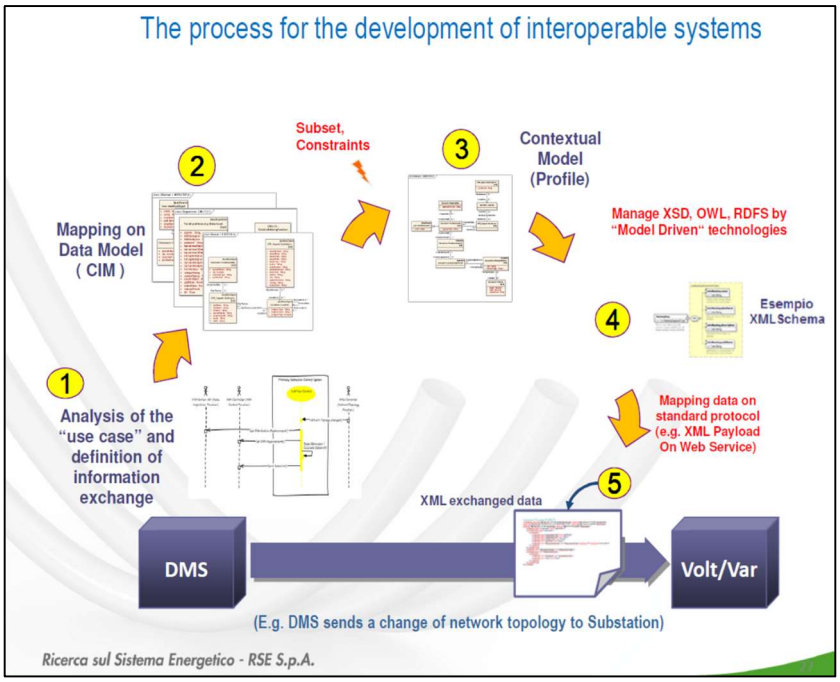

Figure 2: ***The process for the development of interoperable systems***

Profiling process

The concept of a profiling process, in order to specify which standards (parts) of a defined context have to be used and how, represents a suitable tool to achieve interoperability between systems.

The concepts "Basic Application Profile (BAP)" and "Basic Application Interoperability Profile" (BAIOP)[7] (e.g. a profile for the interlock function), recommended by the WG Interoperability of the SGCG, are aimed at this approach. Groups of BAPs and BAIOPs provide functionality at a higher level. Granularity of profiles and guidelines for the definition of BAPs and for their generation are deemed urgent matters of discussion.

Interoperability Certification System

A mutually acknowledged "certification system" for interoperability testing should be implemented with the twofold aim of:

- Certifying the interoperability performances of devices and systems against the developed specifications, possibly leading to the appointment of a sort of "interoperability label".

[7]In the terminology of the Smart Grid Coordination Group, conformance tests are based on Basic Application Profiles (BAP), whereas interoperability tests are based on Basic Application Interoperability Profiles (BAIOP).

- Accrediting certification laboratories in conformity with agreed interoperability certification procedures.

This system should be based on a set of agreed procedures, similarly to initiatives already implemented at international and EU level (e.g. through IECEE[8] and CAB[9]. See also EA: European co-operation for Accreditation[10]).

The certification system should be operated by a neutral entity which must closely collaborate with the relevant standards' user groups and the testing organisations.

A mutually acknowledged certification system ensures that interoperability tests performed in different countries and by different laboratories against the same use cases and profiles and procedures produce the same results. This could be a great commercial value for equipment and system producers. Certification by an accredited laboratory is typically required for verification of conformance to regulatory provisions, for instance when security and stability are concerned, whereas usual standards conformance can also be asserted by a self-declaration of the manufacturer. However, interoperability tests typically involve devices from different vendors and rather complex settings as compared to the usual conformance tests, so that availability of the testing infrastructure will mostly be limited to dedicated testing laboratories.

EU funded projects

EU funded projects could be a suitable context to validate the interoperability tests specifications against large scale use cases. Good practice 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 starting already in the concept phase (interoperability by design).

The system interoperability approach developed by means of EU funded projects and supported by the stakeholders is the most economical and effective way if it can produce standard solutions at EU level. Interoperability is a time demanding issue and the proposed process timing is adequate; in any case, it is not longer than the current one. This approach could help to remove any objections and further advance the SG transformation process. Targeted calls, e.g. within H2020, should be launched. They should be pushed by the industry (user groups) and focus on system solutions through networking actions (e.g. within ETP and EJI initiatives) with the objective to elaborate standards.

Proposals for organisation and financing

Some stakeholders (e.g. manufacturers and system integrators) complain that requirements for interoperability tests may affect the costs of equipment and the

[8] http://www.iecee.org/html/AboutIECEE.htm
[9] https://cabforum.org/
[10] http://www.european-accreditation.org/

market penetration capacity. This aspect must be taken in due account when elaborating the related standards and when selecting those use cases where the interoperability should be validated with tests in order to limit the requirement for 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. Hence, manufacturers and system integrators could for example access specific funds or incentives for the certification of the interoperability tests. A specific cost-benefit analysis should support these decisions.

In certain cases, e.g. when the interoperability certification can be derived from the analogy of other use cases, a third-party certification or a self-declaration by device producers could be accepted to state the interoperability conditions conformance.

In common usage, suitable testing infrastructures that are usually, but not necessarily, outside standardisation bodies and hold multidisciplinary competences, are indispensable to provide assistance to manufacturers and to carry out interoperability tests. Tests procedures should be optimised (e.g. automated) to the cost reduction extent.

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).

4.5. Expected impact

The costs of executing interoperability tests might increase the costs for equipment and system providers. However, the “interoperability certification” may constitute a “quality label”, which could facilitate the procurement phases and the value for money of the validated products. The use of a quality label from the interoperability certification has already been employed for years in other sectors than energy, as for instance in telecommunications[11]. 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.

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

Interoperability tests validate the use case step-by-step: this allows, among others, validating early implementation of standardised technologies and providing feedbacks to standardisation bodies for the validation of the standards themselves.

[11] See e.g. WI-FI Alliance interoperability Certification Programme (ref: http://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-announces-certification-plans-for-ieee-80211g-wireless-lan)

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

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 initially cover the costs of requirements for interoperability tests and this will affect their competitiveness.

4.6. Implementation of the recommendations

The basis of the implementation of the interoperability tests is the definition of the use cases which are being referred to. As already mentioned, this task particularly calls for Smart Grids stakeholders in cooperation with ICT and telecommunication operators. Some progress has already been made in this direction within the activities of the SGCG, and further coordination by the ESOs would be valuable. Future work should be based on the definition of high-level services and functionalities by the EC task force for Smart Grids[12] and the identification of generic high level use cases by the SGCG.

Common efforts of Smart Grids stakeholders participating in the standardisation committees should be addressed to select "interoperability-critical" to use cases and 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 be in charge of the preparation and maintenance of relevant standards to ensure that these contain sufficiently detailed testing requirements (test set-ups and test procedures) in order to facilitate the implementation of the recommendations. Direct participation of SMEs and sector associations is strongly recommended for the sake of transparency and to supervise aspects like the cost-benefit issues.

National standards bodies need uniform, clear and transparent information provided and agreed by the stakeholders to develop suitable requirements for testing specifications. This implies a continuous coordination with relevant users' groups and laboratories, which participate to the works prepared in the related technical committees.

A certification system for the most interoperability-critical Smart Grid use cases should be established by the industry in close collaboration with testing and certification organisations. This activity should also be coordinated with the

[12] http://www.gt-engineering.it/uploads/allegati/25expert_group1.pdf

development of testing specifications by the standardisation organisations. The introduction of a corresponding Smart Grid interoperability label could help to foster the visibility of such an activity. In any case, broad participation of stakeholders is essential to gain relevance.

4.7. Priority and urgency

Interoperability as the prerequisite 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).

4.8. Good practices

4.8.1. Take advantage of EU funded projects to develop interoperability test use cases and specifications

A good reference is the use case of "Voltage Control in Medium Voltage Grid" developed within the project SmartC2Net[13].

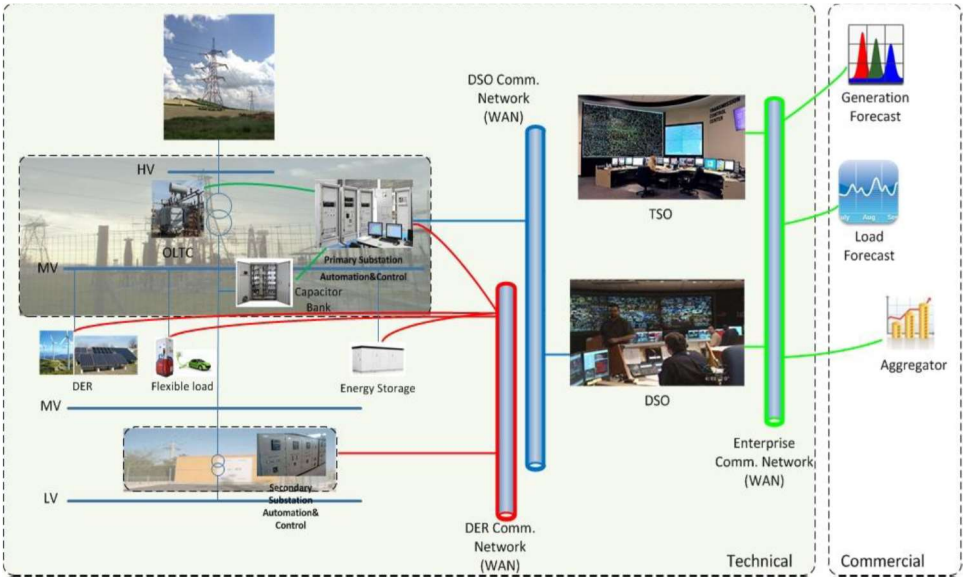

Figure 3: ***Overview of a medium voltage control use case***

See also the EU-FP7 Project: COTEVOS – Concepts, capacities and Methods for Testing EV Systems and their interoperability within the Smart Grids[14].

[13] http://smartc2net.eu/SmartC2Net_UC_VoltageControl-Medium%20Voltage%20Grid.pdf
[14] www.cotevos.eu

4.8.2. 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 standardised 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 industry and putting it in a position to offer the market modular, integrated, interoperable, and rational applications[15].

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

5. R4: Augmentation of information and communication security and privacy

This recommendation is addressed to policy makers and regulatory authorities (at European and national levels).

5.1. Summary

The Smart Grid is intrinsically a system highly sensitive to information security problems. The overall operation of the electric/energy infrastructure, strongly relying on the interaction with communication infrastructures, exposes the entire system to risks of malicious (physical and cyber) attacks. 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 become ineffective against attacks aimed at the Smart Grid operation and associated information and communication systems. 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 and are being supervised by the SGIS (Smart Grid Information Security) experts group. The efforts to cover the standardisation gaps related to 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 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 legislative framework should be harmonised at EU level.

The increasing availability of personal data in the Smart Grid context raises severe privacy concerns. In order to protect the end customer and to generate trust in Smart Grid technologies, the latter should be strictly based on the “privacy by design and by default “principle, which means that (1) the protection of personal data from unauthorised use is considered from the very beginning of the development cycle to the Smart Grid technology, and (2) that the highest protection levels are enabled by default with no need of an explicit action/confirmation by the customer. Standards could help to translate generic privacy provisions from the legislative framework into appropriate technical requirements.

5.2. Main recommendation

Develop a standards framework for security against physical and information attacks as well as for data protection encompassing the requirements of Smart

Grids with a coordinated and systemic approach. The latest report produced by the SGIS group can be a good supporting reference for this goal.

5.3. Corollary recommendations

- Stakeholders should clarify and agree on the requirements for information security and data privacy. Cooperation of the operators of the involved networks is essential for this.
- Stakeholders should use standardised formats, language and data models for the specification of requirements for 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 electric power sys-tem and the protection of data.
- Collect the minimum amount of personal information needed with-out compromising the quality of the provided services. Assure that the individual identity is anonymous.
- Transparency: inform the customer about the collection, use and dis-closure of their personal details and accept their preferences. Always obtain the express consent before disclosing personal information to third parties. Allow the consumer to access their 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.

5.4. Explanation

ICT technologies will enable the Smart Grid paradigm, improving efficiency, reliability and sustainability of the power system, allowing new functionalities but increasing the potential threats and attacks.

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, interfaces and deployed technologies (e.g. the monitoring network) dramatically increase the number of vulnerabilities that can be exploited. Security shall be considered regarding the operation of the

Smart Grid and also the user acceptance (e.g. data privacy of Smart Meters, which was identified as a critical issue during the STARGRID assessment).

The same issues directly impact the operational security. The latter is not specifically addressed by this recommendation: the topic is covered in the 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 permanently ensure the electric power system security"[16].

However, the correlation of information security and operational security is obvious. It is enough to consider, for example, 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 data exchange: there should not exist any barriers between the different actors involved, especially not those caused by malicious actions.

Along with this, consumer privacy shall not be sacrificed when exploiting the benefits of the Smart Grid. Smart Meters and smart appliances will provoke a data explosion of private details about the consumers' daily life (consumer behaviour and characteristics) and it is not clear who, apart from the utility companies, will have access to this information without obtaining the necessary consent from the customer.

No consensus exists on privacy implications of the Smart Grid and there is a lack of standards and procedures to deal with this issue. Translation of legal concepts on personal data protection into technical requirements needs further support by the appropriate standards. 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 attacks aimed at the Smart Grid operation and information system. A new secure scheme is necessary on the basis of 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 above all: asset identification, security control on each level, perimeters security, physical security, personnel and training, and recovery management.

Security is a global issue, requesting measures in every layer of the architecture and an overall approach to face new vulnerabilities and risks (e.g. use of a public network instead of private and segregated ones, physical security of smart Meters). Again, the certification process is paramount. However, certification alone is not enough: security aspects should be considered already in the Smart

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

Grid conceptualisation (including innovation and research) and design stages according to the "security-by-design concept".

5.4.1. 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[17] 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

5.5. Expected impact

Facing the security issues that are associated with such an approach is difficult and expensive to implement, due to the complexity of the problem and the huge number of internal actors, electricity market players and technologies involved. In fact, each node (player/technology) may introduce vulnerabilities to the system.

The approach requires the thorough definition of the use cases for 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"[18]). The elaboration of the use cases done by the SGCG-FSS maps connections, protocols and standards on the SGAM, but does not go into details about 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.

---

[17] CEN-CENELEC-ETSI Smart Grid Coordination Group First Set of Standards (ftp://ftp.cen.eu/EN/EuropeanStandardization/HotTopics/SmartGrids/First%20Set%20of%20Standards.pdf)

[18] http://www.soes-project.eu

A risk analysis of each use case should be performed 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.

Utilities are concerned with the costs not only of security, but of Smart Grid implementation in general and different attitudes towards the issue may arise country-by-country, depending on their business dimensions and country-specific regulations. In this respect, the results of the EU FP7 project ESCORTS (European Network for the Security of Control and Real Time Systems[19]), which assessed the vulnerabilities of computer networks and SCADA architectures in the energy domain, should be taken into account.

Energy and communication network operators 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.

5.6. Implementation of the recommendations

It can be said that there already are well-established security standards for different target groups and topics, which can establish the basis for Smart Grids security. However, existing and new developed technologies, policies, best practices and use cases shall be incorporated.

An approach similar to the one proposed for the standardisation of an interoperability testing methodology (see R3) could be adopted at least regarding the selection and definition of the related use cases. The proposed Smart Grid security approach has several aspects in common with the R3 approach: definition of the actors and their interfaces, type of information exchanged, data models and protocols used, etc. Furthermore, the solution for various interoperability issues in the different domains is a prerequisite of all aspects of security, e.g. standardisation/harmonisation of protocols and unified information models.

Requirements for security/privacy are not clear and agreed enough which 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 order to reach a common understanding based on those standards. Standards must unify and simplify the design process of information security and facilitate a dedicated security level on technical, organizational and procedural levels.

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

[19] http://cordis.europa.eu/project/rcn/87538_en.html

provides a high-level guidance on how standards can be used to develop Smart Grid information security and how to integrate it into daily activities. In addition to a selection of adequate security standards that are mapped on SGAM, the group analyses several use cases to show the applicability of the standards in depth.

ISO/IEC is working on the series 27000, describing a general approach for information security management systems mostly related to governance aspects (risk assessment, industrial processes, policies), but touching also on some technical aspects and domain-specific recommendations. In this context, the ISO/IEC TR 27019 (Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry) is especially worth mentioning.

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

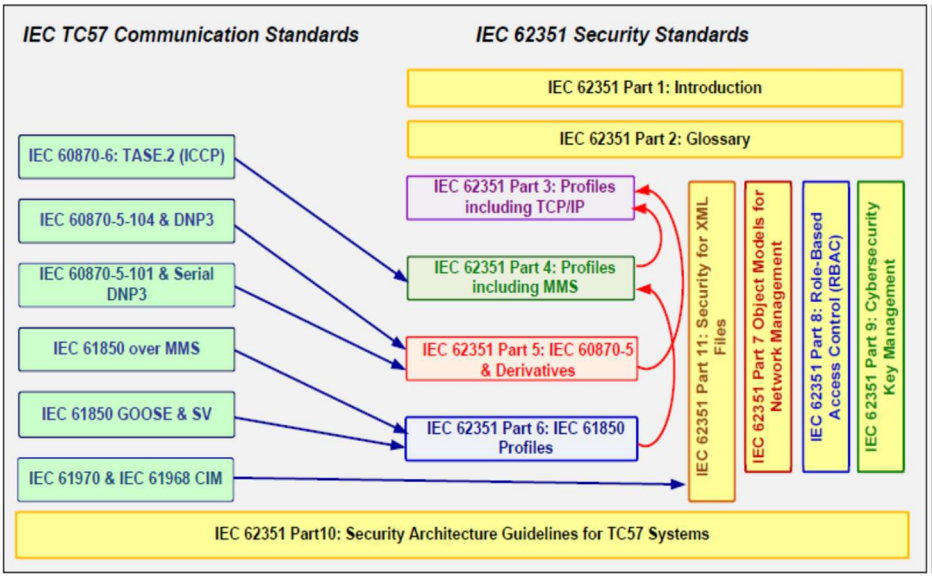

Figure 4: ***Security Architecture Guidelines for TC57 Systems***

Since they have some aspects in common, there is a clear request for harmonisation between industrial process control and associated operations of the electric power system management (see Figure 3). Collaboration agreements between committees are in place, normally formalised in IEC as “liaison actions”.

The works in progress on the IEC 62351 standard series are of particularly high relevance and reflect the complexity of a critical subject such as security in the Smart Grid. IEC 62351 specifies the end-to-end security of the IEC/TR 62357-1 reference architecture (definition of a secure communication infrastructure for energy management systems). It covers most of the IEC TC57 communication

protocols (IEC 60870, IEC 61850, IEC 61970, IEC 61968 series), but does not cover information about security management issues (as included in other standards like IEC 62443 and the ISO/IEC 27000 series).

IEC 62351 is composed of 11 parts, some of them being under revision or are not completed yet:

- Part 1 (introduction and overview of security in energy infrastructures, protection goals and measures)
- Part 2 (glossary of terms and description of essential security concepts)
- Part 3 (security aspects of protocols based on TCP/IP)
- Part 4 (security aspects of protocols based on MMS)
- Part 5 (security aspects of protocols based on IEC 60870-5)
- Part 6 (security aspects of IEC 61850 profiles)
- Part 7 (specification of network and system management data object models for controlling and monitoring the network and connected devices, which facilitate the detection of attacks and fast reactions)
- Part 8 (role-based access control)
- Part 9 (cyber-security key management for power system equipment)
- Part 10 (security guidelines for power system architectures and location of security standards in the IEC reference architecture)
- Part 11 (security for XML files)

Two new technical reports have been proposed recently: part 12 (resilience and security recommendations for power systems with DER), and part 13 (security topics to be covered by standards and specifications).

In the USA, Canada and parts 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.

Moreover, in the USA the NISTIR 7628 is a reference work composed of several volumes: volume 1 describes the overall approach, the risk assessment process and the high-level architecture (high level security requirements for domains, interfaces, etc.); volume 2 includes recommendations for privacy when dealing with personal information in Smart Grids; volume 3 integrates the analyses and

references used to develop the high-level requirements and tools contained in the NISTIR series.

In addition to the already commended initiative of ENTSO-E, the works of ENISA[20] (European Union Agency for Network and Information Security) are important as well, especially the ones related to security and resilience of the critical infrastructures which mainly are power and transport.

The conclusions of the mentioned ESCORTS project emphasised the need to increase awareness of potential cyber-attacks and to encourage best practices jointly between manufacturers and end users. ESCORTS also recommended reducing the divergence between current standardisation efforts on process control and power system control and developing test platforms for cyber-security assessment and testing.

The efforts to bridge 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 in making gaps analysis and providing 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 selection 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 risk management and decision making.

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 prerequisite 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, significant country-by-country differences still exist. Legal provisions on data protection in ICT technologies are not yet adequate or harmonised in EU countries. Standards for the 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

[20] http://www.enisa.europa.eu

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. No supplementary actions by customers using these technologies should be required for guaranteeing their privacy. Consumers must have control about their electricity consumption and their private information to generate the trust needed for their 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 regarding smart metering, but in the near future also smart appliances and electric vehicles). From this perspective, the transfer to standardisation of the validated mechanisms complying with the relevant requirements should be pushed to completion.

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.

5.7. Priority and urgency

Security and privacy in Smart Grids are among 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).

5.8. Good practices

5.8.1. Take advantage of EU funded projects to develop security use cases and specifications.

The project SoES[21] has developed reference security analysis for fundamental use cases: "Voltage Control in Medium Voltage Grid", "Photovoltaic Storage and Generation", "Load reduction programmes" and "Smart Meter Configuration ".

[21] www.soes-project.eu

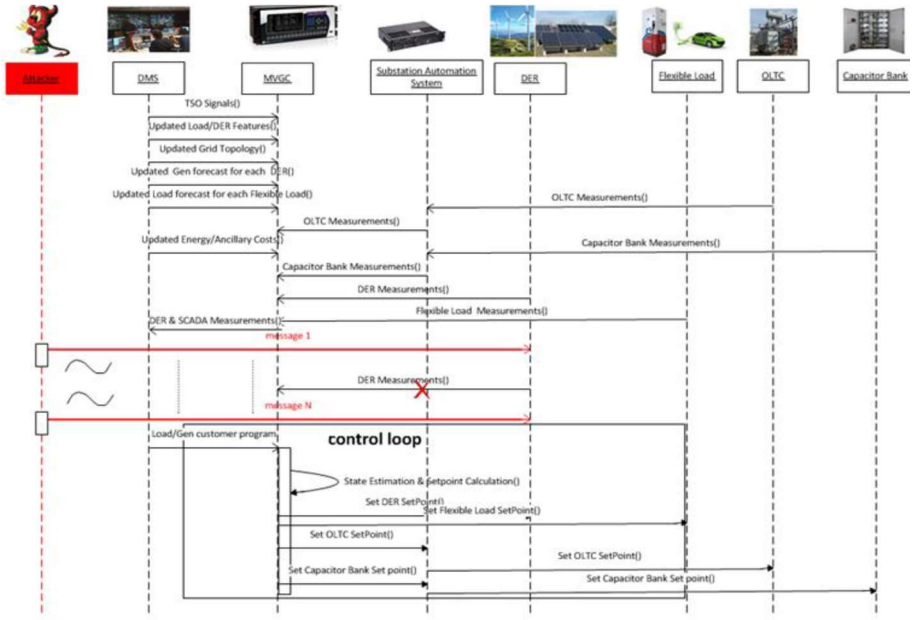

Figure 5: ***Voltage control use case from the SOES project***

6. R5: Augmentation of the stakeholders' participation in the standardisation process

This recommendation is addressed to standardisation bodies.

6.1. Summary

A broad level of participation in the standardisation process is essential to ensure that standards cover the requirements of all affected stakeholders. This is particularly true for Smart Grid topics, which can impact the interests of a wide range of industries and users of technologies. A prerequisite for strong participation, but also of significant relevance in itself, is the dissemination of planned and ongoing standardisation projects.

Whereas participants in the STARGRID stakeholder survey consistently attributed high importance to the standardisation of Smart Grid technologies, the level of awareness of current standardisation projects appears to be considerably lower. Presumably, this also affects the level of participation in the committees. We present some ideas on how standardisation bodies can improve their dissemination activities, based largely on examples of good practice, like a central online database of standards and projects.

For small and medium enterprises (SMEs) the participation in standardisation committees is particularly challenging, so there is a risk that their interests are not well represented. Possibilities to address this issues could be the inclusion of standardisation tasks in innovation projects or industry associations representing SMEs in standardisation processes.

6.2. Main recommendation

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

6.3. 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 level. System committees can be an effective tool to coordinate the work of different committees.
- 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 limit of the respective mandates.
- 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.

6.4. Explanation

A) Dissemination

The advent of the Smart Grid increased the necessity for many stakeholders of the electric power system to keep track of technological developments and standardisation activities in domains they were not traditionally concerned with, and where they are not represented in a technical committee. This also leads to new challenges for the standardisation bodies which need to ensure an adequate dissemination of their activities. For instance, stakeholders require information about ongoing standardisation projects, planned revisions, etc., in an easily accessible way.

European Standardisation Organisations (ESOs: CEN, CENELEC and ETSI), as well as international standardisation organisations (e.g. IEC and ISO) provide a

lot of information on their websites about ongoing standardisation work and list publications and projects for all technical committees and subcommittees. Although this is valuable work, it remains difficult to really follow up on the developments from outside a committee, since usually little information on the content of a new/revised standard is communicated before the public enquiry stage and a structured search for standards according to classified content is not always possible[22].

The national "mirror" committees to the European/ international technical committees are expected to participate in the standardisation process to ensure the formulation of coherent national positions by directly involving all categories of stakeholders. Organisations represented in national technical 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 a suitable mechanism in place to disseminate information on the work programme 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 the majority 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 limited communication channels and related information access. Increased dissemination activities, such as the provision of online information (see for instance 6.7.1. VDE Verlag drafts library; 6.7.3. ISGIS) regular newsletters and open workshops, could enhance the stakeholders' involvement in the process and increase the outreach of standardisation.

A central database of existing standards and current projects, besides access via the web page of individual committees, would help to 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 during the enquiry stage. Besides basic information about the responsible committee, planned publication date, title and abstract if available, etc., for current projects, the database should provide some information on the objectives of the work, why it has been initiated, and what major changes are to be expected in case of a revision.

Such information is important from both the point of view of standards implementation and also the participation in the process, but currently it does not seem to be readily available outside the respective committees. A classification of

[22] Most standardisation organisations provide a search mask on their web page that allows filtering standards by issuing committee and publication date. Filtering based on content classification is usually not possible, but requires a free text search. See for instance the IEC pages (the same tools is used by CENELEC):
http://www.iec.ch/dyn/www/f?p=103:104:0::::FSP_LANG_ID:25

documents and corresponding filtering possibilities would be valuable as well, as in the references of "Good practice 6". The STARGRID survey analysis[23] outcome shows that the industry representatives have a rather scarce awareness of the standardisation initiatives 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 targeted at a multidisciplinary system like the Smart Grid. Frameworks like SGCG, SMCG, eMCG should be maintained and supported beyond the time limits of the respective mandates and the Smart Grid architecture(s) developed by these groups should be promoted.

The concept of the "Steering Committee" should be fostered to supervise the activities of the various technical committees. Cooperation between industry initiatives active in Smart Grid standardisation and standardisation bodies should be enhanced by jointly developed standardisation mechanisms. Industry alliances are often more agile for developing standardised specifications and this mechanism can be an efficient strategy towards the formulation of a final standard.

Generally, the experts participating in the technical committees of a standardisation body 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. In this context, STARGRID supports the CEN/CENELEC recommendation[24] of including specific standardisation sessions in the structure of publicly funded projects. Recommendation to this task should be included in the H2020 and other research/innovation work programmes. It is a fact that standardisation can help bridge the gap 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

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

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

the whole value chain, innovation projects ensure development beyond the state of the art, share and promote the project outcomes among the stakeholders.

A publicly funded environment would guarantee the applicability of standards 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 to the implementation and validation of the reference use cases which are to be included in the 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.

6.5. Expected impact

- Bringing together the ideas and experience with products, materials, processes or services of different companies, academic experts, researchers, SMEs, consumers and regulators will lead to higher quality standards.

- Involving SMEs and end users will ensure consensus in standardisation activities.

- Involving all affected stake-holders in the development of standards will lead to a high acceptability and better applicability.

- 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, sharing and promoting project outcomes among 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 harmonised and transparent standardisation process.

6.6. Implementation of the recommendations

The maintenance and implementation of guidelines for stakeholders to be involved in standardisation remain the responsibility of national standardisation bodies. Funding agencies should promote standardisation contributions in innovation projects.

6.7. Good practices

6.7.1. VDE Verlag drafts library

The German standardisation organisation DKE offers free access to draft standards via its online standardisation library[25]. All drafts are visible during their public enquiry stage. This enables simple access to drafts and the possibility for stakeholders who could not participate in the committee itself to make comments. A notification can be set up for particular standard series.

6.7.2. IEC Smart Grid Standards Map

The mapping tool of the IEC provides a user-friendly graphical overview of standards related to the Smart Grid, including also non-IEC standards[26].

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

The STARGRID consortium has likewise created a database on Smart Grid standards[27]. 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 organization, SGAM cells, etc.

6.7.3. ISGIS

An example of good practice of coordination initiatives among Smart Grid stakeholders is the ISGIS: Italian Smart Grid Industry System[28], whose aims are:

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

6.7.4. EU projects

The development of the Voltage Control Use Case within the activities of FP7 project SmartC2Net[29] is a good example for an EC funded project.
Other examples to be mentioned are FINSENY[30], Green e-Motion[31] and Grid4EU[32].

---

[25] https://www.entwuerfe.normenbibliothek.de/; in German
[26] http://smartgridstandardsmap.com
[27] http://stargrid.iwes.fraunhofer.de
[28] http://www.solarexpo.com/files/convegni/convegni-e-seminari/2014/ISGIS_Italian%20Smart%20Grid%20Industry%20System_presentazione.pdf
[29] http://smartc2net.eu/
[30] http://www.fi-ppp-finseny.eu
[31] www.greenemotion-project.eu
[32] www.grid4eu.eu

7. R6: Harmonisation of the regulation and standardisation framework for DER interconnection rules

This recommendation is addressed to policy makers, regulatory authorities and standardisation bodies.

7.1. Summary

A coherent harmonisation of the regulation/standardisation framework is needed to ensure an effective, transparent and economically fair integration of DERs in the electric grid. The massive penetration of DERs into the grid requires an effective regulation to avoid putting the stability and security of the electric system at risk. In some countries the availability of a coherent regulation/standardisation framework to manage the related problems is particularly urgent. At EU level, on the regulation front, ENTSO-E is working on the set of network codes (NC), some of which have already passed the comitology stage. At the same time, 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, even if developed to some extent with contributions from independent views, may generate inconsistencies with the provisions and country-by-country discrepancies if it lacks a coherent and harmonised approach. Stakeholders of DER integration, mainly DER producers and system integrators and designers, warn against 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 imperative to avoid overlapping and confusion.

7.2. Main recommendation

Foster the coherent harmonisation of the regulations/standards framework to ensure an effective, transparent and economically fair integration of DERs in Smart Grids.

7.3. Corollary recommendations

- Expand and strengthen the cooperation between network operators (TSOs and DSOs) both in the definition and agreement of rules and requirements as well as in the demonstration of their feasibility and effectiveness through appropriate initiatives.

- Use European standards to provide guidance for a progressive alignment of the national legal frameworks avoiding product variance and facilitating further deployment of DER.

- The new standardisation Approach is suitable for the scope. The opportunity of elaborating EN 50438 and TS 50549 1-2 to be part of a set of harmonised standards should be explored.

- Elaborate a regulation and standardisation approach to foster the integration of prosumers equipped with small and low-cost equipment compatibly with the system operation needs.

- Upgrade the standardisation process so as to foster a more active and conscious participation of stakeholders (see 6. R5: Augmentation of the stakeholders' participation in the standardisation process).

- Pro-actively complete the standards framework including new needs coming from the extended integration of DERs at LV grid level, e.g. needs concerned with monitoring.

- Foster a mutual acknowledgment system, based on EU standards, for conformance testing related to Smart Grids and DER integration to promote the competitiveness of the industry and enhance the quality of products.

7.4. Explanation

The massive penetration of DERs into the grid, especially from non-programmable energy sources, is posing more and more challenges to the stability and security of the electric networks. These challenges require effective control and management rules. This fact is generally well acknowledged by all stakeholders (mainly regulatory authorities, network operators, DER operators and producers) and there is an increasing interest of the public on the matter, too.

A coherent harmonisation of the regulation/standardisation framework is needed to guarantee an effective, transparent and economically fair integration of DERs in the electric grid. Harmonised connection rules for DERs will boost the optimal use of the grid for the benefit of all participants. Furthermore, they will enable the best possible way of operating the network and the ancillary services which the operators are required to provide for ensuring continuation of the quality level of supply as imposed by regulatory authorities. It is essential that the greatest part of the cooperating network operators (TSOs and DSOs) agrees insofar on rules and standardised requirements and validates them through common demonstration initiatives requiring huge investments. Joint TSO/DSO R&D activities are strongly recommended, such as those already planned within the ENTSO-E and EEGI R&D roadmaps implementation plan[33] [34].

Harmonising DER interconnection rules has therefore the highest priority. Many requirements come from TSOs: they must be unified at European level due to the

[33] https://www.entsoe.eu/publications/research-and-development-reports/rd-implementation-plan/Pages/default.aspx
[34] http://www.gridplus.eu/eegi/roadmap_and_implementation_plan

interconnected transmission grid. Some actions at national level could be ineffective if they were not coordinated all over the European grid.

ACER, under solicitation of the EC, has entrusted ENTSO-E with the issuing of regulations at EU level and ruling the connection of generators to the grid. In March 2013, this led 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 adjust their national codes accordingly. With the aim of giving guidance to national implementation of the RfG NC, ENTSO-E has also issued a dedicated implementation guideline (October 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 (TS 50549-1:2015 “Requirements for generating plants to be connected in parallel with distribution networks - Part 1: Connection to a LV distribution network and above 16 A; and TS 50549-2:2015 “Connection to a MV distribution network”, which receive the provisions of the code with the objective of constituting reference for national implementations and further specifications of values and ranges of non-exhaustive requirements contained in the code itself.

Concurrently at national level, 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 for local areas specifying requirements for the connection of generators to the grid.

For instance in Italy, the relevant TSO – TERNA - has produced the so-called Allegato 70: “Technical regulation of system requirements for distributed generation” already in 2012, i.e. long before the final approval of the mentioned RfG code, whilst the national standardisation body issued the standards CEI 0-16:2012 and CEI 0-21:2012, which are dealing with the connection of generators respectively to the MV and LV grids. As a cascade effect, the Italian distribution network operator imposed mandatory connection/disconnection rules and thresholds on the energy producers connected to the grid, with an obligatory span time for the implementation. A similar situation exists in Germany, with the revision of the VDE AR N 4105 from 2011.

These running initiatives clearly reflect the rush 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.

Such national initiatives may also be motivated by an attempt to protect the national industry from the impact of new requirements introduced by European

standards, since they can defer the entering into force of conflicting prescriptions for a certain grace period.

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

7.5. Expected impact

Firstly, harmonisation and coordination of regulations/standardisation initiatives prevents security problems for the system. Security and stability is paramount for the EU interconnected electric system and sharing of essential requirements is the basic reason for issuing common (and national) network codes and corresponding standards.

Moreover, there is some concern from certain stakeholders, mainly generator producers, about a number of issues regarding the integration of DER, which could arise from a non-sufficiently harmonised regulations/standards framework at EU level. These issues deal primarily with:

- new technical solutions necessary to fulfil requirements varying country-by-country
- higher costs associated with the implementation of technical solutions
- competitiveness conditions to access the energy market.

The tendency to implement national regulations before consolidating the EU interconnection rules created country-by-country discrepancies. Of course, these discrepancies are justified by the need to deal with the local grid situations, but it is a fact that they may impact the industry's competitiveness by constituting obstacles to the free circulation of products in the EU. The following figure (Figure 4) shows the great differences within the EU regarding the LVFRT provisions for PV plants connected to the MV grid.

New versions, variants, explanation guidelines following one another may generate confusion if not suitably coordinated, even though they are justified by the need of tracking changes in reference documents. As an example, the Italian standard CEI 0-21 "Reference technical rules for the connection of active and passive users to the LV electrical Utilities" needed two updates since the approval in June 2012 before the consolidated version was published in December 2013. The latter shows inconsistencies with the Italian standard CEI EN 50438 "Requirements for micro-generating plants to be connected in parallel with public low-voltage distribution networks", published in July 2014 (receiving the EU standard EN 50438), which will prevail until April 2016. Furthermore, some parts of the same CEI 0-16, not fully developed yet thanks to their intrinsic difficulty, are still labelled as "under study".

At EU level, the already mentioned specifications CLC/TS 50549-1 and CLC/TS 50549-2, even if they are only technical specifications, will constitute reference guidance for national standards in the EU countries especially for those countries

which have not developed an own standardisation framework for DER connection yet. It is therefore advisable that possible discrepancies will be clearly solved in the subsequent documents in order to come to a full agreement on those specifications which are not yet accomplished. This is especially important, if the documents will become EN standards, as envisaged by some stakeholders. For instance, comments on the last committee draft of the TS submitted for review included evidence on important issues on which consensus is still lacking: in particular, some requirements imposed on generating units are deemed too stringent by the commenters since they exceed current standard values and/or the ENTSO-RfG requirements.

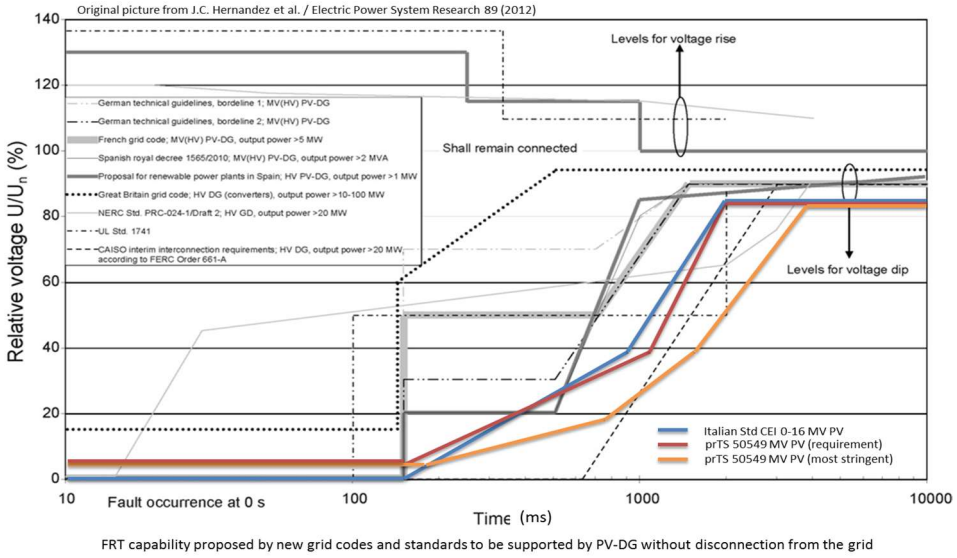

Figure 6: ***FRT capability proposed by new grid codes and standards to be supported by PV-DG without disconnection from the grid***

Lack of harmonisation may also cause higher costs for some stakeholders. It is a fact that the RfG code does not imply the full harmonisation of the rules across the EU and important country-by-country differences may remain. 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. Certain technical capabilities set in the network codes may constitute impediments on DER deployment in some countries as they can lead to increased equipment costs and to protracted connection procedures. Just as an example, the active participation of small generators (< 1 kW) is potentially considered in the RfG (and in the mentioned TS 50549-parts 1 and 2 recently published), whilst in Italy they are not included in the connection standards. These discrepancies may ultimately result in the need of oversized solutions in order to cover the requirements of different countries and therefore in higher costs and lower competitiveness.

Some stakeholders (DER operators and manufacturers) suggest that the level of requirements should be proportionate to the power of the equipment and some common minimum thresholds to their implementation should be fixed. This would mean that some provisions should not be applied to small and low cost equipment which have only little influence on the grid. This approach could be accepted, provided that it does not affect the operational needs of the system. Minimum thresholds should be fixed based on an operation impact analysis, which should not only take into account the power of the considered unit, but also the number (i.e. the cumulative power) of the units that can potentially be interconnected and controlled. Further, a cost-impact analysis should be carried out.

In any case, general requirements should be fixed by standards, ideally at EU level, that contain at least a minimum set of mandatory specifications. Details on the implementation could be left to specific agreements with the grid operator according to its needs and within the limits set by the applicable standards or grid codes. In some contexts these agreements could be managed by intermediary stake-holders, e.g. aggregators.

Manufacturers and DER operators could raise concerns if retrofitting were necessary for the integration of existing equipment in the grid according to the new rules. In general, such requirements should not be imposed without a prior cost-benefit analysis, demonstrating the real benefits. However, in many cases compliance with new requirements can be achieved by simple adaptations of the equipment 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 taken by the stakeholders and the analysis of specific standards related to integration issues, evidenced other aspects which are more tied to the consistency of the documents with the real application conditions, which also need to be considered in a harmonisation process. To take a single example, compliance tests have high relevance in the RfG code. Corresponding standards should provide clear and thoroughly detailed functional test specifications in order to not generate incongruent provisions for conformance tests with respect to the laboratory capacity. Designers and laboratory operators are the actors primarily concerned with this aspect.

Moreover, in accordance with an EU harmonisation policy, compliance procedures should be defined by a European standardisation approach in order to avoid additional challenges especially caused by low-size generators, i.e. third party product certificates should be allowed along the lines of “one standard, one test, accepted everywhere”. A mutual acknowledgment system for conformance testing is needed, so that a certification in one country could be extended to other countries. This would reduce costs and promote competitiveness of industry and enhance the quality of products.

The impact of this recommendation on main stakeholders is the following:

- 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 obstacles caused by disharmonic rules and approaches differing country-by-country.
- Designers and manufacturers promote well-defined and coherent technical specifications.
- Testing/certification labs ask for coherent requirements for conformance tests.

7.6. Implementation of the recommendations

Considering the complexity of the system itself and the stakeholders involved, often with conflicting interests, harmonisation of the standards framework in the case of Smart Grid requests a wide sharing and agreement on all options. The new approach of assigning standardisation topics to system committees, e.g. IEC[35], aimed at elaborating upper-level models (i.e. definition of system architectures) is deemed a good basis for an effective coordination of standardisation works in complex systems like the Smart Grid. This could lead to a consideration of the upgrading of the standardisation process, with modifications that allow a stricter and more frequent consultation of the stakeholders.

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

The proactive role of the stakeholders is indispensable to the process: instruments like technology platforms and joint industry initiatives are strategic. Participation in standardisation-targeted EU collaborations and multidisciplinary projects is deemed an economical and effective way forward. Specific standardisation-targeted calls could be launched within the current research programmes (e.g. H2020). The process timing should not be more time consuming than the current standardisation process. A further advantage is the possibility, within the projects themselves, of demonstrating/validating the proposed provisions and assessing their impact.

In general, a more active and conscious participation of stakeholders should be fostered, as well as the adoption of measures and instruments to allow for a more deep and extended consultation of the involved stakeholders.

[35] http://www.iec.ch/about/ activities/systemswork.htm

For instance, ICT tools, like webinars, could be more extensively used to this extent during the standardisation process. This will guarantee more transparency and non-discriminatory conditions, instead of unilateral decisions driven by more influential stakeholders. For proposals on how to increase transparency in the standardisation process see also recommendation R5: Augmentation of the stakeholders' participation in the standardisation process.

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 CLC/TS 50549-1 and CLC/TS 50549-2 technical specifications towards complete 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.

A possible strategy, coherent with the new standardisation approach, is to generate a set of DER interconnection standards, including EN 50438 and future EN 50549, as harmonised standards. In normative appendixes, these could also include national settings and requirements as well as detailed specifications for conformance tests.

Although considering the reservations and reluctances as previously mentioned, there is, in general, the need of speeding up the completion of the regulation and standards framework for specific aspects, both at EU and national level. For instance, monitoring the state of the system is a prerequisite for the management of the DER integration and is becoming more and more complex. Difficulties already occur at MV level, but will drastically multiply when the monitoring needs will be extended to the LV. A set of measurements and information can already be obtained from advanced inverter technologies. However, to guarantee the quality of the supply and the security of the entire system, it will be necessary to define specifications of the algorithms/methods used for the measurement of each electric value (voltage, frequency, current, etc.): excessive requirements of the monitoring may result in unpredictable results due to the fact that the very basic measurements methods are neither defined nor standardised. Finally, harmonised standards could also impact features of the controller and measurement concentrator at the station level and cause potential problems regarding the physical location of the instrument, the architecture of the ICT solutions, the information needed, the aggregation criteria of the measurements or their connection to the communication infrastructure. In Italy for instance, there are currently as many as 500,000 secondary stations that will potentially host this technology. Some of these aspects still request specific investigation through related EU funded projects.

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

A mutual acknowledgment system for conformance testing should be implemented for accreditation of laboratories dealing with Smart Grids and DER integration. This system should be based on a set of EU standards and procedures, similarly to the initiatives already implemented at EU level (e.g. through IECEE[36] and CAB[37]).

7.7. 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 (2015-2016).

[36] http://www.iecee.org/html/AboutIECEE.htm
[37] https://cabforum.org/

Acknowledgements

In October 2014, a preliminary report on recommendations was handed out to experts from various branches of the Smart Grid ecosystem, and their feedback has been used in this updated version of the report. The STARGRID team is very grateful for this support.

Disclaimer: STARGRID – Standard Analysis supporting smart eneRgy GRID development – was supported by the 7th Framework Programme of the European Commission.
STARGRID is solely responsible for this publication, it does not necessarily reflect the opinion of the European Commission. The European Commission is not responsible for any use that might be made of this publication.

Publisher: Technology & Science Publishers - Zühlcke & Strauß GbR
Wegmannstr. 31, D-34128 Kassel, Germany

STARGRID is a collaborative Coordination and Support Action funded by the European Commission under the 7th Framework Programme, which provided a comprehensive analysis of the current Smart Grid standardisation efforts, including new industry developments and initiatives. The project partners are Fraunhofer Institute for Wind Energy and Energy System Technology (IWES) (coordinator), Romanian Standards Association (ASRO), European Distributed Energy Resources Laboratories (DERlab), Ricerca sul Sistema Energetico SpA – RSE and TECNALIA Research & Innovation.
Project duration: October 2012 – January 2015.

STARGRID has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement No 318782.