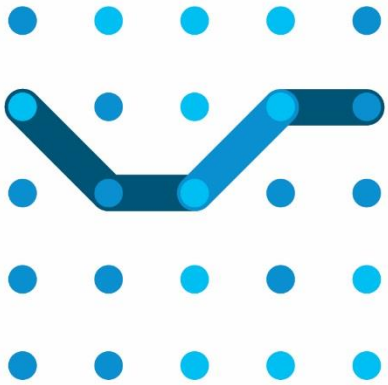


bridge

HORIZON 2020

Cooperation between Horizon 2020 Projects in the field of Smart Grids and Energy Storage

Main findings and recommendations

Data Management Working Group

July 2019

This report has been elaborated with the support of DOWEL MANAGEMENT within the INTENSYS4EU Coordination and Support Action. The INTENSYS4EU Project supports the BRIDGE activities and has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 731220.

Disclaimer: While aiming to consider the new provisions stemming from the Clean Energy Package (CEP), the report may not entirely reflect the new rules. Proposals for follow-up are without prejudice to main short-term priorities decided during the General Assembly of BRIDGE held in March 2019.

Authors of the present report

Name	Organization	E-mail	Project
Olivier Genest	Trialog	olivier.genest@trialog.com	Interflex
Lucas Pons	Grupo Etra	lpons.etraid@grupoetra.com	CROSSBOW
Paul Valckenaers	UCLL	paul.valckenaers@ucll.be	STORY
Florin Crihan	Siveco	Florin.Crihan@siveco.ro	inteGRIDy

Leading team of the BRIDGE Working Group on Data Management

Chairman of the Working Group

Name	Organisation	E-mail	Project
Marco Baron	ENEL	marco.baron2@enel.com	COORDINET

Rapporteur

Name	Organisation	E-mail	Project
Olivier Genest	Trialog	olivier.genest@trialog.com	INTERFLEX

Guidance from European Commission

Name	Organisation	E-mail
Mario Dionisio	DG.ENER	Mario.DIONISIO@ec.europa.eu
Patricia Arsene	DG.CNCT	patricia.arsene@ec.europa.eu
Mariana Stantcheva	EC/INEA	Mariana.STANTCHEVA@ec.europa.eu

Editor

Name	Organisation	E-mail	Project
Ilaria Rosa	RSE	Ilaria.Losa@rse-web.it	INTENSYS4EU

Table of Contents

Introduction to the BRIDGE initiative

Purpose of the initiative

BRIDGE is a cooperation group involving Low Carbon Energy (LCE) Smart-Grid and Energy Storage projects funded under the Horizon 2020 program over the last five years (2014-2018). It aims to foster the exchange of information, experience, knowledge and best practices among its members.

BRIDGE wants to provide field experience, feedback and lessons learned from the participating projects to help overcome the barriers to effective innovation. It aims to gather coordinated, balanced and coherent recommendations to strengthen the messages and maximize their impacts towards policy makers in view of removing barriers to innovation deployment.

BRIDGE Working Groups

This cooperation group involves four different types of activities (Working Groups) addressing cross-cutting issues enlisted as follows:

Data Management

- **Communication Infrastructure**, embracing the technical and non-technical aspects of the communication infrastructure needed to exchange data and the related requirements
- **Cybersecurity and Data Privacy**, entailing data integrity, customer privacy and protection
- **Data Handling**, including the framework for data exchange and related roles and responsibilities, together with the technical issues supporting the exchange of data in a secure and interoperable manner, and the data analytics techniques for data processing

Regulations

- As regards to **energy storage**, the regulatory framework needs to provide clear rules and responsibilities concerning ownership, competition, technical modalities and financial conditions, for island and mainland cases
- In terms of **smart grids**, regulatory challenges arise regarding the incentives for demand-side response, commercial arrangements, smart meter data, etc.

Customer Engagement

- Customer Segmentation, analysis of **cultural**, **geographical** and **social** dimensions,
- **Value** systems - Understanding Customers
- **Drivers** for Customer **Engagement**
- Effectiveness of Engagement Activities
- Identification of what triggers **behavioral changes** (e.g. via incentives)
- The **Regulatory** Innovation to Empower Consumers

Business Models

- Defining common language and frameworks around **business model description and valuation**
- Identifying and evaluating **existing and new or innovative business models** from the project demonstrations or use cases
- The development of a **simulation tool** allowing for the comparison of the **profitability of different business models** applicable to smart grids and energy storage solutions is being developed and tested by the Working Group members

Projects involved in the Data Management Working Group

Presentation of the report

This report aims at identifying the main barriers faced when handling data within smart grid and storage systems, and detailing recommendations for each barrier. The full life-cycle of the data is considered, and also interoperability, cyber-security and privacy transversal point of views are taken into account.

The results detailed in this document are based on the answers from 16 smart grid and storage projects to a Data Handling questionnaire, in the scope of the BRIDGE Data Management WG.

Barriers and recommendations are covering technical, technological, legislation, market, ethical and strategic issues.

Scope of Data Handling

This chapter details the scope of this “Data Handling” analysis.

Full data life-cycle

This report aims at covering the full data life-cycle:

- **Capture**: the data is captured thanks to a sensor or user input. It is then created within the capturing device, ready to be exchanged with other devices.
- **Exchange**: the data is exchanged between devices or actors by relying on two levels of interoperability. The communication interoperability corresponds to the communication protocols used for the transmission of the data from the originator to the destination. The semantic interoperability corresponds to the way the data is modelled to carry its semantic information (i.e. its meaning). Both levels are required and need to be taken into account to allow a proper data exchange between actors.
- **Storage**: the data may be stored by the data destination, e.g. for future use or to provide access to it. This data may be stored “as is” or may be post-processed e.g. to anonymize or aggregate it.
- **Access**: the access to the data is provided depending on the contractual agreements, the sensitivity of the data and the local regulation.

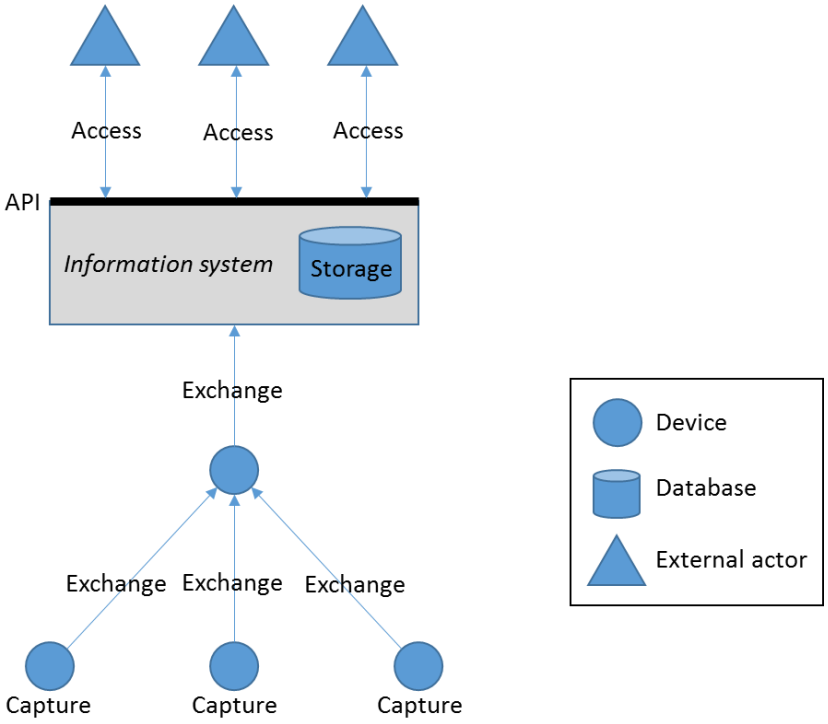


Figure 1 : Data life-cycle

Focus on some selected data flows

Many data flows may occur in a smart grid system. As an example, the NIST Logical Reference Model (LRM) [NISTIR 7628] has identified 137 interfaces, between 47 different actors.

This report focuses on four data flows, which have been identified as the most common interfaces between the contributing projects, based on the answers received to the 1st Data Handing questionnaire in May 2018[1] :

1. **DSO to Aggregator**: this data flow mainly covers flexibility request from the DSO to the aggregator.
2. **Aggregator to Prosumer**: this data flow mainly covers demand-response commands from the aggregator to the prosumer.
3. **Prosumer to Aggregator**: this data flow mainly covers demand-response feedback from the prosumer to the aggregator.
4. **Prosumer to DSO**: this data flow mainly covers metering and grid quality measurements from the prosumer to the DSO.

When considering the Smart Grid Architecture Model (SGAM), as defined by CEN-CENELEC-ETSI under M/490 mandate, the data flows can be schematized as follows:

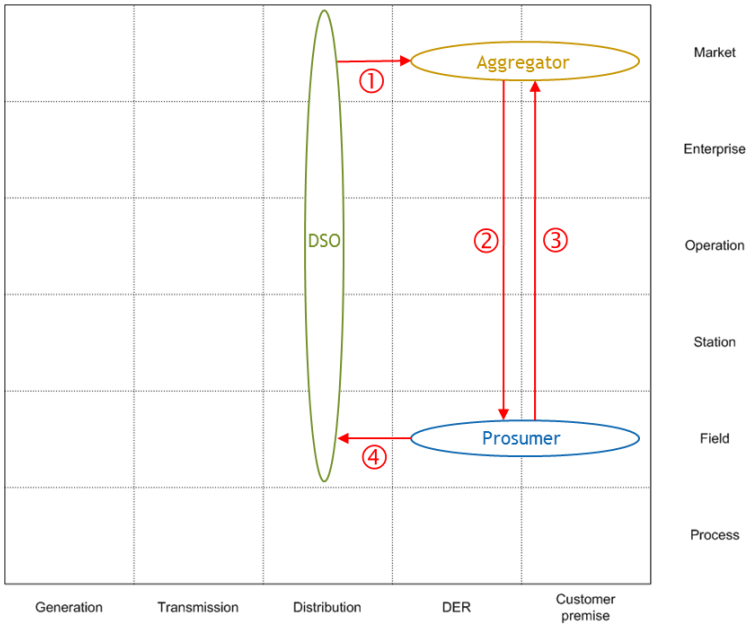


Figure 2: Data flow focus of this report depicted in SGAM diagram

Transversal topics

This report covers not only the data handling functions from data capture to data access, but also the two main transversal requirements:

- **Interoperability**: *"Interoperability is a characteristic of a product or system, whose interfaces are completely understood, to work with other products or systems, present or future, in either implementation or access, without any restrictions."*[2] Interoperability is required to allow several actors, systems or sub-systems to exchange data and understand the underlying

[1] It has to be noted that, at that time, most of the contributing projects were distribution-oriented (H2020 calls LCE-07-2014 "Distribution grid and retail market", LCE-08-2014 "Local / small-scale storage", LCE-02-2016 "Demonstration of smart grid, storage and system integration technologies with increasing share of renewables: distribution system", etc.)

[2] Source : http://interoperability-definition.info/en/ (AFUL Interoperability WG)

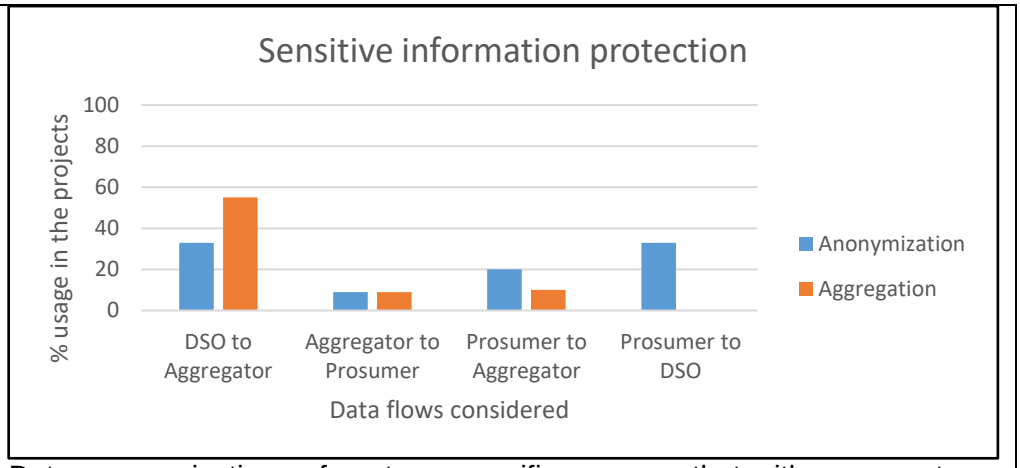
information the exact same way. It is a key requirement for any system in which several actors are handling and sharing data.

- **Cyber-security and privacy**: Cyber-security is required to ensure the confidentiality, authenticity and integrity of the data. Privacy practices, including data protection, are also required to ensure that the handled data are exchanged and accessed in compliance with the contractual agreements between the commercial actors and the General Data Protection Regulation (GDPR) as far as citizen data are concerned.

Main findings and barriers from BRIDGE projects

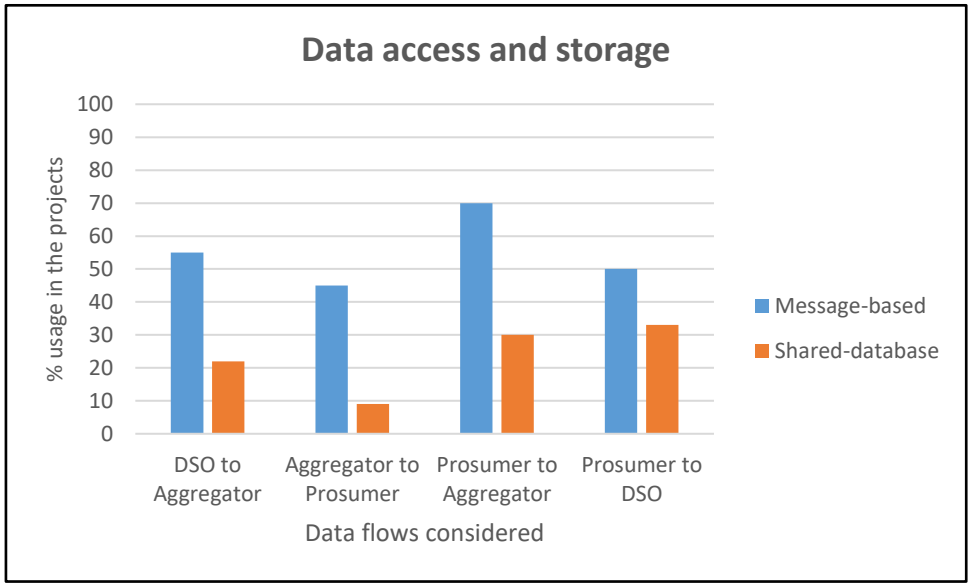
Technical / technological

Topic	Data access and storage
Name	**Handling of sensitive information**
Barrier	GDPR specifies some principles that may affect the flow of personal data among actors in the smart grid. 1) **Purpose limitation principle** prevents from using personal data for new purposes if they are 'incompatible' with the original purpose for collecting the data. The original purpose could be well defined and know by the user but the transmission of these data to other actor for other purpose is not allowed by default. 2) **Data Minimisation principle** states that data collected and processed should not be held or further used unless this is essential for reasons that were clearly stated in advance to support data privacy This affects and limits the exchange of sensitive data between actors in the smart grid system. The results of the questionnaire show the percentage of projects that exchange personal sensitive information in the considered data flows (1 to 4). The numbers are respectively: 11%, 45%, 83% and 100%. When such type of data is exchanged, the aforementioned GDPR principles should be considered and all the actors must do the necessary to **handle and distribute the sensitive information in an appropriate way**. These criteria impose restrictions on the capture, storage and distribution processes that should be carefully analysed by the partners.
Recommendation	Different techniques exist to ensure the privacy of peoples' data when it has to flow to another actor. These techniques could fall in any of these two categories: - *Physical*, where the system somehow creates a logical boundary and ensures the data does not flow out of it (geo-blocking, de-military zone-only access, secure communication, etc.) and - *Logical*, where the information is **sanitized** before exchanged, meaning that it has to be transformed before it is exchanged, e.g. by encrypting or removing personally identifiable information from data sets, so that the people whom the data describes remain anonymous. Physical mechanisms could not be always feasible, because it imposes physical restrictions and is hard to implement. According to the questionnaire, the most popular techniques are **anonymization** and **aggregation:**



Data anonymization refers to a specific process that either encrypts or removes personally identifiable information from data sets, remaining anonymous the people whom the data flows.
Data aggregation concerns the process followed for their gathering and their representation in a report-based format that summarizes the main outcomes/most important information of all the received information, upon the requirements set by each service provided.
It is natural that data flows 2 and 3 have fewer usage of these techniques, since they require for their processes the exchange of detailed (and possibly sensitive) information between prosumer and aggregator in both directions, and there is always a contract formalizing this relation. The other data flows that involve DSO are more restrictive because the DSO business do not normally require to have access to individual information nor have a contract signed with the end user, and thus data sanitization is very likely required before exchanging with other parties.
The low percentages of usage of the techniques show that more effort must be given in the projects to these processes.
Sometimes the needs of using these techniques are relaxed by requiring in the projects the end users to explicitly give their consent to the transmission and usage of their personal data (100%, 81%, 100% and 83% respectively). Although this solution could comply with GDPR and be acceptable in the pilot projects, the usage of such techniques should still be more carefully investigated as the explicit user consent solution might not be feasible in real systems. For instance GDPR states that consent needs to be freely given and specific per purpose; actors like DSO that are legally entitled to capture real time data for their internal processes (even with no explicit consent from end user), may not use this grant to freely distribute the sensitive data to other actors, and an update of the consent conditions could be hard to explain and obtain from the end users.

Topic	**Data access and storage**
Name	**Data management model**
Barrier	There is not a **common strategy for data management model**. Some projects opt for a *shared database* model, and others opt for a *message-based* integration of remote systems.

Recommendation	The questionnaire depicts that the projects have opted mainly for a message-based integration:  The recommendation is to go for a message-based model, because of multiple benefits: loose coupling, better security mechanisms and much better scalability. **Shared-database integration model** is a model were the data repository is unique and both ends exchanging information just write and read the same resource, acting as data generator and receiver respectively. In the **message-based integration model**, the raw physical data repository is only accessed by some data services that allows other processes and services to query for pieces of information, acting as a historian or current data holder. The data sent to the clients is tailored to the needs and permissions of the receiver, and thus tasks like data transformation, aggregation or anonymization is easily achieved by requiring all data flows to go through these data services. The side benefit on this is that the attack surface area is reduced. A common variant of this messaging architecture is the one based on publish-subscribe pattern, where the actor requiring information expresses their willing to receive some information whenever it is available or changes. Hohpe [HOPHE] defined 4 different integration approaches among different applications: File Transfer, Shared Database, Remote Procedure Invocation and Messaging, each one with its distinct advantages and disadvantages. Although the message-based approach may seem preferable in the performed survey among the EU smart grid technology projects due to its simple implementation, this may not be the case on a real scale smart grid. In such system, the amount of data gathered is huge and the existence of duplicate data may be prohibited. As Kappagantu [KAPPAGANTU] states “from employing smart meter that enables reading at each min instead of once in a month increases the data almost 3000 times”. Thus, big-data database schemes have been suggested, many of them cloud-based. Even then, there are attempts to compress the stored data, and a survey can be found by Wen [WEN]. For example, in SMILE project in the Orkney demo site, the Event Hub service of Microsoft Azure platform will be used for telemetry, data management and for other smart grid services as well.

Topic	**Interoperability**
Name	**Information model interoperability**
Barrier	The ***information model*** is broadly flagged as a serious barrier. To quote a remark describing the present situation: "*A lot of standards are existing in parallel; and you find a lot of proprietary models*".
Recommendation	More standardisation does not appear to offer a solution. More standards would only exacerbate the problem. Pressuring parties and nudging people to use or support standards first requires a more in-depth understanding to be effective/beneficial; failure to appreciate the complexity and subtleties of applications causes serious damage whenever core business (i.e. whatever determines effectiveness, efficiency and/or competitiveness) is involved. Naïve usage and/or indiscriminate enforcement of badly-suited standards is only adequate/beneficial for non-core business activities (e.g. invoicing). When (inadequate) information models collide with harsh reality, significant losses become inevitable when the effectiveness and/or competitiveness is affected. Efforts to achieve interoperability have been delivered for decades by highly motivated and skilled professionals. There can be little doubt that the communities involved have been "*doing things right*" for many years. Yet, the results are not addressing the challenges adequately. To address this wicked challenge, it is necessary to reflect about and dedicate efforts to "*solving the right problem*" by pursuing interoperability with the ultimate goal in mind (i.e. to have the energy systems cooperate) and by looking beyond the ICT dimension (incl. semantics).

Topic	**Interoperability**
Name	**Information communication interoperability**
Barrier	The ***information communication*** is enjoying general progress in this domain (e.g. reflected by Wi-Fi and 4G being widely available). To quote a remark from a project: "*Existing standards already quite okay*".
Recommendation	Communication – its availability, support, ease-of-use – has improved significantly in recent years. Smart energy has enjoyed and benefited from this progress. To preserve this enjoyable situation, smart energy needs to speed up its adoption of widely available means of communication (e.g. MQTT, REST API, etc.) and avoid inventing its own solutions (which fail to recruit sufficient users). It shall interact with the wider IT community to have it adopt and widely support functionality that is needed/desired (and currently absent).

	Practically, engineering teams need to welcome the required IT expertise and “listen to these IT experts”. In other words, when only energy experts and industrial automation experts decide about the IT, a significant risk remains that communication constitutes a more serious obstacle than necessary (e.g. when adopting an obsolete information technology that refuses to operate in a subordinated role/manner). Today, IT is a top-level concern and decisions are not to be taken solely from an energy (industrial equipment) perspective.

Topic	**Cyber-security and Privacy**
Name	**Grid communication infrastructure security**
Barrier	With smart grid we are looking at two types of communication: Home Area Network (HAN) the one that connects the smart meter with other potential (in-house) smart devices and Wide Area Network (WAN) connecting smart meters, services and electric utility providers. To some extend smart grid actors/stakeholders agree upon the necessity of designing a secured grid **communication infrastructure** as this requires a common approach between countries and manufacturers. This approach is vulnerable on the level of communication between utilities and customers and on data transmission level. Altering or distorting data transmission from smart meters affects the entire value chain from consumer, prosumer, DSO to TSO or energy communities and introduces new threats and attack vectors due to the lack of standardization, mainly encryption standardization.
Recommendation	Context Starting from the SGAM architectural perspective [CEN14] and the graphical representation at http://smartgridstandardsmap.com/ this topic aims at exploring all security aspects corresponding to each specific layer: • **Component Layer**. (participating components in the smart grid context: device, networking, physical infrastructure) • **Communication Layer** (protocols and mechanisms for the exchange of information between components in the context of the underlying use case, function or service) • **Information Layer** (data format, data type and data models) • **Function Layer** (describes functions and services including their relationships from an architectural viewpoint) • **Business Layer** – (dynamic behavior, semantic interoperability)

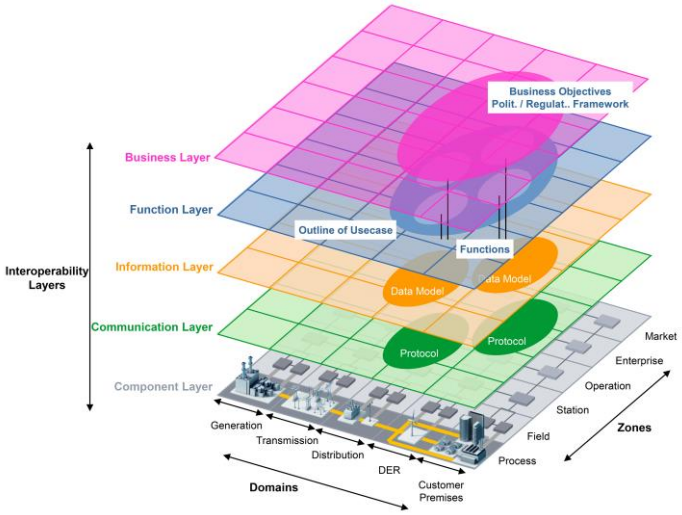


Figure 3. SGAM Framework – Component reference architecture [CEN12]

The standards from the [SGC] represents the starting point for an in-depth analysis of the security in terms of vulnerabilities and threatens for each layer addressing each and every component/item.

- **Function layer.** Security solutions should be designed to defence against man-in-middle, connection hijacking, replay, reflection, and denial-of-service (DOS) attacks on unsecured networks. https://tools.ietf.org/html/draft-weis-gdoi-iec62351-9-04
- **Business layer**. Lack of accessibility of standardization documents considering security requirements and solutions in energy field leads to poor risk assessment and vulnerabilities of smart grids.
- **Component layer**. Investing in digitization of components requires the assessment of associated risks for DSOs as well as large investments and R&D efforts.
- **Information and Communication layer.** As DSOs operate critical infrastructure (equipments) results of vulnerabilities assessments should be confidential.

Based on the proposed list of security requirements and solutions two prospects are relevant for cyber security [SGC]:

- **Relevance for Products**: The standard directly influences component and/or system functionality and needs to be considered during product design and/or development. It addresses technology to be used to integrate a security measure.
- **Completeness**: The standard addresses not only one specific security measure but addresses the complete security framework, including technical and organizational means.

Recommendations

- The impact of security solutions considering the energy efficiency should be explored.
- Specific standards considering both security requirements and solutions (as listed in M490) should be accessible to all potential business actors in energy field.
- Specific guidelines for cyber security solutions for smart grids should be created.

	- Initiatives (strategy, funding, feasibility study, case study, incentives) on Smart Grid Cyber Security should be launched. - The accountability distribution of IT security solution among IT solution provider and DSO should be assessed. - The awareness on the importance of cyber security in DSO environment should be raised. - The existence of solutions to secure data (e.g. encryption) inside smart grid communication infrastructure should be assessed. - Minimum requirements and standards for the security layer of a smart grid communication infrastructure or smart grid devices should be defined. - A standardized encryption scheme between system components of smart grid should be investigated.

Legislation

Topic	**Data access and storage**
Name	**End user rights**
Barrier	There are different requirements that should be fulfilled by the data management process in order to be considered compliant with the GDPR policy. One of them is the compliance with the **right of the end users with regards to their personal data stored** in the system. The rights are: - Information - Access - Rectification - Withdraw consent - Object - Automated processing - To be forgotten - Data portability The need for featuring tools and mechanisms for the users to apply for these rights could also be a barrier, especially if the IT systems do not consider this possibility from the very beginning.
Recommendation	All the energy projects must consider these, even though their nature of a research project could relax a little bit the processes. The questionnaire depicts that the projects allow data can be changed on users' request in different percentage according to the data flow: 11%, 27%, 40% and 50% respectively. Also, the projects normally advertise end users on their data storage and usage (22%, 72%, 100% and 83% respectively) To better handle this, the data store must be tailored so that the request of the end users rights is possible and do not break the rest of the system. In real projects, the mechanisms to provide end users a way to request for the application of their rights should be implemented and made publicly available.

Topic	Interoperability
Name	**Regulation impact on interoperability**
Barrier	Regulation remains a serious barrier, certainly when it causes/reflects a power imbalance among the parties involved. To quote a remark from a project: "Authorization issues and service tariffs directly impact on the **viability".** In other words, inadequate regulation will not only hold back developments; it is able to prevent desirable and much-needed progress from happening.
Recommendation	Identify where regulation is clearly unsound, e.g. when a neighbourhood located at the outer edges of a distribution grid needs to pay a DSO to improve the behaviour of their subnet/line, the regulation needs improving. The gap between reality and a regulation's view on reality needs to become as small as possible, e.g. when costs are related to capacity, billing shall not be based on consumption. Tax schemes must not induce undesirable behaviour. Next to obvious opportunities and needs to improve, a more in-depth understanding (cf. information model in interoperability) will be instrumental for the improvement of regulations. Here, a common concern is to capture relevant reality without inducing a specific purpose too early and deeply. Indeed, to cope with future developments and to keep the options open, mirroring reality in a lean fashion is a valid course-of-action.

Topic	Cyber-security and privacy
Name	**Cross-border law enforcement in energy field**
Barrier	The potential existence of **vulnerabilities** into smart grid technological solutions could allow unauthorized persons to access personal/sensitive data from consumer profile and historical data stored. Therefore, it is required to limit the amount of collected and stored data, or to rely on aggregated/consolidated data. However, meter data must typically be retained for many years to satisfy emerging regulatory requirements.
Recommendation	A clear and coherent regulation should be available to implement solutions of cyber security, including prevention, monitoring and rapid reaction mechanisms that minimise the damages of cyber attacks and unauthorized accesses to sensitive data. Additionally, cross-border law enforcement should be pushed forward in the field of energy. Existing technologies are actually sufficient, e.g. TLS v1.2 and above, but need to be incorporated into solutions.

Market behaviour

Topic	Interoperability
Name	**Interoperability requirement from market**
Barrier	Equipment and installations often are lagging the state-of-practice in (general) ICT. Market behavior is the root cause. Often, being competitive in the energy domain suffices (e.g. top-quality sensing, best-in-class mechanical reliability) and it does not require the vendor to offer state-of-the-art IT services. The market does not induce equipment vendors to offer up-to-date ICT when the available and really obsolete IT suffices (e.g. RS232C) to be competitive.
Recommendation	This issue is insufficient to warrant market intervention (e.g. deny access to the market when only supporting obsolete ICT). However, the issue can be made more visible by listing it as deprecated technology, denying access to quality (green) labels, etc. Importantly, obsolete IT that is poorly suited to be deployed in a subordinated role can be flagged as the worst case. Note that the issue scales from “not really important” in large installations (expensive but in small numbers) to “determines the viability” for small installation deployed in very large numbers. A research and innovation project will have the resources to cope obsolete IT (and implement a work-around) but the subsequent exploitation will falter when obsolete technology equals high installation and maintenance costs.

Topic	Cyber-security and privacy
Name	**Consumer behaviour in digitalization of energy grids**
Barrier	Several countries are facing a strong **consumer resistance** in installing smart meters due to invasion of privacy. At device level, with pseudo-professional devices, unauthorized persons may access and read remotely consumption/generation data.
Recommendation	<u>Context</u> The business layer represents the business view on the information exchange related to smart grids. SGAM can be used to map regulatory and economic (market) structures and policies, business models, business portfolios (products & services) of market parties involved. Also business capabilities and business processes can be represented in this layer. In this way it supports business executives in decision making related to (new) business models and specific business projects (business case) as well as regulators in defining new market models [CEN12] [CEN12]. Modernization of energy infrastructure (smart grid) is part of the way of life technology is offering to us. Installation of smart meters puts an end to estimation billing providing a real perspective on electricity consumption in “real-time” (most of the deployed smart meters offer reading at 15 minutes interval). Precise consumption measurements, real-time meter data access

	and anti-fraud detection allow utilities to avoid unnecessary technical losses. [INT18] Recommendations Each smart metering manufacturer or operator should ensure data protection solutions for devices as they are prone to cyber-attacks. These data protection solutions should cover device protection, communication protection and information system protection, at both physical and logical levels. Also, communications should be performed to explain how privacy is tackled by smart metering systems and disprove rumours and fake news. This problem is inherited in every smart device in our IoT days. This can be limited by informing the users not to use devices of unknown origin or manufacturer, along with them asking for accredited products.

Topic	**Cyber-security and privacy**
Name	**Prosumers engagement in digital energy grid**
Barrier	As the consumer has access to detailed own consumption data and to price rates, it becomes aware of the available options to use electrical energy efficiently and maybe to reduce the cost of own invoice. Providing the user with data that create direct connection between own consumption and billing may encourage behavioral change and increase energy efficiency. Smart meters equipped with demand response features provide consumer with the possibility to save energy during peak demand events. [INT18] Personal data of prosumers are stored in databases with controversial access rights. These data might include consent letters with sensitive data such as signatures and tax information.
Recommendation	Define strict policies of access rights with user-based classification and complex authentication system has to be implemented in repositories that store personal and sensitive user data.

Ethical

Topic	**Data access and storage**
Name	**GDPR impact on data access and storage**
Barrier	The GDPR also defines the **storage minimization principle** and states that sensitive data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. In that sense actors are expected to **limit the processing, collect only that data which is necessary, and not keep**

	personal data once the processing purpose is completed. This would effectively bring the following requirements: - Forbid processing of personal data outside the legitimate purpose for which the personal data was collected. - Mandate that no personal data, other than what is necessary, be requested. - Ask that personal data should be deleted once the legitimate purpose for which it was collected is fulfilled. All the projects must adhere to these requirements in their data handling mechanisms and this may affect the internal processes of the actors involved if not consider appropriately.
Recommendation	The questionnaire depicts that the projects are currently implementing some of the requirements in the considered data flows: A process for destroying historical data periodically is used for the projects implementing the different data flows (22%, 27%, 40% and 50% respectively). More effort is needed in the removal of personal data when the processing is finished. This does not necessarily mean to delete all the historical data, but can link to the anonymization or aggregation of these data after it has been used (for instance, the time resolution of the data can be reduced after the processing is finished, aggregating by hour or day). The purpose of the data exchanged must be clearly identified. The questionnaires reflect that the intended usage of the data in the different data flows is similar in all the projects (grid management for DSO data flows, flexibility and DR for aggregators and prosumers, etc.); Nevertheless, the research projects also explore alternative usages and business models for these data. This is also legitimate, but in any case, the boundaries of the data, their persistence their resolution and the fields that are really required must be identified in the most restrictive way possible (the minimum required by the processes and no more). The recommendation for overcoming this barriers is **to consider them from the very beginning** and to keep end user rights related-processes at the same level as the other required processes.

Topic	**Data access and storage**
Name	**Impact of prosumers' data collection**
Barrier	The way that data are collected from the prosumers' premises should not interfere and disturb their convenience in the houses or other buildings.
Recommendation	Data gathering by the DSO or Aggregator from the Prosumer should be accomplished by equipment that has small physical size, use minimum local resources (electrical power and bandwidth) and is safe for the installation areas at all weather conditions (certified equipment only). All the maintenance and upgrade activities and non-remote data collection should be executed by experienced personnel. The prosumer should be fully informed about the foreseen maintenance periods and the possibilities for unexpected events that required the presence of the technical staff at the premise.

Strategic

No strategic barrier identified so far.

Conclusion and recommendations

In this report, based on answers from 16 contributing projects, 13 barriers have been identified, covering Technical/technological, Legislation, Market behaviour and Ethical points of view.

The recommendations from the contributing projects and the BRIDGE Data Management WG experts define how the current or future innovation projects may overcome these barriers when deploying, testing, scaling up or replicating smart grid and storage systems.

This work still needs to be enhanced by covering additional data flows and additional points of view.

List of references

[NISTIR 7628]: NIST / Smart Grid Interoperability Panel / Cyber Security Working Group, “Guidelines for Smart Grid Cyber Security”, September 2010.

[HOHPE] Gregor Hohpe and Bobby Woolf “Enterprise Integration Patterns: Designing, Building, and Deploying Messaging Solutions”, Addison-Wesley Professional, 2004.

[KAPAGGANTU] R. Kappagantu and S. A. Daniel, “Challenges and issues of smart grid implementation: A case of Indian scenario,” Journal of Electrical Systems and Information Technology, Feb. 2018.

[WEN] L. Wen, K. Zhou, S. Yang, and L. Li, “Compression of smart meter big data: A survey,” Renewable and Sustainable Energy Reviews, vol. 91, pp. 59–69, Aug. 2018.

[CEN14] CEN-CENELEC-ETSI Smart Grid Coordination Group (2014) SGCG/M490/G_Smart Grid Set of Standards 24, Version 3.1

[CEN12] CEN-CENELEC-ETSI Smart Grid Coordination Group Smart Grid Reference Architecture https://ec.europa.eu/energy/sites/ener/files/documents/xpert_group1_reference_architecture.pdf

[SGC] SGCG/M490/G_Smart Grid Set of Standards Version 3.1

[INT18] D2.5 D2.5. Smart Grid Deployment, Infrastructures & Industrial Policy applicable to the inteGRIDy pilot, http://integridy.eu/content/d25-smart-grid-deployment-infrastructures-industrial-policy-applicable-integridy-pilot-cases

List of Acronyms and Abbreviations

API	Application Programming Interface
DR	Demand Response
DSO	Distribution System Operator
GDPR	General Data Protection Regulation
ICT	Information and Communications Technology
IT	Information Technology
LCE	Low Carbon Energy
MQTT	Message Queuing Telemetry Transport
NIST	National Institute of Standards and Technology
REST	REpresentational State Transfer
SGAM	Smart Grid Architecture Model
TLS	Transport Layer Security
TSO	Transmission System Operator
VPN	Virtual Private Network
WAN	Wireless Area Network
WG	Working Group

Report developed by DOWEL Management
within the INTENSYS4EU Coordination and Support Action
(H2020 Grant Agreement n° 731220)

More information at http://www.h2020-bridge.eu/