Cybersecurity and Resilience

Data Management Working Group

December 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.

Document Information (Intensys4EU project)

Report number	D3.12.e
Report name	Cybersecurity and Resilience - Data Management Working Group
Reviewed by	DOWEL Management
Date	December 2019
Work Package and Task	WP3, task 3.4
Lead Beneficiary for this Deliverable	BRIDGE Data Management Working Group

Version Control

Version	Date	Authors	Description of Changes
V0.1	11/10/2019	see below	First draft based on BRIDGE projects contribution
V0.2	21/11/2019	Olivier Genest	Second draft based on EC feedback and the conclusions of October 23rd meeting
V1.0	10/12/2019	Olivier Genest	First complete version
V1.1	18/12/2019	Stephanie Petit	Final review of the document

Authors of the present report

Name	Organization	E-mail	Project
Olivier Genest	Trialog	olivier.genest@trialog.com	InterFlex & GIFT
Isidoros Kokos	Intracom Telecom	isik@intracom-telecom.com	E-LAND
Heribert Vallant	Joanneum Research	heribert.vallant@joanneum.at	STORY
Javier Valiño	Atos	javier.valino@atos.net	InteGRIDy
David Sanchez	Trialog	david.sanchez@trialog.com	InterFlex & GIFT
Mark Purcell	IBM	markpurcell@ie.ibm.com	GOFLEX

This report has been prepared based on the answers from the following projects: E-LAND, EU-Sysflex, GIFT, GOFLEX, inteGRIDy, InterFLEX, INTERRFACE, INVADE, MERLON, OSMOSE, SMILE, STORY, TDX-ASSIST.

Leading team of the BRIDGE Working Group on Data Management, quality check of the present report

Chairman of the Working Group

Name	Organisation	E-mail	Project
Olivier Genest	Trialog	olivier.genest@trialog.com	InterFlex & GIFT

Guidance from European Commission

Name	Organisation	E-mail
Cristobal Irozaqui	ENER.C2	Cristobal.IRAZOQUI@ec.europa.eu
Patricia Arsene	CNCT.H5	Patricia.ARSENE@ec.europa.eu
Mariana Stantcheva	INEA	Mariana.STANTCHEVA@ec.europa.eu
Stefan Moser	ENER.B4	Stefan.MOSER@ec.europa.eu
Michaela Kollau	ENER.B4	Michaela.KOLLAU@ec.europa.eu
Domenico Ferrara	CNCT.H1	Domenico.FERRARA@ec.europa.eu

Editor

Name	Organisation	E-mail
Stéphanie Petit	DOWEL Management	stephanie.petit@dowel.eu

Table of Contents

List of Acronyms and Abbreviations

AI	Artificial Intelligence
CaaS	Cybersecurity as a Service
CAPEX	CAPital EXpenditure
CISO	Chief Information Security Officer
DSO	Distribution System Operator
EC	European Commission
eIDAS	electronic IDentification, Authentication and trust Services
ES	Energy System
EU	European Union
EV	Electrical Vehicle
H2020	Horizon 2020
ICT	Information and Communications Technology
IT	Information Technology
IoT	Internet of Things
LCE	Low Carbon Energy
MFA	Multi-Factor Authentication
NA	Not Applicable
NIST	National Institute of Standards and Technology
OPEX	OPerational EXpenditure
OT	Operational Technology
PKI	Public Key Infrastructure
R&I	Research & Innovation
SLA	Service Level Agreement
TSO	Transmission System Operator
WG	Working Group

Executive Summary

The energy system is one of the most complex and largest infrastructures in Europe as well as one of the most critical assets for a modern society and as such, is the backbone for its economic activities, welfare and stability. Today, the energy sector is undergoing a very rapid change in terms of infrastructure and market developments - to appropriately accommodate the increasing share of renewable energy sources and decentralized generation, as well as an increasing number of prosumers. The sector is subject to an accelerated digital transformation, with Big Data and the Internet of Things, 5G and artificial intelligence, smart grids and smart meters, smart homes, smart appliances, smart storage and smart charging being key drivers for its success.

This digitalization brings new challenges for the sector, in particular with respect to cybersecurity. This challenge is strengthened by the particularities of the energy sector: real-time requirements, cascading effects and the combination of legacy systems with new technologies [1].

BRIDGE is a European Commission (EC) initiative gathering all the Horizon 2020 Smart Grids and Energy Storage projects. These projects have been asked to answer a questionnaire covering the following main questions:

- How is cybersecurity addressed in the projects? What issues are faced?
- How a cybersecurity certification could help to ensure that systems are cyber-secured?
- How the EC recommendation on cybersecurity in the energy sector [1], published on April 3rd, 2019, could be applied in projects?

This report, by gathering and summarizing the answers of thirteen H2020 smart grid projects, offers a comprehensive outlook and feedback on these three main questions. Based on this, the main recommendations are:

- To take care of complexity, cost and required effort when considering cybersecurity recommendations, such as in [1].
- To develop a certification framework with a focus on: definition of minimal requirements for devices/products; development of tools, processes and guidelines for audit and tests; process and lifecycle management.
- To develop and demonstrate attack detection, situational awareness, incident management and resilience systems.
- To share threat intelligence information (past or current attacks) between relevant actors to help them preparing and reacting successfully.
- To promote best practices, such as cyber-hygiene, at every level of the concerned organizations.

1 Introduction

The Data Management Working Group (WG) aims to cover a wide range of aspects ranging from the technical means for exchanging and processing data between interested stakeholders to the definition of rules for exchange, including security issues and responsibility distribution in data handling. Accordingly, the WG has identified 3 areas of collaboration around which mutual exchange of views and discussions have been set:

1. **Communication Infrastructure**, embracing the technical and non-technical aspects of the communication infrastructure needed to exchange data and the related requirements
2. **Cybersecurity and Data Privacy**, entailing data integrity, customer privacy and protection and general security of energy systems
3. **Data Handling**, including the framework for data exchange and related roles / 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

This report fits into the 2nd area “Cybersecurity and Data Privacy” and is covering the topic of “Cybersecurity and Resilience”.

This topic of “Cybersecurity and Resilience” has been discussed and its scope defined during the BRIDGE General Assembly on March 12th and 13th 2019. Three main questions were identified:

- How is cybersecurity addressed in the projects? What issues are faced?
- How a cybersecurity certification could help to ensure that systems are cyber-secured?
- How the EC recommendation on cybersecurity in the energy sector [1], published on April 3rd, 2019, could be applied in projects?

Within the BRIDGE Data Management WG, the contributing projects have been solicited to answer a questionnaire (see Annex) covering the topics mentioned above in July and August 2019. The topic leader and the active contributors have then analysed the answers to summarize the main findings, identify and highlight the main barriers faced within the projects and defined some recommendations to overcome them in future projects and deployments.

2 Particularities of the energy network

The energy sector has inherent and distinctive characteristics making it especially delicate regarding the implementation of cybersecurity policies. Traditional Information Technology (IT) approaches on cybersecurity are often not enough or not fully aligned with the criticality and real time requirements of energy systems.

This section is devoted to providing a view on these cybersecurity special needs identified as particular to the energy sector. This way, section 2.1 introduces the vision of the European Commission on most common particularities, as published in the "Commission Recommendation on cybersecurity in the energy sector" released in April 2019 [1].

This recommendation has been analysed by BRIDGE project experts on cybersecurity, and section 2.2 describes the conclusions reached as per:

1) the agreement of the threefold particularity approach as proposed by the EC; and
2) the potential suggestion of additional items (either as new particularities or as sub-particularities to be considered within what is already defined).

Section 2.3 builds on top of all aforementioned and previous sub-sections and provides the link with IT common cybersecurity approaches and the required adaptation to energy systems.

Finally, the potential impact on costs (if done through the analysed projects) is considered in section 2.4. The approach followed and the preliminary findings in this respect, for those projects including this part in their activities, are presented.

2.1 Description of the three particularities defined in EC requirements [1]

The combination of criticality of the energy sector and of the assets being handled, the challenges arising from climate change and the transition to a low-carbon economy, and the increasing digitalization of the sector are all posing cybersecurity risks, which European Union (EU) countries should be aware of.

That is why the European Commission found it useful to publish a recommendation in this respect. This publication is accompanied by a Staff Working Document [4] that provides the policy context for cybersecurity, the elicitation of particularities of the energy sector, the relevant activities performed by the EC and the baseline international standards.

For Research and Innovation, the part describing cybersecurity particularities is of special interest. The BRIDGE Data Management WG distributed this information to all projects to raise awareness of these results and provide feedback on the current proposal.

The EC document underlines the following particularities:

1. **Real-time requirements**. Some of the actionable parts of the energy systems have reaction times under the 5ms (milli-second) threshold. On the contrary, commonly used cybersecurity protocols and mechanisms consider, for instance for message authentication, using certain cryptographic features, response times above 10ms. Therefore, special considerations should be taken into account when applying cybersecurity to energy systems.
    a. Segregation of networks. Separation in logical zones and processes might allow implementing the most suitable policy per zone.
    b. Secure communication and authentication. This is a must for all energy systems. The proper selection and exhaustive testing of the cybersecurity solutions covering this topic is critical.

c. Asset management through classification. Classifying the assets for all systems is a pre-requisite. This classification must include the real-time potential constraints to clearly identify those assets with special needs.

d. Public and private infrastructure. Isolating the network as a private system is the most secure way to operate, but this is not always cost-effective. Proper cybersecurity mechanisms should be put in place to support real-time requirements over hybrid (private/public) networks.

e. Physical security & hardening of interfaces. Use of standards (when commercially available) and use of additional physical security (if upgrading is not an option) must be applied.

2. **Cascading effects**. Given the current strong interconnection between electricity/gas pipelines, and the fact that the stability of the grid, at EU level, depends on the whole integrity of the network for the union (and beyond), cascading effects upon a cyberattack on a particular region are a huge risk cause a failure at large scale due to a domino effect.

   a. Criticality and setting appropriate measures. As for the real-time requirements, classification of assets and their careful assessment regarding criticality, dependencies and potential impact on stakeholders is a must to properly enforce cybersecurity policies.

   b. Consideration of possible cyber-physical spill-overs. Resilient grid architecture and plans to ensure business continuity should be established.

   c. Establishment of design criteria and architecture for a resilient grid. Segregation should be applied to limit potential failures. Identification of critical nodes and enforcing digital controls to avoid single point of failure for several nodes must be taken into account.

   d. Proper communication and cooperation. Cooperation among energy operators and stakeholders is crucial, as the control of cyber-attacks goes beyond the control of a single actor.

3. **Legacy technology combined with new technology**. Energy systems combine legacy equipment, in some cases installed decades ago and not prepared to deal with cybersecurity, with state-of-the-art new digital equipment following the security-by-design principle, but commonly exposing some of the legacy equipment to unforeseen digital threats. In addition, the Internet of Things (IoT) devices incorporation into energy systems leads to an additional risk. Most of these devices are not compliant with the strict requirements for security of energy networks and there is a high risk of malicious usage if connecting them with no security or trust assurance.

   a. Sufficient knowledge about the security of assets and infrastructure. OT/IT collaboration is especially critical at this point, as Operational Technology (OT) operators need to be aware of the new threats introduced by the IT systems being put in place. In addition, awareness campaigns about usage of secure IoT/Smart home devices should be launched to educate end users about the fact that an attack on their installed devices might be harmful not only for them but for the whole network.

   b. Specific risk analysis. Cybersecurity risk analysis should be done on a regular basis targeting legacy devices and systems, including also devices interfacing with the system. If not per asset, at least per asset category.

   c. Systematic patch management and alternative procedures where patch management is not possible. Systematic patch management should be enforced to keep the

system secure. When possible, this should be combined with segregation and maintenance operations.

d. Physical security. Physical protection reinforcing legacy devices (reviewed on a regular basis) is an important policy to be implemented.

e. Strengthened security in the supply chain. Technology providers should take action and design cybersecurity compliant devices (by design) and carry out appropriate cybersecurity certification if possible.

2.2 Feedback from projects on these particularities

As part of the assessment of projects with respect to the list of energy system specific cybersecurity needs, BRIDGE project participants were asked whether they agree with the topics identified in the publication as explained in section 2.1 and to provide additional considerations in case they understand the current list does not reflect each and every particularization needed.

Regarding the agreement with the three macro-topics, **the response was unanimous acknowledging those** (real-time, cascading effects and legacy technology) **as the most relevant items making the energy systems special and where cybersecurity actions and policies should be more carefully studied and implemented**. As a side comment, there is also a consideration regarding real-time and the fact that this criticality must not be considered as an excuse to implement less-restrictive cybersecurity policies but, the other way around, to implement advance and real-time capable security mechanisms.

In addition, BRIDGE projects have also proposed a number of additional considerations that should also be taken into account when applying cybersecurity policies to energy systems. In the following, these recommendations are listed. They are categorized as either extensions (underlined) for already existing items listed in the EC analysis or new items (**bold**) for a particular topic.

- Extension to point 1e (Use of standards). The energy grid is very heterogeneous in terms of security needs, so it would be hard to maintain. In any case, there is a need to prevent massive attacks. Standardisation of interfaces for interoperability is good, but not everybody should use the same platform.

- Extension to point 2d (cooperation among stakeholders). The fact is that the energy sector has presence of multiple actors/operators with not aligned cybersecurity skills and resources. Certification of minimal requirements will ensure that all parts of the system are at least minimally secured.

- Extension to point 2d (cooperation among stakeholders). Sharing threat information (previous or current attacks) would be highly appreciated so other stakeholders in a similar situation can prevent and prepare contingency plans allowing everybody to easily and quickly react upon the discovery of an attack.

- Extension to point 3a (usage of unsecured IoT devices). Sensors / physical measures can be hacked meaning that falsified data will be captured resulting in wrong decisions (Cyber-attacks could in theory manipulate this data (data poisoning) leading to inaccurate forecasts of energy consumption and/or production).

- Extension to point 3e (usage of unsecured devices). Special attention should be paid to distributed renewable generation, which is not under the control of the DSO, as the enforcement of cybersecurity on those assets rely on third parties but affects the whole network.

- **New item for point 3 (Legacy devices)**. Investment in cybersecurity measures comes usually after an attack has been discovered and not before. Ensuring the cybersecurity

investment, even for critical assets, is hard to achieve. **Awareness campaigns and cost-benefit analysis** for implementing cybersecurity policies, confronted with **risks and potential losses** of not applying them should be conducted to educate energy system operators on the need to secure their assets.

2.3 Additional measures with respect to telecommunication networks

This section is devoted to the analysis and identification of additional measures that need to be considered over and above what is provided by common telecommunication networks for securing their links.

This section is linked to section 2.2 as the additions should be in line with the new requirements identified as particularities to the energy systems.

The most critical considerations have already been presented in the combination of sections 2.1 and 2.2. Nevertheless, this section includes a number of comments building on top of the already presented security threats:

- Since the monitoring and control architectures are mostly built using paradigms derived from telecommunication networks, additional issues can be related to the **authentication/integrity of commands**. This aspect, however, may generate a concern related to the timeliness of application and processing burden. The additional aspect is related to the endpoints installed in the end-user perimeter like, for example, the smart meters.
- Energy networks are cyber-physical infrastructures interconnected by telecommunication networks, so energy networks need to include application level security measures, such as user **authentication and role based access control**, in addition to measures of telecommunication networks adapted to the operational context, such as **firewall**, **intrusion** detection systems, **hop authentication** and **data encryption**.
- Currently, any decentral device can be connected to the energy grid, such as EV Charging Stations, heat pumps and home energy management systems. Since these are developed and managed by companies other than the operators of the grid, some form of security “test” or **certification** should be applied. This should not only be in place for the devices themselves, but also for the management systems.
- Cybersecurity attacks could in theory abuse “high numbers” of decentral devices that could directly impact energy networks. If, for example, all devices from one manufacturer contain a security vulnerability, this could lead to many device installations that are vulnerable.

2.4 Impact on cost

As the final step for the analysis on the cybersecurity threats and the potential costs of implementing appropriate policies in the energy systems, BRIDGE projects were asked about the way in which this can be proven.

As a result, the unanimous response was that **the evaluation of the enforcement of real cybersecurity policies is hard to be realised through a Research and Innovation (R&I) project**.

Nevertheless, some BRIDGE projects have some reduced use case testing scenarios and are planning to provide an assessment on the potential costs. Unfortunately, those projects having this objective in scope are still in an early phase, so no result can be shared. The input that can be

provided at this stage entails a number of recommendations/suggestions on how to approach this issue:

- The cost evaluation must be performed following a **risk assessment process** to investigate which are the most relevant areas to intervene and to assess if it is enough to intervene at process level or at technical/technological level.
- Cost estimation should be split among all the actors involved and include cost of **training** personnel, **updating organisational** procedures, CAPEX/OPEX related to the **hardware/software extensions** of the infrastructure, and OPEX costs of **personnel in charge** of security management.
- A more specific **framework** should be defined to be able to give cost estimations to addressing these particularities.

3 Experience of BRIDGE projects on cybersecurity

This section is devoted to communicating the experience of BRIDGE projects on cybersecurity issues. More specifically, the panel of projects participating in the survey is presented, detailing their topic and positioning the importance of cybersecurity.

An aggregated view of the particularities that are addressed per project is presented, along with an analysis detailing specific cybersecurity issues that were tackled by individual projects.

Furthermore, the relevance of possible solutions (i.e. CaaS, Cyber-hygiene) is highlighted and the necessity of a Cyber-security certification framework is documented.

Finally, different aspects that can be explored in future R&I calls are analysed.

3.1 Description of the panel of projects

The survey was completed by thirteen (13) projects (over 21 registered). The allocation of these to the different topics of H2020 work program is presented in Figure 1. This analysis highlights that the survey material concerns many DSO-oriented projects, with no cybersecurity-focused projects.

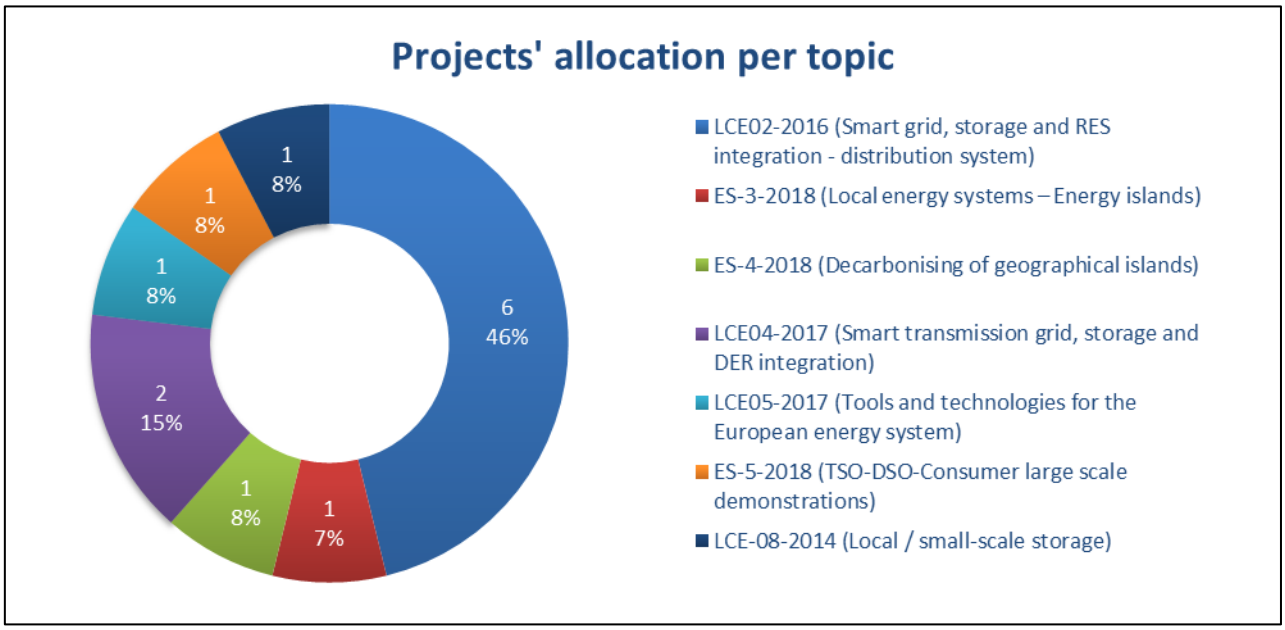

Figure 1 Allocation per H2020 topic for projects participating in the survey

Cybersecurity is explicitly part of the outcome of six (6) out of the thirteen (13) projects as presented in Figure 2, meaning one or more tasks are dedicated to this subject, whilst in most of the cases cybersecurity is seen as supportive task.

On a H2020 topic basis, ES-4-2018 and LCE02-2016 are mostly engaged in the subject. Projects from the former topic should deliver practical recommendations arising from project experiences with data management, data processing and related cybersecurity. On the other hand, projects from the LCE02-2016 topic, shall include a detailed analysis of current regulations, standards and interoperability/interface issues applying to their case, in particular in connection to ongoing work in the Smart Grid Task Force and Experts Groups in the field of Standardization (e.g. CEN-CLC-ETSI M/490), regulatory environment for privacy, data protection, cybersecurity, smart grid deployment, infrastructure and industrial policy.

Another outcome of the analysis is that, whilst very focusing on prosumers at DSO scale, cybersecurity at the level of stations/substations is not addressed in these projects.

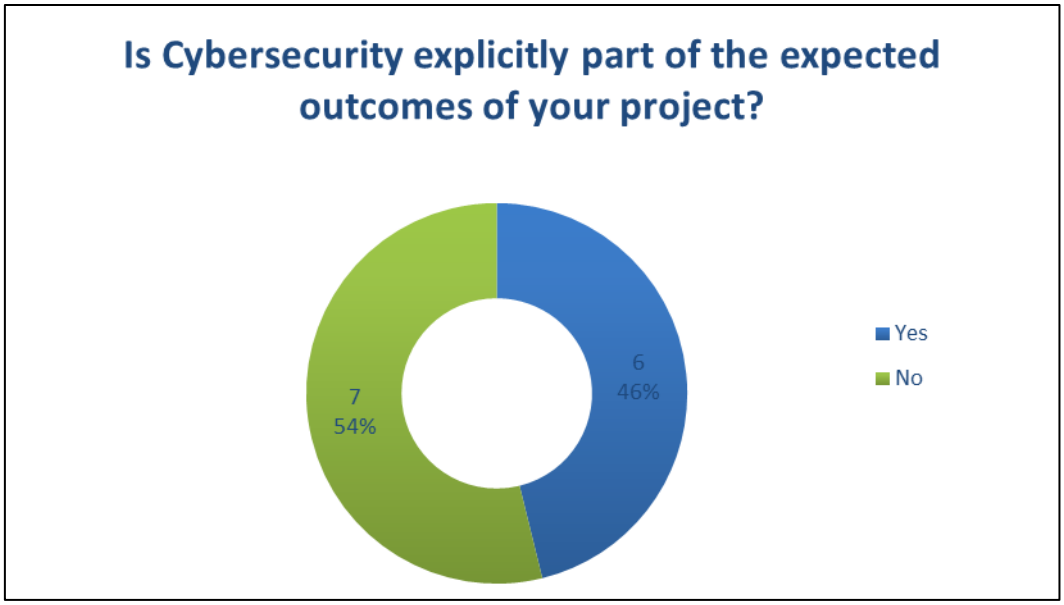

Figure 2 Cybersecurity as explicit outcome

After this short introduction on the boundaries of the engagement in cybersecurity analysis of the survey participants, follows a presentation of the particularities that were addressed: *Real-time, Cascading Effect, Legacy Systems*.

The analysis of survey with regards to this aspect are presented in Figure 3. Integration of legacy systems was the main particularity faced by the nine (9) projects identified on facing one of these particularities. Five (5) of the projects face only one of the three particularities, three (3) of them face two particularities and only one (1) faces all three particularities, as presented in Figure 4.

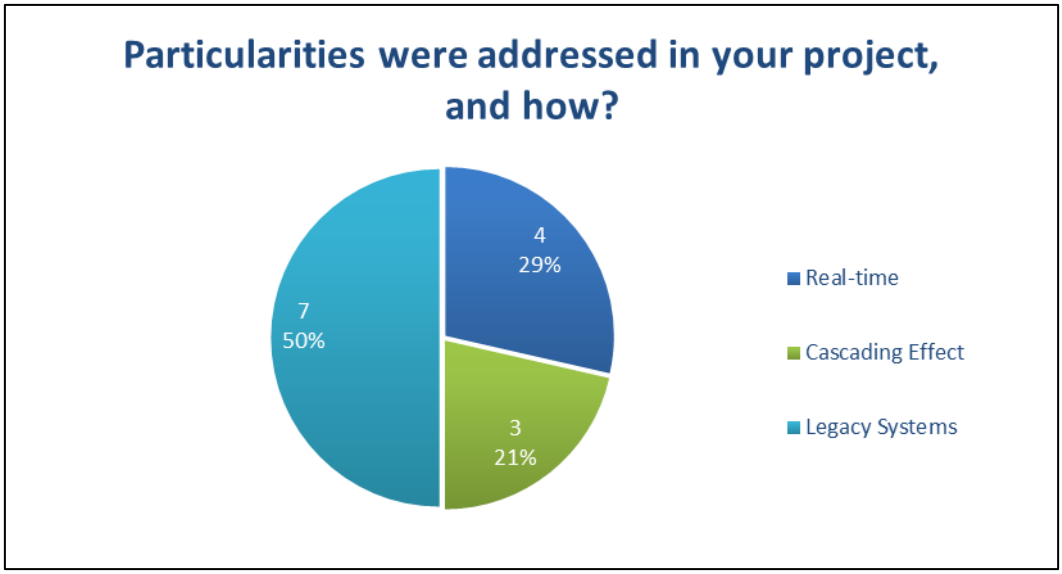

Figure 3 Frequency of particularities faced

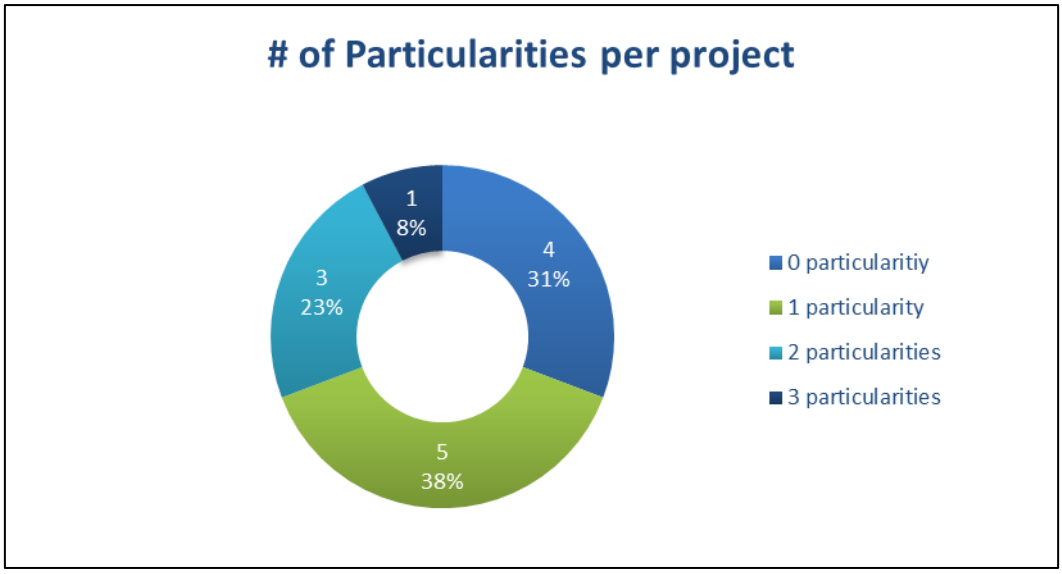

Figure 4 Number of identified Particularities per project

The detailed mapping between the projects and the particularities is depicted below:

Project	Real-time	Cascading effect	Legacy systems
E-LAND			✓
EU-Sysflex			✓
GIFT			
GOFLEX			
inteGRIDy	✓		✓
InterFLEX			
INTERRFACE		✓	✓
INVADE		✓	
MERLON			
OSMOSE	✓	✓	✓
SMILE	✓		✓
STORY	✓		
TDX-ASSIST			✓

3.2 Cybersecurity issue(s) faced during the projects

When answering the survey question on the cybersecurity issue(s) faced by each project, only three (3) out of the thirteen (13) projects reported identification of cybersecurity issues (Figure 5). These concerns are:

- Issues identified during the design phase, leading to the adoption of a combination of security measures;
- Threats identified during the integration phase, by performing a variety of security checks (e.g. weak cipher suites, default passwords, whitelisting, exposed services to the public).

One of the barriers identified concerns the compliance of commercial products with international standards.

Nevertheless, the reduced scope both in terms of size and duration of H2020 projects makes it unlikely for them to face any real cybersecurity threats.

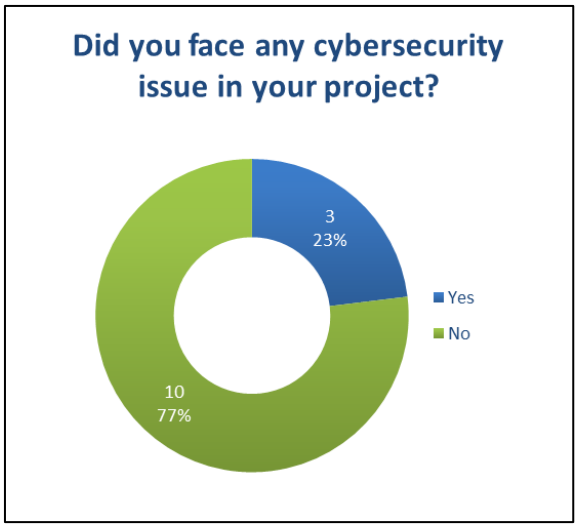

Figure 5 Cybersecurity Issues identified

The identification of qualified experts was apparently not a significant issue as reported by eight (8) of the projects, with enough expertise existing in the consortium on several occasions, especially if cybersecurity is within the scope of the project. On the other hand, two (2) participants in the survey reported not being yet in the phase of the project necessitating such an inquiry of relevant expertise, whilst one (1) reported difficulty in hiring the right expert. The results are presented in Figure 6.

On top of the above, one significant aspect that should be considered in this response is that the requirements imposed by the H2020 Research and Innovation topics – even those with pilot deployments - might differ from industrial deployments of similar technologies. Identifying the right experts might involve searching for more sophisticated skills, which in many cases might require having both ICT security and electrical & power engineering skills.

Figure 6 Qualified Experts

3.3 Relevance of possible solutions

3.3.1 Cybersecurity as a service

The specific answer to the question “Would you consider a Cybersecurity-as-a-Service approach with Service Level Agreements (SLA’s) a relevant solution?” was quite different: two (2) projects stated a strong “no” due the data sensitivity and the importance of cybersecurity to be kept inside. The overall picture shows that this could be a good option; especially outsourcing of particular applications was seen as a workable solution (Figure 7). Also, for small scale organizations, this cybersecurity as a service approach could be a solution in combination with a cybersecurity strategy established and managed within the organization.

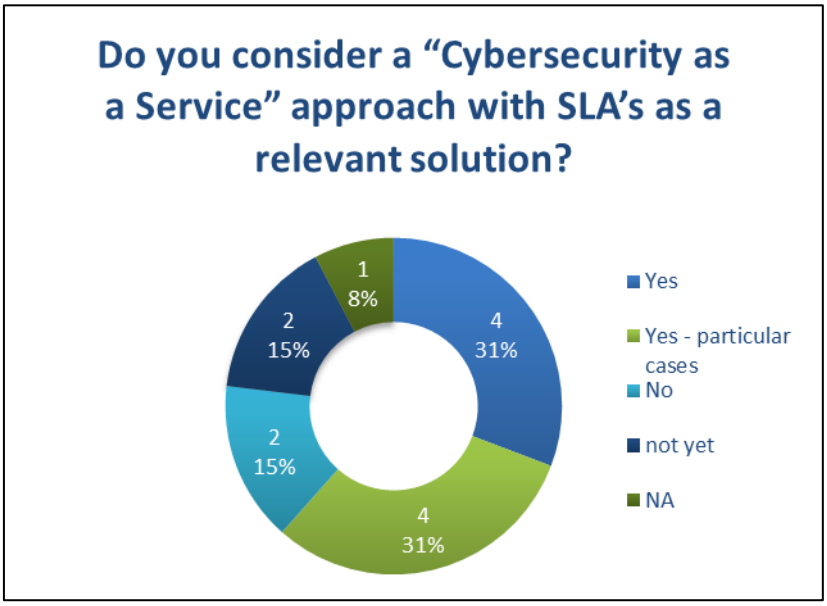

Figure 7 Cybersecurity as a service

3.3.2 Cyber-hygiene

The evaluation of the results regarding the cyber-aware organizational culture reflects a positive trend, as most of the projects are already applying this, while respectively due to the early stage of some projects this has not yet been addressed. The results are presented in Figure 8.

Within the consortia’s different organizations, many perform this in different ways and address this via internal defined processes and guidelines, up to quality and security standards like ISO/IEC standards (e.g. ISO 27001 [2]) or NISTIR 7628 [3].

The importance to show to operators explicitly the risks and their role in the system was mentioned. Also, the involvement of the consortia member CISOs, to work out the procedure on how to raise the cyber awareness and risks from human errors, was mentioned.

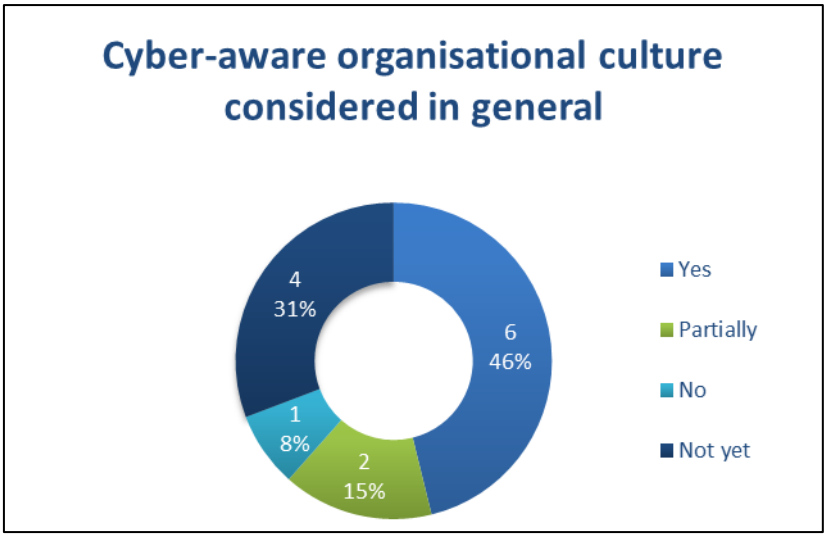

Figure 8 Cyber-hygiene

3.3.3 Cybersecurity certification framework

3.3.3.1 How would a European certification framework be useful for your project?

The European certification framework was generally being seen as very useful to ensure the proper cybersecurity of the whole system and used products. It could be helpful when all the necessary steps and checks have been performed, starting from the conception of the system up to its implementation and later integration and deployment. Such a certification would be used in the future procurement phase of commercial devices from the market and, during the design phase, to address basic security elements and to evaluate that cybersecurity is adequately addressed.

Some projects are already in an advanced stage and therefore this is not applicable anymore but would be considered for future projects.

3.3.3.2 How would the European certification framework be useful in the exploitation of the results of your project?

Here the commercialisation and added value of bringing certified products to the market is the key aspect, which would imply that security is adequately handled. The trustworthiness is seen as an important factor when such a solid certification approach is undertaken.

3.3.3.3 What should be the scope of this certification framework: products? processes? services? system? (also explain why).

From the scope of such a certification framework the majority thinks that products and processes should be addressed (Figure 9). Especially, products should be certified to ensure that the purchased devices are compliant, that they have no weak spot and thus that they will not introduce security issues to the used infrastructure. The certification of products should also include real-time aspects and the communication protocols / interfaces that are used by the products. Processes are also very useful to address the certification of integration issues, the compliance of the system design and its operation, and the cybersecurity incident counter measures.

Services would also be useful but were seen as very complex with diverse approaches which can not easily be handled.

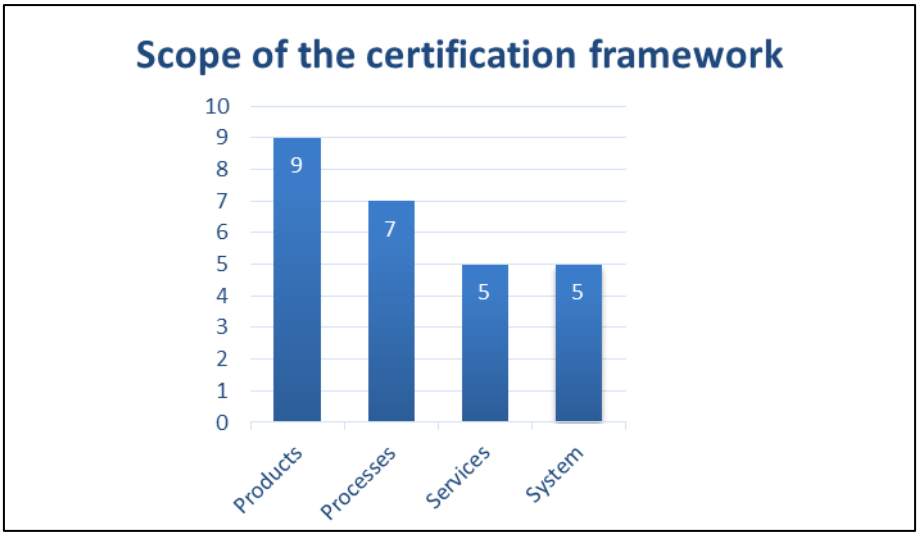

Figure 9 Scope of certification framework

3.4 Axis to be explored and potential topics for future R&I calls

The main axis to be explored is the building of more resilient, reliable and capable situational awareness and incident management tools covering online energy platforms, not usable air-gapped[1] systems, human aspects, cascading aspects and deployment of counter measures.

For the situational awareness the detection of attacks in real-time is very important, also research into the detection of unknown future attacks is necessary. Therefore, novel big data and IA-based learning techniques should be investigated. After detection, the handling of emergency situations caused by cybersecurity attacks is a big issue which can be supported by modelling and simulation tools for deployment of counter measures.

Besides that, a review of best practices should be available to ensure baseline cybersecurity measures for the energy domain.

The security of smart meters was seen as a critical entry point in the distribution network which could drive unprecedented hacking wars. Also, the escalation of smart metering data via different data exchange communication protocols should be addressed (e.g. ontology).

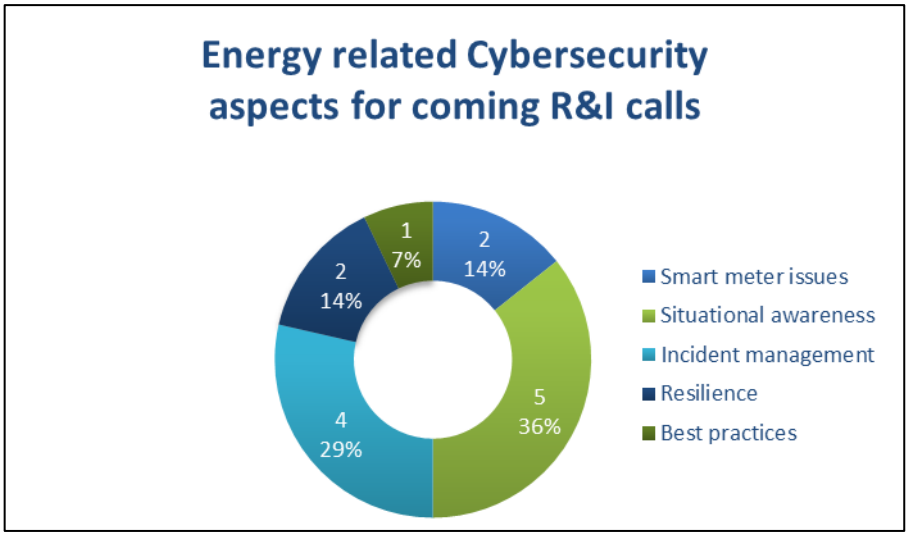

Figure 10 Topics for future R&I calls

[1] Air-gap refers to devices, networks or systems that are not connected directly to the internet or to any other devices, networks or systems that are connected to the internet.

4 Detailed feedback on EC recommendations for cybersecurity in energy [1]

4.1 Relevance

With the objective of gathering feedback on EC recommendations [1], BRIDGE projects have been asked if they implement, or would implement, controls in line with each of the items described in guidance 4 and 5 (related to real-time requirements); 8 (cascaded effects); 11 and 12 (use of legacy systems). As shown by the Figure 11 below, most recommendations have received affirmative answers from BRIDGE projects, confirming their relevance with current cybersecurity needs in the energy sector.

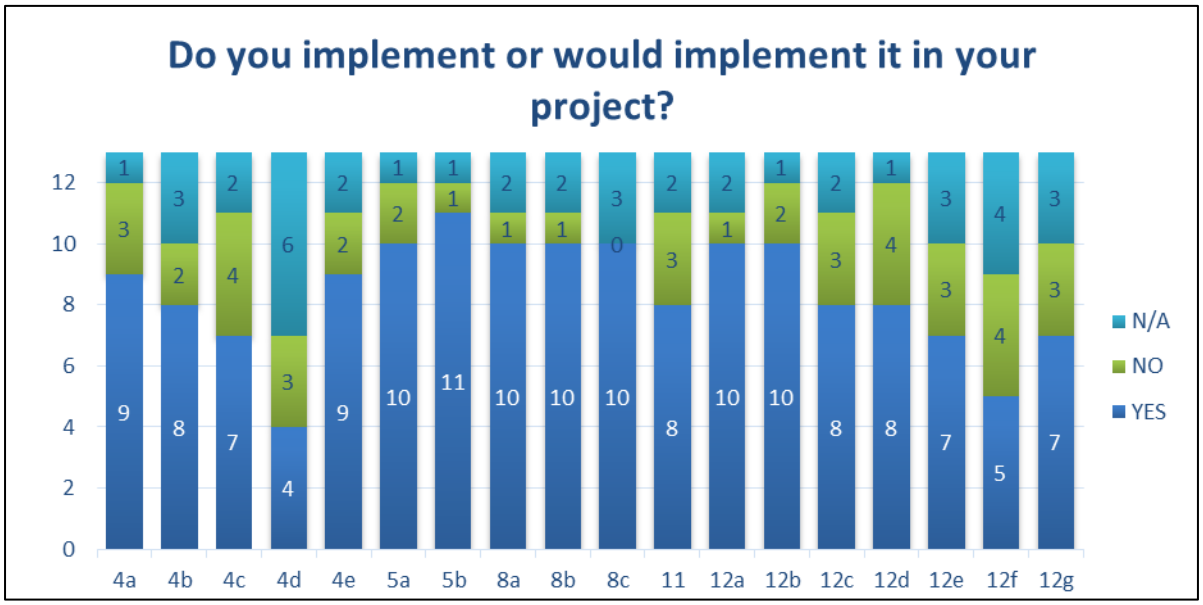

Figure 11 Implementation of EC recommendations

Recommendation 4.d, which asks network operators to consider privately owned networks, has received a remarkably high number of non-positive answers (including “not applicable”) given the scope and budget limitations of BRIDGE research and innovation projects. As only half of BRIDGE projects address legacy systems, EC recommendations related to their maintenance, update, monitoring and contracting terms have also received a high number of non-positive answers.

4.2 General barriers

4.2.1 Cost, complexity and effort

Title	Slow implementation of EC guidance due to high cost / effort needed
Barrier	In order to follow the guidance on cybersecurity, network operators need to devote additional financial and human resources. Lack of cybersecurity skills further increases the overall expense, as network operators will need to acquire the necessary knowledge. Unfortunately, return on such cybersecurity investments is not clear, which reduces the priority of their implementation. Even though this barrier affects the implementation of the whole cybersecurity guidance, BRIDGE projects highlighted 4 costly processes: • adaptation of legacy systems to current cybersecurity practices

	(12.e); • integration and certification of international standards (4.b); creation and maintenance of private networks (4.d); • setting up infrastructure required for testing and upgrading cybersecurity solutions (11).
Recommendation	BRIDGE projects have confirmed that cybersecurity investments are usually the result of a risk management process. Hence, to overcome this barrier, future guidance and recommendations shall support decision makers to assess underlying risks and estimate costs and/or efforts required to implement the respective mitigation activities. Future cybersecurity training shall include risk management, including assessing consequences of unmitigated risks, as a core topic.

4.2.2 Multitude of heterogeneous devices and systems

Title	**Device ecosystem is growing in complexity and heterogeneity**
Barrier	With the irruption of IoT devices in the energy ecosystem, network operators have seen an enormous increase in the attack surface. Such an increase is not only driven by the number of devices, or entry points to the network, but also by the diversity of technical protocols and scale of cybersecurity features implemented by such devices. This poses a challenge not just to integrate all devices into the energy network, but also in applying a homogeneous level of cybersecurity, keeping all devices monitored, constantly updated and tested with a view to continuous improvement. Manually updating devices may take a significant amount of time and money, due to the need to physically access remote sites. Similarly, the calculation of a cybersecurity risk for such complex ecosystems is much more complicated.
Recommendation	A certification tailored to IoT could help in categorizing devices into different levels of cybersecurity practices and configurations. If all devices in a supply chain follow the same certification, the integration and aggregation of the chain will be easier because they will use the same general semantics, formats and protocols. This will effectively reduce the complexity of asset classification, their respective risk analysis and configuration. Besides, technological advances towards a centralized and automated software update process executed by IoT devices would support protection of energy networks.

4.2.3 Proprietary systems

Title	**Market is not aligned with EC recommendations**
Barrier	BRIDGE projects have shown their concerns about readiness of the cybersecurity market. In particular, - It is unclear if current market solutions and security protocols can operate under the real-time constraints suggested by recommendation 4.c, 4.e, 5.a and 5.b. - Closeness of proprietary components may hamper the necessary in-depth analysis of their interfaces (recommendation 12.a), vulnerabilities and risks to the integrated system (recommendations 8.c, 12.c, 12.d).

	- It is unclear how technology suppliers may provide "tested solutions for security issues in legacy or new technologies free of charge" (recommendation 11) without pre-allocating resources to such endeavour and, hence, charging network operators in advance. - Clarifying vendor liability at tender's stage (recommendation 12.f) seems too ambitious and unrealistic.
Recommendation	Further guidance on these topics may be required, especially to clarify the vendor's liability and to set expectations for free-of-charge security updates. Certification schemes may help in reducing uncertainty towards readiness of market offerings, as well as ensuring integration and analysis of cybersecurity capabilities within proprietary components.

4.3 Specific barriers

Title	**Insufficient monitoring of critical cyber-physical systems (12.c)**
Barrier	Monitoring, storing and analyzing event logs of critical systems and security components have not been always the top priority of TSOs and DSOs. As a result, network operators have heterogeneous levels of details of the status of their systems, not necessarily useful for ensuring proper functioning and auditing of security and data protection policies.
Recommendation	Network operators shall aim at increasing their situational awareness by creating a map of the attack surface and monitoring capabilities of each component. Updates shall then be made based on the criticality of the site and cost, with the ultimate goal of providing evidence of their proper functioning to both internal and external consumers.

Title	**Heterogeneous authentication mechanisms (5.b)**
Barrier	In general, when talking about strong cybersecurity practices, the preferred method would be to implement strong authentication schemes (using certificates and PKI, MFA, biometrics). This is not always the case when dealing with data exchange of energy platforms across EU.
Recommendation	Further guidance and regulations towards agreeing on how authentication is handled, especially with new flexibility services coming to the market and keeping in mind that user interaction and easy access should also be handled. eIDAS compliance should be taken into consideration for such authentication schemes.

5 Conclusion

This report, by gathering and summarizing the answers of thirteen (13) H2020 smart grid projects, offers a comprehensive outlook and feedback on:

- The way cybersecurity is addressed by such projects, what issues are faced and what solutions would be relevant;
- The relevance and feasibility of the European Commission Recommendation on cybersecurity in the energy sector [1];
- The expected added value of a cybersecurity certification program.

Based on this outlook and feedback, the main recommendations are:

- To take care of complexity, cost and required effort when considering cybersecurity recommendations, such as in [1].
- To develop a certification framework focusing on definition of minimal requirements for devices/products; development of tools, processes and guidelines for audit and tests; process and lifecycle management.
- To develop and demonstrate attack detection, situational awareness, incident management and resilience systems.
- To share threat intelligence information (past or current attacks) between relevant actors to help them preparing and reacting successfully.
- To promote best practices, such as cyber-hygiene, at every level of the concerned organizations.

List of figures

List of references

[1] European Commission Recommendation of 3.4.2019 on cybersecurity in the energy sector {SWD(2019) 1240 final}
Link: https://ec.europa.eu/energy/sites/ener/files/commission_recommendation_on_cybersecurity_in_the_energy_sector_c2019_2400_final.pdf

[2] ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements

[3] NISTIR 7628 Rev. 1 – Guidelines for Smart Grid Cybersecurity
Link: https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf

[4] European Commission staff working document, accompanying the document [1] {C(2019) 2400 final}
Link: https://ec.europa.eu/energy/sites/ener/files/swd2019_1240_final.pdf

Smart Grid Task Force Expert Group 2 – Recommendations to the European Commission for the Implementation of Sector-Specific Rules for Cybersecurity Aspects of Cross-Border Electricity Flows, on Common Minimum Requirements, Planning, Monitoring, Reporting and Crisis Management, Final report, June 2019
Link: https://ec.europa.eu/energy/sites/ener/files/sgtf_eg2_report_final_report_2019.pdf

Annex I Questionnaire on Cybersecurity and Resilience

The questionnaire below has been submitted to all the projects participating to BRIDGE Data Management WG.

Scope

Note: the text below is extracted from the Agenda of the BRIDGE General Assembly of March 2019 (introduction to Session 5 – Cybersecurity and Resilience).

The energy system is one of the most complex and largest infrastructures in Europe as well as one of the most critical assets for a modern society and as such the backbone for its economic activities, welfare and stability. Today, the energy sector is undergoing a very rapid change in terms of infrastructure and market developments - to appropriately accommodate the increasing share of renewable energy sources and decentralized generation, as well as an increasing number of prosumers. The sector is subject to an accelerated digital transformation, with Big Data and the Internet of Things, 5G and artificial intelligence, smart grids and smart meters, smart homes, smart appliances, smart storage and smart charging being key drivers for its success.

This digitalization brings new challenges for the sector, in particular with respect to cybersecurity. In cybersecurity, one size does not fit all. Security paradigms from the internet may not be directly suitable and applicable to the energy sector. It is, therefore, indispensable to look at the particularities of the energy sector that create challenges in terms of cybersecurity:

1. First, we have real-time requirements: Some energy systems (e.g. circuit breakers) need to react so fast, in fact in milliseconds, that standard security measures (e.g. authentication of a command) can simply not be introduced due to the delay they would bring.
2. Second, we have to be aware of the cascading effects: Electricity grids and gas pipelines are strongly interconnected across Europe and well beyond EU Member States. An outage in one country might trigger black outs in other sectors and countries.
3. The third particularity of the energy system is the combination of legacy systems with new technologies: Many elements, such as most cables, were designed and built well before cybersecurity considerations came into play. They often have a lifetime of 30-60 years. This now needs to interact with the most recent state-of-the-art equipment for monitoring, automation and control, such as smart meters or connected appliances, the Internet of Things. The energy sector therefore needs to find ways to embark on the digital future taking along its analogue legacy.

General questions

1. What is the name and scope of your project?
2. Is Cybersecurity explicitly part of the expected outcomes of your project?
3. What is the background/profile of the expert(s) replying to this questionnaire? (i.e. is IT and/or physical security and/or cybersecurity part of their fields of expertise?)

Topic #1: Implementing Cybersecurity in Energy – needs and barriers

1. Do you agree with the list of particularities described in §0? (real-time requirements, cascading effect, legacy systems)
2. Do you see any additional particularity of the Energy sector?
3. Which of these particularities were addressed in your project, and how?

4. How would you estimate the costs of addressing these particularities? Can you provide examples?
5. Did you face any cybersecurity issue in your project? If yes, for each of them:
    a. During which phase? (e.g. design, implementation, integration, operation, etc.)
    b. What solution did you put in place?
    c. Did you identify any specific barrier?
6. Did you face difficulties in identifying qualified experts?
7. Do you consider a "Cybersecurity as a Service"[2] approach with SLA's as a relevant solution?
8. Have you considered factors like Cyber hygiene, internal processes and norms related to Cybersecurity or the promotion of a cyber-aware organizational culture, in general? If yes, please provide details on the approach; if not, please provide reasons for non-considering the respective factors.
9. Do you think there should be additional measures in terms of cybersecurity to be considered in the energy networks compared to the telecommunication networks? If yes, please explain and provide concrete examples.
10. What specific energy related Cybersecurity aspects could possibly be relevant for the coming R&I calls?

Topic #2: Feedback on EC recommendations

The European Commission has published a Commission Recommendation on cybersecurity in the energy sector on April 3rd 2019 (link).

For each of the 18 considered elements[3]:

1. Which of these elements are implemented or would you implement in your project?
2. Do you see any barrier(s) preventing the implementation of the considered elements of the Recommendation in your project?
3. Is there any element from the Recommendation you would add as relevant to your work to the mentioned 18?

Topic #3: Cybersecurity certification

The Cybersecurity Act[4] entered into force on 27 June 2019, establishing the first EU-wide cybersecurity certification framework to ensure a common cybersecurity certification[5] approach in the European internal market and ultimately improve cybersecurity in a broad range of digital products (e.g. Internet of Things) and services.

1. What would your project expect from this certification framework?
2. How would a European certification framework be useful for your project?

---

[2] Cyber-security as a Service (or Security as a service) is an outsourced model of cybersecurity management: a company outsource its cybersecurity management to a third-party vendor, typically on a pay as you go basis, rather than handling it in-house where it may have limited resources and expertise.
[3] Items 4a, 4b, 4c, 4d, 4e, 5a, 5b, 8a, 8b, 8c, 11, 12a, 12b, 12c, 12d, 12e, 12f, 12g
[4] https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act
[5] https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework

3. How would the European certification framework be useful in the exploitation of the results of your project?
4. What should be the scope of this certification framework: products? processes? services? system? (also explain why).

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

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