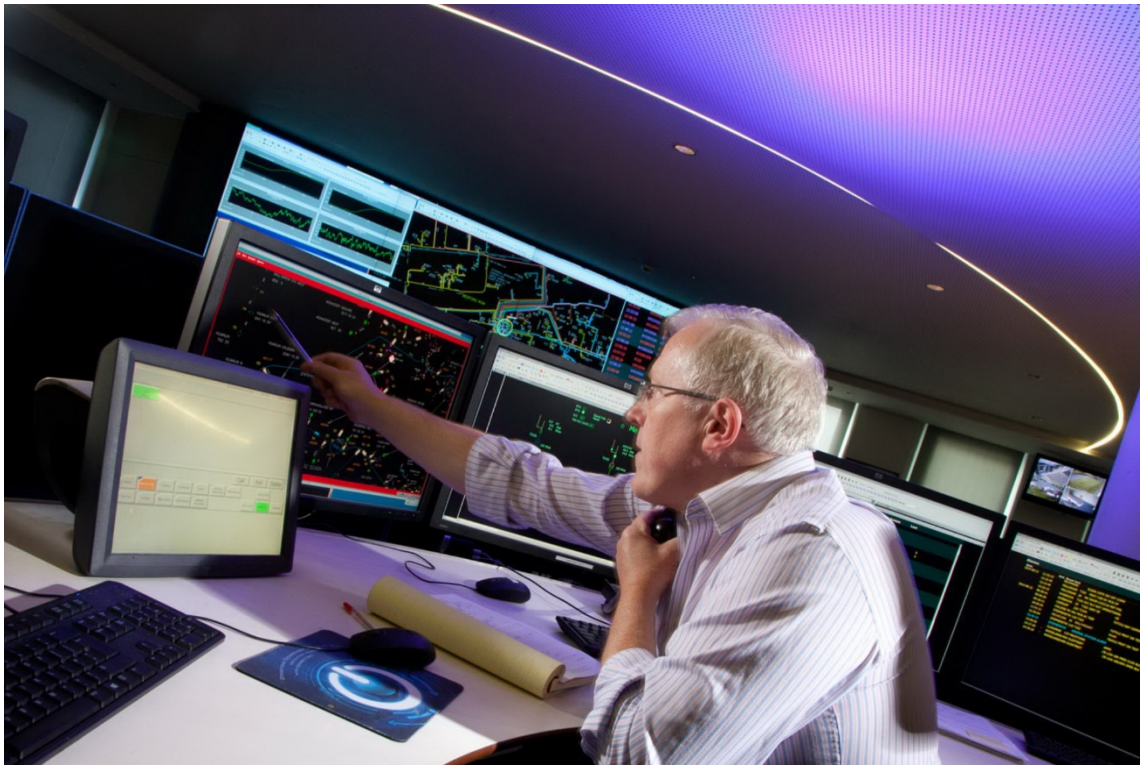
SUCCESS

A European Security Analytics Network for Critical Infrastructures

Whitepaper



Courtesy: ESB Networks Ltd

Executive Summary

Lately, there has been an increasing adoption of ICT among Critical Infrastructures (CIs), such as the electricity, water and gas grids. For example, a transition of the traditional electricity grid to a Smart Grid is currently taking place as an important step for the achievement of the European energy targets. However, the sheer integration of ICT also poses risks to utilities, due to the growing number of cyber threats.

SUCCESS's Security Solution includes monitoring of critical energy infrastructures and attack detection on a local level – within the network of one or several CI operators – as well as on a pan-European level. For the latter, SUCCESS is developing a European Critical Infrastructure Security Analytics Network (CI-SAN) that will be connected to all European CI operators, will collect grid status information as well as publicly available information and will rely on advanced data analytics to detect attacks and identify attack patterns. The CI-SAN has a strong potential to prevent a wide spread of cyber attacks.

This white paper presents the efforts and suggested time plan for the adoption of the CI-SAN concept into the European framework, both in terms or necessary discussions with and among regulatory bodies as well as in terms of administrative decisions needed for its operation.

The CI-SAN is designed within SUCCESS with provision of the European legislation. Moreover, further regulation for the CI-SAN concept may be necessary by the respective policy making bodies due to its wide scope. This white paper communicates an active dissemination plan for authorities and CI operators, towards increasing the awareness and contributing to the adoption of a CI-SAN implementation.

Authors

Partner	Name	e-mail
P3 COMMUNICATIONS GMBH (P3C)		
	Panagiotis Paschalidis	Panagiotis.Paschalidis@p3-group.com

Table of Contents

1. Introduction

Critical Infrastructure (CI) operators have been utilising Information and Communication Technology (ICT) in their networks, as ICT enables operators to monitor their CIs and offer improved services to their customers. For instance, the Smart Grid, the evolution of the traditional energy grid, meets the targets of the 21st century for more efficient energy use, increased participation of the consumers in the energy value chain and smooth integration of intermittent renewable energy sources (RES) and electric vehicles (EVs). At the low voltage level, the integration of the ICT is conducted via the deployment of smart (metering) devices, referred to throughout this document as smart meters, which transmit real-time information on consumption allowing monitoring of the CI network status, the demand and the available supply.

Although the modernised CIs offer new opportunities to the customers and the operators, this evolution also comes with a few challenges, as it introduces new vulnerabilities and could be subject to various types of attacks. Vulnerabilities and attack types are discussed frequently in the recent literature, for example in [1], [2] and in the SUCCESS Deliverable D1.2 [3]. Vulnerabilities are created, for instance, through the transmission of customer's private data [4] and an increased attack surface caused by the connection of millions of smart devices. Some potential attacks are malware injection, Denial of Service (DoS) attack and eavesdropping, all of which undermine the secure operation of the smart devices and the whole service of the network.

The basic security targets of information systems, availability, integrity and confidentiality, cannot be ensured in the CIs unless security measures against cyber attacks are implemented. The detection of potential attacks is thus crucial, and is the focus of the SUCCESS Security Solution. SUCCESS proposes to defend the security of CIs by an architecture that monitors the smart devices and the grid status, analyses the exchanged data in order to detect anomalies and possible attacks and initiates countermeasures to mitigate the attacks. As new threats are constantly emerging, this architecture needs to be flexible and able to identify and incorporate new threat patterns in the data analysis system as well as to optimise the triggered countermeasure for each detected attack.

The monitoring of the CIs is a task of the respective operators in charge, each of which shall supervise their area of operation. This enables operators to detect attacks in their network. Attacks with a wider scope, on national or even international level should be, however, detected and eliminated as well. It may be the case, that an adversary carefully plans an attack, so that the values obtained by a certain smart meter or a group of smart meters seem legit and normal. In this case, the attack can remain undetected for a long time and cause great damage to a large area [5]. A solution to this challenge is the establishment of a security analytics network that gathers data from multiple operators, analyses them and detects attacks in a wide region based on the aggregated data. Since the grids of many CIs in Europe are interconnected this monitoring unit should ideally gather data from all European operators.

The exchange of information and cooperation between different national operators is essential to ensure a greater effectiveness of the countermeasures taken and therefore for the safety of CIs. An European infrastructure control and protection system is important as many infrastructures in Europe are interconnected and an attack on one of them at national level can have a domino effect on the whole continent. A typical example of transnational CI is the Power Grid.

The SUCCESS project develops a Security Solution that performs monitoring of CIs at a local and at the European level and protects them through attack detection and triggering of countermeasures. As a paradigm, SUCCESS will demonstrate this Solution in 3 trial sites, where use cases of attacks against the Smart Electricity Grid will be demonstrated and the efficiency of the proposed solution will be validated. The focus of the project is, therefore, on

collecting electricity grid data from smart meters located in consumers' /prosumers'[1] premises; with part of the Security Solution at DSO level (CI-SOC) and part of the solution as a European Critical Infrastructure Security Analytics Network (CI-SAN). However, this concept can be easily extended to other CIs as well. The flexibility of the Security Solution's applicability stems mainly from the fact that the CI-SOC and the CI-SAN analyse data from IT systems of the electricity grid and that IT systems are largely used in all critical infrastructures. Therefore, the solution could be utilised, with minor or larger modifications, in sectors such as gas, water, oil, transportation, health, finance and telecommunications.

Within the project, a plan for the dissemination of the project results is also implemented, which aims, among others, to harmonise the developed and demonstrated Security Solution with existing policies and frameworks. The harmonisation will lead eventually to the integration of the SUCCESS Security Solution into the European Smart Grid and other CIs in Europe.

The more complex component, in terms of integration in the CIs, is the CI-SAN, because it is conceptualized as a network spanning over and gathering data from all participating countries in Europe. The integration of a CI-SAN implementation will require, therefore, a consensus among national authorities and/or stakeholders, which will also need to determine responsibilities and eventually liabilities.

The aim of this white paper is to indicate the considerations of the SUCCESS consortium and a plan for the required activities that will facilitate this integration of the CI-SAN to the European CIs.

2. A Monitoring System Detecting European-wide Attacks

We first provide a short description of the CI-SAN concept and specific development within the SUCCESS architecture and discuss the importance of the implementation of the CI-SAN.

2.1 General concept

The vision of the CIs' operation with integrated smart meters includes the smart meters installed at various points of a CI, where they measure some parameters about the status of the CI. In the case of the Smart Electricity Grid, these parameters may be frequency, voltage. They subsequently transmit these data to the responsible operator and other stakeholders, if needed. They also transmit the security logs that are temporarily stored in them, such as antivirus scans, firewall scans, attempts of unauthorised access and improperly installed new software. The operator can then analyse the data and detect any attacks at the Neighbourhood Area Network (NAN) of the CI network.

As the deployed smart meters per operator will be tens of thousands, a challenge for the state-of-the-art Intrusion Detection Systems emerges in terms of efficiency and real-time monitoring. A novel automated process needs to be implemented that can accurately detect ongoing attacks, identify threat patterns and match them to appropriate countermeasures that will mitigate the detected attacks. This requires a database with attack-countermeasure pairs that is continuously updated, by adding new pairs and optimising countermeasures according to the state of the art in security practices. A human machine interface (HMI) should allow the responsible personnel to have an overview of the grid status, of any alerts and of the status of the mitigation actions.

For the detection of European-wide attacks the collected data of all local operators are transmitted to the CI-SAN. Each operator may send the threat patterns detected by its Critical Infrastructure Security Analytics Network, security data from other internal sources (such as IT-component logs etc.) and/or pure status data originating from the smart meters, so that further data analysis can be performed with the aggregated data. The kind of information (detected

[1] Persons that consume but also produce energy (e.g. through own Distributed Energy Resources)

threat patterns, security data or data about the status of the CI) to be transmitted depends certainly on the size of the data, the transmission rate and the computing capabilities of the CI-SAN.

CI security architectures have been proposed in other research projects, such as SEGRID [6] and ECOSSIAN [7]. In SEGRID, the necessity of "a team to analyse and respond to the alerts" at the DSO level of the Smart Grid is mentioned in [8]. This team is linked to the creation of a Security Operation Centre (SOC), which will perform all activities described above. ECOSSIAN addresses the protection of all European CIs and proposes three levels of SOCs for them; an Operator Security Operation Centre (O-SOC), a National Security Operation Centre (N-SOC) and a European Security Operation Centre (E-SOC). Each tier communicates with the adjacent tiers, exchanging critical security data. The difference of SUCCESS's approach compared to ECOSSIAN lies in the fact that SUCCESS implements a security logic in the CI-SAN that performs data analysis and attack detection, whereas ECOSSIAN's E-SOC is mainly used for sharing cyber attacks information.

2.2 Benefits

The implementation of the CI-SAN concept will benefit largely CI operators but also the society in general, as many cyber attacks with disruptive consequences for the CIs will be prevented or immediately mitigated. Particularly:

- Through the analysis of the aggregated data from CIs all over Europe, widely orchestrated attacks with severe consequences can be detected,
- An incrementally populated attack-countermeasure pairs database, which will be also located at CI-SAN level, will suggest the optimal countermeasure to be initiated by the compromised CI upon detection of an attack,
- Through the threat pattern sharing mechanism, CIs can be informed in a timely way about vulnerabilities of their own systems and take preventive measures (e.g. add patches),
- Through an HMI, visualisation of the status of the CIs and of the countermeasures progress will be available and authorised personnel will be able to act manually, if required.

Furthermore, long-term cost savings will be achieved, as cyber attacks and system disruption of CIs induce high negative impacts on the economies of the countries. In several cases, cascading effects occur upon compromise of one CI, thus multiplying the costs for restoration. For instance, an attack on the electricity grid rendering it unavailable will have serious consequences on other critical sectors, such as banking and transportation. Although the probability of an extensive damage of a CI due to a cyber attack is relatively low, the large potential impact of a successful attack to the economy, as well as the further side effects – from environmental disasters to even human losses – showcase the significance of the CI-SAN.

2.3 Development within the project

As the scope of SUCCESS was originally targeted in the Smart Electricity Grid, most of the investigated use cases refer to the electricity grid. Nevertheless, as already mentioned before, the described solution can be implemented in CIs at large.

The SUCCESS solution spans from the smart meters to the CI-SAN, including the development of new-generation smart meters (Next Generation Open Real Time Smart Meter - NORM), the Critical Infrastructure Security Operations Centre (CI-SOC), a Breakout Gateway (BR-GW), which enhances the communication between NORMs and CI-SOC, and the CI-SAN.

As depicted in Figure 1, the CI-SOC is a separate actor that communicates with the NORMs through a channel of higher security compared to traditional actors. Traditional actors are considered the energy supplier, an aggregator, an Energy Service Company (ESCO) and the customer, in the case of the electricity grid. The first level of security between the Security Agent

module of the NORM and the CI-SOC is a standard VPN connection, which is also established for the communication with the traditional actors. Furthermore, the NORM contains a Physically Unclonable Function (PUF), which is used as a second level of security between the Security Agent module of the NORM and the CI-SOC, for hardware-based authentication of the NORM and for encryption of the transmitted data. The transmitted data contain only information about the status of the grid and of the NORM and do not reveal the consumers' behaviour, thus the consumers' privacy is not infringed. More information about the types of transmitted data can be found in Annex A of SUCCESS Deliverable D3.7 [9]. The BR-GW between the NORM and the CI-SOC offers higher transmission rates, integrity controls and can implement countermeasures, such as isolation of compromised NORMs from the rest of the network.

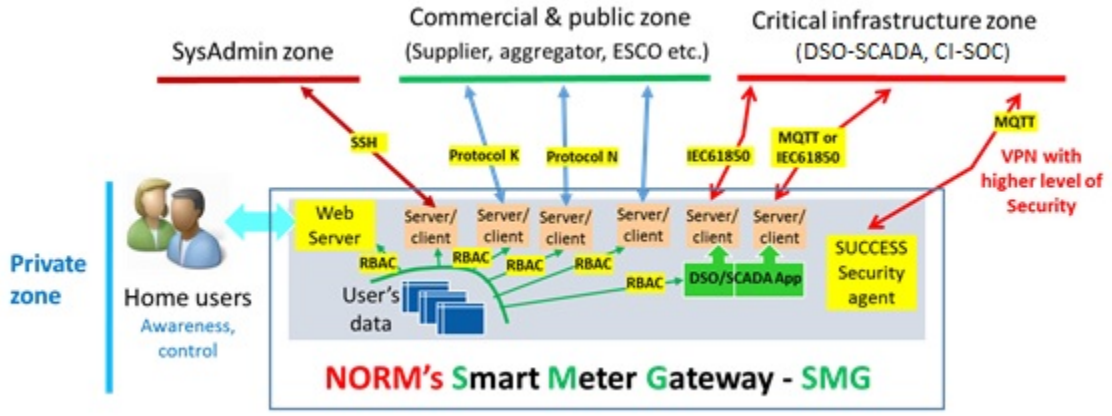


Figure 1: Actors communicating with a NORM

Figure 2 illustrates in a generic case the communication between CI-SOC and CI-SAN. SUCCESS's CI-SAN consists of Security Analytics Node (SA Node) instances, which perform data analysis at regional, national or international level, and Security Data Concentrator (SDC) instances, which gather data from CI-SOCs and transmit them to an SA Node. There is a flexibility on the locations of the SDC and SA Node instances (regional, national or international) depending on the actual needs for monitoring and attack detection. For example, it may be that:

- several utilities belonging to the same CI (e.g. electricity) share a common monitoring infrastructure,
- there is regional-level or province-level monitoring,
- there is monitoring which is cross-critical infrastructure (at local, regional/provincial or higher levels).

There is also a communication channel connecting SDC instances with each other, which is used for the immediate transmission of alarm messages about incidents and detected attacks, achieving system redundancy.

Each SA Node receives data from several SDC instances and from external public sources (not depicted in Figure 2). Within the network of the SA Node instances data analysis is performed and wide-area-orchestrated attacks that cannot be detected at a local/regional/provincial level are identified. In case of a detected attack, the responsible CI-SOC is informed by the communicating SA Node instance, so that appropriate countermeasures can be initiated. The liability for the triggering of the countermeasures is on the operators.

The CI-SAN, as it is proposed and developed by SUCCESS, offers additional benefits:

- The SDC receives anonymised data from the CI-SOC instances; therefore, any personal or operator-internal data originating from the various internal sources are not exposed to third parties.
- The inter-SDC communication enables the fast transmission of critical alarm messages and threat patterns, which could otherwise be delayed several seconds or minutes,

depending on the amount of data each SA Node receives and the computing capabilities of the network.

- The inter-SDC communication can support a fallback mode of the CI-SAN, in case an SA Node is compromised or otherwise unavailable; it creates redundancy and availability of the architecture even under adverse conditions.
- The SA Node instances, through combining information from all operators and from external sources, such as social media, weather forecast and satellite information, can detect various attacks targeted at a European level.

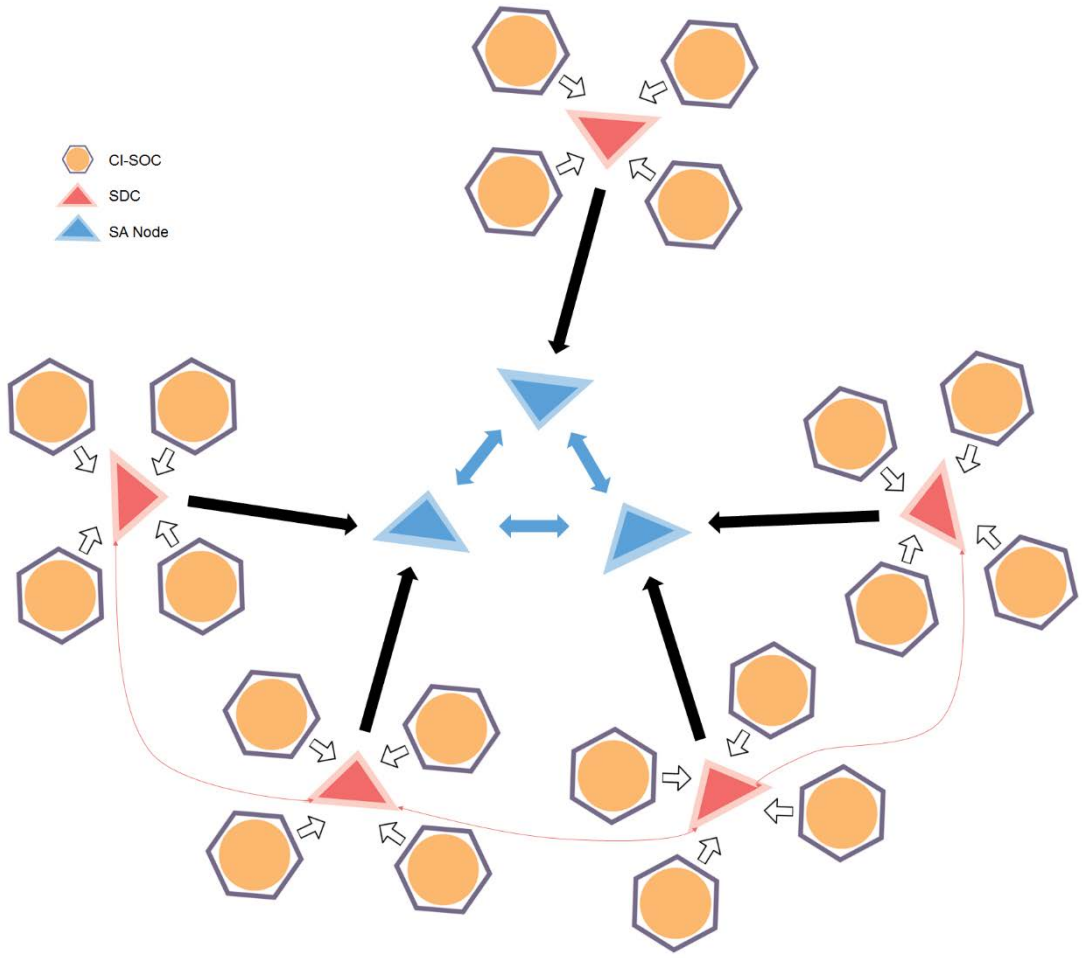


Figure 2: Functional description of SUCCESS's CI-SAN

3. Conformance to Existing Regulation

Since the adoption of ICT in CIs has already started in the EU countries and has been partly regulated, the design of a CI-SAN implementation needs to comply with the requirements and specifications set by the regulators.

The two European laws that apply to the CIs, the Network and Information Security (NIS) Directive [10] and the General Data Protection Regulation (GDPR) [11], are described in this Section.

3.1 Network and Information Security Directive

The NIS Directive includes requirements and recommendations for operators of critical services. Of particular importance to the Security Solution is the operators' obligation to "notify, without undue delay, the competent authority or the CSIRT[2] of incidents having a significant impact on the continuity of the essential services they provide" as well as the recommendation to use "European or internationally accepted standards and specifications relevant to the security of network and information systems" [10]. The competent authority and the CSIRT of each country belong to a European network, in which ENISA and the European Commission (EC) participate as well. They share knowledge and cooperate in order to mitigate detected attacks and prevent future attacks.

In SUCCESS's concept, the CI-SOC provides data to the respective local SDC module including security incidents. The SDC subsequently forwards the processed data to the SA Node and potentially to other SDC instances. Thus, the SUCCESS's CI-SAN network is similar to the European network described in the Directive but it includes only those CI operators that belong thereto. Currently, the concept was developed as a stand-alone network without the need for active involvement of ENISA or the EC. Nevertheless, an integrated concept could follow several approaches. A more separated one would treat the CI-SAN as a separate network and the CI operators will use then the CI-SAN to exchange security data and separately notify the competent authority, according to the NIS Directive, of security incidents. Another alternative is the integration of CI-SAN as the European network defined by the Directive. The latter requires an adaptation of the initial concept to the specifications of the Directive.

As far as the use of internationally accepted standards is concerned, the SUCCESS consortium has recognised its importance since the beginning of the project. A certification plan for all components developed within the project, including the CI-SAN, has been prepared and will be finalised until the completion of the project in October 2018. It includes certification of the components against European and internationally recognised standards. This will ensure to a large extent the effectiveness of their security functions and their interoperability within the SUCCESS architecture as well as with other smart and legacy devices of the CIs. More information regarding the certification plan can be found in SUCCESS Deliverable D6.7 [12]. Moreover, SUCCESS partners have been participating in meetings with standardisation bodies and stakeholder associations, disseminating the project results and promoting the integration of these results in the development of new standards. These activities have been reported in SUCCESS Deliverable D6.5 [13].

3.2 General Data Protection Regulation

The GDPR includes requirements for controllers and processors of personal data. SUCCESS has given much attention to show compliance with the Regulation; consumers' personal data are not to be sent from the NORMs to the CI-SOC for data analysis. Consequently, the SUCCESS's CI-SAN cannot receive any personal data, either. The anonymization process conducted at the CI-SOC guarantees the transmission of non-private data to the CI-SAN. Furthermore, any received social media data will correspond only to valuable public information (e.g. switching off all lights during a planned "Earth hour") and not to personal consumer behaviour. The provision for protection of personal data has led to the creation of 3 project deliverables so far, D2.1 [14], D3.2 [15] and D5.7 [16]. Their status is, however, confidential and they are thus not publicly available.

[2] Computer Security Incident Response Team

4. How to Foster the Establishment of CI-SAN

The compliance of the CI-SAN with the European legislation frameworks is a necessary but not sufficient condition for its integration in the CIs. The approach to facilitate this integration is the dissemination of the concept to respective actors that can contribute to the establishment of the CI-SAN. To this direction, SUCCESS has considered three approaches:

- To contact authorities and progress with a regulation of CI-SAN related aspects,
- To contact DSOs, TSOs and other CI operators to implement the CI-SAN concept as a market need and
- To contact DSOs, TSOs and other CI operators to influence authorities towards regulating the CI-SAN concept.

The consortium members that can undertake this task, irrespective of the adopted alternative, are the DSOs participating in the project, namely ASM Terni S.p.A from Italy [17] , Electrica SA from Romania [18] and ESB Networks Ltd from Ireland [19], as they – as end users of the system - can convey the need to local/national authorities and other domestic and foreign DSOs and CI operators. The goal is not to promote the specific implementation of a CI-SAN, as it is designed and developed in SUCCESS, but to promote the benefits of the CI-SAN concept in general.

In the first scenario, SUCCESS's DSOs contact authorities with the aim to convey the importance of securing the CIs of their countries and at a pan-European level, so that security considerations are added to regulation. The adoption of the CI-SAN, along with the entire SUCCESS general architecture can be made in the form of relevant legislation on the operation of such a system and will be accepted by all involved stakeholders.

The second scenario triggers an initiative from the operators, who will decide on the implementation of the CI-SAN based on the market need for more protection of the CIs against all kinds of cyber attacks. There will be no legislation for the establishment of the CI-SAN, except if it attracts the attention of national or European authorities at a later stage of the implementation phase.

Finally, in the last case we assume a hybrid version of the above two, where CI operators from many European countries are contacted in order to join a coalition with SUCCESS towards promoting the integration of a CI-SAN implementation in the CIs. Through this coalition, addressing authorities at a local, national and European level will be facilitated and can be more effective compared to the case that SUCCESS acts individually.

Practically, these scenarios are not mutually exclusive and will be addressed in parallel by SUCCESS. The primary vision of SUCCESS is to – ultimately – approach policy makers at a European level and regulate the CI-SAN. The establishment of the CI-SAN as an industry need without a regulatory framework can motivate stronger interest from authorities.

In Table 1, a consolidated time plan for the action points that are necessary so that CI-SAN can be established under one of the above scenarios is presented. The first couple of steps that concern the SUCCESS's DSOs making initial contacts are controllable and within the scope of influence of SUCCESS. The rest of the action points, although necessary, cannot be guaranteed by SUCCESS, because they involve communication between persons and authorities beyond SUCCESS's scope and may be delayed by various external factors. For this reason, the consortium will monitor the progress of the dissemination plan through feedback from the DSOs' initial contacts and through feedback from the EC, which supports the work of the project and will be aware of lobbying activities towards the establishment of the CI-SAN.

The following sections discuss in detail the processes that need to be followed in each approach.

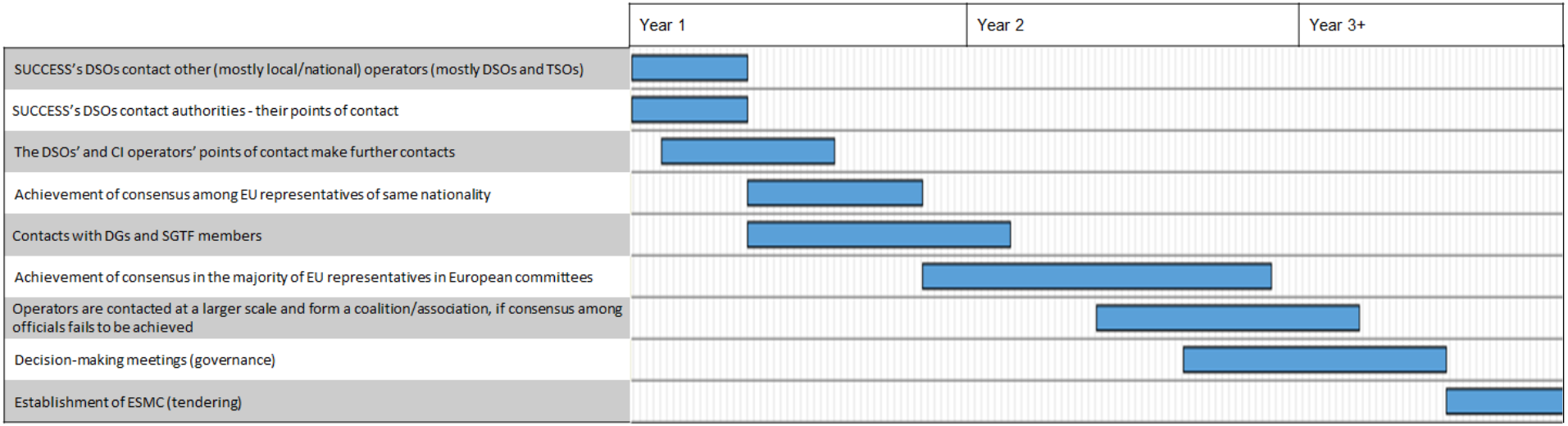
5. Direct Contact of Authorities

The processes that can be followed in this case are depicted in Figure 3 and Figure 4, since the flow of communication is not fixed and is only estimated in SUCCESS. Both processes include 5 phases, as listed below:

1. Each DSO-SUCCESS member contacts local or national authorities, who can be considered as the points of contact for the DSO.
2. The DSO points of contact address national representatives at a European committee that is related to CI protection and cyber security affairs, such as the Internal Market and Consumer Protection Committee[3], (Figure 3) or they move at a local level and address persons from other similar local/national authorities (Figure 4).
3. The people that have been contacted in Phase 2 communicate with (more) national representatives from multiple related European committees.
4. Following the same rationale as Phase 3, the word is spread among all representatives of several countries that comprise a decision-making committee at a European level.

[3] The Internal Market and Consumer Protection Committee has supported the creation of the NIS Directive and is, therefore, deemed as appropriate for the legislation of CI-SAN.

Table 1: Time plan of phases towards establishing the CI-SAN



5. In this Phase an official discussion is conducted and legislation for the CI-SAN is formulated.

The following subsections explain these phases in more detail.

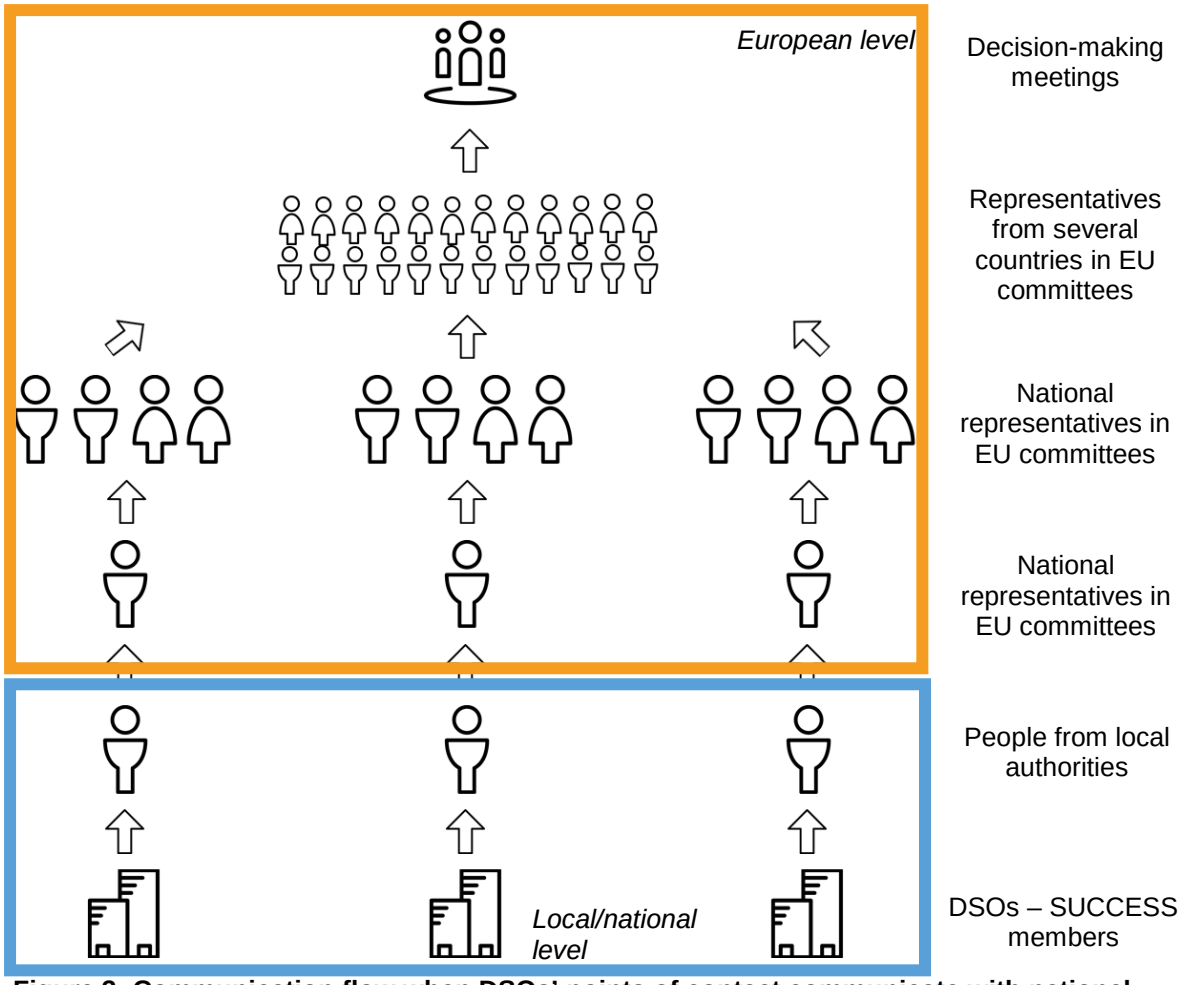


Figure 3: Communication flow when DSOs' points of contact communicate with national representatives at EU committees

5.1 DSO points of contact

DSOs participating in the SUCCESS project have points of contact in local or national authorities, whose jurisdiction may vary depending on the influence of the DSO on the society. Such points of contact can be regarded to be:

- Mayors
- People working in the ministries of energy, economy or internal affairs (ministers, secretaries etc.)
- People working in agencies that influence directly policy makers

The communication of the DSOs with local authorities is already in progress, as mentioned before, although still at an early stage to give results. At this phase, argumentation at a technical and financial level is required. The benefits of the CI-SAN compared to the current situation or to other possible implementations of a European network for security analytics of CI data, as they have been already discussed in the consortium meetings and are partially described in Chapter 2, are mentioned in the discussions between the DSOs and their points of contact.

Furthermore, the respect of the proposed solution to the consumers' personal data and privacy is stressed. Definitely, the kind of argumentation depends on the position of the point of contact and of his/her expertise. In the end, they need to act as multipliers of the concept of CI-SAN and its benefits further (such as to officials with EU influence) or to officials from other domestic or foreign ministries or agencies.

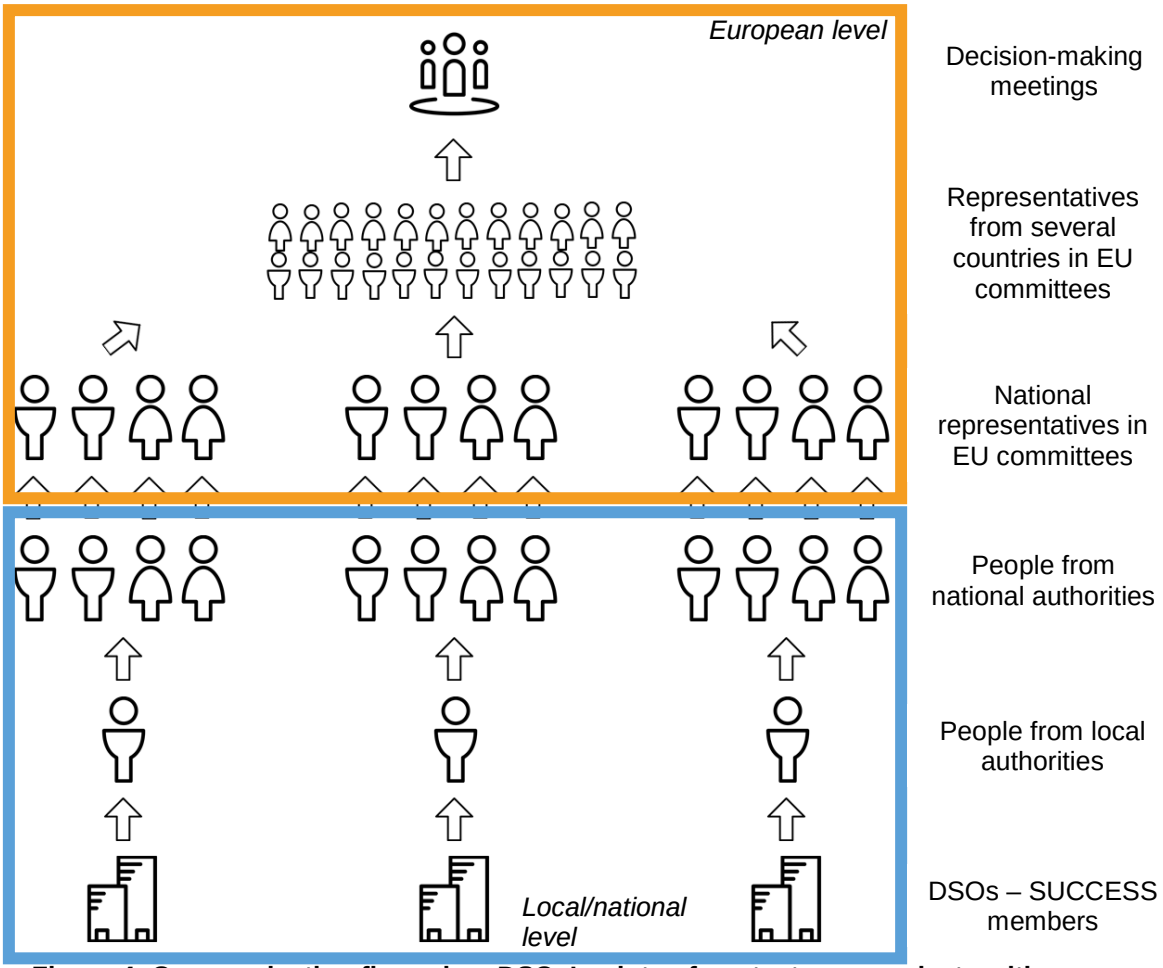


Figure 4: Communication flow when DSOs' points of contact communicate with more people from authorities

5.2 Surpassing the local level

The points of contact of the DSO, depending on their position, their affiliations with other authorities or their personal connections, can further promote the CI-SAN concept as they seem fit and contribute to relevant legislation.

At this phase, it is recommended that the benefits of the CI-SAN implementation at national and at EU level are stressed in the discussions.

5.3 Initial achievement of consensus among EU representatives

This Phase is the beginning on the attempt to achieve a European consensus about legislating on the CI-SAN. The people that have been contacted in the previous Phase can address a number of EU representatives at decision-making committees. Nationality and similar interests play often a significant soft factor role in support quests.

Due to the European perspective, the collaboration and active participation of groups that have been widely involved in the regulation of the European Smart Grid and in relevant initiatives can boost the concept of SUCCESS and facilitate its promotion. The Smart Grids Task Force (SGTF) and members of the Directorate-General (DG) committees, particularly DG Energy, DG Internal Market, Industry, Entrepreneurship and SMEs, and DG Research and Innovation are considered relevant.

Within the SGTF, Expert Group 2 focuses on regulatory recommendations for privacy, data protection and cyber-security in the Smart Grid environment. In 2017, a Working Group was launched with the aim to set the necessary conditions for a resilient and secure European Smart Grid. Among the addressed topics, cooperation and incident sharing is also investigated; therefore, CI-SAN can be introduced as a solution to this issue. In fact, the Working Group is willing to acknowledge and use work already done rather than develop a solution anew [20].

The Working Group in SGTF Expert Group 2 consists of representatives from the European Utilities Telecom Council (EUTC) [21] and the Union of Electricity Industry EURELECTRIC [22] , which are active associations for ESB Networks LTD and Electrica SA respectively. Therefore, CI-SAN can be introduced to the Working Group through these representatives, as they can be easily approached during the EUTC and EURELECTRIC meetings.

5.4 Spreading the word among members of committees

This Phase is necessary in order to ensure that many committee members are aware of and willing to support the proposal of relevant legislation on the CI-SAN. Informal discussions and agreements between peers often precede support during the official decision-making meetings.

5.5 Decision-making

Once consensus has been, informally, achieved among the members of the committee, the proposal of the legislation of CI-SAN, probably in the form of a Directive or a Regulation, can be supported and voted by the participants.

6. Contact of Operators and Industry Initiative

In this scenario, DSOs and other CI operators not participating in the project ally with the SUCCESS members and form a coalition that pursues to establish the CI-SAN. In fact, DSOs and energy network companies from various European countries have exhibited great interest in the ongoing research on the Smart Grid [23]. Particularly in the Smart Grid security domain, a number of DSOs have participated in consortia of relevant research projects, some of which are exemplarily presented in Table 2.

Table 2: DSOs participating in research projects about Smart Grid security

Research project	Participating DSOs
SEGRID [6]	Liander NV (the Netherlands), EDP (Portugal)
SPARKS [24]	SWW Wunsiedel GmbH (Germany)
SCISSOR [25]	SEA Società Elettrica di Favignana S.p.a. (Italy)
SoES [26]	Enel (Italy and worldwide)

The process that will be followed in this case is depicted in Figure 5 and consists of 3 steps:

1. The 3 DSOs participating in the project contact affiliating operators and discuss about the relevance and importance of CI-SAN.

2. The operators that have been contacted in the previous Phase contact more operators and create consensus on a large scale.
3. The operators that intend to implement the CI-SAN participate in a series of meetings that will lead to the de facto establishment of the CI-SAN.

Affiliating operators that can be approached are DSOs participating in common councils and associations with the SUCCESS-DSOs, at local/national or even European level. For example, ESB is a member of the EUTC, along with energy utilities from all over Europe, such as EDP (Portugal), E.ON (Sweden), Enel (Italy) and Iberdrola (Spain). These DSOs are members in other associations as well, such as the European Distribution System Operators' Association for Smart Grids (EDSO) [27], the European Network for Cyber Security (ENCS) [28] and the Smart Energy Demand Coalition (SEDC) [29]. Similarly, Electrica is affiliated to EURELECTRIC and to several national associations. Through the regular meetings of all these groups, the concept of CI-SAN can be fostered and consensus at European operators level can be achieved.

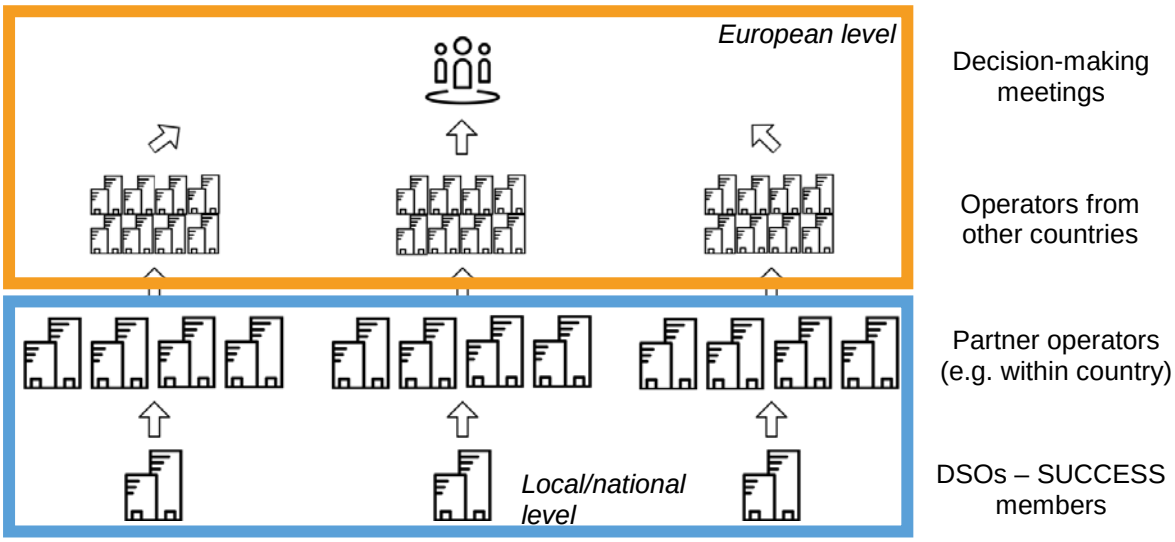


Figure 5: Communication flow when DSOs contact operators and establish CI-SAN as a market need

6.1 Phases 1 and 2: Spreading the word among operators

The first two phases aim to create a coalition of operators that will be aligned with the concept of the CI-SAN, as it is proposed by SUCCESS. These are necessary steps, as CI-SAN is based on knowledge sharing and the participation of many operators will lead to a more efficient operation of CI-SAN.

6.2 Decision-making

The operators that have agreed on the implementation of CI-SAN can, then, form an association that will discuss some important aspects regarding the CI-SAN, such as who may be the responsible actor for running and supervising the CI-SAN, tendering procedures for buying the necessary equipment and financial planning.

7. Contact of Operators to Promote Legislation

The process that will be followed in this scenario is presented in Figure 6 and consists of 5 phases. Since a desirable goal is the establishment of CI-SAN related regulation at a European level, these phases are quite similar to the respective ones described in Section 5. The differences lie in the first phases, at which the 3 DSOs participating in the SUCCESS project contact other operators. Subsequently, all operators, including the 3 DSOs-SUCCESS

members, communicate with their points of contact in order to promote the formulation of a legislation at European level.

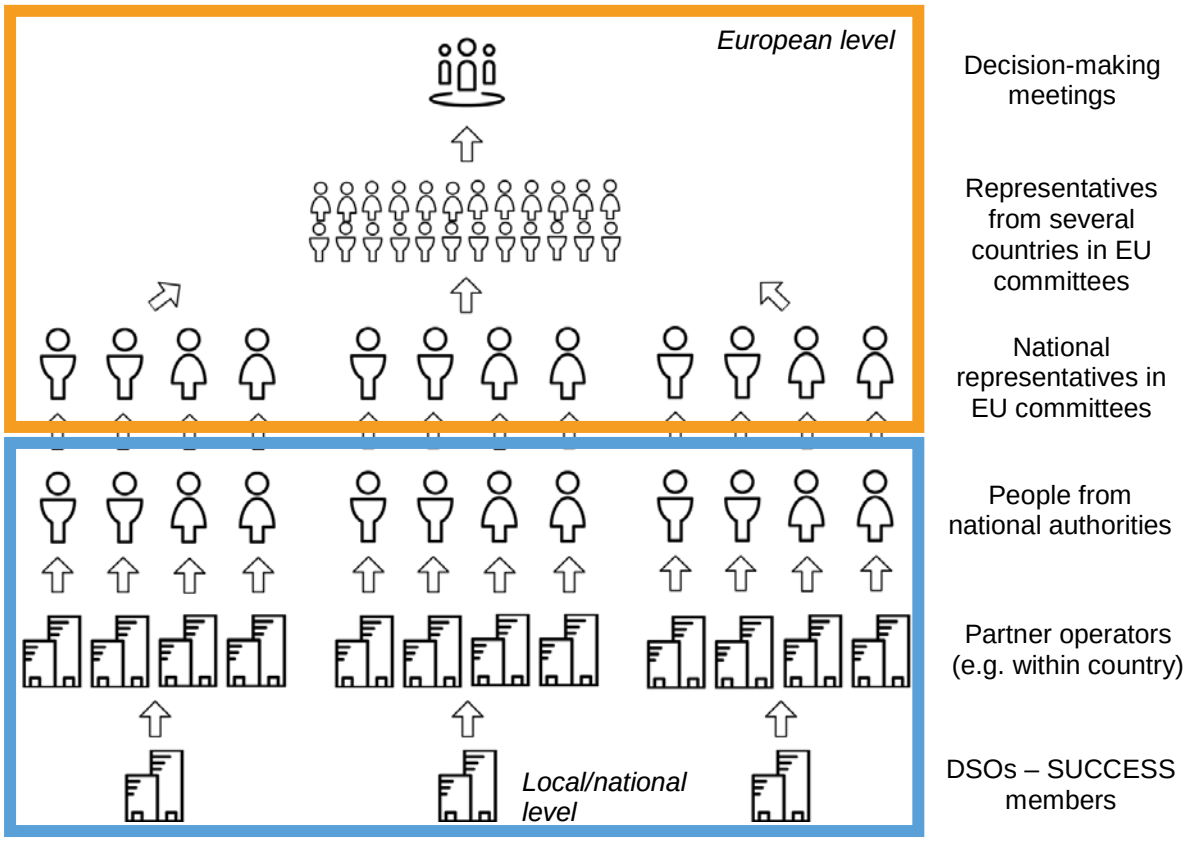


Figure 6: Communication flow when DSOs contact operators and jointly address regulators

8. Conclusion

The transition to a modernised CI network with ICT capabilities gives many new opportunities to operators, end users and other stakeholders but also creates vulnerabilities. There is thus a need for a plan from authorities, standardisation bodies and CI operators, so that the CIs can be secure and resilient against attacks.

The SUCCESS project proposes an architecture that monitors and eventually protects CIs from cyber attacks. Among the developed components, the CI-SAN distinguishes as the component that enables attack detection at a pan-European level. SUCCESS is developing a prototype of the CI-SAN, which needs to be accepted by national and European authorities. There are also some aspects in the implementation plan that need to be decided by high-level officials. SUCCESS comes with an effective dissemination plan that includes contacting authorities and operators, so that the implementation of the Security Solution and the CI-SAN in particular is promoted. Initial steps to this direction have already been triggered by SUCCESS's members and SUCCESS aspires that the dissemination plan will progress as expected.

These attributes are very important for a research project as they bridge the gap between a prototype implementation and its actual deployment according to legislation and industry needs and enable a smooth adoption of the proposed architecture.

9. References

[1] F. Aloul, A. R. Al-Ali, R. Al-Dalky, M. Al-Mardini and W. El-Hajj, “Smart Grid Security: Threats, Vulnerabilities and Solutions,” September 2012. [Online]. Available: http://www.ijsgce.com/uploadfile/2012/1011/20121011121836539.pdf. [Accessed 6 November 2017].

[2] California State University Sacramento, “Smart Grid Cyber Security Potential Threats, Vulnerabilities and Risks,” May 2012. [Online]. Available: http://www.energy.ca.gov/2012publications/CEC-500-2012-047/CEC-500-2012-047.pdf. [Accessed 6 November 2017].

[3] SUCCESS, “Deliverable D1.2: Identification of existing threats V2,” 2017.

[4] M. R. Asghar, G. Dán, D. Miorandi and I. Chlamtac, “Smart Meter Data Privacy: A Survey,” IEEE Communications Surveys & Tutorials, vol. 19, no. 4, pp. 2820-2835, 2017.

[5] A. Teixeira, G. Dán, H. Sandberg, R. Berthier, R. B. Bobba and A. Valdes, “Security of Smart Distribution Grids: Data Integrity Attacks on Integrated volt/VAR Control and Countermeasures,” Proc. of American Control Conference (ACC), 2014.

[6] SEGRID, “SEGRID project website,” [Online]. Available: https://segrid.eu/. [Accessed 6 November 2017].

[7] ECOSSIAN, “ECOSSIAN project website,” [Online]. Available: http://ecossian.eu/. [Accessed 6 November 2017].

[8] SEGRID, “Security for smart electricity GRIDs,” 1 June 2017. [Online]. Available: https://segrid.eu/wp-content/uploads/2017/07/Whitepaper-SEGRID.pdf. [Accessed 6 November 2017].

[9] SUCCESS, “Deliverable D3.7: Next Generation Smart Meter, Version 1,” 2017.

[10] European Parliament and Council, “Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union,” 6 July 2016. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN. [Accessed 6 November 2017].

[11] European Parliament and Council, “Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation),” 27 April 2016. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN. [Accessed 6 November 2017].

[12] SUCCESS, “Deliverable D6.7: Report on Certification Preparation V1,” 2017.

[13] SUCCESS, “Deliverable D6.5: Report on Standardisation and Policies V2,” 2017.

[14] SUCCESS, “Deliverable D2.1: Recommendation on How to Develop Data Privacy Compliant Countermeasures,” 2016.

[15] SUCCESS, “Deliverable D3.2: Privacy-Preserving Information Security Architecture V2,” 2017.

[16] SUCCESS, “Deliverable D5.7: Data Management Plan for Trials V1,” 2017.

[17] ASM Terni S.p.A, “ASM Terni S.p.A website,” [Online]. Available: http://www.asmterni.it/. [Accessed 16 November 2017].

[18] Electrica S.A., “Electrica S.A. website,” [Online]. Available: https://www.electrica.ro/en/. [Accessed 16 November 2017].

[19] ESB, “ESB website,” [Online]. Available: https://www.esb.ie/. [Accessed 16 November 2017].

[20] Smart Grids Task Force, “Documents for input to define the Terms of Reference For the Working Group on Cybersecurity,” [Online]. Available: https://ec.europa.eu/energy/sites/ener/files/documents/eg2_-_tor_cyber.pdf. [Accessed 5

December 2017].

[21] EUTC, “EUTC website,” [Online]. Available: https://utc.org/europe/. [Accessed 5 December 2017].

[22] EURELECTRIC, “EURELECTRIC website,” [Online]. Available: http://www.eurelectric.org/. [Accessed 5 December 2017].

[23] C. Cambini, A. Meletiou, E. Bompard and M. Masera, “Market and regulatory factors influencing smart-grid investment in Europe: Evidence from pilot projects and implications for reform,” 25 March 2016. [Online]. Available: https://ac.els-cdn.com/S095717871630073X/1-s2.0-S095717871630073X-main.pdf?_tid=9c7eb054-cab3-11e7-8620-00000aacb35f&acdnat=1510826023_12cf16c0276f4a0d8b02d40b2cd3503b. [Accessed 16 November 2017].

[24] SPARKS, “SPARKS project website,” [Online]. Available: https://project-sparks.eu/. [Accessed 8 November 2017].

[25] SCISSOR, “SCISSOR project website,” [Online]. Available: https://scissor-project.com/. [Accessed 8 November 2017].

[26] SoES, “SoES project website,” [Online]. Available: http://www.soes-project.eu/. [Accessed 8 November 2017].

[27] EDSO for smart grids, “EDSO for smart grids website,” [Online]. Available: https://www.edsoforsmartgrids.eu/. [Accessed 5 December 2017].

[28] ENCS, “ENCS website,” [Online]. Available: https://encs.eu/. [Accessed 5 December 2017].

[29] SEDC, “SEDC website,” [Online]. Available: http://www.smartenergydemand.eu/. [Accessed 5 December 2017].