21, rue d'Artois, F-75008 PARIS
http://www.cigre.org

PS2-13

D2 Colloquium 2019

Cyber security requirements of multi-operator IT/OT architectures based on NISTIR 7628 guidelines

M. G. TODESCHINI*, G. DONDOSSOLA
RSE - Transmission and Distribution Technologies Department
Italy

SUMMARY

Whenever a power system control architecture has to be extended with new functionalities it is necessary to manage the effects of design choices on cybersecurity. Standards, methodologies and support tools can provide indications already in the early design phases, preventing costly corrective actions; this paper describes the approach proposed in the European project OSMOSE "Optimal System-Mix Of flexibility Solutions for European Electricity". Within OSMOSE a new Zonal Energy Management System (Z-EMS) is being designed; it is an EMS conceived to operate at the scale of few Italian administrative regions with the objective to manage the power congestions on the sub-transmission grid by coordinating different sources of flexibility (e.g. industrial loads, power flow control systems and generators), favouring at the same time the production of energy from Renewable Energy Sources (RES). The Z-EMS has to be integrated into a pre-existing monitoring and control architecture; its main inputs are the network state, the forecasts on loads and renewable generators and the capacity limits of the lines, while its output provides the corrective dispatching actions that the operators have to implement to avoid the risk of congestion.

This paper describes the methodology used to determine the cybersecurity requirements to be applied to the extended IT/OT (Information Technology/Operational Technology) control architecture resulting from the introduction of Z-EMS; in particular, starting from the high-level architecture of subsystems interacting with Z-EMS, a series of high-level cybersecurity requirements were determined by applying the NISTIR 7628 guidelines. Initially the high level-architecture has been specified and mapped to the SGAM (Smart Grid Architecture Model) plane with the support of specific software tools, focusing on the identification of the fundamental subsystems involved by the main data exchanges. The subsystems were then associated to the actors identified by the NISTIR 7628 guidelines; while doing this it has been necessary to enrich some NISTIR actors with new interfaces because those made available were not adequate to represent the functionalities of the updated architecture subsystems; the extensions were done in analogy and in accordance with the NISTIR methodology.

In summary the contribution of this paper consists in the application of the NISTIR 7628 methodology for the definition of high-level security requirements of an innovative smart grid application. This activity should be applied whenever a new power control architecture needs to be made secure by design or when a pre-existing architecture needs to be significantly modified.

KEYWORDS

Cyber Security - Smart Grid – Information Technology/Operational Technology - Congestion Management

* maurogiuseppe.todeschini@rse-web.it

1 INTRODUCTION

Whenever a power system control architecture has to be extended with new functionalities it is necessary to manage the effects of design choices on cybersecurity. The Z-EMS which is being designed within OSMOSE European project [1] is conceived to operate at the scale of few Italian administrative regions with the goal to mitigate power congestions on the sub-transmission grid by coordinating different sources of flexibility (e.g. industrial loads, power flow control systems and generators), favouring at the same time the production of energy from Renewable Energy Sources (RES). The Z-EMS has to be integrated into a pre-existing monitoring and control architecture, which must be appropriately extended and adapted in order to allow the necessary exchange of information.

This paper describes the methodology used to determine the cybersecurity requirements to be applied to the extended IT/OT (Information Technology/Operational Technology) architecture resulting from the introduction of Z-EMS; the architecture comprises the relevant subsystems of the Transmission System Operator (TSO) and of the main third parties: industrial flexible-loads operators, renewable power plants owners and aggregators of flexible resources. The methodology follows NISTIR 7628 guidelines [2] with ad hoc extensions.

Hereafter the NISTIR 7628 guidelines are introduced, which define the fundamental process which has been followed to determine security requirements. In order to fulfil the process, SGAM Toolbox software support tool has been adopted as it is briefly presented. High-level OSMOSE architecture components are introduced to present the key step of mapping the components to NISTIR actors. Subsequently the other relevant steps of identifying logical interfaces and their categories are described, which lead directly to the list of security requirements which is the final objective of the work reported.

2 NISTIR 7628 GUIDELINES

NISTIR 7628 “Guidelines for Smart Grid Cybersecurity” is a reference document of U.S. National Institute of Standards and Technology to provide guidance to organizations operating in the field of smart grid in order to prevent or mitigate the effects of cybersecurity threats. In particular the guidelines provide an analysis process to select and modify security requirements applicable to the smart grid.

The process is centered around a set of actors and domains which have been identified and are relevant for the operation of the smart grid; between the couple of actors which routinely interact, NISTIR 7628 has identified logical interfaces which handle support information flows and operation of the actors. Actors are the nodes and interfaces are the arcs of the graph called Logical Reference Model of Figure 1.

Each interface transports a set of information which has security requirements that NISTIR 7628 assigns on the base of a category. Categories are defined on the nature of data handled, on the performance requirements of the interface, on the owners of the systems and of the data, on the potential impact that an incident involving the interface has on confidentiality, integrity and availability of information, and other criteria. A set of security requirements are assigned to each category; usually a single security requirement is associated to multiple interfaces. In particular NISTIR 7628 identifies three macro-categories of requirements:

- Unique Technical Requirement (UTR): are specific of a subset of interfaces but not all the interfaces of the model.
- Common Technical Requirement (CTR): are general enough to be applied to every logical interface identified in the guidelines.
- Governance, Risk, and Compliance (GRC): are centered around policies procedures and compliance activities and are addressed to the organizational level more than the technical level.

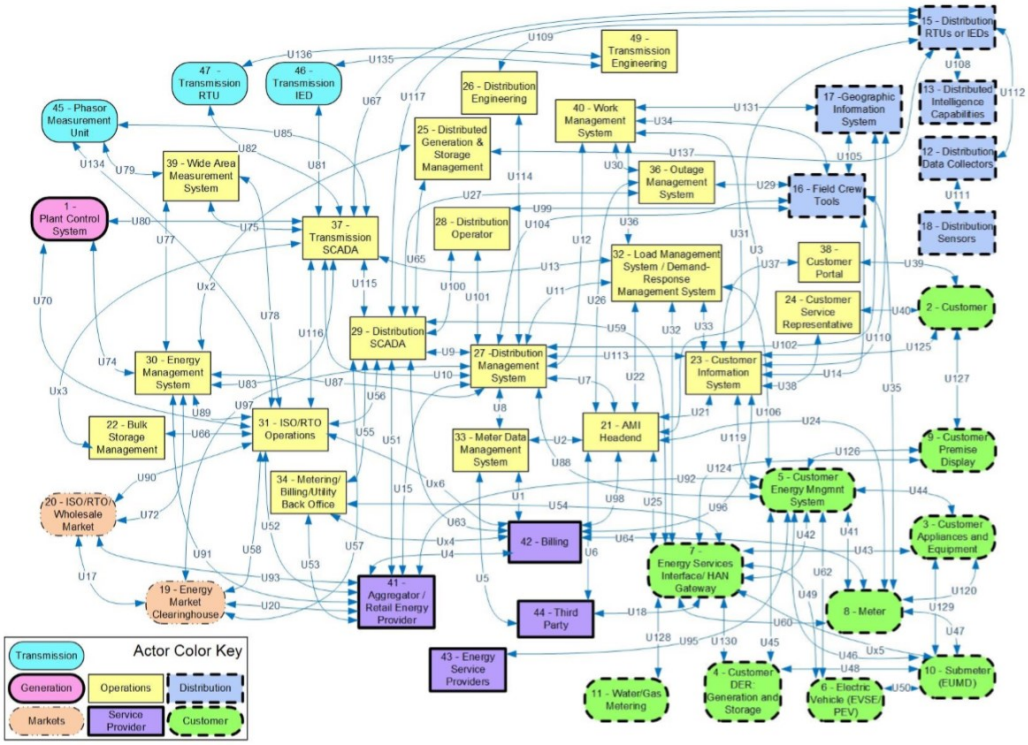

FIGURE 1: NISTIR 7628 LOGICAL REFERENCE MODEL

2.1 SGAM TOOLBOX

The Smart Grid Architecture Model (SGAM) introduced by the Smart Grid Coordination Group [3] is a suitable instrument to architect smart grids. Following SGAM, smart grids are designed on multi-layer planes each representing information exchange with a specific point of view and level of detail. Each SGAM plane organizes the components involved in smart grid operation in a grid of domains and zones which are specific to the electrical energy supply chain.

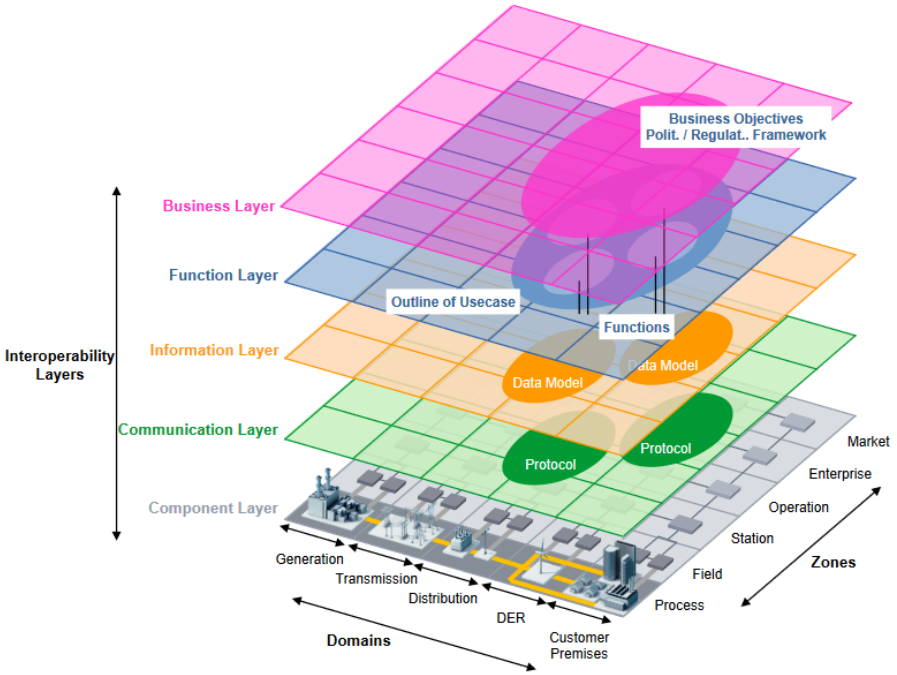

FIGURE 2: SMART GRID ARCHITECTURE MODEL

In order to support the identification of security requirements for project OSMOSE the software support tool SGAM Toolbox [4] has been leveraged, which merges SGAM framework and NISTIR 7628 LRM allowing designing the architecture and supporting the identification of relevant security requirements.

3 OSMOSE ARCHITECTURE

As part of the OSMOSE project, a set of subsystems, components and operators (components) have been identified that must interact in order to support the functionalities that the Z-EMS component will provide. The interaction can consist in:

a) data access: Z-EMS needs data about the current state of network, forecasts regarding energy needs at different segments and weather conditions that influence energy need and transmission, load distribution, network topology and lines capabilities;
b) information output: some components can collect/generate/provide information to support other systems or human operators in making decisions about conduction or corrective actions that have to be applied to the sub-transmission network. These components are output devices for information in a suitable format that can be consumed by the intended user (human or system);
c) command input: some components have the capability to be used as interfaces to enter instructions to change the operation of power transmission grid or to control the operation of other components of the system. These components are input devices for commands addressed to the components of the system including those that can control the performance and operation of the power grid.

In particular the data exchanges which has been categorized at points b) and c) of the previous list are not necessarily associated to different components: in general it is quite common that a single component which allows an operator to input commands intended to modify the operation of the power grid or to modify the behaviour of a component (as in point c)), also integrate the facilities which provide the output to support operator situation awareness and decision making, and to verify that commands have been applied or queued.

The relevant component which have been identified in OSMOSE project are listed in Table I.

TABLE I: CONGESTION MANAGEMENT - RELEVANT COMPONENTS

Component	Function
Aggregator	An aggregator joins multiple generation and/or load systems and intermediates the access to the resources.
Ancillary services market	Access to ancillary services market provides Z-EMS the information about flexibility market which is required by Z-EMS to provide its services.
DTR (Dynamic Thermal Rating) system and sensors	A system to evaluate power lines performance and limits.
EMS (Energy Management System)	National level EMS which provides the dispatch schedule, grid topology, network status and relevant electrical measurements.
Generation and load forecasting system	A system that provides short term forecasts of generation and load.
Generation system	A single generation system (e.g. a RES) connected to the zonal sub-transmission grid.

Component	Function
Load system	A single load that is connected to the zonal sub-transmission grid and provides flexibility/interruptability on demand.
NCC (National Control Center)	An operator of NCC who is in charge of operating or controlling the zonal sub-transmission High-Voltage (HV) grid.
PFC (Power Flow Control) device	D-FACTS (Distributed Flexible AC Transmission System) can be used to control power flow by changing the effective impedance of a transmission line.
RCC (Regional Control Center)	An operator of RCC who is in charge of operating or controlling the zonal sub-transmission High-Voltage (HV) grid.
Z-EMS (Zonal EMS)	Z-EMS reduces zonal congestions on the sub-transmission HV grid by exploiting flexible loads, PFC devices, RES generators and storages.

All the components listed in Table I are not necessarily single hardware component but may be complex systems composed by a set of sub-components; complex systems can be reduced to a single (macro)component as long as the information exchange, in terms of data security (e.g. confidentiality, integrity and availability) and bandwidth/latency requirements, are well defined and categorized.

Some components, more than others, require human intervention; it is the case in particular of NCC and RCC which are not discrete components but can be thought as the interfaces which support the operator in making decisions and applying commands to ensure optimal performance.

In some cases only the "border" component is considered as in the case of the `Aggregator` which mediates the information exchange with a set of third party generation systems and loads; indeed the focus of this analysis is on all information flows involving the Transmission System Operator.

The information flow between components is the relevant aspect on which NISTIR 7628 focuses; each flow has specific security/reliability requirements which depend on the nature of data that is transferred and its purpose; the flows of OSMOSE architecture are shown with blue lines in Figure 3. The guidelines support the activity of identifying requirements by following a multi-step procedure which begins with the mapping of the components of OSMOSE architecture with a set of actors that have been identified in the guidelines.

Since OSMOSE project introduces a new component in an operational architecture, the focus is on the repercussions in terms of security of this extension and on the security measures which have to be applied to protect the information handled by Z-EMS.

4 MAPPING OSMOSE COMPONENTS TO NISTIR 7628 ACTORS

In order to leverage the NISTIR 7628 process, the components of the Congestion Management architecture have been mapped to NISTIR 7628 actors; the mapping has been addressed by similarities in purpose, performance and manipulated information. In some cases the analogies are evident also from the terminology used to indicate the components of the Congestion Management architecture and NISTIR actors, as in the cases of Aggregator, EMS and Z-EMS. In other cases there is no identity but, taking into consideration the level of detail of the requirements provided by the NISTIR guidelines and the methodology that allows them to be obtained, a suitable analogy has been found between the behaviour of components and actors that ultimately lead to the identification of the corresponding security requirements; this happens for example for DTR system and sensors, which are mapped, respectively to WAMS and PMU. Sometimes instead of mapping all the sub-components of a complex system, the system has been mapped to a single relevant actor which in reality would correspond only a sub-component of the whole: this has been possible if the sub-component/actor handles most of the

information exchange or is a gateway of the data manipulated by the whole system. This happens for example to Load, Generation and PFC devices. A noteworthy circumstance regards NCC and RCC which, similarly to the previous situation are complex systems mapped to a single actor which in principle represents only a limited subset of their functionalities and activities. In this case anyway information flow from Z-EMS is intended primarily to human operators from the SCADA back ends, therefore NCC and RCC are both mapped to Transmission SCADA actor which, among NISTIR 7628 set, better summarizes the kind of operations that are foreseen and therefore the security requirements which should be satisfied.

TABLE II: MAPPING COMPONENTS-ACTORS

Component	**NISTIR 7628 Actor**
Aggregator	Aggregator/Retail Energy Provider
Ancillary services market	Independent System Operator/Regional Transmission Organization Wholesale Market (ISO/RTO)
DTR system	Wide Area Measurement System (WAMS)
DTR sensors	Phasor Measurement Unit (PMU)
EMS	Energy Management System (EMS)
Generation and load forecasting system	N/A
Generation system	Plant Control System – Distributed Control System
Load system	Distribution Remote Terminal Unit/Intelligent Electronic Device (RTUs or IEDs)
NCC	Transmission SCADA
PFC device	Transmission IED
RCC	Transmission SCADA
Z-EMS	Energy Management System (EMS)

As reported in Table II no NISTIR 7628 actor has been mapped to the component "Generation and load forecasting system"; this component is really a set of components which gather information from very diverse sources and make them accessible to Z-EMS. Associating a component to an actor eases the following steps of NISTIR 7628 process, but is not essential: interfaces and categories can be associated on the base of NISTIR classifications.

5 OBTAINING CYBER SECURITY REQUIREMENTS

The process of determining NISTIR 7628 security requirements passes through the identification of the category of the logical interfaces which handle interoperation between actors. Having identified actors associated to OSMOSE components eases this step since NISTIR has identified a set of predefined interfaces between pairs of actors which routinely interact and has associated categories to these interfaces.

In Figure 3 the interfaces are shown in green labels near the information flow they refer to; the interface category is written in white labels below interface name.

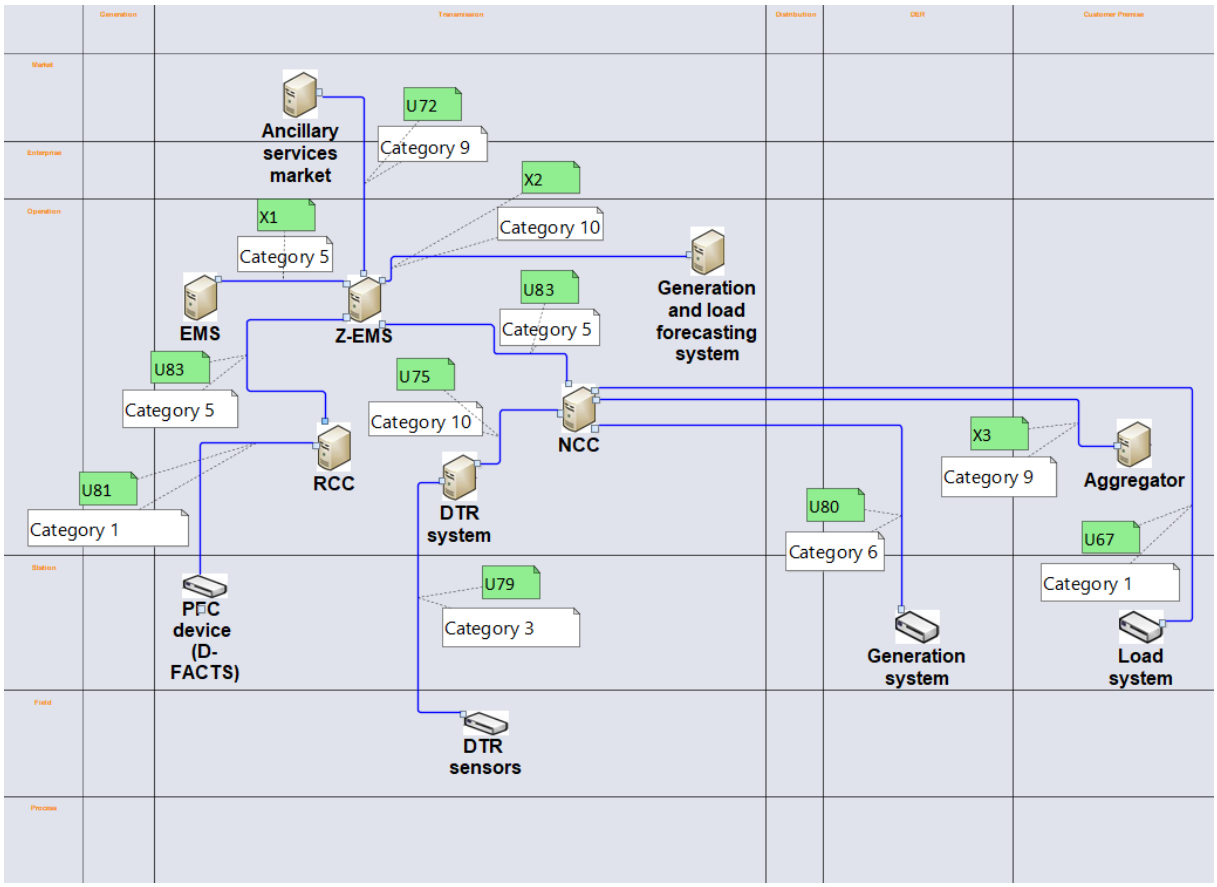

FIGURE 3: CONGESTION MANAGEMENT ARCHITECTURE

Interface names starting with letter 'U' are directly suggested by NISTIR guidelines as is their category; sometimes a limited number of alternative categories are indicated and the solution designer has to select the most suitable to the use case, based on its expertise and the suggestions of the guidelines.

The interfaces whose name starts with letter 'X' are not directly suggested by NISTIR 7628 but have been introduced in the model as an extension and in conformity with the guidelines; in particular:

- X1: NISTIR doesn't define interfaces between actors of the same type, but *Category 5* has been considered the most suitable because of the description (see Table III) and the examples of the guideline which show that it can be used for actors of the same type.
- X2: *Generation and load forecasting system* has not been associated to an actor, but it is likely to be composed of non-control systems which conform *to Category 10* description.
- X3: the guidelines don't identify a direct interface between *Transmission SCADA* actor (NCC) and *Aggregator*. Information exchange should be similar to NISTIR interface U51 between Distribution SCADA and Aggregator, which NISTIR assigns to *Category 9*.

TABLE III: NISTIR 7628 INTERFACE CATEGORIES

NISTIR 7628 Interface Category	Description
Category 1	Interface between control systems and equipment with high availability, and with compute and/or bandwidth constraints
Category 3	Interface between control systems and equipment with high

NISTIR 7628 Interface Category	Description
	availability, without compute nor bandwidth constraints
Category 5	Interface between control systems within the same organization
Category 6	Interface between control systems in different organizations
Category 9	Interface with B2B connections between systems usually involving financial or market transactions
Category 10	Interface between control systems and non-control systems

The list in Table IV is obtained merging the UTR requirements that NISTIR 7628 associates to each category. For brevity only UTR requirements are reported because they are directly dependent on the Congestion Management architecture; the GRC and CTR requirements must also be evaluated during the design phase, but being more general they are likely to be less impacted on an architecture update determined by the introduction of Z-EMS.

TABLE IV: NISTIR 7628 SECURITY REQUIREMENTS

Requirement Id	Description
SG.AC-11	Concurrent Session Control
SG.AC-12	Session Lock
SG.AC-13	Remote Session Termination
SG.AC-14	Permitted Actions without Identification or Authentication
SG.AC-15	Remote Access
SG.AU-16	Non-Repudiation
SG.IA-4	User Identification and Authentication
SG.IA-5	Device Identification and Authentication
SG.IA-6	Authenticator Feedback
SG.SC-3	Security Function Isolation
SG.SC-5	Denial-of-Service Protection
SG.SC-7	Boundary Protection
SG.SC-8	Communication Integrity
SG.SC-9	Communication Confidentiality
SG.SC-17	Voice-Over Internet Protocol
SG.SC-26	Confidentiality of Information at Rest
SG.SC-29	Application Partitioning
SG.SI-7	Software and Information Integrity

The solution designer has to evaluate each requirement to determine how it can be implemented in the specific application scenarios. As an example, requirement SG.SC-17 for protecting the use of VoIP could be ignored if Voice Over IP is not allowed within the operator's control network. NISTIR provides description of each requirement with information on when and how to apply the requirement, as well as on how to make it more effective if the impact of a security breach would have significant consequences. The NISTIR guidelines in fact give an indication of the impact of security breakdown for each individual category and which impact each requirement is recommended.

6 CONCLUSIONS

In this paper NISTIR 7628 guidelines have been applied to the control scenario of the European project OSMOSE where it is planned to implement a new functionality within an already existing and operational architecture. The guidelines are effective already from the early design phases of the architecture because they can be easily realigned to the evolution of the architecture, especially using a support software tool. In situations not already covered by the guidelines, extensions have been introduced in accordance with existing logical interfaces and categories.

The result is a list of security requirements that the guidelines suggest to the solution designer; part of the requirements depend on the architecture, while others are independent. Globally the methodological approach provided by the guidelines proved to be quite effective in supporting the security analysis, although the requirements must be further evaluated by IT/OT competent technicians to verify how to implement them and which alternatives to prefer.

7 ACKNOWLEDGMENT

This work has been financed by the European Union's Horizon 2020 Innovation Action OSMOSE under grant agreement n°773406, and by the Research Fund for the Italian Electrical System in compliance with the Decree of Minister of Economic Development April 16, 2018.

BIBLIOGRAPHY

[1] "OSMOSE - Optimal System-Mix Of flexibility Solutions for European electricity," [Online]. Available: https://www.osmose-h2020.eu/. [Accessed 13 02 2019].

[2] NIST - U.S. Department of Commerce, "NISTIR 7628 Revision 1 - Guidelines for Smart Grid Cybersecurity," 2014. [Online]. Available: https://doi.org/10.6028/NIST.IR.7628r1. [Accessed 31 01 2019].

[3] Smart Grid Coordination Group, "Smart Grid Reference Architecture," CEN/CENELEC/ETSI, 2012.

[4] Neureiter, M. Uslar, D. Engel and G. Lastro, "A Standards-based Approach for Domain Specific Modelling of Smart Grid System Architectures," in *Proceedings of International Conference on System of Systems Engineering (SoSE)*, Kongsberg, Norway, 2016.