Cyber Security of Smart Grid Communications: Risk Analysis and Experimental Testing

Giovanna Dondossola and Roberta Terruggia

Abstract. The book chapter deals with the cyber security evaluation of active distribution grids characterized by a high level penetration of renewable Distributed Energy Resources (DER). This evolution of the energy infrastructure introduces significant changes in the control and communication functions needed for meeting the technical, security and quality requirements during the grid operation. The risk analysis and treatment of fully controllable smart grid energy infrastructures require effective evaluation tools and scalable security measures. The analysis focuses on a Voltage Control function in medium voltage grids addressing voltage stability of the power grid when a consistent amount of distributed renewable sources are connected. For this reason the chapter analyses the most relevant security scenarios of an ICT (Information and Communication Technology) architecture implementing this control application. The risk level resulting from the analysis are linked to security requirements and standard measures whose deployment in real scale infrastructures requires the security testing of application architectures. The chapter presents an experimental environment for the security testing and evaluation of voltage control communications. This includes the test bed set up, the test cases and the evaluation framework to be used for measuring the attack effects on substation-DER communications and verifying the mitigation capability of standard security measures.

1 Introduction

The evolution of the energy markets all over the world is imposing a significant enhancement in the control and operation infrastructures of electrical distribution grids. The new infrastructures of the energy grids are characterized by more complex system topologies, where high, medium and small size generators, loads and storage devices are connected at the different voltage levels of the electrical

Giovanna Dondossola · Roberta Terruggia
Ricerca Sistema Energetico RSE SpA, Via Rubattino 54 20134 Milan, Italy

S.K. Khaitan, J.D. McCalley, and C.-C. Liu (eds.), *Cyber Physical Systems Approach to Smart Electric Power Grid*, Power Systems, DOI: 10.1007/978-3-662-45928-7_7

networks. The SCADA (Supervisory Control And Data Acquisition), automation, control and protection systems currently deployed in bulk generation plants, transmission and distribution substations and their field devices have to be enhanced with new control functionalities needed for the technical and economic optimization of the grid operation. The underlying ICT architectures of smart grids are necessarily based on heterogeneous systems and third party telecommunication services allowing to economically and efficiently support the communication needs of multiple actors. In this power grid technological evolution the role of ICT is becoming increasingly relevant and the power system community is now aware that the security and efficiency of the power delivery depend on the resilience of the intrinsically vulnerable electronic technologies. The need of managing the ICT risks mainly motivates the high priority given to the cyber security aspects by all smart grid research roadmaps.

The methods and technologies developed for securing mass IT applications and telecommunication services are a starting ground, but new solutions specific for the power environment are needed. For this reason the state of the art of smart grid security is progressing towards the development of standard methodologies and measures declined in the context of the smart grid functions. The needs perceived from the smart grid stakeholders fall in the areas of risk assessment, security requirement definition and measure evaluation. The objective of the chapter is to exemplify, through a representative application of the power grid evolution, the correlations between the risk analysis and the evaluation of the security requirements.

The structure of the chapter is as follows: Section 2 provides an overview of related works in cyber security of smart grids; Section 3 introduces the key elements of the Voltage Control use case ICT architecture. Section 4 presents the benchmark grid and the security scenarios addressed in the analysis. Section 5 describes the use of a qualitative approach for the risk analysis of the Voltage Control scenarios. Section 6 identifies the security requirements and technical standards that need to be implemented considering the risk levels analysis. Section 7 focuses on the architecture and key features of the experimental environment implemented taking into account the Voltage Control scenarios and the related security measures. Finally Section 8 provides some highlights about future research directions.

2 Related Works

In the last five years several European and International initiatives related to the standardization of the energy grid technologies ([1],[2],[3],[4]) stressed the importance of cyber security in the smart grid context.

A first significant reference about the security of smart grid architectures and communication interfaces is the NIST report [5].

Two years later the European Smart Grid Coordination Group issued the First Set of Standards report [6] mapping the information, communication and security standards over the Smart Grid Architecture Model (SGAM), the Use Cases report

[7] about the use case approach, and the Smart Grid Information Security (SGIS) report [8] suggesting, among other things, a qualitative method for the risk analysis of the use cases.

Also the academic research moves towards these themes for example with the development of specific solutions as the CySeMoL (Cyber Security Modeling Language) tool for evaluating the security of SCADA architectures [9]. Within the Cigré working group D2.31 a first exercise on the application of CySeMoL for the estimation of attack probabilities to the Voltage Control architecture has been published [10].

In [11],[12] a Petri's net tool is used as an alternative approach of modeling the effects of cyber attacks to a SCADA architecture, in combination with a power flow simulator estimating the impact of some attack scenarios on the power infrastructure. More detailed attack models may be developed by means of the ADVISE tool [13], recently used for studying the attack probabilities to energy management systems in the customer domain [14].

A survey of the cyber physical system approach for design of power grids is presented in [23] and [24].

The communication security of smart grids is also addressed by several European projects. In the SmartC2Net project the use case methodology has been adopted for the description of the control functions and the communication requirements of a set of reference use cases and an integrated architecture view has been presented [15]. This chapter provides an insight of the communication security of the SmartC2Net Voltage Control use case. The SGIS method has been applied to this use case and the NIST security requirements have been linked with its most critical information assets. A subset of the smart grid standards are related to the tests described in this chapter, including standards for data communication with DERs [16], [17], towards control centers [18] and cyber security [19].

3 Voltage Control - ICT Architecture

The evolution from the fixed balance power grid to a dynamic balance smart grid involves to extend the control functionalities for targeting new balancing scenarios. The Voltage Control function and its related communications become important aspects because the connection of DERs to medium voltage grids can influence the status of the whole power grid affecting the capacity of the DSO (Distribution System Operator) to comply with the contracted terms with the TSO (Transmission System Operator) and directly the quality of service of their neighbor grids. This difficulty not only could be transferred into charges to the DSO, but it may also impact on the TSO operation because the scheduled voltages at grid nodes could not be observed and voltage stability problems cannot be managed properly. In order to maintain stable voltages in the distribution grids the Voltage Control (VC) function is introduced. The main functionality is to monitor the grid status from field measurements and to compute optimized set points for DERs, flexible loads and power equipment deployed in HV/MV substations. Figure 1 shows the input/output schema of the VC function.

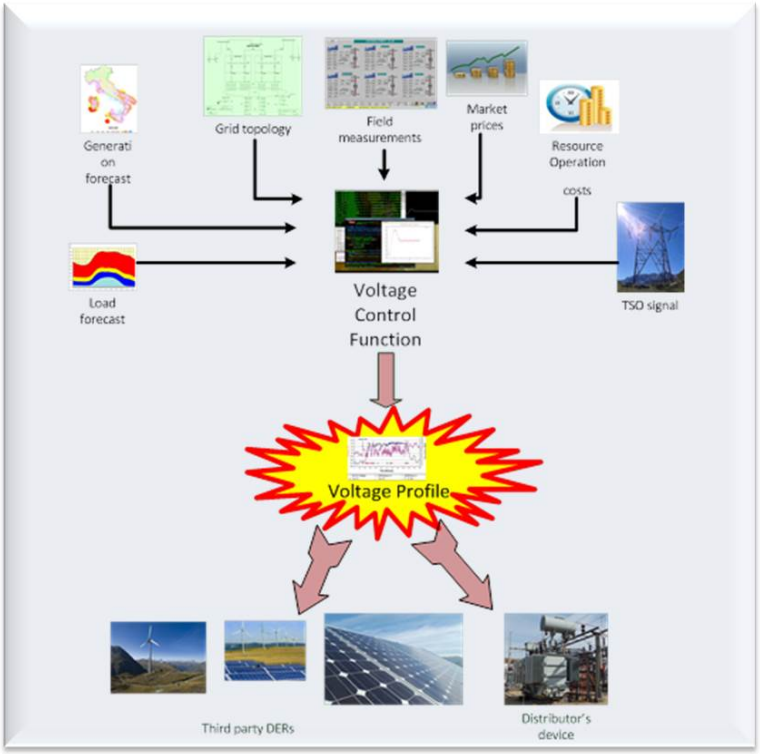

Fig. 1 Voltage Control - function

Since the DER may be outside the control of the utility and the optimization algorithm requires inputs from actors external to the DSO, the resulting overall architecture span over a multi-domain space interconnecting a variety of ICT entities and network segments. Figure 2 introduces the actors/sub-functions of the VC use case and shows how they can be mapped over the Function layer of the Smart Grid Architecture Model (SGAM) [8]. The actors of the use case are placed into the Transmission, Distribution and DER domains in the horizontal axis. The zones in the vertical axis vary from the Market zone of the Aggregator to the Field zone of the control functions of the OLTC (On Load Tap Changer), Capacitor bank, DER and Flexible Load. In the middle we have the Generation and Load Forecast functions placed in the cell Enterprise zone/Distribution domain. The EMS (Energy Management System) and DMS (Distribution Management System) control functions are in the Operation zone hosting all the active grid operation functions. The Substation Automation System (SAS) and the Medium Voltage Grid Controller (MVGC) functions are located in the Station zone.

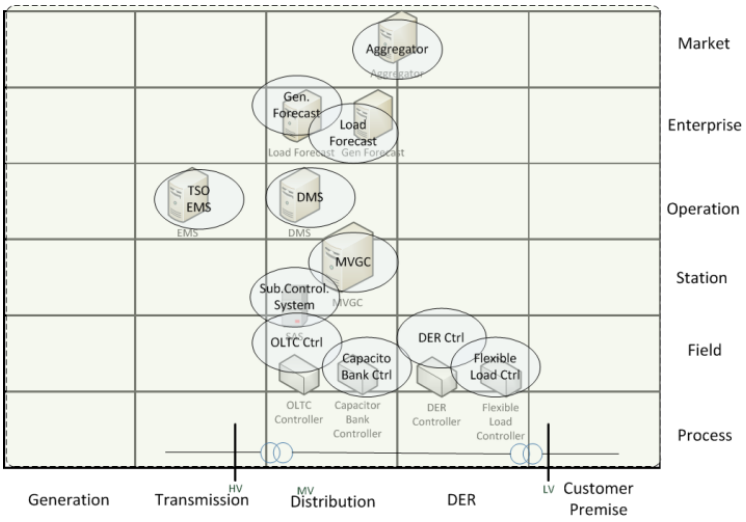

Fig. 2 Voltage Control - SGAM mapping

In order to analyze the communication and security aspects of this use case, we need to highlight the main interactions between the actors involved. The main control and communication components are presented in Figure 3. The VC function is performed by the MVGC on a node of a HV/MV substation control network. In order to compute an optimized voltage profile the algorithm involves communications through components inside the DSO area, but also exchanges of information with systems outside the DSO domain.

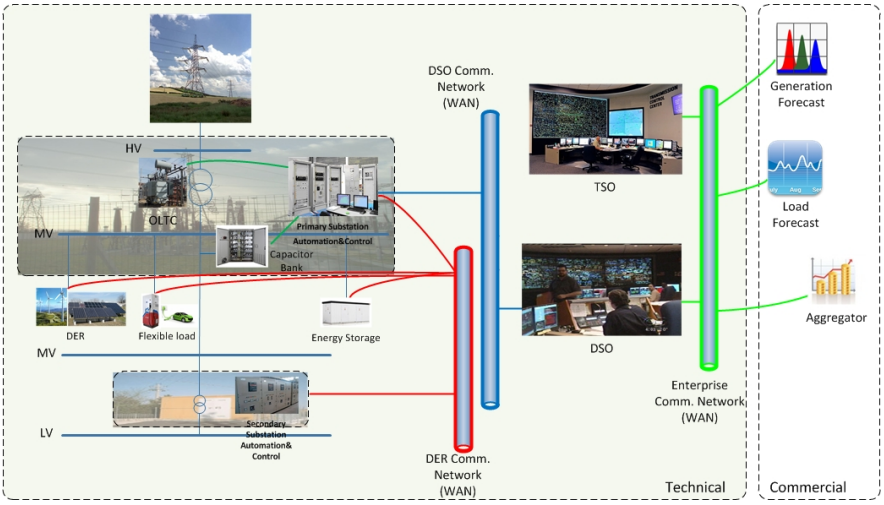

Fig. 3 Voltage Control - architecture

The TSO control center interacts through a permanent link between the TSO control network and the DSO enterprise network with the DMS in order to send the signals triggering the execution of the voltage control optimization cycle. The Aggregator provides the market prices and DER operation costs to the DMS via the DSO enterprise network. Also the Load and Generation forecast interact with the DMS through the DSO enterprise network. The DMS sends /receives information to/from the MVGC through the DSO control network. The MVGC is connected through the Substation Automation System with the Capacitor Bank and with the OLTC in the substation network. DERs and Flexible loads communicate with the MVGC via the DER /Flexible loads control network, possibly deploying heterogeneous communication technologies available in different geographical areas.

Table 1 Voltage Control - information assets

Information Exchanged	Description
Grid Topologies	Information regarding the characteristics of the grid elements (substations, loads, generators and lines). Configuration changes of the controlled grid (grid topology reconfigurations, new DER/load installations)
Weather Forecasts	Weather forecast, weather data
TSO Signals	Signals influencing the execution of the voltage control algorithm (e.g. changing optimization criteria or overriding commands): Voltage setting, Reactive Power setting, Automatic Voltage Regulator inclusion/exclusion
Generation Forecasts	Active power production plan on an hour base for a time horizon of 36 hours (36 values of active power). Generation coefficient 0<C<1
Load Forecasts	The future load is predicted on the basis of reference loads (seasonal patterns), stochastic fluctuations, active demand effects, weather forecast, calendar day. Load coefficient 0<C<1
Energy/Ancillary costs	Costs for the modulation of active and reactive power and reward schemes
Load/DER Features	DER Nominal Power, Capability, Controllability
OLTC Measurements and States	Voltage values, Automatic Voltage Regulator included/excluded
Capacitor Bank Measurements and States	Voltage values, Reactive power values, Capacitor included/excluded
DER Measurements	Voltage values, Active and Reactive power values
Flexible Load Measurements	Voltage values, Active and Reactive power values
Grid State Estimations	Estimation of the grid current state
Capacitor Bank Set Points	ΔQ +/-; ΔV +/-
OLTC Set points	ΔV +/-
DER Set points	ΔP +/-; ΔQ +/-
Flexible Load Set points	ΔP +/-; ΔQ +/-

Table 1 and Table 2 report the list of the basic VC information assets and the main steps of the control loop, respectively. The full template reporting a step by step analysis of the VC use case control loop is available in [15].

Table 2 Voltage Control - control steps

Step Name	Primary Actor	Triggering Event	Pre-Condition	Post-Condition
Generation Forecast Estimation	Generation forecast	Periodically	New info available	New generation forecast available
Information acquisition	DMS	Periodically / Asynchronous	TSO signal or new info	Info integrated in the data base
Forward of Forecast data	DMS	Periodically /Asynchronous	DMS receives new data	MVGC obtains input for the control algorithm
Grid measurement dispatch	Third party DER / Distributor's device	Periodically	Field dispatches new measurements	MVGC obtains new measurements
Forward of grid monitoring data	MVGC	Periodically	SAS has new SCADA and DER monitoring data	DMS receives new monitoring data
Execution of control voltage algorithm	MVGC	Values out of range	The state is not acceptable	Computation of new setpoints
Set Setpoints	SAS / MVGC	New setpoint	New setpoints computed	Devices change their settings

4 Benchmark Grid and Security Scenarios

The architecture details of the VC use case represent a key starting point in order to study the risk levels, but a real grid scale has to be set to analyze the overall system exposure to cyber threats and their global impact on the whole infrastructure. The definition of a benchmark grid for the cyber risk analysis is given in Table 3.

According to the Italian territorial configuration, the geographical area of the benchmark grid covers 19 regions served by thousands of primary substations controlled by 29 centers. As for the RES penetration a realistic 2020 scenario [20] installing 40GW of renewables in the Italian medium voltage grids is used in the analysis. The 2020 scenario will require the extension of the grid through the installation of new substations: the estimated number of substations per center is shown in Figure 4.

Table 3 Benchmark grid - cyber risk analysis

Parameter	Description
Area	Geographical extension of the area covered by the grid service: multination, nation, region, province, city
DER penetration	Total amount of Power from Renewable Energy Sources (RES)
Regulation	Applicable regulations
DER size	Installed DER capacity
Grid size	Installed grid capacity
Grid Topology	# HV/MV substations
	# MV loads
	# MV/LV substations
	# generators
	# storage devices
	# MV lines
Telecontrol Network Topology	# Control centers
	# substation links per center
	# of DER links per substation
Population density	# of people in the area

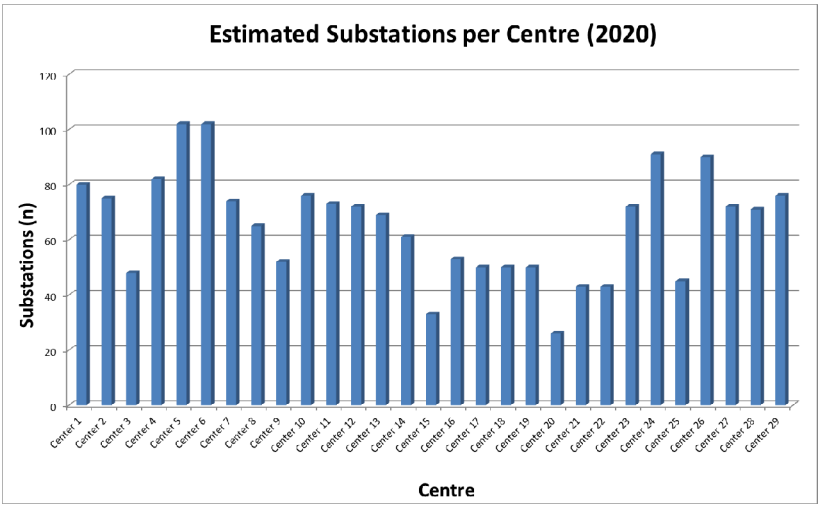

Fig. 4 Benchmark grid - telecontrol topology

According to the Italian grid code and the related connection rules [21], the size of renewable generators that have to be mandatory connected to the medium voltages falls within the power range of [0.2, 6]MW. Depending upon climate conditions in the Italian regions, the targeted amount of renewable power varies according to the estimated distribution in Figure 5.

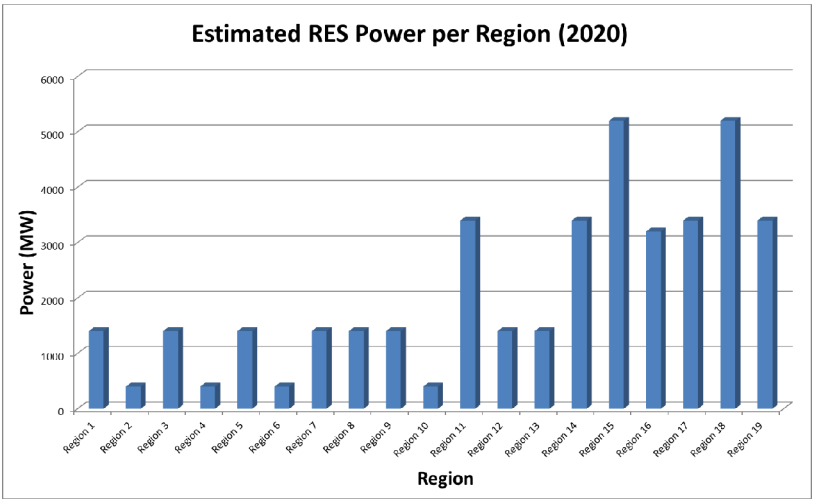

Fig. 5 Benchmark grid – regional RES distribution

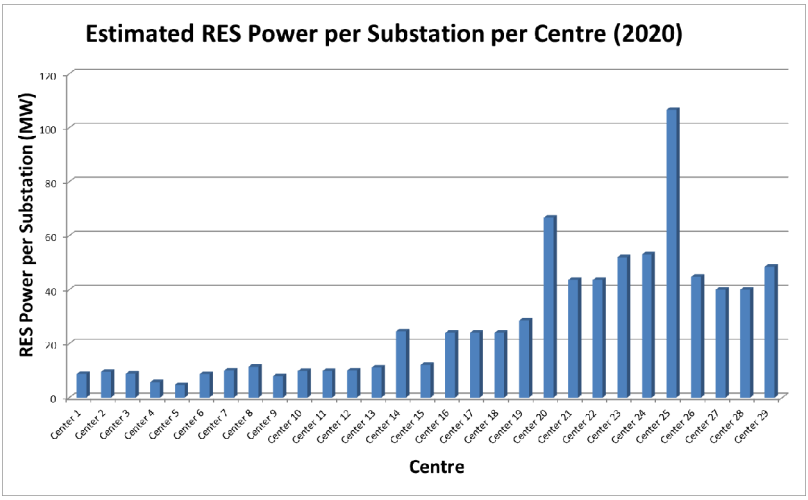

Fig. 6 Benchmark grid - RES Distribution at Substation Level

The relative distribution of population per center, calculated by currently registered population in the area, is shown in Figure 7.

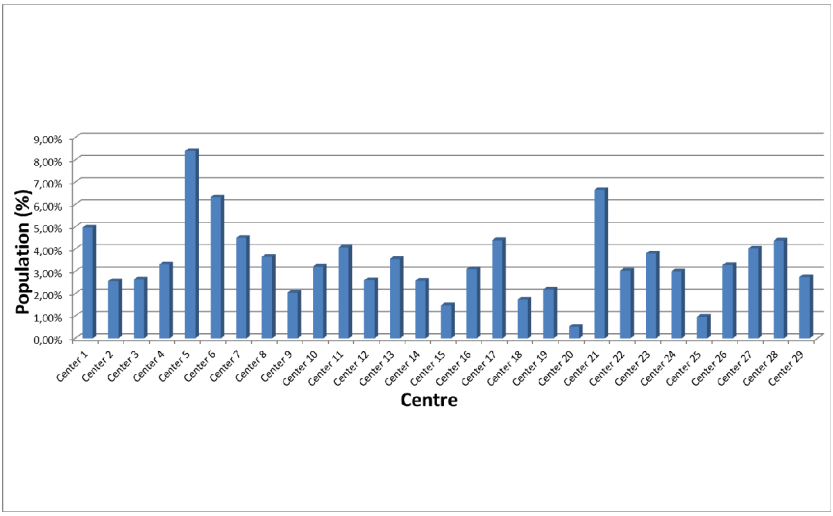

Fig. 7 Benchmark grid - population distribution

The effect of attacks to the telecontrol network of the benchmark grid depends upon the security (i.e. integrity, availability, confidentiality and non-repudiation) scenarios in the scope of the analysis, where a given security scenario is characterized by the parameters in Table 4.

Table 4 Security scenarios

Parameter	Description	Voltage Control Scenario
Attack Target	Network interface targeted by the attack	DER interfaces, substation2DER interfaces, substation2center interfaces, center2substation interfaces
Attack effect	Loss of messages (availability); insertion of fake messages (integrity)	loss of inputs to the VC algorithm, loss of output set points fake inputs to the VC algorithm, fake output set points, faked monitoring data
Attack extension	# network interfaces under attack	# DER networks # substation networks # center networks
Data frequency	Periodic / Asynchronous	periodic and asynchronous VC inputs/outputs

By instantiating the security space on the specific VC network topology and information assets, our use case security space (Figure 8) covers the security scenarios reported in the third column of Table 4.

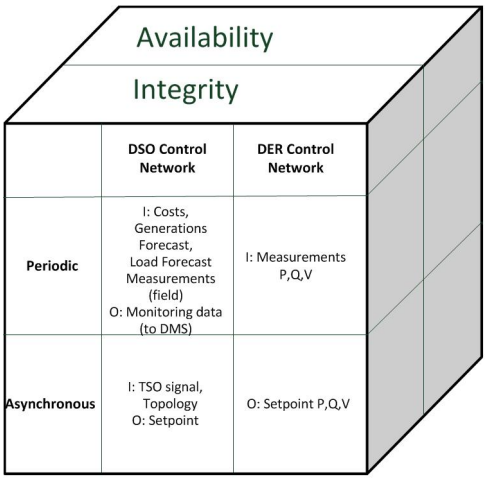

Fig. 8 Voltage Control - security space

5 Risk Analysis - A Qualitative Approach

The risk analysis of the Voltage Control ICT architecture is based on the SGIS working group of the Smart Grid Coordination Group by CEN-CENELEC-ETSI in charge of the European Mandate E/490 on smart grid standardization, and uses this method to derive qualitative Security Levels of voltage control information assets. According to the SGIS risk analysis process [8] the evaluation of the risk levels of a given smart grid use case goes through the application of the impact and threat likelihood analysis to the scenarios of the use case information assets in the security space. A risk level for each information asset/security scenario can be obtained combining the related impact and likelihood levels.

5.1 Impact Analysis

The impact of attacks is evaluated through the five-scale impact matrix in Figure 9 defining the levels of operational, financial and additional risks. From the application of the SGIS impact levels to the benchmark grid, the operational Risk Impact Levels can be assigned to the information assets/security scenarios of the VC use case. Let's evaluate the operational risks starting from the "Energy Supply" risk category (leftmost column in Figure 9). The focus is on the extreme case analysis, i.e. on those regional grids with maximum DER penetration (i.e. regions 15 and 18 in Figure 5), highest power demand and integrity scenarios introducing fake messages causing loss of loads, generators disconnections or substation trips. The loss of energy supply varies with the attack target and the damaged information assets. In the case of substation2DER interface attacks, where the setpoint information is compromised or the DER measurements are perturbed, the loss may be up to

100MW (yellow circle in the picture). The worst case considers that more than one DER connected to a specific substation is out of control (the sent setpoints differ from the computed setpoints or the measurements regarding DER status are not the real ones and so the algorithm is based on wrong values (see Figure 8). More serious is the case if the substation2center interface is attacked: in this case the entire substation (information flow) domain may be compromised and the impact may be up to 1 GW (orange circle) because the information impacting on the substation capacity, and not only specific DER capacities, is perturbed or missing. The criticality increases if the center2substation interface is under attack: in this case the information flows related to a wider grid area may be compromised and several substations may be tripped, amounting an impact value up to 6GW (red circle). As for the impact of such attack effects on the registered population, the voltage control use case falls into the medium level, while the impact on critical infrastructures may be high or critical, depending on the presence of essential or national infrastructures in the sub-regions under attack. In order to estimate these impact levels we have considered the extreme case achieving the values presented in Figure 9.

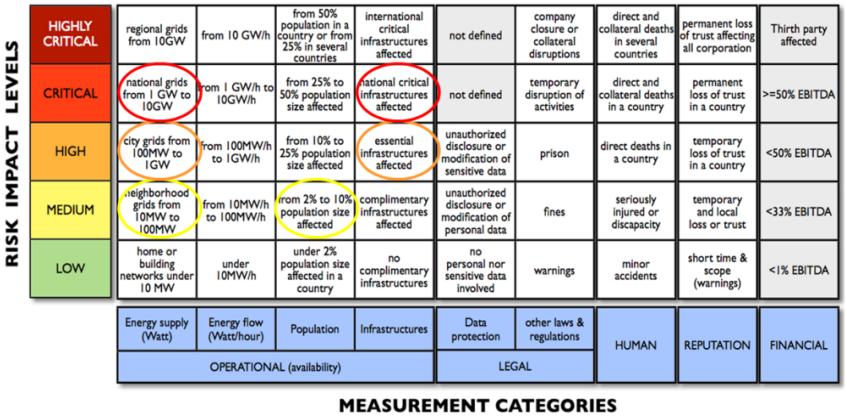

Fig. 9 Voltage Control - SGIS Impact Levels

5.2 Threat Analysis

The likelihood of threat/attack occurrences represents the other key indicator to be estimated in order to compute the risk level. The level of likelihood is evaluated for every information asset considering parameters such as threat sources/actors, their motivations and capabilities to achieve an attack effect through compromise methods and in presence of essential security counter-measures.

The threat source represents the entity (person or organization) that wants to break the security barriers for obtaining benefits of some type. Examples of threat sources are listed in Table 5.

Table 5 Threat sources

Disaffected or dishonest employees
Foreign Intelligence Services
Amateur or professional hackers
Virus and other malware writers
Vandals
Thieves
Terrorists
Investigative journalists
Commercial competitors (i.e. industrial espionage)
Political pressure groups/activists
Organized criminal groups

Considering their different levels of capability (from formidable to very little) and priority (from focused (very high) to indifferent (very low)) it is possible to realize an identikit of the possible threat sources. In order to reach his/her scope, the threat source "uses" a threat actor that materially performs the attack. Threat actors are entities potentially having capability, opportunity and motivation to attack an asset. The different capabilities of threat actors can be used in order to delineate the possible threat actor profiles. In some cases the threat source and the threat actor could coincide and be the same entity.

Table 6 Threat Actors

Threat Group	**Profile**
System and Service User	Privileged User
	Normal User
	Service Consumer
	Shared Service Subscriber
Actors with business or network connection with the assets	Information Exchange Partner
	Service Provider
Actors indirectly connected to an asset through directly connected actors	
Actors having access to hardware and software before the asset commissions or are those that are responsible for implementation, configuration or management of the asset	Supplier
	Handler
Actors having physical access to the asset	Privileged User
	Normal User
	Bystander
	Person Within Range
	Physical Intruder

The threat actor is relative to an asset. A threat actor with particular privileges respect to an asset might not have the same privileges, and so not be able to attack also the other assets. The threat actors can be grouped considering the relationship with respect to a specific asset and similar applicable compromise methods. The threat actors have authorized logical access to the different assets and any service they provide. Table 6 includes sample groups of threat actors and associated profiles.

Coming back to the Voltage Control use case, possible threat sources should be identified by correlating investigative data. For now we assume that they may be employees, industrial espionage agents, vandals, cyber hackers, viruses and worms, thieves and terrorists. Both the identification of threat actors and the evaluation of their threat capabilities to compromise the information assets may be driven by the analysis and management of roles in the control application. By focusing on the DSO domain of the VC use case, we may have several user/service roles for grid operation and ICT maintenance that could become threat actors. Examples of possible user roles are: local power operator, remote power operator, normal ICT user, ICT administrator, ICT security administrator. Examples of possible service roles are: DER controller, MVGC, SAS and DMS. Each role defines a trust level and it is used to take authorization decision. For this reason an authentication mechanism is associated to each role. The access control matrix assigns to each data type for each (user or service) role specific rights (read, write, update, delete). In the VC use case, for example, only MVGC has the right to write set point to DER. Furthermore an important aspect to take into account is the number of users/services for each role.

A further step of the threat analysis considers architecture characteristics such as types of services running on the components, technologies and implementation aspects. In the VC use case the key components are the control IEDs (Intelligent Electronic Devices), the servers and the routers at different DSO subdomains such as ICT maintenance center, control center or substation. For each of them it is necessary to consider the configuration parameters of software layers/modules, for example the operating systems and protocols used for implementing the communications. In the VC use case we suppose that the servers run a UNIX based Operating System. DER-substation and intra-substation communication uses the standard IEC 61850 over the MMS protocol and for substation-center information flows the IEC 60870-5-104 standard protocol is used. They both are connection-based flows supported by the TCP/IP reliability mechanisms. The VC use case might exploit heterogeneous network technologies. The center-substation links usually deploy IP based wired networks, whereas the substation-DER links might use wired as well wireless networks depending on the geographical coverage of the technology.

Besides these “structural” aspects the knowledge about the control loop behavior, as reported in Table 2, is essential for building effective attack processes whose actual effectiveness also depends on the data frequency. For example the success of DoS (Denial of Service) attacks, such as flooding, buffer overflows and resource exhaustion will be higher on periodic information flows (e.g. measurements and monitoring data) than on asynchronous information flows (e.g. setpoints).

By grouping the VC use case information assets and attack scenarios considering similarity in their parameters, we identify three main categories of assets according to the attack target interfaces and five most relevant attacker profiles.

By applying the SGIS five scale likelihood levels in [8], the analysis described above identifies for the VC use case the threat levels presented in Figure 10**.**

	substation2DER	substation2centre	centre2substation
Dishonest employee (Admin)	Very High	Very High	Very High
Dishonest employee (normal user)	High	Medium	Medium
Vandal	Very High	High	Low
Hacker	Very High	High	Medium
Terrorist	Medium	Very High	Very High

Fig. 10 Voltage Control - Likelihood Levels

5.3 Risk Levels

Figure 11 represents a numerical approach for the calculation of risk levels proposed by SGIS, where the qualitative values of impact and likelihood are summed.

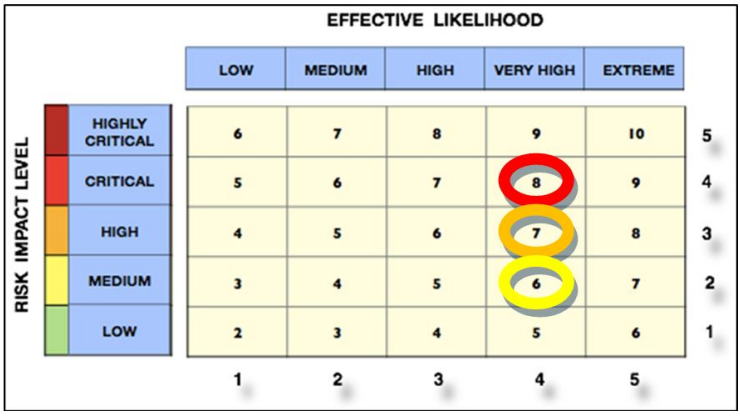

Fig. 11 Voltage Control - risk calculus

These numerical values are mapped through the matrix in Figure 12 where the risk (security) levels are identified.

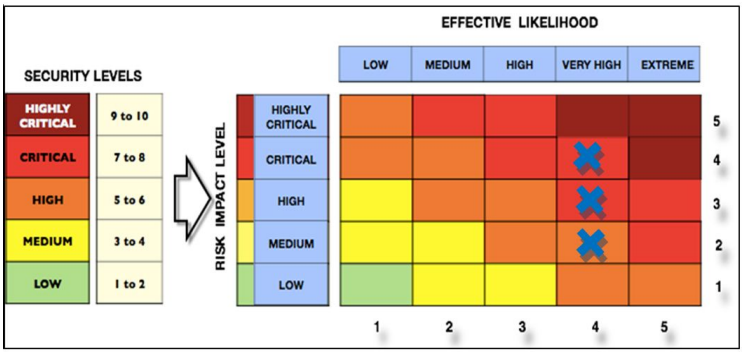

Fig. 12 Voltage Control - Risk Levels

Combing the VC impact levels (Figure 9) with the likelihood levels (Figure 10) by means of the SGIS risk matrix, the High and Critical risk levels are identified for the VC use case, depending on the information assets/security scenarios under consideration. To be noticed that the combination of the impact with the likelihood analysis has increased the need of security protection of substation-DER communications (from a medium impact level to an high risk).

Qualitative approaches as the SGIS toolkit provide only a rough estimation of the risk value for each assets and scenario. In order to obtain more precise evaluations the application of quantitative risk assessment methods is envisaged.

6 From Risk Levels to Security Standards

Considering the information assets and scenarios related to the VC use case, the impact and likelihood levels have been evaluated in order to obtain the corresponding risk levels. From the outcome of the risk analysis a set of security requirements have to be associated to the considered information assets. With reference to the NIST requirement categorization in [5], the following groups of security requirements have been identified as relevant to the VC use case assets/scenarios achieving the critical and high risk levels:

- Access Control (SG.AC)
- Identification and Authentication (SG.IA)
- Smart Grid Information System and Communication Protection (SG.SC)
- Smart Grid Information System and Information Integrity (SG.SI)
- Cryptography and Key Management.

In order to meet the Voltage Control use case security requirements, the list of security measures from technical standards in Table 7 can be selected. To be noticed that the maturity level of the selected standards varies from available international standard to work in progress.

Table 7 Voltage Control - security standards

Standard Type	Standard Reference
Communication protocol security standards	IEC 62351 Parts 3/4/5/6
Network security standards	IEC 62351 Part10
Role-based access control	IEC 62351Part 8
Key and certification management	IEC 62351Part 9
XML security	IEC 62351Part 11
Enabling standard IT security protocols	TLS
	IPSEC
	SNMP
	https
	ssh

Figure 13 depicts where the different parts of IEC 62351 have to be applied according to the communication protocols of the VC use case. Depending on the risk levels of the related information assets, more or less costly implementations of the security measures, i.e. for the key management and the grid/network monitoring, will be deployed.

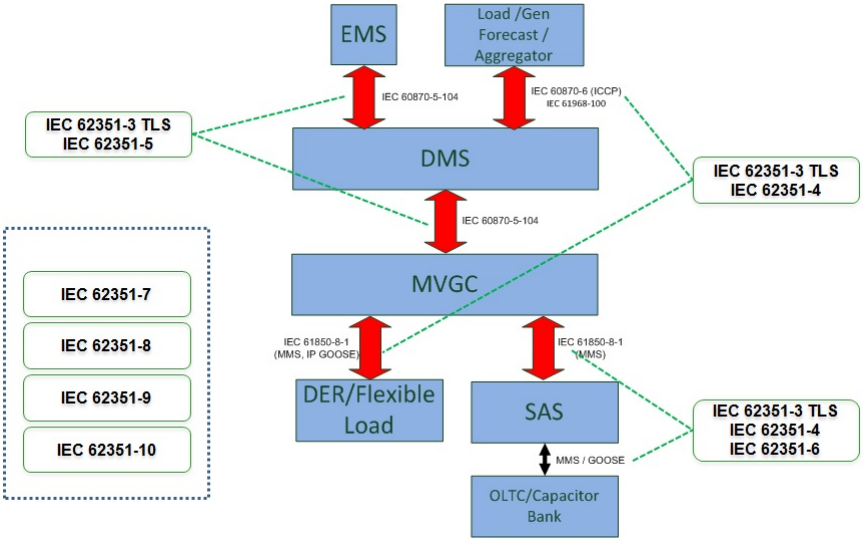

Fig. 13 Voltage Control - mapping of IEC 62351 parts

Figure 14 summarizes two examples of the overall security analysis process considering a couple of the assets identified during the analysis.

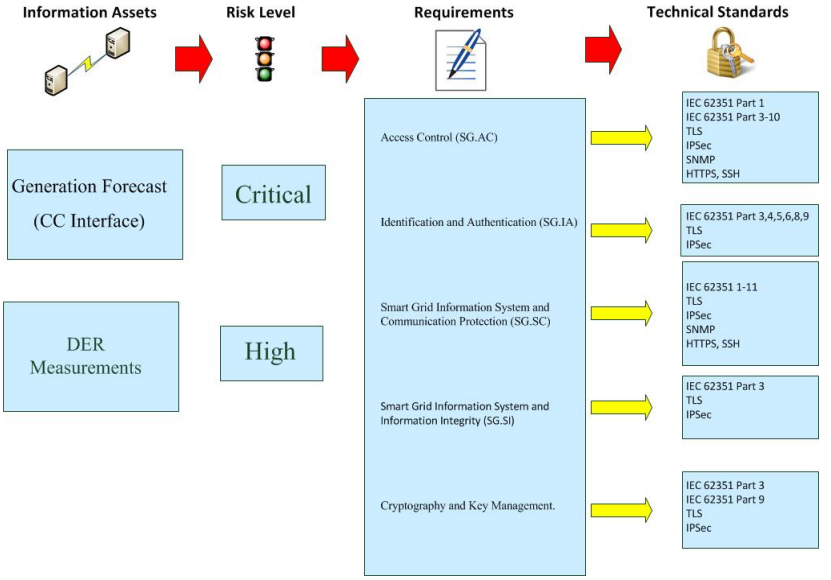

Fig. 14 Schema of the approach

7 Experimental Environment

In order to collect precise measurements about the deployment of security measures in control applications an experimental test bed is implemented focusing on the Voltage Control communication in active distribution grids. The test bed architecture is based on the use case described in the previous sections and covers the components and networks highlighted by the red oval in Figure 15.

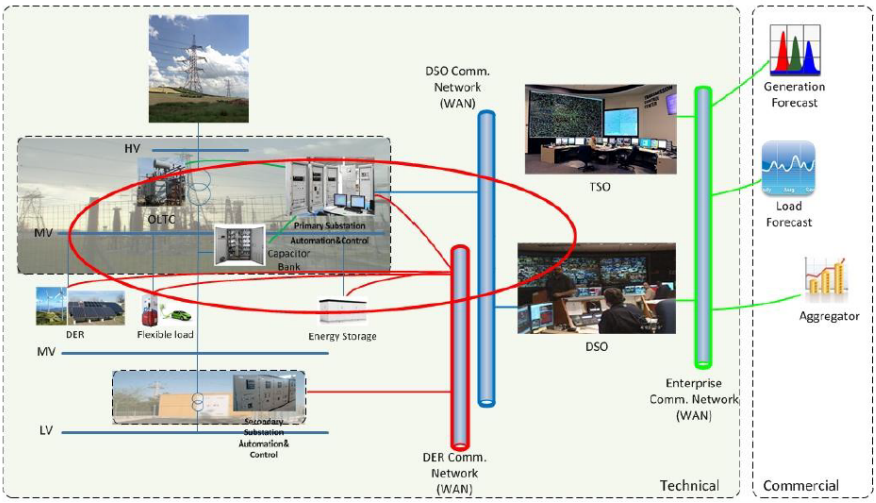

Fig. 15 Test bed – use case coverage

A schematic view of the test bed ICT architecture is presented in Figure 16, whose components and networks are described in Table 8.

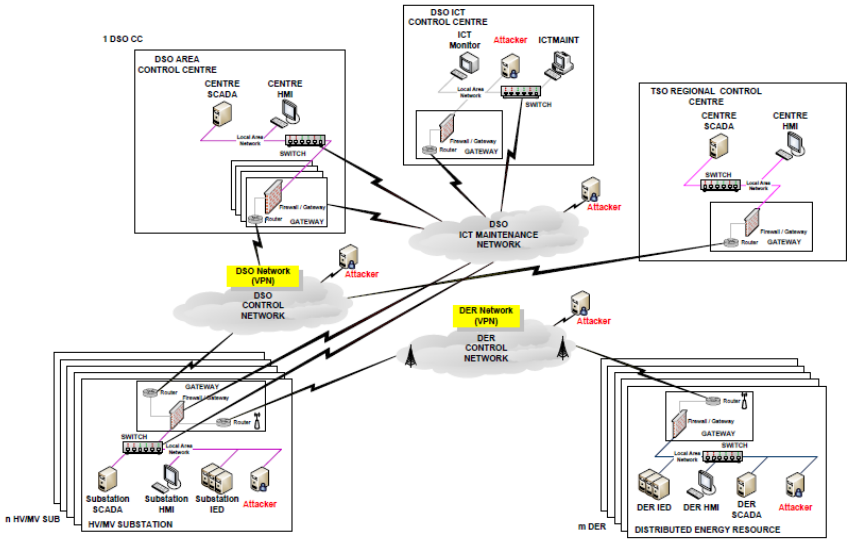

Fig. 16 Test bed – architecture

From the outcome of the VC risk/security analysis described in the previous section (risk levels, security requirements and technical standards), the test bed has given priority to the implementation of the Part 3 of the IEC 62351 security standard for the substation/DER communications based on the IEC 61850/MMS protocol. Part 3 is dedicated to describe the TLS (Transport Layer Security) implementation aspects that may be included in power system information exchanges in order to preserve the integrity and the authentication of the messages. A further priority is given to the integration in the test bed of the functions addressed by the new edition of the Part 7, currently still under development. Part 7 is related to the network and system management performed through the identification of specific data objects used to monitor and control end systems and networks. The SNMP (Simple Network Management Protocol) protocol is used in the test bed for the implementation of the monitoring data objects relevant for the VC security scenarios.

In order to measure some security key performance indicators several test runs may be performed collecting experimental data of VC communications. Table 9 describes the types of tests to be executed in order to verify the communication behavior during different operating/security/attack conditions.

Table 8 Test bed - components and networks

Component/Network	Description
DSO Control Center	It remotely controls a partition of the distribution grid. Each DSO CC interacts with different HV/MV substations where the MVC function is executed
HV/MV Substation	It includes automation, communication, SCADA and Operator HMI functions. Each substation may control different DER sites
TSO Center	It supervises critical regions of a transmission grid
DER site	It includes large DER connected to MV grids
ICT maintenance control center	It remotely controls the ICT components of DSO networks. Collects data statistics related to network monitoring and attack successfulness measuring the effects of cyber attacks to the communications involved in grid operation and maintenance
Attacker	It performs malicious actions. It may be placed inside the DSO ICT control center, substations, DER sites and corresponding control networks
DSO control network	It connects the DSO control center with the HV/MV substations. It uses a dedicated service on a shared, possibly third party, infrastructure. The protocol IEC 60870-5-104 is used for these communication flows
DER control network	It connects each DSO substation with multiple third party DER sites located in different geographical areas possibly deploying heterogeneous wired/wireless communication technologies. The communication uses the MMS profile of the IEC 61850 standard
ICT maintenance network	It is used for the configuration and management of the control and communication devices deployed in the DSO control center and HV/MV substations
Local Area Network	Each site deploys its own Local Area Network for the interactions among the local components

Table 9 Tests

Test Case	Description
Normal	Tests verifying the VC communications with essential security measures in absence of ICT faults/attacks
Secured	Tests verifying the VC communications deploying enhanced security measures in absence of ICT faults/attacks
Attack	Tests verifying the VC communications with varied degrees of security measures in presence of ICT attacks

The test cases may be applied to different information flows involving the Control and Monitoring of the power grid and of the ICT network. More in specific, we address the control center –Substation communications, the Substation – DER communications and the ICT communications.
Considering the attack scenarios described in the risk analysis section the following attack processes are experimented:

- DoS Attacks to DER (gateways). The traffic between DER and Voltage Controller is perturbed and some DER measurements are not able to reach the Voltage Controller.
- DoS Attacks to Substation (gateways). The traffic between the Voltage Controller and the DMS is perturbed; some DER and SCADA measurements are not able to reach the DMS.
- Fake DER setpoints. Either an (additional) fake setpoint is sent to DER, or a legal setpoint is intercepted and modified with wrong set point values
- Fake TSO signals. A fake TSO signal is sent to the Voltage Controller.

For each test case a set of tests may be performed and the results compared. Quantitative requirements related to network measurements may be verified as latency, bandwidth and packet loss. Grid related requirements may also be evaluated such as # of DER affected by the attack, # of Substation, amount of power delivered and power quality.

7.1 Test Analysis: Normal Test Case versus Secured Test Case

In this subsection an example of test performed and results obtained are presented. They address the DER – Primary Substation communications for the exchange of the DER measurements and setpoints. In our tests we assume that the DER emits the measurements periodically every 2 seconds and the MVGC sends the setpoints every 30 seconds (this information flow is mostly sent in asynchronous mode, but in order to obtain comparable results in this test we consider it as a periodic one).

We performed normal and secured tests composed by different runs: in the secured tests we protected the communication by the use of the TLS protocol. The evaluated communication measures are presented in Table 10.

In Table 11 we compare the results obtained in the two test cases. The overhead brought by TLS on the different metrics can be seen in the table: the results show that the inclusion of the TLS causes the increase of the time for each single communication phase. In the Handshake Time we have an extra time of 0.03137 sec for the TLS handshake. We can conclude that the total time for the initial handshake and session phases is 0.141333 seconds without TLS and 0.176704 including TLS security which means an overhead of 0.035371 seconds corresponding to an increment of 25% of the total time. Also the measurement and setpoint communications are perturbed by the introduction of the TLS, but not in a critical way.

Table 10 Evaluation measures

Measures	Description
Handshake Time	Time interval needed to create the connection at different stack levels
RTT (Round Trip Time) -Measurements	Time interval between the output of a Measurement and the reception of the corresponding TCP ack by the DER
RTT-Setpoint	Time interval between the output of a setpoint request and the reception of the corresponding TCP ack by the MVGC
Inter-Measurements Time	Time interval between each two consecutive Measurements
Inter-Setpoint Time	Time interval between each two consecutive setpoints

Table 11 Test results

Test Case	Metrics (time in seconds)				
	Handshake Time	*Inter-Measurements Time*	*RTT-Measurements*	*Inter-Setpoint Time*	*RTT-Setpoint*
Normal	0.141333	2.0105	0.0000981	30.0637	0.00111
Secured	0.176704	2.0105	0.0000992	31.0588	0.00117

8 Conclusions and Future Work

In the research context about smart grid cyber security the chapter addressed the perceived need of tools and measures mitigating the risks originated by intrinsically vulnerable ICT infrastructures. In order to estimate the SGIS impact and likelihood levels the chapter includes a study of the Voltage Control use case detailed ICT architecture as well as benchmark grid data and attack scenarios. Through their application to the use case, the key steps of the security analysis process have been performed to illustrate the parameters and the outcome of the risk analysis and their links with the security requirements and ongoing standards. The value of security testing of control scenarios is emphasized by detailing the test performed using a Voltage Control experimental architecture.

The results obtained by the experimental activity will be used as inputs for more comprehensive analysis based on simulation and analytic modeling [22]. The experimental measures will allow to test the accuracy of the models and the

model based evaluations will calculate the key performance indicators scaling the addressed scenarios up to the benchmark grid.

Acknowledgments. The research leading to these results has received funding from both the EU 7th Framework Program (FP7/20072013) under grant agreement no 318023 for the SmartC2Net project, and by the Ministry of Economic Development with the Research Fund for the Italian Electrical System for the project "Distributed Generation and Active Networks".

References

[1] IEC Smart Grid Standardization RoadMap. SMB Smart Grid Strategic Group SG3, Edition 1.0 (2010)
[2] EPRI Smart Grid Resource Center (August 2010), http://www.smartgrid.epri.com/
[3] Smart Grid Mandate M/490 EN, Standardization Mandate to European Standardisation Organisations (ESOs) to support European Smart Grid deployment (March 2011), http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/2011_03_01_mandate_m490_en.pdf
[4] European Technology Platform for the Electricity Networks of the future (2012), http://www.smartgrids.eu/
[5] National Institute of Standards and Technologies, The Smart Grid Interoperability Panel Cyber Security Working Group NISTIR 7628 "Guidelines for Smart Grid Cyber Security" (2010)
[6] CEN-CENELEC-ETSI Smart Grid Coordination Group SGCG/M490/B_Smart Grid Report First set of standards Version 2.0 (November 16, 2012)
[7] CEN-CENELEC-ETSI SGCG/M490/E_Smart Grid Use Case Management Process — Use Case Collection, Management, Repository, Analysis and Harmonization (2012)
[8] CEN-CENELEC-ETSI Smart Grid Coordination Group. Smart Grid Information Security (November 2012)
[9] Sommestad, T.: A Framework and theory for cyber security assessment. PhD Thesis in Industrial Information and Control Systems, Royal Institute of Technology, Stockholm (November 2012)
[10] Ekstedt, M., Korman, M., Terruggia, R., Dondossola, G.: Application of a cyber security assessment framework to smart grid architectures. Paper D2-01_11 in the Proceedings of the Cigré Study Committee D2 Information Systems and Telecommunication, 2013 Colloquium, Mysore – Karnataka, India, November 13-15 (2013)
[11] Ten, C.-W., Hong, J., Liu, C.C.: Anomaly Detection for Cybersecurity of the Substations. IEEE Trans. Smart Grid (2011)
[12] Ten, C.-W., Govindarasu, M., Liu, C.C.: Cybersecurity for Critical Infrastructures: Attack and Defense Modeling. IEEE Trans. Systems, Man, and Cybernetics – Part A: Systems and Humans, 853–865 (July 2010)
[13] LeMay, E., Ford, M.D., Keefe, K., Sanders, W.H., Muehrcke, C.: Model-based Security Metrics Using ADversary VIew Security Evaluation (ADVISE). In: Proceedings of the 2011 Eighth International Conference on Quantitative Evaluation of SysTems (QEST 2011), pp. 191–200. IEEE Computer Society, Washington, DC (2011)

[14] Hägerling, C., Kurtz, F., Wietfeld, C., Iacono, D., Daidone, A., Giandomenico, F.: Security Risk Analysis and Evaluation of Integrating Customer Energy Management Systems into Smart Distribution Grids. In: CIRED Workshop 2014 (June 2014)
[15] SmartC2Net European Project, Deliverable D1.1. SmartC2Net Use Cases, Preliminary Architecture and Business Drivers (September 2013), http://www.smartc2net.eu
[16] International Standard IEC 61850-7-420 ed1.0. Communication networks and systems for power utility automation - Part 7-420: Basic communication structure - Distributed energy resources logical nodes, Technical Specification (2009)
[17] International Standard IEC 61850-8-1. Communication networks and systems in substations - Part 8-1: Specific Communication Service Mapping (SCSM) - Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3. International Standard, 2nd edn. (June 2011)
[18] International Standard IEC 60870-5. Telecontrol equipment and systems - Part 5-104: Transmission protocols – Network access for IEC 60870-5-101 using standard transport profiles. International Standard, 2nd edn., Reference Number IEC 60870-5-104(E) (June 2006)
[19] International Standard IEC 62351. Power System Management and associated information exchange - Data and Communication Security – Parts 1-11
[20] Petroni, P.: Smart Grids Operation, automation and protection issues. In: Cired 2012, Lisbon, May 29-30 (2012)
[21] Comitato Elettrotecnico Italiano Norm CEI 0-16. Reference technical rules for the connection of active and passive consumers to the HV and MV electrical networks of distribution Company (2013)
[22] SmartC2Net European Project, Deliverable D5.1. Methodologies Synthesis (September 2013), http://www.smartc2net.eu
[23] Khaitan, S., McCalley, J.: Design Techniques and Applications of Cyber Physical Systems: A Survey. IEEE Systems Journal PP, 1–16 (2014)
[24] Khaitan, S., McCalley, J.: Cyber Physical System Approach for Design of Power Grids: A Survey. In: IEEE PES GM 2013, Vancouver, BC, July 21-25, pp. 1–5 (2013)

Acronym	Definition
DER	Distributed Energy Resource
DG	Distributed Generation
DMS	Distribution Management System
DoS	Denial of Service
DSO	Distribution System Operator
EMG	Energy Management Gateway
HV	High Voltage
ICT	Information and Communication Technology
IED	Intelligent Electronic Device
IP	Internet Protocol
LAN	Local Area Network
LV	Low Voltage
MIM	Man In the Middle
MMS	Manufacturing Message Specification

MV	Medium Voltage
MVGC	Medium Voltage Grid Controller
OLTC	On Load Tap Changer
P	Active power
Q	Reactive power
RES	Renewable Energy Sources
SAS	Substation Automation System
SCADA	Supervisory Control And Data Acquisition
SGAM	Smart Grid Architecture Model
SGIS	Smart Grid Information Security
SNMP	Simple Network Management Protocol
TLS	Transport Layer Security
TSO	Transmission System Operator
V	Voltage
VC	Voltage Control
WAN	Wide Area Network