Smart Grid Cybersecurity Risk Assessment

Experiences with the SGIS Toolbox

Lucie Langer and Paul Smith
AIT Austrian Institute of Technology
Vienna, Austria
{firstname.lastname}@ait.ac.at

Martin Hutle
Fraunhofer AISEC
Garching, Germany
martin.hutle@aisec.fraunhofer.de

***Abstract*—As much as possible, it is important that the smart grid is secure from cyber-attacks. A vital part of ensuring the security of smart grids is to perform a cybersecurity risk assessment that methodically examines the *impact* and *likelihood* of cyber-attacks. Based on the outcomes of a risk assessment, security requirements and controls can be determined that inform architectural choices and address the identified risks. Numerous high-level risk assessment methods and frameworks are applicable in this context. A method that was developed specifically for smart grids is the *Smart Grid Information Security (SGIS) toolbox*, which we applied to a voltage control and power flow optimization smart grid use case. The outcomes of the assessment indicate that physical consequences could occur because of cyber-attacks to information assets. Additionally, we provide reflections on our experiences with the SGIS toolbox, in order to support others in the community when implementing their own risk assessment for the smart grid.**

Keywords—risk assessment; smart grid; SGIS toolbox; cybersecurity

I. INTRODUCTION

At the core of the smart grid are increased monitoring and control capabilities, primarily in medium- and low-voltage networks, that are supported by Information and Communication Technology (ICT) and Supervisory Control and Data Acquisition (SCADA) systems. An example use of these systems is to support dynamic voltage control strategies that enable the deployment of volatile Distributed Energy Resources (DERs), such as photovoltaics, without the need for installing new and expensive grid capacity. Use cases of this nature will result in ICT and SCADA systems playing an increasingly critical role in the operation of electricity distribution networks; cyber-attacks to these systems could have a significant impact.

Alongside these smart grid developments, a number of cyber-attacks have targeted industrial control systems and energy sector organizations. The motivation for these attacks is varied, and includes industrial espionage and causing physical damage to equipment. For the moment, the latter is the exception, and can require expertise that is difficult to acquire and in-depth knowledge of the target environment. In order to address these threats, it is important to implement a cybersecurity risk assessment. In short, one assesses the impact of cyber-attacks to information assets, and the likelihood of attacks occurring – the product of these two items is used to determine risk. Likelihood is typically a function of the vulnerabilities a system (or organization) has and the nature of the threat. Based on the outcomes of the risk assessment, security requirement can be identified, e.g., that certain systems should be authenticated, which can be realized via a security architecture and controls.

There are a number of high-level risk assessment methods (or frameworks) that an organization can use to support the implementation of a cybersecurity risk assessment for the smart grid. Examples include OCTAVE [1], HMG IS1[2] and Magerit [3] – many of these are based on the principles identified in ISO 27005 [4], which provides guidelines on how to implement an information security risk management framework within an organization. We discuss these methods in more detail in Sec. II on related work. Whilst these risk assessment methods are useful, they do not provide specific guidelines for the peculiarities of the smart grid. For example, in the smart grid, cyber-attacks can have physical impacts on the quality of energy supply or cause damage to power equipment. Furthermore, attacks could result in safety-related incidents happening, resulting in injury or loss of life. In this context, it would be helpful to provide specific guidance on how to assess these aspects.

As part of CEN-CENELEC-ETSI's response to the EU Mandate 490, the Smart Grid Information Security (SGIS) working group developed the SGIS toolbox [5] – a set of high-level guidelines for assessing the cybersecurity risks associated with smart grid use cases. The SGIS toolbox includes a number of notable smart grid-specific aspects, such as the enumeration of different impact categories that reflect the nature of the smart grid. We summarize the SGIS toolbox in Sec. III. Ultimately, the SGIS toolbox was apparently not very-well received in the community, receiving extensive critique [5]. Nevertheless, in the EU-funded SPARKS project, we applied the SGIS toolbox to a smart grid voltage control and power flow optimization use case. A summary of the use case that we investigated is presented in Sec. IV. Our intention was to gain applied insights into the challenges of performing a risk assessment for the smart grid that, despite its shortcomings, the SGIS toolbox appeared to be well-suited. In Sec. VI, we summarize some of the key findings from this exercise, highlighting how cyber-attacks to selected information assets in this use case under examination can have physical consequences. Additionally, we provide reflections on our experiences from using the SGIS toolbox in Sec. VII, which we will take forward in the SPARKS project, as we develop our own approach to risk assessment and management.

Table 1: Relevant Methodologies and Frameworks for Risk Assessment

Name		Short Description	Applicability to Smart Grids
Frameworks	ISO/IEC 31000	Framework for general risk management	A good starting point to set up a risk management process with all relevant subcategories
	ISA/IEC 62443	Framework for the security of industrial automation and control systems, including Industrial Automation and Control System (IACS) cyber-security aspects and Cyber Security Management System (CSMS) for risks	Describes how to handle risks in the context of IACS, which include smart grids
	COSO Risk Assessment	Committee of Sponsoring Organizations of the Treadway Commission (COSO) issued description of the basics of risk assessment and methodologies used in Enterprise Risk Management (ERM)	The basic aspects and described methodologies are applicable to smart grids
	IRGC Framework	A comprehensive approach towards understanding, analysing, and managing important risk issues	A modified version of this framework considers identifying and managing ICT-related risks faced by EU critical energy infrastructures
Quantitative Methods	VIKING Impact Analysis	A part of the VIKING project concerned with the impact of attacks on communication signals to and from Remote Terminal Units (RTUs) in the power grid	A quantitative mathematical method for analysing the impact of adverse events in the area of SCADA/EMS systems at the transmission level. Some of the tools developed could be applied to the smart grid
Qualitative Methods	OCTAVE	Focuses on activities, threats and vulnerabilities, using an expected value matrix (incorporating subjective impact and probability estimates) to determine the expected value of a risk	An asset-driven risk assessment method that highlights the importance of self-assessment. It has a broad interpretation of what constitutes an asset, which could be interesting for smart grid
	SGIS Toolbox	Defines and analyses use cases to determine risk impact levels for each information asset, identifying supporting components and running an inherent risk analysis to appropriately select standards to protect every information asset based on security level	This method is dedicated to the area of smart grid security, we describe it further in Sec. III
Support Tools	Good Practices Guide on NNCEIP	Good practices in ICT risk management frameworks to address cyber-related terrorist risks to Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP)	Overviews different risk management frameworks and proposes risk management approaches for energy infrastructure

II. Related Work

In this section, we present a brief summary of a number of risk assessment methods and frameworks, highlighting their applicability to the smart grid. In general, current risk assessment frameworks are mostly focused either on conventional ICT systems, or on traditional power grids, and little consideration has been given to smart grids and their idiosyncrasies. Table 1 provides a summary of the most closely related overarching risk assessment methods and frameworks that we have identified, and provides a brief analysis of their applicability to the smart grid.

The European Network and Information Security Agency (ENISA) maintains a repository of risk assessment standards, methods and tools [6]. The Guidelines for Smart Grid Cyber Security developed by National Institute of Standards and Technology (NIST) (NIST-IR 7628 [7]) provide a set of high-level recommendations applicable to the proposed smart grid architecture for the United States of America. This document and ISO 27002 have been the basis for a report on smart grid security by ENISA [8]. It provides a set of specific security measures for smart grid service providers, aimed at establishing a minimum level of cybersecurity. The importance of performing a comprehensive risk assessment before selecting appropriate measures is pointed out, but no specific methodology is recommended.

III. The SGIS Toolbox

The Smart Grid Information Security (SGIS) toolbox [5] was issued by the standardisation bodies CEN, CENELEC and ETSI to address cybersecurity and risk assessment in smart grids in response to the M/490 Smart Grid Mandate by the European Commission. As such (and because there are few other risk assessment methods that apparently target the specific needs of the smart grid), the SGIS toolbox has the potential in the smart grid sector to be a primary choice for stakeholders to use for a risk assessment. Despite numerous criticisms that have levelled at the SGIS toolbox [5], upon initial inspection, the approach advocated in the toolbox has a number of merits. For example, we suggest that an asset-driven approach to risk assessment is valuable, and the different impact categories that an assessor must consider, e.g., in terms of power loss, reputation, human impact, etc. are important to consider for the smart grid.

The SGIS toolbox estimates the inherent risk for individual information assets. Ultimately, the assessment results in information assets relating to one of five Security Levels (from Low to Highly Critical), which are interpreted in terms of power loss: highly critical assets are those that could lead to a power loss above 10GW when disrupted (i.e., a pan-European incident), while the lowest level applies to assets whose disruption could lead to a power loss under 1MW (i.e., a town or neighbourhood incident). The Security Level for an information asset determines a set of essential security requirements for that asset. To determine the Security Level for an information asset, the SGIS toolbox foresees six steps:

1) Identify relevant information assets: Relevant information assets are identified through a comprehensive use case analysis. In addition, the supporting assets that a primary asset relies on must also be identified and considered in the risk assessment as part of a dependency map, as these may have vulnerabilities that can be exploited in order to harm the primary asset. In case a particular information asset appears in different use cases, they should either be grouped and considered collectively, or the highest risk impact level for that asset across all use cases may be considered.

2) Estimate risk impact: Risk impact is estimated, and expressed in five Risk Impact Levels that use different measurement categories. These are organised into an overall impact table (see Figure 2). To determine the Risk Impact Level for a specific information asset, every category has to be evaluated for different analysis scenarios and for each of the Confidentiality (C), Integrity (I), and Availability (A) properties individually. Eventually, every information asset obtains three Risk Impact Levels (one each for C-I-A); if different levels are assigned per analysis scenario, then the highest level is considered.

3) Identify supporting components: Supporting components for the information assets are identified through a dependency map. This step is implemented to understand the potential cascading effects that are associated with an information asset.

4) Estimate attack likelihood. The SGIS toolbox does not propose its own toolset for vulnerability and threat analysis. Instead, it suggests the use of the HMG IS1 standard for those purposes [2]. This method is highly focused on possible threats by looking at capabilities and motivation for attackers, thus losing view of vulnerabilities and countermeasures.

5) Identify Security Level: The Security Level for every information asset is identified by taking the Risk Impact Level and the likelihood. The Security Level is identified using a risk matrix that identifies criticality levels, depending on the impact and likelihood of an information asset being compromised.

6) Determine security measures: Based on the Security Level that has be determined for every information asset, appropriate security measures are selected which represent high-level recommendations based on NISTIR 7628 [7].

Since risk assessment is a continuous process, these steps should be repeated periodically or when the nature of use cases changes.

To implement the SGIS toolbox for our initial risk assessment, we first develop a use case associated with voltage control that is instantiated in the context of a of a small German DSO supplying about 80 GWH of electricity to businesses and approx. 20.000 residents. The description of the use case is presented in Sec. IV. Following on from this, we implement the risk assessment based on the use case by performing an impact assessment that aims to identify the impact of information assets being compromised in terms of the different security objectives (i.e., confidentiality, integrity and availability), and a threat analysis using the HMG IS1 standard. The first item is summarised in Sec. V, while the second item is not detailed in the paper due to space constraints. Based on these assessments, we can then determine a Security Level for the information assets that are defined in the use case.

IV. A Voltage Control Use Case

For our risk assessment using the SGIS Toolbox we elaborated on the Voltage and VAR Control and Power Flow Optimisation (VVO) (WGSP-0200) use case that was defined by the CEN-CENELEC-ETSI Smart Grid Coordination Group on Sustainable Processes [9].

In our study, we consider a grid control function that uses distributed voltage measurements from Distributed Energy Resources (DERs), such as photovoltaic and wind turbines, and Power Equipment (PE) as input to an algorithm that adjusts the settings of an On-Load Tap Changer (OLTC) and DERs, in order to manage voltage levels on a low-voltage distribution line. Without the presence of DERs, the voltage on a line is expected to go down the further away from a substation it is measured, primarily because of loads (see Figure 1). However, in the presence of DERs, which feed-in power on a line in a distributed fashion, voltage levels could also rise. It is these aspects that are intended to be managed by the functionality described in this use case.

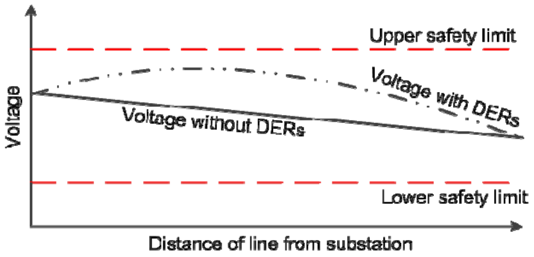


Figure 1: A simplified representation of the voltage properties on a distribution line with and without the presence of DERs; the control algorithm used in our use case aims to control voltage levels so they remain within the upper and lower safety limits.

In summary, the voltage control algorithm operates as follows: if voltage measurements are found to be above or below specified safety thresholds for a given power line (see Figure 1), the control control algorithm will signal to an OLTC to tap down or up, respectively, to shift the voltage levels within safety limits. If voltage levels remain outside safety thresholds, and the OLTC has reached an extremity of its settings, the algorithm attempts to signal DERs, such as photovoltaics, to adjust the amount of reactive power they consume. By consuming more reactive power, DERs can be used to reduce voltage on a line. A more detailed description of this control strategy has been presented by Stifter et al. [10].

In the context of this use case, a number of information assets can be identified that influence the behaviour of this control strategy and could be exploited as part of a cyberphysical attack, leading to incorrect or sub-optimal commands being sent to power equipment and DERs, for example. A summary of prominent information assets is given below:

DER reactive power state: The level at which DERs consume reactive power, which can be used as a voltage control mechanism.

Distributed voltage measurements: Voltage measurements that are taken at different points on a distribution line, e.g., by DERs, smart meters and at a substation.

Current tap setting: The current setting of a tap that is being controlled. Adjusting this setting shifts the voltage band on a line up or down.

Set point commands: The commands that are sent to DERs and an OLTC, for example, to change their state.

Table 2: Protection Mechanisms for the Use Case

Protection Mechanisms	Description
Bad Data Detection	A software component that checks the validity of the measurements that are used by the Substation Control System (SCS). For example, it ensures that voltage measurements are sensible with respect to a model of the grid. If readings are found to be missing or nonsensical, previous values are typically used as substitutes. The assumption with bad data detection is that sensors, due to faults, can either fail to transmit readings or send erroneous data. Studies have shown such bad data protection mechanisms can prove effective in mitigating such issues [11].
Reactive Power Control	Distributed Energy Resources (DERs), such as photovoltaics, have the capacity to consume reactive power — the consumption of reactive power reduces voltage levels. In overvoltage situations — if detected — limited voltage control could be achieved by controlling the amount of reactive power that is consumed by DERs.
Controllable Loads	In order to reduce voltage levels, large controllable loads, e.g., associated with an industrial plant, (or collections of controllable loads, such as electric vehicles) could be instructed to operate. Conversely, when voltage levels are sufficiently low that consumer equipment could be damaged, controllable loads could be instructed to reduce their consumption, e.g., by time shifting their activities.
DER Overvoltage Protection	Equipment associated with DERs, such as PV inverters, locally measure voltage levels; when they become too high, potentially causing damage to equipment, they disconnect from the grid, thus protecting the DER equipment.
Tap Changer Wear Protection	Due to the physical wear from changing tap settings, a tap changer has protection mechanisms to ensure that unusually high numbers of changes do not prematurely reduce its lifetime. For example, such protection ensures that no more than two tap positions can be changed as a consequence of one change command. Moreover, a timeout period, e.g., lasting a number of minutes, is initiated after each tap setting change. This protection mechanism is intended to reduce the impact of erroneous commands, e.g., caused by faults, that rapidly invoke tap changes.
DER Grid Connection Tests	When a DER, such as a PV inverter, attempts to connect to the grid it carries out a number of tests to check the status of the grid before making the final connection. This process can take in the order of minutes to achieve, including the start-up of the inverter.

V. ANALYZING CYBER-PHYSICAL IMPACTS

In order to carry out the cyber-physical attack impact assessment, we chose to use a structured (or semi-formal) approach to support our analysis. To this end, we applied a form of event tree analysis [12] to examine the impact, of an information asset being compromised. In general, event tree analysis is a modelling technique that can be used to inductively explore the potential outcomes associated with an initiating event. Different outcomes can occur, depending on the success or failure of a series of protection measures that are intended to mitigate the effect of the initiating event. These are not cyber-security mechanisms, such as firewalls or intrusion detection systems, but are power system protections that exist in the context of the use case (see Table 2). We acknowledge that additional mechanisms exist in medium and low-voltage distribution networks, such as circuit breakers, but we suggest they have a limited role in the context of our use case.

In summary, we examined the impact of distributed voltage measurements being spoofed to be outside the voltage thresholds for a line (see Figure 1), the effect of voltage measurements being oscillated (i.e., transitioning between the two previously mentioned states), and an unusually wide distribution of measurements being presented to the SCS. Furthermore, we have examined the potential impact of manipulating DER reactive power state, such that it is set to be at its highest and lowest setting, in terms of the amount of reactive power that is being consumed by DERs, and explored the impact of falsifying the current tap setting. Similarly, we have examined the impact of manipulating the commands that are sent to power equipment, such as DERs and the tap changer. Here, we present a single example in some detail – that of tampering with voltage measurements so they appear below the minimum voltage threshold. A summary of the success and failure outcomes for each of the protection measures that are shown in Table 2 is presented in Table 3: if the bad data detection protection measure does not successfully identify that measurements have been tampered with (outcome 1f), a number of failure outcomes could occur. In this scenario, given that DERs (2f) and controllable loads (3f) are likely not to be engaged because control mechanisms are arguably not currently in place to enable this, we foresee the most likely outcome to be 4s (preceded by 1f, 2f, 3f): by repeatedly presenting spoofed voltage measurements under the minimum voltage level for a line, the tap control algorithm will move the tap to its highest setting in order to adapt voltage levels, increasing the real voltage on the affected line. This may result in overvoltage, which could be further compounded during periods when there is low load and high in-feed from DERs. Consequently, DERs may disconnect from the line because overvoltage protection mechanisms are engaged.

With an understanding of the potential outcome from compromising voltage measurements, we can consider the impact of the attack in terms of the impact classes that are defined by the SGIS toolbox and the modified impact levels that are presented in Figure 2. The results of this assessment are presented in Table 4. The impact assessment for the security objectives of confidentiality and availability is not presented here due to space constraints, but is summarized in Sec. VI, as is the likelihood assessment that was carried out using the HMG IS1 standard [2] as suggested by the SGIS toolbox.

Table 3: Summary of the protection mechanisms and success / failure outcomes from the initiating event of spoofing voltage measurements to be too low

Protection Mechanism	Outcomes
Bad Data Detection: A software component that checks the validity of the measurements that are used by the SCS. For example, voltage measurements are sensible given the physical nature of the grid.	(1s) The bad data detection component successfully identifies that measurements have been spoofed. Consequently, previous known-good measurements are used, for example, as input to the SCS
	(1f) The bad data protection component fails to detect that voltage measurements have been tampered with. Subsequently, the tap setting is set to its highest value, potentially causing high voltages that are unsafe. This situation could be compounded by high DER in-feed
Reactive Power Control: Based on measurements that represent the *real* voltage levels on the targeted line, e.g., that have been measured locally, the reactive power settings of DERs are changed so that more reactive power is consumed, thus reducing the actual voltage on a line. Voltage levels cannot be changed significantly using this measure.	(2s) Sufficient reactive power is consumed such that voltage levels are reduced to safe levels on a line
	(2f) Real voltage levels on the line are still too high, despite the consumption of reactive power by DERs
Controllable Loads: In order to reduce actual voltage levels on the line, large controllable loads, e.g., loads associated with an industrial plant (or collections of controllable loads, such as electric vehicles) are instructed to operate. This protection mechanism could learn of actual voltage levels (that are problematic), based on local measures or being instructed remotely.	(3s) Sufficient quantities of controllable loads can be started and the overall real voltage level on the line is reduced
	(3f) Insufficient controllable loads can be initiated, resulting in actual voltage levels on the targeted line remaining unsafely high
DER Overvoltage Protection: DERs, such as PV inverters, locally measure the actual voltage on the line, when voltage levels become too high, in such a way that there could be damage to equipment, they disconnect from the grid.	(4s) Overvoltage protection functions correctly and DERs are protected and disconnected from the line
	(4f) Overvoltage protection mechanisms do not work, resulting in damage to DER equipment

Table 4: Impacts associated with voltage measures that have been tampered with to appear lower than in reality

Impact Category	Justification	Impact Level
Energy Supply	75 kW loss	High
Population	95 people	Low
Infrastructures	No complimentary infrastructures affected	Low
Data protection	No personal or sensitive data involved	Low
Other laws and regulations	Warnings	Low
Human	No/minor injuries	Low
Reputation	Temporary loss of trust by < 10% of population	Low
Financial	The following financial costs could be incurred: 1) Compensate prosumers for potential in-feed not consumed 2) Purchasing of active power to compensate shortfall 3) Reduction in grid efficiency because of over use of reactive power 4) Compensating controllable load users 5) Remedy costs (e.g., engineer's time / installing new equipment)	Low

VI. Assessment Key Findings

The SGIS toolbox suggests that a Security Level should be determined for each information asset and security objective based on Risk Impact level and threat likelihood. These are shown in Table 5, Table **6** and Table **7**. It can be seen from this analysis there are number of information assets that have a Highly Critical Security Level.

For the confidentiality security objective, the smart meter consumption measurements are highly critical, largely because of the potentially high impact to the DSO if disclosed; our analysis suggests that a compromise of confidentiality could result in a significant number of customers being affected with consequent financial implications.

Table 5: Security levels for the *confidentiality* security objective

Information Asset	Impact Level	Likelihood	Security Level
DER reactive power state	Low (1)	Severe (5)	High (6)
Distributed voltage measurements	Low (1)	Severe (5)	High (6)
Smart meter consumption measurements	Highly Critical (5)	Severe (5)	Highly Critical (10)
Current tap setting	Low (1)	Severe (5)	High (6)
SCS and set point algorithm	Low (1)	Severe (5)	High (6)
Tap setting command	Low (1)	Severe (5)	High (6)
DER reactive power set point command	Low (1)	Severe (5)	High (6)
DER state command (i.e., on or off)	Low (1)	Severe (5)	High (6)

With respect to the integrity security objective, a number of information assets have a Highly Critical Security Level – these largely relate to the fact that a number of information assets could result in inappropriate commands being sent to an OLTC and DERs, causing under- or overvoltage situations and DERs to disconnect. In addition, if an attacker is able to compromise the integrity of the messages that are sent to DERs to switch them on or off, a high impact for the DSO could be incurred. At this stage of our analysis, it is unclear whether such an attack could result in grid instability, and is an issue for further investigation.

Table 6: Security levels for the *integrity* security objective

Information Asset	Impact Level	Likelihood	Security Level
DER reactive power state	Low (1)	Severe (5)	High (6)
Distributed voltage	Critical (4)	Severe (5)	Highly

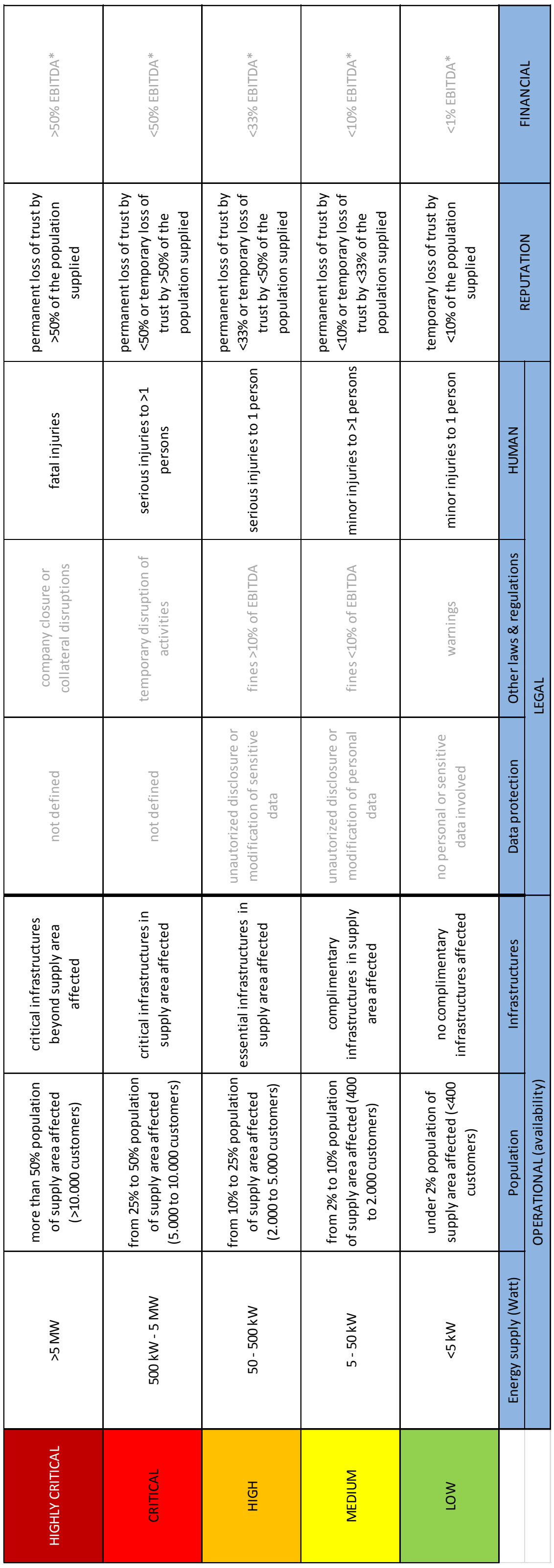
measurements			Critical (9)
Smart meter consumption measurements	Low (1)	Severe (5)	High (6)
Current tap setting	Critical (4)	Severe (5)	Highly Critical (9)
SCS and set point algorithm	Critical (4)	Severe (5)	Highly Critical (9)
Tap setting command	Critical (4)	Severe (5)	Highly Critical (9)
DER reactive power set point command	Low (1)	Severe (5)	High (6)
DER state command (i.e., on or off)	Critical (4)	Severe (5)	Highly Critical (9)

In general, the Security Levels associated with the availability security objective are somewhat lower than for integrity. The exceptions to this rule are the "SCS and set point algorithm" and the "Tap setting command". For both of these information assets, if the grid is in a nominal state, we anticipate minimal impact. However, if an under- or overvoltage situation occurs, the lack of availability of these information assets (and their capacity to control such situations), could lead to a significant impact for the DSO. This point highlights how the incorporation of ICT components to manage potentially critical grid functions that are required in non-nominal states should be realized with care.

Table 7: Security levels for the *availability* security objective

Information Asset	Impact Level	Likelihood	Security Level
DER reactive power state	Low (1)	Severe (5)	High (6)
Distributed voltage measurements	Low (1)	Severe (5)	High (6)
Smart meter consumption measurements	Low (1)	Severe (5)	High (6)
Current tap setting	Low (1)	Severe (5)	High (6)
SCS and set point algorithm	Critical (4)	Severe (5)	Highly Critical (9)
Tap setting command	Critical (4)	Severe (5)	Highly Critical (9)
DER reactive power set point command	Low (1)	Severe (5)	High (6)
DER state command (i.e., on or off)	Low (1)	Severe (5)	High (6)

With an understanding of the Security Levels associated with the information assets of the use case that is under consideration, suitable countermeasures should be selected. Again, this is an aspect of the SGIS toolbox in which limited and unclear guidance is given (see Section 7 of Annex B in [5]). To the best of our knowledge, the Security Level defines whether classes of security measure should be mandatory (or otherwise) and at what level of maturity measures should be realised. These security measures are selected from a table in Annex A of [5], and appear in a number of categories such as access control, awareness and training, audit and accountability, and incident response. Depending on the Security Level, measures are either classed as being subject to "stakeholder decision" or are "recommended". The Security Level for all of the information assets in our use case is either High or Highly Critical. Consequently, it is recommended that all of the security measures that are defined should be implemented. The countermeasures table references security requirements and example technologies in NISTIR 7628 [7]. The maturity of the measures that are implemented should depend on the identified Security Level; however, there is little guidance from the SGIS toolbox on how this should be done.



FINANCIAL	REPUTATION	LEGAL			OPERATIONAL (availability)			
		HUMAN	Other laws & regulations	Data protection	Infrastructures	Population	Energy supply (Watt)	
<1% EBITDA*	temporary loss of trust by <10% of the population supplied	minor injuries to 1 person	warnings	no personal or sensitive data involved	no complimentary infrastructures affected	under 2% population of supply area affected (<400 customers)	<5 kW	LOW
<10% EBITDA*	permanent loss of trust by <10% or temporary loss of trust by <33% of the population supplied	minor injuries to >1 persons	fines <10% of EBITDA	unautorized disclosure or modification of personal data	complimentary infrastructures in supply area affected	from 2% to 10% population of supply area affected (400 to 2.000 customers)	5 - 50 kW	MEDIUM
<33% EBITDA*	permanent loss of trust by <33% or temporary loss of trust by <50% of the population supplied	serious injuries to 1 person	fines >10% of EBITDA	unautorized disclosure or modification of sensitive data	essential infrastructures in supply area affected	from 10% to 25% population of supply area affected (2.000 to 5.000 customers)	50 - 500 kW	HIGH
<50% EBITDA*	permanent loss of trust by <50% or temporary loss of trust by >50% of the population supplied	serious injuries to >1 persons	temporary disruption of activities	not defined	critical infrastructures in supply area affected	from 25% to 50% population of supply area affected (5.000 to 10.000 customers)	500 kW - 5 MW	CRITICAL
>50% EBITDA*	permanent loss of trust by >50% of the population supplied	fatal injuries	company closure or collateral disruptions	not defined	critical infrastructures beyond supply area affected	more than 50% population of supply area affected (>10.000 customers)	>5 MW	HIGHLY CRITICAL

Figure 2: Adjusted SGIS impact table for the DSO under consideration

VII. SGIS Toolbox Reflections

The SGIS toolbox has been used on a number of occasions and has been subjected to a critique and recommendations for improvement (see Section 11 and Annex C of [5]). These include criticisms regarding the presentation of the overall methodology, which we agree with. Here, we present a brief summary of our reflections on using the toolbox, which may affirm previously identified issues.

1) Evaluating inherent risk: The SGIS methodology evaluates inherent risk, i.e., it considers assets without any security measures in place. While this approach is useful to express the importance and significance of assets in general, and performs an important role, it goes only part of the way towards an overall risk assessment evaluating the effect of existing controls on the risk. This position is particularly problematic given that the smart grid, for the most part, is an evolving infrastructure that includes legacy systems – considering a clean slate approach to risk assessment is challenging.

2) Future smart grid topologies: The SGIS toolbox is understandably dedicated to traditional grids, and their topology and hierarchy. It is not well-suited to the new topologies that are proposed in smart grids, such as microgrids, distributed generation, etc. It does not offer support for a hierarchal approach in dealing with smart grids, which is required when dealing with smart grids as a collection of distributed microgrids. Furthermore, the thresholds set in the impact assessment of the toolbox are not applicable to the localised nature of individual microgrids, which makes it difficult to assess local risk. Similarly, in our study, we had to adjust the impact levels to the DSO infrastructure under consideration. The tool itself is not domain-specific; it requires supporting tools to deal with localised and domain-specific impact analysis, which are not provided for.

3) Limitations of HMG IS1 for likelihood assessment: The HMG IS1 standard used by SGIS toolbox is a method for business information technology (IT) and does not reflect the specifics of critical infrastructure. It also seems to be more focused on information channels that are present by design, and less so on possibilities through vulnerabilities. For example, when considering network-based attacks, (almost) every threat source might use the Internet, which therefore automatically makes them the threat actor too. It is focused on persons, clearances and access rights, and has no capabilities for technical analysis of system. Since clearance levels are not significant in the smart grid domain, it is not strictly relevant to the security of critical infrastructure. Similarly, it fails to consider technical security measures.

4) Information loss throughout the process: To implement the SGIS methodology, an assessor has to gather a great deal of information about the use case they are considering, and perform a detailed impact and threat analysis. Having collected all of these important details, the result of the assessment is a Security Level, which indicates the amount of power loss associated with a risk (i.e., an impact and threat pair associated with an information asset). This Security Level is then used as a basis for identifying the security measures that should be implemented by an organization. This loss of information from the detailed analysis through to the very coarse grain Security Level makes it challenging to relate implemented security measures back to the particular threat they are addressing, and therefore challenging for someone to analyse the security improvement that has been introduced.

5) The challenges of identifying assets: The SGIS toolbox provides limited guidance on how information assets should be identified based on a use case description. There is the potential for a very large number of information assets to exist for a given use case, many of which could have limited relevance for a risk assessment. Furthermore, it is not clear what precisely an information asset should be – for example, whether an information asset is a system, data item (in transit or at rest), or a functional component. In our assessment, we primarily chose to focus on information assets that sit at the border of the cyber and physical domain, i.e., those that can directly influence power systems, such as tap changers and DERs. When attempting to understand the impact of a cyber-attack on the power system, it may be more appropriate to initially determine the important power equipment assets, and then identify the information assets (and how they can be compromised) as a secondary activity.

6) A lack of tools support for assessment: Analysing the cyber-physical impact of attacks to a smart grid is a complex task – in our example, we attempted to use event-tree analysis to support this analysis. It is both challenging to assess the power loss and potential safety implications of a cyber-attack. Additionally, analysing emerging multi-stage attacks, such Advanced Persistent Threats (APTs), is challenging. The SGIS toolbox does not provide any specific tools support for these forms of analysis, and provides no recommendations about suitable modelling approaches that can be used. This situation results in experts having to infer the impact and likelihood of attacks to the smart grid, which is a process that is known to be problematic. The SPARKS project will aim to address this shortcoming with tools and guidance about appropriate modelling approaches for vulnerability, threat and impact assessment.

VIII. Conclusion and Next Steps

The results presented in this paper demonstrate the challenges encountered whilst assessing cybersecurity risks to smart grids. In this deliverable, a brief survey of existing risk assessment methodologies and frameworks, and an in-depth analysis of the SGIS toolbox reveal the shortcomings in each of them. The shortcomings of the SGIS toolbox are further demonstrated by performing a risk assessment using a use case of voltage control and power flow optimisation. The exercise also uncovered several lessons to be learnt regarding the SGIS methodologies and the requirements for support tools.

The major outcomes of our assessment indicate that compromising the integrity of information assets that are used as a basis for voltage control can have some impact on the operational behaviour of a smart grid, and dependent infrastructures. The latter is especially the case when under-voltage situations are created, for example, when voltage measurements are tampered with in such a way to cause an OLTC to reduce the overall voltage on a line. This is the case, despite a number of existing grid protection measures being present, such as bad data detection functions and overvoltage protection systems. For the most part, we argue that compromising the availability of information assets under nominal conditions has limited impact, as many grid protections measures assume that sensors may fail, resulting in measurements not being present. In the use case analysed, very few of the information assets relate to personally identifiable information, with the exception of smart metering data. This data, in more sophisticated instantiations of the use case, could be used for forecasting and subsequently optimising power flows, for example. We understand that if an attacker were to compromise the confidentiality of this information asset (metering data), the impact to the DSO under consideration could be significant when considering the categories of impact that are proposed by the SGIS toolbox that relate to the overall population affected and reputational damage.

Based on this assessment, the SGIS toolbox recommends a number of security measures that could be used to mitigate the risks that have been identified. The recommendations are wide-ranging, and include improvements to organisational security and various technology areas, e.g., introducing encryption and authentication. However, because the SGIS toolbox ultimately derives a high-level Security Level for information assets that maps to these recommendations, it is challenging to prioritise which of them should be implemented, given a potentially limited security budget. In future work, we intend to build on these lessons learned when proposing the risk assessment methodology within the SPARKS project.

ACKNOWLEDGMENT

The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement No. 608224.

REFERENCES

[1] OCTAVE Information Security Risk Evaluation, http://www.cert.org/octave/

[2] CESG National Technical Authority for Information Assurance, HMG IA Standard No. 1 Technical Risk Assessment, October, 2009.

[3] MAGERIT v.3: Methodology of analysis and risk management information systems, http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html?idioma=en

[4] ISO/IEC 27005:2011 Information technology — Security techniques — Information security risk management (second edition), http://www.27000.org/iso-27005.htm

[5] CEN-CENELEC-ETSI Smart Grid Coordination Group, Smart Grid Information Security, Nov 2012.

[6] ENISA, Inventory of risk management/risk assessment methods and tools http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory

[7] National Institute of Standards and Technology, NISTIR 7628 Revision 1 – Guidelines for Smart Grid Cybersecurity, 2014.

[8] ENISA, Appropriate security measures for smart grids, Dec 2012.

[9] CEN-CENELEC-ETSI, Smart Grid Coordination Group. Reports in response to Smart Grid Mandate M/490, 2012.

[10] M. Stifter, B. Bletterie, H. Brunner, D. Burnier, H. Sawsan et al, DG DemoNet validation: voltage control from simulation to field test. Presented at Innov. Smart Grid Technol. (ISGT Europe) 2011, 2nd IEEE PES Int. Conf. Exhib., pp. 1–8, Manchester, UK.

[11] A. G. E. Ali Abur, Power System State Estimation Theory and Implementation, CRC Press, 2004.

[12] E. Hong; I. Lee, H. Shin, S. Nam and J. Kong, Quantitative risk evaluation based on event tree analysis technique: Application to the design of shield TBM. Tunneling and Underground Space Technology 24 (3): 269–277.