D2.2 Threat and Risk Assessment Methodology
<table>
<thead>
<tr>
<th>Document control information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Title</strong></td>
</tr>
<tr>
<td><strong>Editor</strong></td>
</tr>
<tr>
<td><strong>Contributors</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td><strong>Requested deadline</strong></td>
</tr>
</tbody>
</table>
Executive Summary

In this deliverable, we present a risk management process for the smart grid, which draws inspiration from the well-established ISO/IEC 27005 information security risk management standard. The process is tailored to address the specific challenges of performing risk management for the smart grid, providing implementation guidance for this context. It leverages previous standards work from CEN-CENELEC-ETSI and the Smart Grid Information Security (SGIS) working group, amongst others. Specifically, for example, the important task of context establishment, whereby the scope of the risk management exercise is defined, is realised using the Smart Grid Architectural Model (SGAM) framework. Building on an SGAM-based description of a smart grid use case, we have developed a threat identification approach, based on attack graphs, that directly uses information that is described in an SGAM model. The consequences of a cyber-attack to a smart grid can be wide-ranging, including implications for quality of supply, safety incidents, and business-related consequences. This fact was identified by the CEN-CENELEC-ETSI working group when the, now defunct, SGIS Toolbox was defined. Here, we have adapted the approach to consequence identification and impact assessment, as advocated by the SGIS working group, and enumerate consequence categories that are of interest to smart grid stakeholders. Additionally, we provide recommendations about how these consequences can be identified using different methods. Finally, a key challenge is to identify security requirements, recommendations and controls that address a set of evaluated risks. To this end, we provide initial guidance about how semantic threat graphs – a form of Ontology – can be used to describe relationships between different entities that influence control selection.
Table of Contents

Executive Summary .......................................................................................................................... 3
Table of Contents .......................................................................................................................... 4
Table of Figures ............................................................................................................................ 6
1 Introduction .................................................................................................................................. 7
2 Related Work ................................................................................................................................. 10
  2.1 Risk Management Processes and Frameworks ....................................................................... 10
  2.2 Threat Identification and Likelihood Assessment ................................................................. 11
    2.2.1 Catalogue-based Analysis ............................................................................................ 11
    2.2.2 Structured Analysis Approaches ................................................................................. 12
3 The SPARKS Risk Management Process ............................................................................... 15
  3.1 Target Audience and Environment ...................................................................................... 16
  3.2 Context Establishment .......................................................................................................... 18
  3.3 Risk Identification ................................................................................................................. 19
    3.3.1 Identification of Assets .............................................................................................. 20
    3.3.2 Identification of Threats ............................................................................................ 20
    3.3.3 Identification of Existing Controls, Requirements and Recommendations....................... 21
    3.3.4 Identification of Vulnerabilities ................................................................................. 22
    3.3.5 Identification of Consequences .................................................................................. 22
  3.4 Risk Analysis ......................................................................................................................... 23
    3.4.1 Impact Assessment ...................................................................................................... 23
    3.4.2 Likelihood Assessment ............................................................................................... 24
    3.4.3 Determination of Risk Level ...................................................................................... 25
  3.5 Risk Evaluation ....................................................................................................................... 26
  3.6 Risk Treatment and Acceptance ............................................................................................ 26
  3.7 Communication, Monitoring and Review .............................................................................. 28
4 Context Establishment with the SGAM Framework ................................................................. 29
  4.1 SGAM Modelling: A Voltage and VAR Control Use Case ................................................ 29
    4.1.1 The SGAM Business Layer ....................................................................................... 30
    4.1.2 The SGAM Function Layer ..................................................................................... 30
    4.1.3 The SGAM Component Layer .................................................................................. 31
    4.1.4 The SGAM Communication Layer .......................................................................... 32
    4.1.5 The SGAM Information Layer .................................................................................. 33
  4.2 Supporting Risk Management with SGAM ......................................................................... 35
5 Threat Identification and Likelihood Assessment with Attack Graphs ..................................... 38
  5.1 Identification of Primary Assets and Attack Goals ............................................................... 39
  5.2 Structured Threat Identification using Attack Graphs .......................................................... 40
    5.2.1 Attack Graphs: Motivation and Definition .................................................................. 40
    5.2.2 Generating Attack Graphs from an SGAM-based System Description .......................... 40
    5.2.3 An Attack Graph Example with the VVO Use Case .................................................. 43
  5.3 Likelihood Assessment based on Attack Graphs ................................................................. 45
    5.3.1 Developing a Threat Model based on HMG IS1 ....................................................... 45
    5.3.2 Assigning Threat Levels to Source Nodes ................................................................. 45
5.3.3 Propagating Threat Levels through an Attack Graph ........................................................ 46
5.3.4 Likelihood Assessment with VVO Use Case .................................................................. 46

6 Consequence Identification and Impact Assessment ................................................................. 49
6.1 Consequence Categories ....................................................................................................... 51
6.2 Identification of Consequences ............................................................................................ 54
  6.2.1 Expert Analysis .................................................................................................................. 55
  6.2.2 Safety and Security Analysis ............................................................................................ 56
  6.2.3 Co-Simulation .................................................................................................................. 60
  6.2.4 System Analysis ................................................................................................................. 61
  6.2.5 From System Analysis to Co-simulation: A Voltage Droop-Control Use Case .......... 62
  6.2.6 Assessing the Economic Consequences of Power Interruption ...................................... 63
6.3 Impact Assessment ................................................................................................................ 64

7 Risk Treatment with Semantic Threat Graph Support .............................................................. 67
7.1 Semantic Threat Graphs ........................................................................................................ 67
7.2 Attack Tree and Semantic Threat Graph Hybrid ................................................................... 69

8 Conclusion ............................................................................................................................... 71

References ....................................................................................................................................... 72

Appendix A – An Introduction to Attack Trees ........................................................................... 76
  Tree Creation .............................................................................................................................. 76
  Likelihood Assessment ............................................................................................................. 77
  Attack Tree Drawbacks ............................................................................................................. 77

Appendix B – Likelihood Assessment Example ........................................................................... 79
  Threat Actor Specific Leaf Node Rating .................................................................................. 79
  A 1.1.1 Exploit Vulnerability .................................................................................................. 79
  A 1.1.2 Physical Access .......................................................................................................... 79
  A 1.2.1 Manipulate Service Device ........................................................................................ 79
  A 1.2.2 Manipulate OS or Running Software ......................................................................... 79
  A 1.3.1.1 Exploit Vulnerability in Webservice ....................................................................... 80
  A 1.3.1.2 Manipulate Connection PSN to DER ..................................................................... 80
  A 1.3.2.1 Vulnerability in Another Service ............................................................................ 80
  A 1.3.2.2 Manipulate Connection PSN to DER ..................................................................... 80

  Threat Propagation ................................................................................................................... 80
  A 1.3.1 Manipulate Webservice ............................................................................................... 80
  A 1.3.2 Manipulate other Service ............................................................................................. 80
  A 1.1 Physical Attack ................................................................................................................. 81
  A 1.2 Local Attack .................................................................................................................... 81
  A 1.3 Remote Attack ................................................................................................................. 81
  A1 Manipulate DER Component .............................................................................................. 81
### Table of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The SPARKS risk management process</td>
<td>17</td>
</tr>
<tr>
<td>2</td>
<td>Determining a security level (a synonym for risk level) with a matrix, as applied in the SGIS toolbox</td>
<td>25</td>
</tr>
<tr>
<td>3</td>
<td>The Smart Grid Architecture Model (SGAM) framework</td>
<td>29</td>
</tr>
<tr>
<td>4</td>
<td>SGAM Business Layer for the VVO use case</td>
<td>30</td>
</tr>
<tr>
<td>5</td>
<td>SGAM Function Layer for the VVO use case</td>
<td>31</td>
</tr>
<tr>
<td>6</td>
<td>SGAM actors to components mapping for the VVO use case</td>
<td>32</td>
</tr>
<tr>
<td>7</td>
<td>The SGAM communication layer for the VVO use case</td>
<td>33</td>
</tr>
<tr>
<td>8</td>
<td>The SGAM information layer for the VVO use case</td>
<td>34</td>
</tr>
<tr>
<td>9</td>
<td>The information objects to data models mapping for the VVO use case</td>
<td>35</td>
</tr>
<tr>
<td>10</td>
<td>The Component, Communication, Information and Function (CCIF) view of the VVO use case</td>
<td>37</td>
</tr>
<tr>
<td>11</td>
<td>An attack goal with a primary asset that sits on the cyber-physical system boundary: on the left, the secondary assets and threats are identified by constructing an attack graph; on the right, the consequence of an attack on the asset is identified</td>
<td>39</td>
</tr>
<tr>
<td>12</td>
<td>Initial tree - manipulating the DER setpoint value at the DER</td>
<td>43</td>
</tr>
<tr>
<td>13</td>
<td>Example – manipulate the DER component</td>
<td>43</td>
</tr>
<tr>
<td>14</td>
<td>Example – manipulate the setpoint at the DMS</td>
<td>44</td>
</tr>
<tr>
<td>15</td>
<td>Example - manipulate the communication from the PSN to DER</td>
<td>44</td>
</tr>
<tr>
<td>16</td>
<td>Example - Manipulate Connection DMS to PSN</td>
<td>44</td>
</tr>
<tr>
<td>17</td>
<td>Example – a weighted attack sub-tree A1 for the attacker “Handler” (HAN)</td>
<td>48</td>
</tr>
<tr>
<td>18</td>
<td>Model of consequence identification and impact assessment methods</td>
<td>50</td>
</tr>
<tr>
<td>19</td>
<td>The relationship between the different aspects of an impact assessment</td>
<td>50</td>
</tr>
<tr>
<td>20</td>
<td>An example event-tree that can be used to examine the potential consequences of an information asset being compromised</td>
<td>57</td>
</tr>
<tr>
<td>21</td>
<td>An inverter-based droop controller under (a1) a reference signal attack at bus i, where the adversary corrupts the corresponding voltage reference signal, and (a2) a measurement routing attack at bus i, where the adversary redirects the voltage measurement from bus j to the controller at bus i, as if it were a measurement from bus i</td>
<td>62</td>
</tr>
<tr>
<td>22</td>
<td>The abstract semantic threat graph model</td>
<td>68</td>
</tr>
<tr>
<td>23</td>
<td>An excerpt of the DER and firewall semantic threat graphs</td>
<td>69</td>
</tr>
<tr>
<td>24</td>
<td>A fragment of an attack tree and semantic threat graph hybrid</td>
<td>70</td>
</tr>
<tr>
<td>25</td>
<td>Example of a simple attack tree with root node “A” followed by the operator OR (\lor) for four sub-goals where node “A.1” is further described by splitting it up in more sub-goals</td>
<td>76</td>
</tr>
<tr>
<td>26</td>
<td>Example of an attack tree with the weight propagated to the root node</td>
<td>77</td>
</tr>
</tbody>
</table>
1 Introduction

The smart grid is an evolution of existing power grids, whereby increased levels of Information and Communication Technology (ICT) and Supervisory Control and Data Acquisition (SCADA) systems are used to support new energy services [1]. These energy services, such as Demand Response (DR) schemes, are, for the most part, enabled by the introduction of new monitoring and control capabilities in the medium- and low-voltage energy distribution networks. Novel ICT and SCADA systems introduce new cybersecurity threats and vulnerabilities, and the use of these systems to support services, which are operationally critical, increases the impact of cyber-attacks. In this context, it is important to understand the cybersecurity risks to the smart grid, so that well-founded security requirements and controls can be identified and implemented, respectively.

The implementation of risk assessment and management practices for the smart grid is particularly challenging, for a number of reasons. The smart grid is a cyber-physical system, i.e., cyber systems – ICT and SCADA systems – are used to control physical systems and processes – tap changers, photovoltaic inverters, etc. Therefore, a major challenge when implementing a risk assessment exercise for the smart grid is to identify the physical consequences of a cyber-attack. Building on this point, cyber-attacks could result in safety-related incidents, i.e., those that result in injury or loss of life. For example, consider a cyber-attack in which the behaviour of remotely controllable circuit breakers could be manipulated. In this deliverable, we give specific guidance regarding how to address these aspects. Additional smart grid risk assessment challenges include managing the organisational complexity of the smart grid; evaluating potential cascading effects, e.g., to dependent infrastructures, from a cyber-attack; and assessing the risk associated with introducing novel ICT and SCADA systems to existing legacy systems. We refer the reader to our previous work that has examined these aspects [2].

In this deliverable, we present a risk management process for the smart grid that is based on the ISO/IEC 27005 information security risk management standard [3]. We have based the process on this standard because it affords us a well-defined approach that is familiar to the information security community. Additionally, it provides a well-established vocabulary for risk management that we have used. Another motivation for basing the process on the ISO/IEC 27005 standard is that the resultant process should be well-aligned with emerging cybersecurity requirements and compliance needs for critical infrastructure protection, such as those to be introduced with the forthcoming EU Network and Information Security (NIS) Directive [4]. Our contribution is to provide guidance on how to implement the risk management process for the smart grid, or more specifically a set of smart grid use cases, considering a number of the aforementioned challenges, building on normative concepts from smart grid standardisation and research domain.

The guidance that we provide is heavily influenced by our experiences and the lessons learned from the implementation of a risk assessment exercise using the Smart Grid Information Security (SGIS) Toolbox – a now largely defunct risk assessment process that was proposed by the CEN-CENELEC-ETSI SGIS working group [5]. An overview of our findings from this exercise is summarized in [6]. Specific insights have been reflected in the process defined in this document:

(i) we found the use of the Smart Grid Architectural Model (SGAM) framework for defining the context of an assessment exercise useful, which we have adopted here;

(ii) we found the categories of impact that are defined for the SGIS Toolbox to be informative and reflect well the many different consequences of cyber-attacks that should be considered for the smart grid – we have elaborated on their use and provide guidelines regarding how to assess different types of consequence;
(iii) the likelihood assessment approach that is defined in the Toolbox is based on an analysis of threat sources and actors, using the HMG IS1 standard [7] – we found this somewhat limited, and have elaborated on how attack graphs can be used, alongside the SGAM framework, to perform a more structured threat analysis that is supported by an HMG IS1-based likelihood assessment; and

(iv) a major criticism that has been levelled at the SGIS Toolbox, which we found in our work, is that a great deal of detail about risks (e.g., impact and threat analysis details) is accrued as part of a risk assessment using the Toolbox, which is lost when a risk level and security requirements are defined. Additionally, an assessment results in almost all controls being recommended for implementation, thus limiting the value of a detailed assessment. We address this shortcoming by proposing the use of semantic threat graphs – a form of Ontology – to explicitly express the relationships between incident scenarios and selected security requirements and controls. This traceability is necessary when evaluating whether to accept certain risk levels, as part of the overall risk management process.

This deliverable is organised as follows: in Section 2, we introduce related work, focusing on closely related overarching risk management processes and frameworks, and threat and likelihood assessment techniques. Approaches for consequence identification are discussed in Section 6.

Following this discussion, in Section 3, we present the overall SPARKS risk management process, which is based on the ISO/IEC 27005 information security risk management standard. We define the purpose of the process, its intended audience, and when necessary provide tailored recommendations about how to implement the process for the smart grid. In many cases, we point forward to specific detailed guidance in subsequent sections, e.g., on threat analysis and likelihood assessment. In some cases, we have had to adjust, or expand on, the semantics of information security management vocabulary for the smart grid context – when necessary, this framing is described in Section 3.

An important initial step for a risk management exercise is to establish its context, including technical and organisational boundaries. For this we advocate the use of the SGAM framework from the CEN-CENELEC-ETSI Smart Grid Coordination Group (SG-CG). We briefly present how the SGIS framework can be used to describe a smart grid use case, with the support of a voltage control example, and summarise how the details that are defined in a model can be used for risk assessment purposes. These items are presented in Section 4.

Attack trees [8] are a well-known approach to examining the steps that an attacker can implement to realise a nefarious goal, such as information disclosure or causing grid instabilities by tampering with control systems. In a similar way, we use attack graphs – a generalisation of attack trees, an SGAM-based model of a smart grid use case, and attack patterns to identify threats to key information assets in a smart grid use case. Key information assets are, for example, those that reside on the cyber-physical systems border that directly influence the behaviour of the grid; we provide guidance on how to identify them, along with the details of our approach in Section 5. Our aim is to support the development of well-structured and comprehensive graphs that describe threats to the smart grid. In addition, we show how an analysis of threat actors and sources, using the HMG IS1 standard, can be used to assess the likelihood of an attack, which is described using an attack graph.

Alongside a threat identification and likelihood assessment, an important part of a risk management exercise is to identify the consequences of incident scenarios and their impact. We describe, in Section 6, a number of consequence categories, e.g., that relate to quality of energy supply, information disclosure and safety, and the metrics that can be used to measure these consequences, such as frequency distortion. We suggest that different smart grid stakeholders are more interested in certain
consequences, and propose what these consequences could be for a number of example stakeholders. Building on this information, we identify specific identification and assessment approaches that can be applied to difference consequence categories. Depending on the amount of information that is available about the target of evaluation, the required fidelity of the results of an analysis, and the amount of effort an analyst would like to expend, different assessment approaches will be more or less suitable. We provide guidance on these aspects. Having identified the consequences of an incident scenario, their impact should be assessed – this aspect is also discussed in Section 6, providing suggestions about how impact tables can be drawn up for incident scenarios that reflect an organisations risk appetite.

Finally, in Section 7, we introduce the concept of semantic threat graphs [9] with the use of an illustrative example. Semantic threat graphs can be used to describe the relationships between assets, threats, vulnerabilities and countermeasures, and can be instantiated for a context such as a specific smart grid use case. Semantic threat graphs can have many uses, e.g., in relation to threat analysis, but we highlight here how they can be used to ensure traceability between identified threats and the countermeasures (e.g., security recommendations or controls) that can be applied to address them. This is important when considering whether risks have been appropriately addressed, when performing a risk acceptance exercise.
2 Related Work

We present an overview of selected risk assessment and management standards, and threat identification and likelihood assessment. Regarding consequence identification, we present a number of relevant methods in Section 6.2, when providing recommendations about different forms of consequence should identified – we refer the reader to this section for a discussion on these techniques.

2.1 Risk Management Processes and Frameworks

As a framework for general risk management, the ISO/IEC 31000 standard [10] represents a good starting point for setting up a risk management process for the smart grid. The standard describes a generic risk management approach, which can be tailored for use in specific application domains. For example, based on the ISO/IEC 31000 standard, the ISO/IEC 27005 standard has been developed for information security risk management [3]. This standard describes the steps that should be taken to implement an information security management system (ISMS) in an organisation, including risk assessment steps. The focal points of the processes that are defined by these standards are the assets that are critical to the operation of an organisation. In many ways, the ISO/IEC 27005 can be understood to be the canonical information security risk management standard, with a number of others being closely aligned. For example, the OCTAVE method [11] is a risk-based approach to identifying an organisation’s security needs. OCTAVE Allegro [12], the latest version of the OCTAVE method, places a strong focus on identifying information assets as a basis for risk assessment. Additionally, the Magerit risk assessment method [13], which is mandated for use by critical infrastructure operators in Spain, is heavily influenced by the ISO/IEC standards – its appropriate use can lead to ISO certification. The HMG Information Assurance Standard No.1 (IS1) is a risk management standard that is used for governmental information technology systems in the United Kingdom [7]. The standard defines a six-step risk management process that is largely focused on analysing threats to assets, which are grouped into a so-called focus of interest. We make use of the threat assessment technique that is defined in HMG IS1 to support likelihood assessment (see Section 5.3). For a further list of risk assessment and management standards, including some of those discussed herein, we refer the reader to a repository that is managed by the European Information Security Agency (ENISA)1.

The aforementioned risk assessment and management standards are targeted for use by organisations that operate information and communication systems, and are therefore focused on information security. However, there are some aspects of the smart grid that invite the use of targeted risk management guidelines, including the challenges that are outlined in Section 1. To this end, the CEN-CENELEC-ETSI Smart Grid Information Security (SGIS) working group developed the so-called SGIS Toolbox – a risk-based approach to identifying security requirements for smart grid use cases [5]. In short, to implement a risk assessment exercise, one initially defines the use case that is being considered using the SGAM framework (for more details about the SGAM framework, see Section 4).

Based on this description of the use case, one examines the impact of the three security objectives (confidentiality, integrity and availability) being compromised for each information asset that has been identified. This impact assessment is undertaken for a number of different forms of impact, including operational, regulatory, economic and reputational aspects. Complementing the impact assessment, a threat assessment is performed using the HMG IS1 standard. Subsequently, the impact and threat levels are used to determine a security level using a set of matrixes that, for example, give higher

---

security levels to infrequent but high impact incidents, for example. Finally, based on the determined security level, security recommendations are identified, which are taken from the National Institute for Standards and Technology (NIST) 7628 guidelines [14]. The SGIS Toolbox was subjected to an evaluation period, with a number of aspects being suggested for improvement [15]; many of the same aspects were highlighted in our work [6]. Finally, the SGIS working group decided to shift focus away from the toolbox, and instead highlight the need for an overall risk management framework (defining what one should consider), and leaving the specific form of risk assessment strategy open, pointing to the aforementioned repository that is supported by ENISA.

Focusing on electric grids, Sridhar et al. [16] define a risk assessment method that reflects their cyber-physical nature, and focuses on identifying vulnerabilities as a basis for a risk assessment. They look at a number of key power applications, e.g., advanced metering, along the power generation and distribution chain, and explore the security vulnerabilities and countermeasures for each of them. Additionally, they provide a categorisation of the control aspects of these applications, e.g., what physical parameters are controlled and devices that are involved, which can be used to support a risk assessment. In line with the approach suggested by Sridhar et al., the SPARKS risk management process also aims to reflect the fact that the smart grid is a cyber-physical system, e.g., when performing the proposed threat and consequence identification steps. However, we suggest the focus on identifying vulnerabilities is limiting. Meanwhile, Nordgård et al. present a risk-based approach to performing asset management in electricity distribution networks, which does not focus exclusively on cybersecurity matters [17]. They highlight a number of different categories of risk and discuss how different analysis methods can be applied, e.g., based on their implementation effort and the amount of knowledge that is required about an infrastructure that is being analysed. We have adapted this approach to our guidelines for consequence identification, wherein we highlight a number of analysis methods that can be applied to different consequence types, and indicate the knowledge and effort that is required to implement the method.

### 2.2 Threat Identification and Likelihood Assessment

A major aspect of risk assessment is identifying threats and assessing their likelihood of occurrence. A threat can be defined as having “the potential to harm assets such as information, processes and systems and therefore organizations” [3]. Identifying and determining the likelihood of threats is a major challenge and is thereby the topic of numerous research activities. Generally, the used methods can be separated into catalogue and structured approaches. While catalogue-based analysis is typically defined in standards and uses fixed analysis elements like checklists, structured analysis approaches are more context specific.

We propose a hybrid solution that uses two structured analysis methods (namely, attack trees and semantic threat graphs), enriched with knowledge from available catalogues. While attack trees enable a comprehensible high level analysis, semantic threat graphs enable an in-depth analysis at a lower technical level, with the ability to embed the knowledge from available catalogues. This approach is described in Section 5. In what follows, we briefly summarise the major related work in the two main areas of threat analysis and likelihood assessment.

#### 2.2.1 Catalogue-based Analysis

Catalogue-based analysis methods typically provide checklists, constraints and scoring spreadsheets to deterministically evaluate a system. Besides providing a score-based rating, these methods often include some form of guidelines, best-practices or advisories to optimize the rating. This ability to support security and evaluation as well as the determinism make catalogue based methods is attractive
for norms and standards (European Commission, ETSI, ISO, MITRE, NIST, etc.). The downside of most of these methods is their abstraction and static character, which could lead to an incomplete analysis, as elements or interdependencies that are not covered by the catalogue are not evaluated properly.

A method for determining the likelihood of an attack is described by ETSI [18]. This method calculates the potential attack rating by an equation of different attack factors. If the sum of these factors exceeds an individual threshold, a corresponding attack is assumed likely. In contrast, typical information security standards, e.g., [7][14][18][19][20], consider the likelihood of a threat occurrence, resulting in an adverse impact, not as a formal calculable percentage, but roughly estimable by available evidence, experience, and expert judgment. Nonetheless, the NIST 800-30 risk assessment guidelines [20] provide a description of potential useful inputs to determine an overall likelihood score. The NISTIR 7628 smart grid security guidelines [14] do not provide any likelihood assessment formalisation, as they consider the effective likelihood as not assessable in a generic sense and may not be known in an early stage of a risk assessment. The HMG IS1 standard [7] considers likelihood as a sub-factor of the risk level and the threat actor. Meanwhile, the CEN-CENELEC-ETSI SGIS Working Group [19] as well as NISTIR 7628 point out the requirement of context specific expert knowledge to assign one of five effective likelihood levels, attributed to the combination of the capability and motivation of a threat source, and a threat actor to attack an asset. The NISTIR 7628 guidelines further appreciates measures to minimize the likelihood of successful cyber-attacks and physical attacks as they minimize the impacts of a cyber-physical attack.

2.2.2 Structured Analysis Approaches

Structured analysis approaches use a sequential, explorative process to gradually identify and evaluate each element of the system under evaluation. While this process enables a more in-depth analysis, it requires an evaluator with some level of knowledge about the target environment and security.

**Attack Trees**

As the canonical example of a structured analysis approach, *attack and threat trees* provide a semi-formal and cost-effective way of structuring the various threats that an asset may encounter [8]. They enable the identification and evaluation of attack vectors by combining several vulnerabilities in one analysis and identifying the most attractive path, e.g., in terms of minimal effort or least resistance, for an attacker. This way it becomes possible to determine the likely points of entry and steps an attacker might choose to achieve specific targets. They provide a top-down approach as a way to determine viable threat vectors (who, why and how a system can be compromised). In practice, these trees are used for threat elicitation and analysis – representing threats at a high-level of abstraction – and have tended not to be used to capture low-level or concrete security configuration detail. In Appendix A – An Introduction to Attack Trees, we present an introduction to the use of attack trees.

Countermeasure-centric extensions of the attack tree model, as presented by [21][22][23][24], enhance the basic model with methods to describe interactions between attackers and defenders. An extension allowing nodes that represent defensive measures to appear at any level of the tree and make this formalism suitable for representing interactions during an attack is described as *attack–defence trees* (ADT) by [24]. This work also provides semantical approaches regarding how to quantitatively analyse attack and defence scenarios using attributes. Adding combinations of detection and mitigation events at all leaf and intermediate nodes, avoiding the state-space explosion problem in the tree analysis, are specified as an *attack countermeasure tree* (ACT) by [23].
### Attack Graphs

An attack graph models knowledge about the inter-dependency between system vulnerabilities and knowledge about a network topology in terms of a graph-based data structure [25][26][27]. Model checking analysis techniques are typically used to determine all possible sequences of an attack against a system [28][29][30]. While attack trees typically focus on the consequence of an attack, attack graphs typically focus on the attacker activity and their interaction with the system under threat [26]. Attack graphs are typically classified as one of the following [31]: a connection-oriented attack graph consists of nodes that represent system and network states; for example, host system, services, network connectivity, and user privilege levels. Graph edges are used to represent exploits which denote state transitions. Both [27] and [30] illustrate examples of condition oriented attack graphs. An exploit-oriented attack graph (exploit dependency graph [32]), is the opposite of a condition-oriented attack graph, with respect to nodes and edges. A condition-exploit-oriented attack graph [33] consists of nodes that represent both states and exploits, whereby an edge represents the relationship between states and exploits [31].

Existing research approaches consider the management of attack graphs. For example, Mehta et al. [29] investigate a number of ranking techniques, such as Google page ranking, as a means of identifying and presenting relevant portions of the attack graph to the security administrator. Noel et al. [33] present a visual framework for managing attack graph complexity that uses ‘hierarchical graph aggregation techniques’ whereby non-overlapping sub-graphs are recursively collapsed to single abstract nodes. Wang et al. [25] state that an analysis of attack graphs is primarily based on proprietary algorithms. Therefore, interactive analysis, similar to decision support systems, is constrained by the current algorithm implementation. They present a relational database model as a basis to perform interactive analysis of attack graphs. An in-depth discussion on attack graphs is beyond the scope of this deliverable and the reader is referred to [31] and [34] for further information.

### Likelihood Assessment with Attack Trees and Graphs

Example applications of attack tree and graph analyses to identify the likelihood and impact of specific attack paths are presented by [35][36][37]. Noel et al. [35] use an attack graph to find the optimal risk mitigation option for a server with Wide Area Network (WAN) access, which requires at least one remote reachable command line interface. To determine the probability of the different attack vectors, a Bayes probability function is used to identify the path with the least successful attack probability, meaning the strongest security functions. Based on these results, the overall system security is improved by removing the other services. Byers et al. [36] use attack trees to model system vulnerabilities in order to assess the technical difficulty, the severity of impact and the probability of detection, finally leading to an overall risk level. As an example use case, an attack against a SCADA system is described. A vulnerability analysis using the original attack tree model to highlight the most significant attack paths to the computer infrastructure of a plant is given by Hutle and Seidel at [37]. The results of the structured attack tree analysis are further used to identify the most urgent points for countermeasures and to estimate their impact.

### Semantic Threat Graphs

Attack trees and graphs tend to be used at rather high-levels of abstraction and are limited with regard to viable threat-only-vectors that contain implicit information such as assets, vulnerabilities and so forth. The approach presented in [9] differs by introducing semantic threat graphs, a variation of the traditional attack tree, which is extended in order to relate semantic information about fine-grained security configuration and, how it relates to assets, threats, vulnerabilities and countermeasures. Thus,
the semantic threat graph approach makes explicit the information that is typically implicit in a threat tree. A semantic threat graph can be defined as a graph that represents the meaning of a threat domain. In addition, semantic threat graphs are extended to include knowledge about qualitative and quantitative risk metrics [38]. Semantic threat graphs have been successfully evaluated against high-level security policy recommendations, best practice standards and low-level systems security configuration [39][40][41]. The use of semantic threat graphs for supporting the risk treatment process, including a more detailed description of their use, is presented in Section 7.
3 The SPARKS Risk Management Process

The SPARKS cybersecurity risk management process, which is depicted in Figure 1, is based on the information security risk management process that is standardised through ISO/IEC 27005. We chose to base the process on the ISO/IEC 27005 standard in order to leverage the well-defined terminology from the standard and its wide-spread acceptance and usage in industry – our intention is not to define an overall novel set of process steps, but to tailor an existing familiar approach to the smart grid. Therefore, to apply the standard in the smart grid domain, we have made some changes to the overall process to reflect the specific challenges of risk assessment for smart grid. Broadly speaking, there are four main topics that are defined in the overall process:

1. **Context establishment** – defining the scope of the risk assessment to be carried out and the overall goals of the stakeholders involved.
2. **Impact assessment** – assessing the impact that incident scenarios will have to a target organisation, such as a DSO, energy supplier or other smart grid stakeholder; these impacts can be both cyber and physical in the context of the smart grid.
3. **Likelihood assessment** – determining the likelihood that an incident scenario will occur, based on a threat and vulnerability analysis.
4. **Security requirements and recommendations** – based on the assessed and evaluated risks, identifying set of security requirements and recommendations, typically drawn from best practice guidelines.

Context establishment is the first step of the process, which establishes the scope of the risk management process. To support the context establishment and provide smart grid-specific guidance when necessary, including aspects such as the business goals and relevant actors, and the underlying system architecture that realises the use case, we make use of the Smart Grid Architecture Model (SGAM) framework. The use of the SGAM framework is intended to build on a well-established standard, in particular in Europe, which should make the implementation of a risk management exercise more structured and straightforward.

The next steps relate to implementing a risk assessment, which contains the following sub-steps: (i) risk identification; (ii) risk analysis; and (iii) the risk evaluation. Whilst Figure 1 suggests a strictly linear implementation of these steps, in reality we anticipate their realisation to be executed somewhat in parallel and iteratively. For example, in many cases, the means to identify threats is tightly coupled with carrying out likelihood analysis. In summary, the purpose of risk identification is to determine what could happen to cause a potential loss and further *how, where and why* the loss might happen. Risk analysis addresses the assessment of impact and likelihood, and finally the determination of a risk level, which is based on the impact and likelihood values. The final sub step to complete a risk assessment is to perform a risk evaluation, in order to prioritise the risks that have been analysed.

After completing a satisfactory risk assessment, risk treatment follows. Initially, security requirements and recommendations for the specific use case are derived. These can be viewed as high-level technical and organisational recommendations that can be realised using a number of different, more specific, controls. Here, we look to specific smart grid recommendations, e.g., based on the NISTIR 7628 [20] and ENISA guidelines [42]. Building on these recommendations, there is the possibility to define specific security controls. We make this distinction between requirements and controls to highlight the different applications of the risk management process: it may be sufficient for an architectural description of an intended smart grid use case to define security requirements, whereas for a deployed system that is being transitioned to a smart grid, specific security controls that will be implemented need to be defined. The choice of security control to implement, such as firewalls and intrusion detection systems or authentication mechanisms, will be based on an organisation’s risk
appetite and the budget allocated to cybersecurity matters. The final aspect of risk treatment is to assess whether the selected requirements and controls conform to an organisation’s requirements. This final sub-step assesses the conformity of a final treatment plan against possible testing, certification standing committee and/or other cybersecurity related requirements for smart grids. If the risk treatment is deemed to be satisfactory, the outcome of this process part (risks and/or requirements/recommendations) is checked against predefined risk acceptance levels, based on the risk management context.

3.1 Target Audience and Environment

As one of the central pillars (critical infrastructures) of our society, energy systems have many stakeholders that could be motivated to conduct a cybersecurity risk management exercise for the smart grid. For example, we foresee Distribution System Operators (DSOs), energy suppliers, solutions providers, researchers, regulators and governmental bodies all having an interest in (and different viewpoint on) performing a cybersecurity risk assessment. For the SPARKS risk management process, we have tried to take this into account and, for example, developed a multi-stakeholder view of the consequences that cyber-attacks could have and the specific approaches to assessing them (see Section 6).

The smart grid is a moving (or an evolving) target. We foresee the target of evaluation – the environment the process is being applied to – could be an architectural design of a future smart grid use case or an existing (operational) smart grid, for example. In the former situation, the SPARKS risk management process can be applied to the development of a secure architectural design for a smart grid use case (following the secure by design principle), whereas for the latter case, the aim is to determine a set of concrete security controls that address a set of cybersecurity risks to an operational system and organisation.

These different motivations for applying a risk assessment will dictate the form of analysis methods that can be undertaken to realise the steps that are outlined in this section. For example, it is clearly not possible to carry out a detailed system vulnerability assessment, using tools such as OpenVAS2, on an architectural description. Likewise, it is likely that a governmental organisation (or other third-party) will not have detailed knowledge of the specifics of a given smart grid deployment, thus limiting their capacity to assess certain types of consequence that relate to quality of supply, for example. Again, we have accounted for this when defining how to realise the steps of the SPARKS risk management process.

In the remainder of this section, we describe the overall SPARKS risk management process in further detail, highlighting the necessary inputs, actions and outputs that are associated with each step.

---

2 The Open Vulnerability Assessment System (OpenVAS): http://openvas.org/
Figure 1: The SPARKS risk management process
3.2 Context Establishment

**Summary**

<table>
<thead>
<tr>
<th>Input:</th>
<th>The information about a high-level use case that is relevant to the smart grid cybersecurity risk management context, based on the specification and analysis of the selected use case using the SGAM framework.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action:</td>
<td>First, the specification and analysis of the use case should be implemented. Second, the boundaries for the risk management exercise should be established, defining its overall scope. This involves defining the basic criteria necessary for risk management (this includes the risk management approach, risk evaluation criteria, impact criteria, and risk acceptance criteria), and establishing an appropriate team to implement the risk management process.</td>
</tr>
<tr>
<td>Output:</td>
<td>The specification and content of the use case using the SGAM framework, definition of the basic criteria, the scope and boundaries, and the responsible parties for the risk management process.</td>
</tr>
</tbody>
</table>

**Implementation Guidance**

It is important to define a boundary (or context) for a risk assessment and management process – we propose that this boundary should be defined via a high-level smart grid use case description, using the SGAM framework. For example, for a given high-level use case, e.g., Voltage and VAR control (VVO), a set of business actors and their goals are defined (at the SGAM Business layer) down to the systems and devices that realise the use case (at the SGAM Component layer). We summarise how to define a high-level use case with an example in Section 4.

Of course, a single high-level use case may not address all of the risk management concerns of an organisation, such as a DSO – this boundary may be somewhat limiting, as an organisation will implement numerous high-level use cases. In this instance, a collection of high-level use cases that collectively describe the risk management concerns of an organisation should be examined. Results from the analysis of one use case could be transferable – e.g., parts of a threat analysis (as described in Section 5) may be reusable for another related use case. Finding opportunities for reuse of this sort can help reduce the overhead of implementing an overall risk management process. However, in order to manage the complexity of a risk assessment and management process, defining its scope via a high-level use case appears to be tractable.

Additionally at this stage, it is important to point out the purpose of the smart grid cybersecurity risk management process. As mentioned earlier, the process may be realised in order to define a security architecture for a future smart grid use case, or to manage the risks associated with a deployed system. This intent should be made clear, for example, in order to determine the analysis methods that can be applied and the means by which the success or failure can be managed – as part of the basic criteria, which are mentioned below.

In general, for a risk management process to be successful and so that one can determine its success or otherwise, it is necessary to define a number of so-called basic criteria. This includes the following aspects:
The risk management approach

Depending on the scope and objectives of the risk management process, different approaches can be applied. The approach also can be changed iteratively. An appropriate risk management approach should be selected or developed that addresses risk evaluation criteria, impact criteria and risk acceptance criteria, which are described next.

The risk evaluation criteria

These criteria should be developed for evaluating the cybersecurity risk for smart grid, considering aspects like the criticality of the assets involved; legal and regulatory requirements, and contractual obligations; operational and business importance of availability, confidentiality and integrity; and stakeholder expectations and perceptions, and negative consequences for goodwill and reputation.

The impact criteria

Impact criteria should be developed and specified in terms of the degree of damage or costs to the smart grid stakeholder that are caused by a cybersecurity event, e.g., breaches of information security, in terms of loss of confidentiality, integrity and availability, loss of business and financial value, and loss of quality of supply. These aspects are described in more detail in Section 6.

The risk acceptance criteria

These criteria should be defined through individual scales for levels of risk acceptance. Risk acceptance criteria often depend on a smart grid stakeholder’s policies, goals, and objectives. In concrete terms, these criteria are for accepting risks and identifying the acceptable level of risk. The following aspects should be considered through setting up the criteria: business criteria, legal and regulatory aspects, operations, technology, finance, and social and humanitarian factors.

Finally, at this initial stage of the risk management process, it should be made clear what roles and responsibilities are necessary – and how they will be filled – in order to make the overall process manageable.

3.3 Risk Identification

The next step is to perform a risk identification exercise. This includes the identification of assets, threats, existing controls, vulnerabilities, and the consequences of cyber-attacks. As mentioned earlier, the process that is outlined in Figure 1 suggests these activities should be implemented in an entirely sequential manner, prior to those for impact and likelihood assessment (see Sections 3.4 on the risk analysis steps). However, it is generally not the case such a sequential approach can be realised, and the approaches for threat identification are closely coupled with those for likelihood assessment, for example (e.g., attack trees can be used to identify threats and their likelihood of occurrence using the same model). The important point is the steps outlined below are implemented, be it in a strictly sequential, parallel or (most likely) iterative fashion.
3.3.1 Identification of Assets

**Summary**

| Input: | The specification of the high-level smart grid use case using the SGAM framework, which details the scope and boundaries for the risk assessment to be conducted. |
| Action: | Identify the *assets* and their *owners* within the specified use case that are necessary to implement the further steps in the risk assessment process. |
| Output: | A list of *assets* and their *owners* to be considered for the risk assessment, and a list of possible business process related assets and their relevance. |

**Implementation Guidance**

In general, an *asset* is anything that has value to an organisation, such as a DSO or energy supplier, or is necessary to realise the functionality that is associated with the high-level smart grid use case that is under consideration. These are the items that need to be protected. Only the assets that are defined within the scope of a high-level use case are relevant for asset identification – this helps to make the assessment and management exercise more tractable. In addition to the asset itself, an *asset owner* should also be identified. This is necessary to have an overview of responsibilities for further risk assessment steps, stakeholder communication and monitoring. In general, an asset owner is best-placed to determine the value of a particular asset.

Example assets in the smart grid context could include the following: Distributed Energy Resources (DERs), Substation Control Systems (SCSs), customers, operating engineers (considering safety aspects), a monitoring system for field measurements, business goals and functions, and information assets such as voltage measurements. Assets can be readily identified using the SGAM framework by examining the Information and Component layers, which are described in more detail in Section 4.

3.3.2 Identification of Threats

**Summary**

| Input: | Information on threats obtained from available sources, including related use cases, analysis tools, external threat catalogues, stakeholder information. Additionally, the high-level use case that is defined using the SGAM framework, including the identified assets. |
| Action: | Threats and their sources should be identified. This can be undertaken in a number of ways, depending on the target of evaluation, including the use of attack graphs, as described in Section 5. |
| Output: | A list of threats with the identification of the threat type and source. This could take the form of an attack graph, without the likelihood assessment in place. |
Implementation Guidance

Threats could be accidental or deliberate and may be of natural or human origin. A threat may arise from outside or inside an organisation, a particular use case or another system. To ensure coverage of the possible threats, their identification should first be done generically and by type, e.g., insiders threats, social engineering or denial of service attacks. After this, individual threats can be identified within the generic classes of threat. Some threats may affect more than one asset. In such cases, they may have different impacts depending on the affected assets. In SPARKS, we advocate the use of attack graphs to identify cybersecurity threats, using the SGAM-based high-level use case description to support the development of the graph. Details of this approach are presented in Section 5.

3.3.3 Identification of Existing Controls, Requirements and Recommendations

Summary

| Input: Documentation that describes the existing security controls, requirements and recommendations, risk treatment implementation plans, and reference catalogues from the likes of NISTIR, ENISA or the IEC. |
| Action: Identify the existing and planned controls, requirements and recommendations by examining documentation, interviewing stakeholders and performing on-site reviews, for example. |
| Output: A list of all the existing and planned security controls, requirements and recommendations, their state of implementation and usage. |

Implementation Guidance

If the target of the risk management exercise is a deployed system, or a risk assessment has previously been performed on an architectural concept, there may be existing security controls, requirements and recommendations in place. It is necessary to identify these items in order to avoid unnecessary duplication of work or cost. The following activities can be used in order to identify existing control, requirements and recommendations:

- Reviewing documents that contain information about the controls, requirements and recommendations (the security artefacts);
- Checking with the people responsible for smart grid cybersecurity and the users that the security artefacts are implemented and followed in practice;
- In the case of a deployed smart grid system, conducting an on-site review of the physical controls, in order to compare those implemented with the list of security artefacts that should be in place, and if they are working correctly and effectively; and
- Reviewing the results of previous audits.

In the end, the risk management exercise should indicate whether the existing security controls, requirements and recommendations are still valid and up-to-date, given current risk levels and an organisation’s risk appetite.
3.3.4 Identification of Vulnerabilities

Summary

**Input:** A list of known assets (see Section 3.3.1), threats (see Section 3.3.2) and existing security controls, requirements and recommendations (see Section 3.3.3).

**Action:** Vulnerabilities should be identified that can be exploited by the previously identified threats, which may result in harm to previously identified assets or an organisation that is considered as part of the context.

**Output:** A list of vulnerabilities in relation to assets, threats and security controls, requirements and recommendations. In addition, a list of vulnerabilities that do not relate to any identified threat for review.

Implementation Guidance

The presence of a security vulnerability does not cause harm in itself, because there is the need for a present threat to exploit it. A security vulnerability without any corresponding threat may not require the implementation of a control, but should be recognised and monitored for changes. Conversely, a threat that does not have a corresponding vulnerability may not result in a risk. Vulnerabilities arising from different sources need to be considered, e.g., those intrinsic or extrinsic to the asset. Vulnerabilities may be found in the following example domains: the physical environment; information system configurations; hardware, software or communications equipment; the system design (in this case, modelled using the SGAM framework); an organisation itself; and processes and procedures.

In the SPARKS risk management approach we propose to model vulnerabilities, along with threats and controls, using semantic threat graphs. The intention is to be able to readily understand the relationships between these aspects, such that suitable controls can be identified. A more detailed explanation of semantic threat graphs, and their use in this context, is presented in Section 7.

3.3.5 Identification of Consequences

Summary

**Input:** The overall context description, a list of assets, business processes (if relevant), and threats and vulnerabilities, where appropriate, related to assets.

**Action:** In this step, one identifies the consequences of assets being compromised. In particular, for cybersecurity aspects, one examines the consequence of the security objectives – confidentiality, integrity and availability – being compromised for information assets. These information assets are defined at the Information layer of the SGAM-based use case description.

**Output:** A set of consequences of the security objectives of (information) assets being compromised, with respect to the stakeholders considered in the risk management
process; further a list of incident scenarios with their consequences related to assets and possible business processes (if relevant).

Implementation Guidance

A consequence can, for example, be a loss of effectiveness, business, reputation, adverse operating conditions, equipment damage, safety-related incident or reduction in quality of energy supply. The purpose of this activity is to identify the damage or consequences to an organisation, e.g., a DSO, energy supplier, or solutions provider, which could be caused by an incident scenario. An incident scenario is the description of a threat exploiting a given vulnerability (or a set of vulnerabilities) that is associated with an asset. Consequences can be of a temporary nature or may be permanent, as in the case of the destruction of an asset.

For the SPARKS risk management process, we draw on experience from the SGIS Toolbox to define a number of consequence categories that may result from an incident scenario. Categories relate to quality of supply, reputational, financial, regulatory, and safety aspects, for example. Additionally, we make proposals regarding how these consequences can be identified using a number of analysis methods – the choice of which method to apply will depend on the infrastructure knowledge at hand and the effort an analyst wishes to commit to the exercise. These details are explained further in Section 6.

3.4 Risk Analysis

Having identified the various risk factors (i.e., the assets, threats, vulnerabilities and consequences), the next step is to analyse them, which results in a risk level. This involves three major activities: (i) impact assessment, analysing the impact a consequence can have on an organisation; (ii) likelihood assessment, determining the probability that an incident scenario will occur; (iii) determining a risk level, which is derived from the impact and likelihood analysis, and is typically considered a product of the two.

3.4.1 Impact Assessment

Summary

| Input: | A list of the incident scenarios, which include the threats, vulnerabilities and affected assets, and the consequences of these incident scenarios (see Section 3.3.5). |
| Action: | The impacts of the identified consequences to the organisation(s) that are defined in the use case are assessed. This involves defining a set of discrete impact levels (e.g., from low to highly critical) for the different consequences that have been considered, and mapping those consequences that have been identified to these levels. |
| Output: | A list of assessed consequences of incident scenarios expressed with respect to assets and impact criteria |

Implementation Guidance

After identifying the consequences of information assets being compromised in the context of an incident scenario, the impact of these consequences should be assessed. The values assigned to the
different forms of assets and an organisation’s overall context and objectives should be taken into account while assessing the impact. In general, (business) impact value can be expressed in qualitative and quantitative forms.

We suggest that different consequences, which can be measured using a number of metrics, are mapped to a discrete set of impact levels that are tailored to the organisation(s) under consideration. For example, a consequence of an incident scenario could be active power losses, measured in kW – for a medium-sized DSO, losses of 50kW could have a medium impact, whereas for a larger DSO these losses could have significantly lower impact. We provide specific guidance and an example of how to approach this assessment in Section 6.3.

The exercise that needs to be implemented in this step is to map the consequences that have been identified to the impacts that were specified when the basic criteria for the risk assessment were established (see Section 3.2).

### 3.4.2 Likelihood Assessment

#### Summary

| Input: | The incident scenarios – threats and corresponding vulnerabilities that relates to assets – that were defined as part of the risk identification process. For an architectural concept of a smart grid use case, a set of concrete vulnerabilities may not be present. |
| Action: | In this step, the likelihood of a threat scenario occurring is assessed. This involves examining the threats that have been identified for their likelihood of occurrence, e.g., with knowledge about the presence and capabilities of threat actors, and the severity of the vulnerabilities associated with the system with respect to how easily they can be exploited. |
| Output: | A set of incident scenarios and the likelihood that they will occur. |

#### Implementation Guidance

A likelihood assessment should be implemented after identifying the incident scenarios. This assessment should take into account how often the threats can occur and how easily the vulnerabilities may be exploited. The likelihood of a threat of occurring can be inferred by performing a threat assessment, wherein one identifies relevant threat sources and actors, and the motivation and capacity of these entities to execute a threat. Determining how easy a vulnerability is to exploit can, for example, be approached by understanding the nature of the vulnerability (e.g., is it a “zero-day” software vulnerability, are patches available for it, and are there know exploits) and how exposed, i.e., readily exploitable, it is.

In a similar manner to the impact assessment, determining likelihood can be approached using quantitative or qualitative analysis techniques. Again, we suggest that discrete values should be attributed to the likelihood of an incident scenario occurring, e.g., from Highly Unlikely (1) to Very Likely (5).

We suggest that likelihood assessment can be realised using the HMG IS1 standard. Using HMG IS1, an analyst follows a structured approach to identifying threat sources and actors, and properties such as their motivation and capability. Collectively, this information can be used to determine the severity.
of the threat. This assessment can then be added to the attack graphs that are used for threat identification. This approach is described in more detail in Section 5.

3.4.3 Determination of Risk Level

Summary

| Input: | A list of incident scenarios, along with an assessment of the impact of their consequences, determined via an impact assessment (see Section 3.4.1), and the likelihood they will occur, which is the result of a likelihood assessment (see Section 3.4.2). |
| Action: | The level of risk should be determined for all relevant incident scenarios. This is typically achieved by taking the product of the likelihood of an incident scenario occurring and its impact. Alternatively, risk matrixes can be used that give relative priority to low likelihood and high impact incidents, or vice versa. |
| Output: | A set of risks with levels assigned. |

Implementation Guidance

Based on the results of the likelihood and impact assessment, the next step is to determine a risk level for each of the incident scenarios. There are a number of approaches to achieving this. A simple, and widely used, approach is to take the product of the likelihood and impact values to determine a risk level. Another method, advocated by the SGIS toolbox, is to use a 5 x 5 matrix that assigns different priorities to low likelihood and high impact events, for example. One such matrix from the SGIS toolbox is presented in Figure 2.

![Figure 2: Determining a security level (a synonym for risk level) with a matrix, as applied in the SGIS toolbox](image)

Using the approach presented in Figure 2, taking the sum of the impact and likelihood, high frequency and high impact incidents are given a higher risk level. In some cases, it may be desirable to give high risk levels to low frequency and high impact incidents, so-called black swan events.
3.5 Risk Evaluation

Summary

| Input: | A set of risks with the levels assigned (see Section 3.4.3) and the risk evaluation criteria that are identified as part of the context establishment step (see Section 3.2). |
| Action: | Risk levels should be compared against the risk evaluation criteria and risk acceptance criteria – the aim is to prioritise the analysed risks. |
| Output: | A list of risks that are prioritised according to the risk evaluation criteria, in relation to the incident scenarios that lead to those risks. |

Implementation Guidance

Risk evaluation is a necessary pre-requisite for being able to select and prioritise different risk treatments (i.e., select suitable security controls, requirements and recommendations). This evaluation is undertaken using the risk evaluation criteria that are determined as part of the context establishment step (see Section 3.2). Risk evaluation criteria that are used for making these decisions should be consistent with the defined requirements for the smart grid cybersecurity risk management process.

Risks are primarily evaluated based on an organisation’s appetite to accept a risk. Furthermore the consequences, impact, likelihood and confidence in the risk identification and risk analysis that has been performed should be considered. It is important to carefully handle an aggregation of multiple low or medium risks, because they could result in much higher overall risks that need to be addressed. In short, the aim is to a) prioritise risk treatments considering the estimated levels of risk; and to b) determine whether a treatment activity should be undertaken for a given risk.

3.6 Risk Treatment and Acceptance

Summary

| Input: | A list of risks that have been evaluated and prioritised according to the risk evaluation criteria (see Section 3.5). |
| Action: | The purpose of this step is to define a risk treatment plan for the target environment, drawing on smart grid security and best practice guidelines, and control specifications. Additionally, this treatment plan should be subjected to an assessment exercise to determine its acceptability with respect to the risk acceptance criteria that are defined in the context establishment phase. |
| Output: | Initially, a risk treatment plan and residual risks or requirements & recommendations list should be produced, which is subjected to the acceptance decision. Subsequently, after assessing the acceptability of the plan, a list of accepted risks with a justification for those that do not meet the predefined risk acceptance criteria. Additionally, a list of accepted requirements and recommendations regarding applicability and feasibility with justification for those that do not meet these aspects. |
Implementation Guidance

Security requirements and recommendations should be defined. There are a number of best practice guidelines and security recommendations that specifically target the smart grid; see Table 1 for an introduction to some of the more prominent contributions from the community. Additionally, we refer the reader to the SPARKS whitepaper on security guidelines for the smart grid [43], which highlights the purpose of these guidelines. This whitepaper has been updated with the SPARKS deliverable D3.2 on Smart Grid Security Guidance [44].

Table 1: Example smart grid related security guidelines, recommendations and controls

<table>
<thead>
<tr>
<th>Organisation</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>ENISA</td>
<td>Protecting Industrial Control Systems Recommendations for Europe and Member States, ENISA, December 2011.</td>
</tr>
<tr>
<td>DHS</td>
<td>Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies, DHS, October 2009</td>
</tr>
<tr>
<td>Council for Internet Security</td>
<td>The Critical Security Controls for Effective Cyber Defense Version 5.1</td>
</tr>
<tr>
<td>ISA/IEC</td>
<td>ISA/IEC 62443 Series of Standards on Industrial Automation and Control Systems (IACS) Security</td>
</tr>
<tr>
<td>CEN-CENELEC-ETSI</td>
<td>CEN-CENELEC-ETSI Smart Grid Coordination Group — Smart Grid Information Security, 2014</td>
</tr>
<tr>
<td>IEC</td>
<td>IEC 62351 standard for addressing security issues of the IEC TC57 series of standards, e.g., IEC 61850.</td>
</tr>
</tbody>
</table>

Additionally, it may be desirable to specify more concrete security controls, that can be used for (i) risk modification; (ii) risk retention; (iii) risk avoidance; and (iv) risk sharing. An important activity to be performed in this step is to clearly identify the residual risk, i.e., the risks that are not being (entirely) addressed by the risk treatment plan. This is necessary when determining whether a given risk treatment plan should be accepted, or otherwise. Finally, a decision should be made and formally recorded regarding whether to accept the risks and responsibilities, based on the risk acceptance criteria that are defined as part of the context establishment.
3.7 Communication, Monitoring and Review

As part of a complete risk management process, information about risks and the risk treatment plan should be communicated to relevant stakeholders and decision-makers. Additionally, the smart grid cybersecurity risk management process should be continually monitored, reviewed and improved as necessary and appropriate. This is necessary in order to ensure the continued relevance of the smart grid cybersecurity risk management process to stakeholder requirements and to indicate when the process may need to be updated.
4 Context Establishment with the SGAM Framework

The first step when carrying out a risk management exercise is to establish its context and define its scope (see Section 3.2). The context description should define organisational issues, such as the business actors, their goals and risk acceptance criteria, and technical factors, including relevant information assets, systems and their relationships. To support context establishment, we propose to build on the Smart Grid Architectural Model (SGAM) [45] – a well-established means of describing smart grid use cases and their architectural realisation. Using SGAM in this way, one can define the context of a risk management exercise through a set of smart grid use cases that are relevant for an organisation – this may be the complete set they support as an organisation or a subset they wish to focus on. This section is divided into two parts: first, it describes the SGAM framework via an example of a Voltage and VAR control (VVO) high-level use case; and second it outlines the use of SGAM in our risk management process and indicates the SGAM entities that are relevant for particular aspects of the risk management process.

4.1 SGAM Modelling: A Voltage and VAR Control Use Case

The SGAM framework is a way of describing the architecture and functionality of the smart grid. Using a layered structure, it supports the requirement of interoperability, combining organizational, informational and technical aspects of the smart grid – three aspects that are important for risk management. SGAM provides a common understanding for different stakeholders and supports the analysis of the smart grid across several viewpoints and levels of detail. As depicted in Figure 3, the SGAM framework models the smart grid in three dimensions: There are five interoperability layers in the model: business, function, information, communication and component layer. Each layer, also called a smart grid plane, is further divided into a two dimensional grid of domains and zones. Domains reflect the physical viewpoint of the electrical delivery process, whereas zones correspond to the hierarchy of the management of this process. SGAM defines five domains (generation, transmission, distribution, DER and customer premise) and six zones (process, field, station, operation, enterprise and market).

Figure 3: The Smart Grid Architecture Model (SGAM) framework
We explain the structure of the SGAM framework with an example of VVO (Voltage and VAR Control) use case [45]. The presented model has been created with SGAM Toolbox, an extension for the Enterprise Architect modelling tool from Sparx Systems. The model is presented layer by layer, indicating the purpose of each layer and its content in the context of VVO use case. First, the business and function layers give an overview of the design of the use case. Subsequently, we describe the realization of the use case provided by the three lower layers: the component, communication and information layers.

### 4.1.1 The SGAM Business Layer

This layer focuses on the business context of the smart grid, including the regulatory and economic structures and policies, market models, business processes and services. The business layer provides an insight into the underlying business processes of the smart grid that indicate what the requirements for the functional and informational architecture are.

![Figure 4: SGAM Business Layer for the VVO use case](image)

Figure 4 shows the SGAM business layer for the VVO use case. In this case, the business actor called Distribution System Operator (DSO) has the goal to improve grid efficiency and stability. Therefore, they use the business case called provide power flow optimization that realizes this goal. The business case invokes the high level use case Voltage and VAR Control. This diagram conveys only a part of the system (related to the VVO use case). The business layer aims to describe the relationships between various business actors, their common goals, the hierarchy of business cases and their realization through high level use cases, such as Voltage and VAR control.

### 4.1.2 The SGAM Function Layer

This layer describes functions and services of the smart grid from an architectural point of view. However, it still provides the flexibility to describe functional elements and their relationships independently from their realization. Flexibility is achieved using abstract descriptions of functions

---

3 The use case management repository we used as a basis for the functional description of the use case for our analysis can be found here: [https://usecases.dke.de/sandbox/](https://usecases.dke.de/sandbox/) (Username and password: LookatMe)


and the use of logical actors (roles) that realize functions, but are not yet determined on the physical layer. The choice of physical realization in ICT systems and power grid infrastructure is described in the bottom SGAM interoperability layers, specifically the communication and component layers.

**Figure 5: SGAM Function Layer for the VVO use case**

Voltage and VAR control is considered to be a high-level use case that includes three functions: (i) status data are collected from a Control Centre (CC), Power Equipment (PE) and DERs, and sent to a Substation Control Centre (SCS); (ii) based on the acquired status data, optimal setpoints are calculated; and (iii) setpoint values are sent to the PE, DER and Flexible Loads (FLs). Figure 5 shows the VVO high-level use case, including three primary use cases (functions) and the logical SGAM actors that are involved in realising the high-level use case.

The three bottom SGAM layers (i.e., the component, communication and information layers) are used to describe the realization of the use case. The process of modelling those layers starts with defining the components that realize the roles of SGAM logical actors.

### 4.1.3 The SGAM Component Layer

The SGAM component layer provides information about the physical components that realize the roles of the logical actors from the function layer. It specifies the systems, applications and physical equipment, i.e., the power grid elements and their controllers, as well as the ICT infrastructure, including computers and network facilities such as routers, cables, switches, and servers.
An actor to component mapping in the context of VVO use case is shown in Figure 6. The Substation Control System (SCS) and Control Centre (CC) are realized by a Distribution Management System (DMS) and Meter Data Management System (MDMS), respectively. The DER functionality is realized by MV Generation (e.g., a wind power plant) represented by the DER MV (Wind) Smart Grid Gateway. The Power Equipment role is realised with a Primary Substation. The flexible load is of unspecified type. It could be a large industrial plant, which is connected directly to the medium-voltage network. Table 2 lists all the logical actors with corresponding components and their placement on the SGAM plane grid.

<table>
<thead>
<tr>
<th>Name</th>
<th>SGAM Actor</th>
<th>Component</th>
<th>Domain</th>
<th>Zone</th>
</tr>
</thead>
<tbody>
<tr>
<td>DMS</td>
<td>Substation Control System (SCS)</td>
<td>Distribution Management System</td>
<td>Distribution</td>
<td>Enterprise</td>
</tr>
<tr>
<td>MDMS</td>
<td>Control Centre (CC)</td>
<td>Meter Data Management System</td>
<td>Distribution</td>
<td>Enterprise</td>
</tr>
<tr>
<td>ER</td>
<td>N/A</td>
<td>Enterprise Network Router</td>
<td>Distribution</td>
<td>Enterprise</td>
</tr>
<tr>
<td>PSN</td>
<td>Power Equipment (PE)</td>
<td>Primary Substation Node</td>
<td>Distribution</td>
<td>Station</td>
</tr>
<tr>
<td>DER Wind SG GW</td>
<td>Distributed Energy Resources (DER)</td>
<td>DER Wind Smart Grid Gateway</td>
<td>DER</td>
<td>Field</td>
</tr>
<tr>
<td>MV FL</td>
<td>Flexible Load (FL)</td>
<td>Medium Voltage Flexible Load</td>
<td>Customer Premises</td>
<td>Process</td>
</tr>
</tbody>
</table>

### 4.1.4 The SGAM Communication Layer

The SGAM communication layer describes the protocols and technologies that are used for the exchange of information between components. An overview of the SGAM communication layer for the VVO use case is presented in Figure 7. The enterprise level devices, namely MDMS and DMS can...
be connected with an Ethernet-based LAN and a Commercial Off-The-Shelf (COTS) router that also provides a connection to the Internet (not show in Figure 7). The PSN has a dedicated Modbus line to this router. Furthermore, the PSN has two GSM modules, which are restricted to a private Access Point Name (APN), to support communicate with the MV FL and the DER Wind SG GW.

![Diagram of SGAM Communication Layer](image)

**Figure 7: The SGAM communication layer for the VVO use case.**

### 4.1.5 The SGAM Information Layer

The purpose of this layer is to describe the information exchanged between SGAM actors and their implementation as components. Information is represented by SGAM entities called *information objects*. Each information object is specified by a data model that is determined by the communication means and protocol used for communication. Figure 8 shows the SGAM information layer for the VVO use case. The relationships between components indicate the direction of the information flows, which are assigned with the information objects that are exchanged. Additionally, a summary of the information objects is presented in Table 3. For the VVO use case, we have defined two data models connected with the protocols that are assigned to the communication paths: Web service data model (for communication between DMS, MDMS and FL), and IEC 60870-5-104 or IEC 61850 for communication between Primary Substation Node and DER Smart Grid Gateways (see Figure 9).
Table 3: Overview of the information objects exchanged in VVO use case

<table>
<thead>
<tr>
<th>Abbrev.</th>
<th>Description</th>
<th>Source-Domain</th>
<th>Source-Zone</th>
<th>Target-Domain</th>
<th>Target-Zone</th>
</tr>
</thead>
<tbody>
<tr>
<td>SM CM</td>
<td>Smart meter consumption measurements</td>
<td>Distribution</td>
<td>Enterprise</td>
<td>Distribution</td>
<td>Enterprise</td>
</tr>
<tr>
<td>CTS</td>
<td>Current tap settings</td>
<td>Distribution</td>
<td>Station</td>
<td>Distribution</td>
<td>Enterprise</td>
</tr>
<tr>
<td>DVM</td>
<td>Distributed Voltage measurements</td>
<td>Distribution</td>
<td>Station</td>
<td>Distribution</td>
<td>Enterprise</td>
</tr>
<tr>
<td>DER RPS</td>
<td>DER reactive power state</td>
<td>DER</td>
<td>Field</td>
<td>Distribution</td>
<td>Enterprise</td>
</tr>
<tr>
<td>FL SP</td>
<td>The set-point for flexible loads</td>
<td>Distribution</td>
<td>Enterprise</td>
<td>Customer</td>
<td>Premise</td>
</tr>
<tr>
<td>TSC</td>
<td>Tap setting command, i.e., tap up or tap down</td>
<td>Distribution</td>
<td>Enterprise</td>
<td>Distribution</td>
<td>Station</td>
</tr>
<tr>
<td>DER SC</td>
<td>DER state command</td>
<td>Distribution</td>
<td>Enterprise</td>
<td>DER</td>
<td>Field</td>
</tr>
<tr>
<td>DER RPSC</td>
<td>DER reactive power set-point command</td>
<td>Distribution</td>
<td>Enterprise</td>
<td>DER</td>
<td>Field</td>
</tr>
</tbody>
</table>

Figure 8: The SGAM information layer for the VVO use case
4.2 Supporting Risk Management with SGAM

The layered SGAM description offers the possibility to map some of the SGAM entities to the steps for risk management, which are summarised in Section 3. To this end, Table 4 presents example uses of the entities that are described in the SGAM framework for risk management. For example, the business context of the use case is relevant in the process of impact assessment, e.g., business actors could be interpreted as stakeholders, whereas business processes give an overview of possible impact categories. Additionally, the use cases that are described at the function layer can be used to support a threat analysis exercise. Information objects can be directly mapped to information assets that are identified also in the process of threat analysis.

For the specific purpose of the threat analysis using attack graphs (see Section 5), we have created a Communication, Component, Information and Function (CCIF) view, which shows the aforementioned SGAM layers collapsed into one view. The CCIF view of the VVO use case is depicted in Figure 10. For practical reasons, combining communication and component layers is appropriate as it identifies and localizes each component of the assessed network. The information layer identifies and localizes all process-relevant information of the assessed network. Based on the CCIF view, an attack graph is constructed with each attack step impairing the identified items. Thereby, each attacker step could be caused by the manipulation of the connection, component, information or function.

Our future work will expand on the use of the SGAM framework for supporting the steps of the risk management process, further detailing the entities that should be described at each layer in order to support risk management. The aim is to develop a tool that can be used to model smart grid use cases and the entities that are important for risk management, and export this information for use with other tools that underpin the implementation of specific steps, such as threat identification with attack graphs.
Table 4: Risk management steps and example usage of the SGAM framework layers

<table>
<thead>
<tr>
<th>Process Step</th>
<th>SGAM Layers</th>
<th>Entities and Short Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Context establishment</td>
<td>Business</td>
<td>The entities described at the business layer, such as the business actors, goals and cases, and their relationship to high-level use cases, can be used to define an overall scope for the risk management exercise.</td>
</tr>
<tr>
<td>Identification of assets</td>
<td>Business, function, information and component</td>
<td>In short, an asset is anything that has value to an organisation or is necessary to realise the functionality that is associated with a smart grid use case. Therefore, the entities that are described at the business layer, e.g., business actors, function layer, e.g., high-level use cases, information, e.g., data objects, and the component, e.g., physical components, can be considered an asset.</td>
</tr>
<tr>
<td>Identification of threats</td>
<td>Function, component, communication and information</td>
<td>Identifying threats can be supported with entities that are described at the function, component, communication and information layer. For example, attack trees could be developed whose goal is to compromise a function or information asset, which is realised via attack steps that compromise entities that are described at the component and communication layer.</td>
</tr>
<tr>
<td>Identification of existing controls and requirements</td>
<td>Component and communication</td>
<td>Existing systems, such as firewalls and access control systems, and communication protocols that are used for security can be identified at the component and communication layer. Of course, organisational controls (such as policies) may be in place, which are not readily described in the SGAM framework.</td>
</tr>
<tr>
<td>Identification of vulnerabilities</td>
<td>Component and communication</td>
<td>If sufficient detail of a smart grid use case implementation is provided, the entities that are described at the component and communication layers can be examined for known vulnerabilities, for example.</td>
</tr>
<tr>
<td>Identification of consequences</td>
<td>Function, component, communication and information</td>
<td>Depending on the approach that has been chosen to identify consequences, the entities that are described at a number of SGAM layers can be used. For example, knowledge of use cases can be used to support expert assessment on attack consequences, whereas detailed knowledge of the component and communication protocols can be used to develop co-simulation models. Further details are provided in Section 6.</td>
</tr>
<tr>
<td>Impact assessment</td>
<td>Business and function</td>
<td>Assessing the impact of attack consequences can be supported by entities that are described at the SGAM business and functions layer. Specifically, knowledge of the mapping between use cases (described at the function layer) to business cases can be used to assess the business impact of cyber-attacks that compromise functions.</td>
</tr>
<tr>
<td>Risk evaluation</td>
<td>Business</td>
<td>A part of risk evaluation is ranking risks and identifying those that require controls – this should be done with knowledge of the overall business goals, which are described at the business layer of the SGAM framework.</td>
</tr>
</tbody>
</table>
Figure 10: The Component, Communication, Information and Function (CCIF) view of the VVO use case
5 Threat Identification and Likelihood Assessment with Attack Graphs

In this section, we describe a process to identify and analyse threats, and determine a likelihood estimation of their appearance in a smart grid infrastructure system. Many current risk assessment methods analyse threats by matching the equipment in place with some predefined tables of threats to the associated assets. Other methods, such as HMG IS1, completely ignore from a technical perspective the equipment in place, and refer to the motivation and capabilities of an attacker to derive a threat level. Such approaches have limitations when one considers multistage attacks, in particular. However, multistage attacks are important threats in networked automation systems, such as the smart grid. Moreover, the lack of security technologies in automation systems leads to the situation that many protection mechanisms rely today on isolation techniques, such as firewalls, data diodes, and zoning concepts. Meanwhile, a structured derivation of threats, e.g., using attack trees, helps to understand the interdependencies between different attacks, and allows the identification of weaknesses that are really relevant. Moreover, such an analysis gives a direct link to necessary countermeasures, and allows the assessment of their impact on the overall threat level, thereby leading to a cost-efficient prioritisation of security measures.

For threat identification in the SPARKS risk management process, we propose to make use of attack trees. Attack trees are a well-established concept with a long history of enhancements (see Section 2.2 for a summary). Our aim is not to propose another extension – the generalization from trees to graphs, which we suggest, is rather straightforward – but show how this concept can be used properly to systematically assess the threats in the smart grid. To do so, we use a step-by-step process, as described in the following sections.

The input to our approach is a model of a system under evaluation, which is described using the SGAM framework, as presented in Section 4. Based on this model, primary assets and attack goals are identified, which form the initial point of our analysis. Using the attack goals and the SGAM description as inputs, we present a structured process to derive an attack graph. The procedure for this can be seen as a best-practice or a catalogue to generate a “good” graph, optimally supporting an exhausting security analysis. The goal here is to achieve a maximal level of completeness and reusability of graphs. Therefore, a “good” graph covers all known threats in a systematic and structured way. We demonstrate the use of our approach on a subset of the VVO use case, which is presented in Section 4.1.

Having generated an attack graph, it is then used to perform a likelihood assessment. For this, to each sink node of the graph (this is the generalization of a leaf node in a tree), a threat level is associated. By propagating the threat level through the graph, a threat level for every attack goal can be estimated. In addition, the threat-level-labelled attack graph allows the identification of major attack trajectories, i.e., those attack vectors that are the easiest from an attacker’s perspective (i.e., the so-called “low hanging fruit”). In order to associate a threat level to every node, an attacker model needs to be specified. For this purpose, we refer to the HMG IS1 standard, which gives a mature methodology to assess attacker capabilities and motivation. Again, the approach is illustrated on the VVO use case.

In what follows, we initially describe how to identify primary assets (from the wider set that are identified as part of the asset identification step), and an attacker’s goals. Subsequently, we present the process for generating attack graphs, based on an SGAM-based model of a target infrastructure. Our approach to likelihood assessment follows, which augments a graph using information derived from a HMG IS1-based analysis.
5.1 Identification of Primary Assets and Attack Goals

In our approach, we start by identifying the so-called primary assets. The basic premise is to identify those information assets that have a direct consequence on the physical power system that is controlled by the information (or control) system. Since we later perform a structural analysis that leads to all the assets that the primary asset depends on, this allows us to reduce the number of attack goals to those of interest to the attacker, and determine the intermediate steps through the threat analysis. This approach is in contrast to those that are typically applied, in which all information assets are identified and evaluated equally. Arguably, our approach is more appropriate for the control systems that are an essential part of the smart grid.

To identify primary assets, we consider the SGAM information layer and define the scope of our analysis. Every information object that leaves the scope of analysis, i.e., the boundaries of the information system under examination, should be considered as a potential primary asset. This includes:

1. information being transferred to other (sub-)networks;
2. control values that are output to the physical process by an actuator; and
3. values that are communicated to humans, e.g., via an Human Machine Interface (HMI).

The next step is to derive potential attack goals. An attack goal describes the violation of a security objective (confidentiality, integrity and availability) with respect to a primary asset. As the consequence identification step in the risk management process has not been undertaken at this stage – if we approach the risk management process in a linear fashion – only attack goals should be excluded from further analysis that clearly have no significant impact. For the VVO use case, an identification of primary assets and relevant attack goals are as follows:

<table>
<thead>
<tr>
<th>Security Objective</th>
<th>Tap changer setpoint</th>
<th>DER setpoint at DER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Integrity</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Availability</td>
<td>●</td>
<td>●</td>
</tr>
</tbody>
</table>

Figure 11: An attack goal with a primary asset that sits on the cyber-physical system boundary: on the left, the secondary assets and threats are identified by constructing an attack graph; on the right, the consequence of an attack on the asset is identified

The next step is to derive potential attack goals. An attack goal describes the violation of a security objective (confidentiality, integrity and availability) with respect to a primary asset. As the consequence identification step in the risk management process has not been undertaken at this stage – if we approach the risk management process in a linear fashion – only attack goals should be excluded from further analysis that clearly have no significant impact. For the VVO use case, an identification of primary assets and relevant attack goals are as follows:

- Compromising the confidentiality of a tap changer or DER setpoint will have no immediate consequences to a smart grid, and is therefore not considered as an attack goal.
In this example, the “Manipulation of DER setpoint at DER” is the attack goal that is derived from the violation of the integrity security objective with respect to the “DER setpoint at DER” information asset.

### 5.2 Structured Threat Identification using Attack Graphs

One way to perform a structured asset-driven threat analysis, suitable for multistage attacks, is to create an individual attack tree for each asset, as described in Section 2.2.2. We have extended this method by using attack graphs that allows a holistic analysis of threats. A necessary input for this method is a system model. To this end, a use case that is modelled using the SGAM framework is chosen as a suitable input for analysis.

#### 5.2.1 Attack Graphs: Motivation and Definition

A standard approach to threat analysis is to create an individual attack tree for every attack goal. However, such an approach suffers from several shortcomings, including:

- attack trees can become very large;
- many parts of the attack tree that are associated with one attack goal might reappear in the attack tree of another attack goal;
- even when considering the attack tree of a single attack goal, a node might already have been considered in another part of the tree; and
- loops in the network structure of a system under consideration might lead to a situation where an explicit representation of an attack tree might lead to a tree with infinite depth, if the process is automated.

To mitigate these conceptual problems, we suggest generalizing attack trees and to generate a common graph for all attack goals. Because of crosslinks between (sub-)goals and loops in the network topology, this graph may contain cycles.

**Definition:** An attack graph is a directed graph \( (V, E) \), where every node \( n \) in \( V \) is labelled with either a logical AND or OR. The graph needs to have at least one source node.

The source nodes of the graph (i.e., all nodes without incoming edges) correspond to the leaf nodes of a conventional attack tree. The sink nodes of the graph (i.e., all nodes without outgoing edges) are also called the root nodes, and refer to the attack goals (see the discussion in Section 5.1).

To facilitate the creation of attack graphs, and to increase the readability of the result, we split the graph into several attack trees. More precisely, when creating an attack graph, we start building a tree and every time the scope is changed, e.g., to another network segment or component, we stop refining the tree and start a new one. The result is a set of attack trees that together form the (cyclic) attack graph for all attack goals.

#### 5.2.2 Generating Attack Graphs from an SGAM-based System Description

In this section, a smart grid environment is considered as a basis to establish an attack tree – the starting point for generating attack graphs. The environment is described by making use of the concepts from the SGAM framework. In order to derive a suitable tree as a basis for a likelihood assessment, the system model for the smart grid needs to be created. This model contains the required information and is created from the communication, component, information and function layer of an SGAM model. For each of these layers, the necessary information is collected in a layer view model, called Communication and Component, Information, and Function (CCIF) view. As mentioned earlier, each SGAM interoperability layer forms a two dimensional grid with five domains (generation,
transmission, distribution, DER and customer premises) and six zones (process, field, station, operation, enterprise, market). To create the CCIF view, a step-by-step approach is used starting from the component and communication layers, subsequently the information and function layers are populated and placed on top of each other. The following subsections describe this layering in more detail, and how it can be used to define an attack tree.

The generation of a tree is initiated with a previously identified attack goal as the root node. As previously mentioned, when the scope changes to a new component, a new tree is started. In this case, the output of the new component is considered as the starting point of the new tree.

**Attack Patterns for Comprising the Output of a Component**

This pattern occurs as the root node of a tree, either because the output is a primary asset, or because a new tree has been started because of a scope change. All potential ways the information asset could be manipulated are added as leaf nodes using a logical OR operator. This could be achieved by adding elements using the following four steps as new attack steps:

- **Consider manipulation of the component emitting the output:** At first, the component that emits the output is identified. Emitting implies forwarding the asset information to other networks outside the SUE scope, to the market or the process, realizing it as a cyber-physical device or displaying it at as HMI.

- **Consider manipulation of the output at the component determining it:** At this step, the manipulation of the output at its source is added as a node. This node hosts all types of manipulation that could directly or indirectly influence the information. This starts with the component creating the forwarded output value within the network as well as the sources that provide factors for relevant calculations.

- **Consider manipulation of components where the information is routed through:** At this step, the components where the information asset is routed through are added. This includes all devices that might recode or simply forward the asset information.

- **Consider manipulation of the communication links that are involved in that information transfer:** Finally, the communication links that are involved in the information transfer are considered. This includes all potential forms of eavesdropping or tampering on wired and wireless connections and busses between and to the previously identified components.

Based on this initial tree structure, a sub-tree for each of the identified items is created. In what follows, we present some attack patterns that can be used as a basis for exploring how this initial tree structure can be expanded on.
Attack Patterns for Compromising Components

The sub-trees that consider how a component could be manipulated are created by analysing the means an attacker has to access a device. Consequently, three basic access types are identified: (i) physical attacks imply the attacker has physical access to the device, meaning they are able to add or remove physical components and software; (ii) local attacks imply that software access is possible, e.g., by instructing a threat actor to perform malicious actions at a terminal or using a virus (e.g., as with the Stuxnet virus that propagated using an infected USB stick); and (iii) remote attacks that imply the ability to perform actions from a remote location by exploiting a running service (e.g., a Web server, secure shell (SSH) service or remote desktop). These three attack vectors are shown in the attack tree below, and should be explored as part of an analysis.

![Attack Tree for Compromising Components]

Attack Patterns for Compromising Communications

The attack tree for each communication link considers the manipulation of each connected device. In addition to the sender and receiver components, this analysis includes all of the devices that are connected physically or via a Virtual Private Network (VPN) to the network, and potential rogue devices and leaks through misconfigured network equipment (e.g., firewalls). This arrangement is summarised in the attack tree below.

![Attack Tree for Compromising Communications]

Attack Patterns for Compromising Functions

The attack tree for each function node includes the function determining and therefore relevant components as well as all input factors like measuring values for this calculation.

![Attack Tree for Compromising Functions]
5.2.3 An Attack Graph Example with the VVO Use Case

To illustrate how our approach to constructing attack graphs can be applied, we present an example with the VVO use case that is presented in Section 4.1. In this example, we examine the attacker goal to “Manipulate the DER Setpoint at DER”, in order to disturb flexible load management.

As mentioned earlier, the first step is to create an initial tree with the attack goal and leaf nodes that examine the four classes of way an asset could be manipulated to realise this goal. Looking at the SGAM component and communication layers (see Figure 10), the component that generates the DER_SP information asset is the DER component itself, making it the first node of the top tree (see node A.1 in Figure 12). The next node relates to the processing of these values, which is performed at the DMS (A.2). Communication aspects are subsequently considered: the only component that is relevant in this context is the PSN, which serves as a proxy that information is routed through; manipulating the PSN becomes the third node (A.3). Finally, the connections between the PSN and DER, and DMS and PSN are added to the initial tree (A.4 and A.5, respectively). Next, each of these leaf nodes is analysed as a sub-tree using the attack patterns that were described earlier.

![Figure 12: Initial tree - manipulating the DER setpoint value at the DER](image)

For the leaf node A.1 in Figure 12 (Manipulate DER Component), the DER component generating and transmitting the asset is analysed using the attack pattern that relates to manipulating components. In our example, A1.2.1 represents a diagnostic tester while A1.2.2 is the locally installed management software of the DER component. The result of this analysis is shown in Figure 13.

![Figure 13: Example – manipulate the DER component](image)

Regarding the leaf node A.2 of the initial tree, the information asset is processed at the DMS. This is based on the input received via the PSN, issued by the DER for the Tap Setting Command (TSC)
information asset, and MDMS for the *Smart Meter Consumption Measurements* (SMCM) information asset (see Table 3). Applying the method described, the following structure is created.

![Diagram A2: Manipulate DER.SP at DMS](image1)

**Figure 14: Example – manipulate the setpoint at the DMS**

For the A.3 leaf node, the manipulation of the components that the information is routed through is analysed. For this case, the analysis is performed in a similar manner to A.1, whereby the different means of compromising a component are expanded on. Finally, for leaf nodes A.4 and A.5, the network connections are analysed. The connection between the PSN and DER at A.4 is considered an IEC 60870-5 connection (see Figure 7), which results in the attack tree that is shown in Figure 15. The connection between DMS and PSN is an Ethernet network – the resulting attack tree for A.5 is presented in Figure 16, which draws on the attack pattern for compromising communications.

![Diagram A4: Manipulate Communication PSN to DER](image2)

**Figure 15: Example - manipulate the communication from the PSN to DER**

In summary, it is evident that certain attack steps reoccur in the different attack sub-trees, for example, the “Manipulate PSN component” attack step (nodes A2.2, A4.1 and A5.2) appears repeatedly. As described in Section 5.2.2, each recurring node is extracted to form a sub-tree, which is further analysed and linked back to the node that references it. This referencing can easily lead to loops, which is not a problem as the manipulation of each component is analysed only once.

![Diagram A5: Manipulate Communication DMS to PSN](image3)

**Figure 16: Example - Manipulate Connection DMS to PSN**
5.3 Likelihood Assessment based on Attack Graphs

In our approach to likelihood assessment, the nodes in an attack graph are labelled with a threat level, which corresponds to the likelihood that an asset will be compromised. The labelling is done by estimating the threat level of the source nodes in the graph and then propagating the values through the graph. This corresponds to a labelling of leaf nodes in the case of an attack tree and propagating values towards the root. As a result of our analysis, we obtain two important pieces of information: (i) a threat level for every attack goal, which is considered as an estimate for the likelihood of a successful attack; and (ii) attack vectors for the respective threat level. The attack vectors are the primary points where countermeasures need to be applied, which is useful when considering risk treatment.

5.3.1 Developing a Threat Model based on HMG IS1

The first step to realise our likelihood assessment is to develop a suitable threat model. We partially use the HMG IS1 standard in order to assess the motivation and capabilities of an attacker. In contrast to the original purpose of this standard, we suggest that the analysis conducted in HMG IS1 leads not directly to a likelihood, but is a rather a method to develop an attacker model. In the standard, access relations and types of attackers are aggregated into Threat Sources (TS) that wish for a compromise to occur, and Threat Actors (TA) that actually carry out the attack. The combination of the capability and motivation of a TA or TS to attack an asset is attributed by a Threat Level (TL) value. For a specific TS, the abilities of TAs can be enhanced with additional resources and combined to reduce the challenge of performing different attack steps. The overhead of considering similarly applicable compromise method details could further be reduced by grouping TAs into families. In this case, depending on the abilities of each actor type, an adjusted likelihood is estimated for their combination. Considering the optimal combination of the actors available to each TS, the TA is swapped whenever a stage that is hard or impossible to achieve by one actor could be executed by another type within the TS.

For example, consider a multistage attack scenario that involves two steps and a threat source that includes two threat actors. While the first step is easy for TA1 (a TL of 5), the subsequent step is considered hard (TL of 2). In contrast, the first step is nearly impossible for TA2 (TL of 1), while the second one is easy (TL of 5). Considering each of these TAs in isolation for the necessary two steps, the threat from TA1 is low and for TA2 it is very low. Although this might appear to be a desirable situation, the threat from a source (TS) that combines both threat actors (TA1 and TA2) represents a maximum threat level, and therefore must be considered. While this process enables the determination of combined abilities, it could lead to an overly pessimistic view, in which the aggregated abilities of an attacker are over-estimated, as not all actors will have the same level of access to a resource or target, for example.

5.3.2 Assigning Threat Levels to Source Nodes

Starting with an attack graph, the source nodes (i.e., those without further children) are rated for each threat actor (family) using one of five discrete levels. This rating represents the severity of a threat, meaning the inverse of how difficult it is to perform the named action (i.e., a TL of 1 implies that an attack is close to impossible to realise, whereas 5 suggests the attack is trivial). In order to be consistent, this rating should ideally be done by using catalogues or expert knowledge, considering the capabilities and motivations that are described in the HMG IS1 standard. Additionally, the factors that are identified in TVRA that are used to rate a malicious activity could be used, if necessary.
5.3.3 Propagating Threat Levels through an Attack Graph

In this step, the threat levels that have been assigned to source nodes are propagated through a graph. As is commonly done with attack trees, the function that is used for this is min/max, which is realised in the follow way:

1. For every logical AND node a threat level is assigned that is the minimum of the threat level of the nodes that have an edge to this node. Intuitively, this reflects the fact that for a logical AND relationship all sub-goals are required to achieve a goal, and thus the hardest sub-goal determines the difficulty of the attack step.
2. For every logical OR node a threat level is assigned that is the maximum of the threat level of the nodes that have an edge to this node. This reflects the fact that for a logical OR node only one sub-goal is sufficient for an attacker to achieve their goal, and thus the easiest sub-goal determines the difficulty of the attack step.

For an attack tree, the propagation of threat levels from the leaf nodes to the root according to these rules is a trivial task. However, for an attack graph, it is not obvious that such propagation is always successful. In particular, due to cycles in a graph, there could be nodes that cannot be labelled, since they circularly depend on each other and therefore a maximum or minimum can be determined. The solution here is to preliminarily calculate a threat level for every node and then later update this value if necessary. In general, such a labelling of the graph does not necessarily stabilize. However, for the graphs that are relevant in our case, namely those that are constructed according the method previously described, a propagation scheme that works as follows leads to the correct labelling of a graph:

1. Label all source nodes of the graph
2. Propagate the values among all unlabelled nodes
3. If there are unlabelled cycles, assign a preliminary value according to the labelled input nodes
4. Adjust the threat level for all nodes so that the min/max condition is fulfilled

A sufficient condition for this algorithm to work is that in the cycles of the graph, only logical OR nodes occur. In such a graph, there is a monotonicity condition on these nodes, such that their value can only increase and thus the algorithm terminates. This is the case for the graphs according to our method, as the cycles induced by the network structure indeed contain only logical OR nodes and the AND nodes are limited to Directed Acyclic Graph (DAG)-like subgraphs that are connected to these cycles.

5.3.4 Likelihood Assessment with VVO Use Case

As an example, the A1.1 branch of the A.1 attack graph (see Figure 13) is assessed (for completeness, the overall A.1 sub-tree assessment is presented in Appendix B). The threat actor specific leaf node assessment and the propagation of the threat level are performed by determining a threat level for three different TAs outlined in the HMG IS1 standard. For our example we adopt the following Threat Actor definitions from the standard [7]:

- **Handler (HAN):** A Handler is someone whose business role requires physical access to the equipment within the focus of interest, but who is not a registered user and does not usually have logical access to the operational system, but may have temporary supervised access for test purposes. This includes people who transport equipment, test repair or replace hardware or dispose of obsolete or damaged equipment. This may also include postal or courier services.

- **Indirect Connected (IC):** An Indirectly Connected threat actor does not have legitimate or authorised business connectivity to the FoI. They may, however, be able to access or make use
of business or network connections because of onward connections from business partners or through networks to which the FoI has a direct connection e.g. the Internet. Where departments have direct or indirect connections to the Internet this threat actor type could include all Internet users. This indirect connectivity could allow threat actors to mount business traffic-borne or network based attacks against the FoI.

- **Normal User (NU):** A Normal User is a registered user or account holder who uses the applications, services and equipment within the FoI to store, process, handle and exchange information in support of business objectives. These users would be provided with ‘standard’ facilities and system privilege as defined in the Departments policy.

Further we adopt the following Threat Level table from HMG IS1, whereby we consider negligible as level 1 up to critical as level 6.

<table>
<thead>
<tr>
<th>Capability Level</th>
<th>1. VERY LITTLE</th>
<th>2. LITTLE</th>
<th>3. LIMITED</th>
<th>4. SIGNIFICANT</th>
<th>5. FORMIDABLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Motivation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>INDIFFERENT</td>
<td>Negligible</td>
<td>Negligible</td>
<td>Low</td>
<td>Low</td>
<td>Moderate</td>
</tr>
<tr>
<td>CURIOUS</td>
<td>Negligible</td>
<td>Negligible</td>
<td>Low</td>
<td>Moderate</td>
<td>Substantial</td>
</tr>
<tr>
<td>INTERESTED</td>
<td>Negligible</td>
<td>Low</td>
<td>Moderate</td>
<td>Substantial</td>
<td>Severe</td>
</tr>
<tr>
<td>COMMITTED</td>
<td>Low</td>
<td>Low</td>
<td>Moderate</td>
<td>Substantial</td>
<td>Severe</td>
</tr>
<tr>
<td>FOCUSED</td>
<td>Low</td>
<td>Moderate</td>
<td>Substantial</td>
<td>Severe</td>
<td>Critical</td>
</tr>
</tbody>
</table>

Recall that the first step in our process is to assess the threat level for all source nodes, in this example A1.1.1 and A1.1.2 (see Figure 17). For the A1.1.1 attack step – *Exploit Vulnerability* – the exploitation of a physical vulnerability using physical means requires minimal technical knowledge. Correspondingly, the threat levels that are assigned to each of the threat actors can be assigned, as follows:

<table>
<thead>
<tr>
<th>Capability</th>
<th>Motivation</th>
<th>Threat Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>HAN</td>
<td>5</td>
<td>2</td>
</tr>
<tr>
<td>IC</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>NU</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>

For the second leaf node in our example – *A1.1.2 Physical Access* – the DER component is assumed to be installed at residential premises with minimal physical access protection, such as fencing, hardened casing, or video surveillance. Consequently, the threat levels that we assign to this attack step are as follows:

<table>
<thead>
<tr>
<th>Capability</th>
<th>Motivation</th>
<th>Threat Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>HAN</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>IC</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>NU</td>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>

The next step is to propagate these source node threat levels through the attack graph. As the evaluated branch contains no loops, the threat propagation is straightforward. The leaf nodes of the A1.1 attack step are connected using the logical AND operator, i.e., both sub-nodes must be completed to implement this attack step; therefore, the minimal (hardest to implement) threat level of each child is propagated. This arrangement is shown in the table below:
As a result from the analysis, the overall threat level for every attack goal as well as a set of the most relevant threat vectors for every threat actor becomes obvious. For example, the handler threat actor is the most likely threat actor to implement the necessary attack steps to realise the physical attack step (A1.1). Furthermore, by assigning colours to the threat levels, the most likely attack paths become readily identifiable. In Figure 17, which shows the complete analysis for the A1 sub-tree for the handler actor, the red nodes correspond to TL 5, which indicates a very high threat level. In contrast, green represents a low the threat level, which implies that performing the named actions is considered very hard or even impossible.

<table>
<thead>
<tr>
<th></th>
<th>TL for A1.1.1</th>
<th>TL for A1.1.2</th>
<th>TL for A1.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>HAN</td>
<td>4</td>
<td>6</td>
<td>4</td>
</tr>
<tr>
<td>IC</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>NU</td>
<td>3</td>
<td>5</td>
<td>3</td>
</tr>
</tbody>
</table>

Figure 17: Example – a weighted attack sub-tree A1 for the attacker “Handler” (HAN)
6 Consequence Identification and Impact Assessment

It is necessary to determine the consequences of a cyber-attack to a smart grid and assess the impact these consequences have on a given set of stakeholders or organisations that are defined in the risk management context – this step of the SPARKS risk management process provides guidance about how this can be achieved. There are a number of different forms of consequence that could occur because of a cybersecurity incident in the smart grid, e.g., from sensitive information disclosure through to the damage of physical power equipment.

Depending on the interests of the stakeholders that are considered in the risk assessment, different consequence categories (or types of consequence) are of interest. Additionally, based on the context of the assessment, e.g., with respect to knowledge of the infrastructure under examination and amount of effort that is to be applied to complete the assessment, different consequence assessment methods will be more or less suitable to implement this step.

Our intention is to provide guidance on how to select an appropriate set of methods to realise this step of a risk assessment. More specifically, this step can be broken down into the following activities:

1. Based on the stakeholder viewpoints that are to be considered in the assessment, select an appropriate set of consequence categories to be targeted, such as economic losses, safety or quality of supply aspects. Some suggested consequence categories are summarised in Table 6. This consequence category selection step reflects the fact that cyber-attacks can have wide-ranging implications in the smart grid that should be considered. This is part of the basic criteria for the risk management process.

2. With an understanding of the consequence categories that are to be considered for the assessment, select suitable methods to identify the consequences of assets being compromised. This selection should be primarily driven by (i) the types of consequences that are to be identified; (ii) the amount of effort the assessor would like to apply, e.g., in terms of person months effort; and (iii) the level of detail that is defined in the established context.

3. Use the selected methods, e.g., expert analysis, event-tree analysis or co-simulation, to identify the consequences of information assets being compromised, with respect to the different security objectives: Confidentiality, Integrity and Availability (C, I, A). The attack goals that are defined as part of the threat identification process, outlined in Section 5.1, can be applied to this analysis. A set of example consequences is shown in Table 7. For example, with respect to quality of supply, factors include a lack of voltage stability, active power outages, harmonic distortion, or frequency variations – these are potential physical consequences of a cyber-attack. These consequences will be measured using metrics, such as deviations from the nominal frequency (Hz) as a percentage.

An approach could be to initially perform an assessment that requires relatively minimal effort, e.g., expert analysis, to identify consequences that have a high impact, which are then explored in more detail with more effort, e.g., via the development of co-simulations.

4. The next activity is to assess the impact of different consequences, based on the established context. This involves defining a range of impact levels, e.g., from Low (1) through to Highly Critical (5), and mapping the severity of consequences to these levels. This arrangement should be done with an understanding of the risk management context. For example, the severity of economic losses will vary depending on the size of the organisation being considered for the assessment – a loss of revenue of €50K for one organisation may have a very high impact (e.g., 5), whilst for another it could be more moderate and tolerable (e.g., 3).
Table 10 presents some example impact levels that have been defined for a small-to-medium sized Distribution System Operator (DSO). With this arrangement completed, the consequences of information assets being compromised, which were previously identified, can then be mapped onto impact levels. Again, many of these aspects are detailed as part of the basic criteria for the risk management process.

To summarise, the model presented in Figure 18 provides an overview of this organisation. Different smart grid stakeholders, e.g., consumers, governmental bodies, DSOs, and solutions providers, are interested in different consequence categories when carrying out a risk assessment. For example, a DSO is arguably primarily interested in the consequences of attacks in terms of quality of supply, economic losses, equipment damage, regulatory penalties, and safety incidents. Different consequences, such as perturbations to voltage stability or the number of lives lost can be identified and assessed using a number of assessment methods: e.g., co-simulation or expert analysis. Not all assessment methods are applicable to every type of consequence. As mentioned earlier, the choice of method that is to be applied is largely dictated by the suitability of the method to assess the consequences of interest, the level of knowledge of the infrastructure – as defined in the context specification – and the implementation effort the assessor would like to commit. For example, brainstorming sessions that are carried out by a group of experts could be applied to determine whether a cyber-attack may lead to active power outages; similarly, co-simulation could be used for this task. For the purpose of a risk assessment, these consequences, which are measured via suitable metrics, should be mapped to discrete impact levels, e.g., from low to high (1 to 5). The context of the assessment determines this mapping, e.g., 20kW losses may have a low impact for a large DSO, whereas this same loss may have a significant impact for a smaller operator.

Figure 19 presents an overview of the relationships between the various concepts for impact assessment: consequence categories (e.g., Quality of Supply) include different consequences (e.g.,
frequency variation, active power outages) that are measured using metrics (e.g., % of variation, total load loss in kW), which are finally mapped to impact levels.

In what follows, we provide indicative guidance that can be used to determine suitable consequence assessment methods, based on the factors that have been discussed.

### 6.1 Consequence Categories

As mentioned earlier, different stakeholders will be interested in considering the impact of cybersecurity incidents in terms of a number of consequence categories that relate to their overall (business) objectives. The stakeholders that are associated with a risk assessment and their objectives will be modelled at the SGAM Business Layer, as part of the context establishment step. Based on the stakeholders that have been identified by the Smart Cities Stakeholder Platform [46], the role of a number of examples is summarized in Table 5.

#### Table 5: Example smart grid stakeholders and their infrastructure knowledge

<table>
<thead>
<tr>
<th>Stakeholder</th>
<th>Short Description</th>
<th>Infrastructure Knowledge</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Policy Makers (PM)</strong></td>
<td>Setup and control of natural monopoly requirements and for highly effective electricity markets.</td>
<td>Little or no knowledge of a specific electrical or ICT infrastructure.</td>
</tr>
<tr>
<td><strong>Producer (P)</strong></td>
<td>Large scale centralized generation, including wind farms, and small- and medium-scale distributed generation of mainly renewable based electricity.</td>
<td>Little knowledge of the electrical infrastructure, but detailed knowledge of its own power generating devices.</td>
</tr>
<tr>
<td><strong>ICT equipment and systems providers</strong></td>
<td>Sales of Information and Communication Technology (ICT System) products and services.</td>
<td>Detailed knowledge of the ICT system, but no knowledge of the physical infrastructure.</td>
</tr>
<tr>
<td><strong>Energy Service Companies (ESCOs)</strong></td>
<td>Provision of a broad range of comprehensive energy solutions, including designs and implementation of energy savings projects, energy conservation, energy infrastructure outsourcing, power generation and energy supply and risk management.</td>
<td>No knowledge of the ICT infrastructure, coarse knowledge of the electrical system.</td>
</tr>
<tr>
<td><strong>Transmission System Operator (TSO)</strong></td>
<td>Provision of services for a secure, efficient and sustainable operation of transmission system. Legal obligation of a high quality, secure planning, operation and maintenance of the transmission grid.</td>
<td>Detailed knowledge of the electrical and ICT infrastructures at the transmission level.</td>
</tr>
<tr>
<td><strong>Distribution System Operator (DSO)</strong></td>
<td>Provision of services for secure, efficient and sustainable operation of electricity distribution systems. Legal obligation of a high quality, secure planning, operation and maintenance of the distribution grid.</td>
<td>Coarse to detailed knowledge of the electrical and ICT infrastructures at the distribution level.</td>
</tr>
</tbody>
</table>

A number of example consequence categories are described in Table 6, together with a possible mapping of the main concerns of different stakeholders. For example, a DSO is concerned with a wide range of consequence categories as a central player in the smart grid. Of course, they operate as a business and are concerned with cybersecurity incidents that could result in economic losses. Their primary role is to distribute electricity to consumers via their infrastructure with a quality that is specified by regulatory authorities. Therefore, incidents that result in an impact to these aspects and impair their capacity to operate the distribution network are of significant interest. Closely related to these aspects is damage to equipment, such as transformers or tap changers. Such damage could result
in a reduction in quality of supply, regulatory penalties and economic losses. Additionally, in some cases, equipment damage could result in safety-related incidents, if human operators are in close proximity of the equipment when it is damaged. All of these consequences could result in reputational damage, which may lead to economic losses or hamper the capacity of the operator to complete future projects, wherein there is a perceived risk from a societal perspective. Finally, a DSO is concerned with data protection and privacy issues, ensuring that consumption information is not compromised as part of an incident.

Table 6: Consequence categories and indicative interest of stakeholders, highlighted with dots

<table>
<thead>
<tr>
<th>Category</th>
<th>Short Description</th>
<th>PM</th>
<th>P</th>
<th>ICTP</th>
<th>ESCO</th>
<th>TSO</th>
<th>DSO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Economic</td>
<td>Economic losses caused by an incident scenario, e.g., because of higher anticipated costs or losses of revenue.</td>
<td>●</td>
<td></td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Safety</td>
<td>Injury or loss of life</td>
<td>●</td>
<td></td>
<td>●</td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Quality of Supply</td>
<td>Consequences that relate to impairments to quality of energy supply</td>
<td></td>
<td></td>
<td>●</td>
<td>●</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Infrastructures</td>
<td>Interdependent infrastructures that are affected, e.g., hospitals or schools.</td>
<td>●</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Regulatory</td>
<td>Breaches of regulatory requirements, e.g., related to quality of supply, that result in penalties</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Reputational</td>
<td>Loss of trust or goodwill amongst stakeholders, e.g., consumers.</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Data Protection and Privacy</td>
<td>Unauthorised disclosure or modification of commercially or personally sensitive data.</td>
<td>●</td>
<td></td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Equipment</td>
<td>Damage to power and ICT equipment caused by incidents</td>
<td>●</td>
<td></td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Population</td>
<td>Measures of the population size that are affected by an incident; related to the other impact categories</td>
<td>●</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

It can be seen from this discussion that consequences can be closely related, e.g., an impact to quality of supply can result in regulatory, reputational and economic losses, and chains of causality can be identified. Understanding the roots of these “consequence causality chains” can be useful to determine
how to approach the task of identifying consequences – in this case, it would be advantageous to consider quality of supply issues first and determine how the identified consequences affect the others that are of interest to an organisation.

Associated with the different consequence categories, there are a number of consequences and metrics that can be identified, and later assessed using different assessment methods. A set of these consequences are summarized in Table 7, together with the corresponding metrics. For instance, within the consequence category of Quality of Supply, there are several consequences of interest to the stakeholders, ranging from lack of stability in important power system parameters, to frequency and voltage variations, both of which may result in range violations and trigger protection devices to disconnect parts of the network.

The severity of each consequence may be assessed by evaluating the corresponding metric listed in Table 7. Given the heterogeneity among the possible consequences, the corresponding metrics may be assessed in terms of binary values, absolute values, or percentages. As examples, lack of stability is assessed through a binary value, active power outages are quantified in absolute values, whereas voltage and frequency variations and harmonic distortions are measured in percentages with respect to the corresponding nominal values. Some of these metrics may be directly related to regulations imposed on the Quality of Supply that limit the admissible fluctuations of important variables. For instance, this is the case for frequency and voltage variations, as well as the harmonic distortion, in which national regulatory standards prohibit variations exceeding 1% of the nominal frequency (50 Hz) and 10% above or 6% below of the nominal voltage (230V at the low-voltage grid)\(^7\), as well as harmonic voltage distortion factors above 5% for low-voltage distribution grids [47].

<table>
<thead>
<tr>
<th>Category</th>
<th>Consequences</th>
<th>Metric</th>
</tr>
</thead>
<tbody>
<tr>
<td>Economic</td>
<td>Cost of electrical losses</td>
<td>Reduced EVA/EBITDA, VoLL (€)</td>
</tr>
<tr>
<td></td>
<td>Customer outage costs, i.e. cost of energy not supplied</td>
<td>Reduced EVA/EBITDA (€)</td>
</tr>
<tr>
<td></td>
<td>Congestion costs, resistive power losses, power import, ancillary service usage</td>
<td>Reduced EVA/EBITDA (€)</td>
</tr>
<tr>
<td></td>
<td>Investigation and repair time, work time lost</td>
<td>Reduced EVA/EBITDA(^8) (€)</td>
</tr>
<tr>
<td>Safety</td>
<td>Minor or serious injury</td>
<td>Percentage of impairment (%)</td>
</tr>
<tr>
<td></td>
<td>Loss of life</td>
<td>Number of lives lost (#); direct or indirect</td>
</tr>
<tr>
<td>Quality of Supply</td>
<td>Lack of stability in voltage, phase angle, frequency</td>
<td>Binary value, stable or unstable system (T</td>
</tr>
<tr>
<td></td>
<td>Active power outages</td>
<td>Amount of load loss (kW)</td>
</tr>
<tr>
<td></td>
<td>Voltage variation (over- / under-voltage)</td>
<td>Percentage of voltage variation (%)</td>
</tr>
<tr>
<td></td>
<td>Frequency variations</td>
<td>Percentage of frequency variation (%)</td>
</tr>
<tr>
<td></td>
<td>Harmonic distortion</td>
<td>Total Harmonic Distortion</td>
</tr>
</tbody>
</table>

\(^7\) Statutory Instruments 2002 No. 2665, The Electricity Safety, Quality and Continuity Regulations 2002, UK

\(^8\) Economic Value Added (EVA), Earnings Before Interest, Taxes, Depreciation, and Amortization (EBITDA), and Value of Lost Load (VoLL)
6.2 Identification of Consequences

As mentioned earlier, depending on the scope of the assessment, the type of stakeholder, and the available models of the system, the consequence identification and severity assessment can be performed with varying degree of resolution and using different types of approaches.

In particular, the analysis of large-scale smart grids by societal stakeholders, such as Policy Makers, is often performed at a coarser granularity level by relying on high-level models of the system. In principle, such stakeholders are mainly concerned with societal consequences (see Table 6), while their available infrastructure knowledge is focused mainly at the top layers of the SGAM model, namely the SGAM Business Layer. Given the target consequence categories and infrastructure knowledge of Policy Makers, consequence identification methods suitable for these stakeholders typically include expert analysis and safety and security analysis, which combine empirical knowledge and high-level system descriptions.

On the other hand, the analysis of smaller systems by operational stakeholders, such as a DSO, can be carried out with finer granularity, usually resorting to detailed models of the lower layers of the SGAM model, through the SGAM Component Layer to the SGAM Function Layer. As summarized in Table 6, operational stakeholders such as the DSO are concerned with a wide range of consequence categories, ranging from Reputational and Safety, to Economic and operational (Quality of Supply) categories. Typical consequence identification methods that are available to DSOs include safety and security analysis using high-level models, as well as co-simulation and system analysis approaches that rely on detailed models of the physical and communication infrastructures and control algorithms.

The specific identification methods that are used by DSOs depend mainly on the target consequence category and the available infrastructure knowledge. Considering target categories that overlap with those of policy makers, such as Reputational and Safety categories, the methods suitable to policy...
makers may also be used by DSOs, namely the expert analysis and the safety and security analysis. On the contrary, for consequences within the Quality of Supply category, identification methods such as co-simulation and system analysis approaches are better suited. As an example, consider the metric Lack of voltage stability within the Quality of Supply category. Voltage stability is a property of the closed-loop model of the power system and voltage control algorithms. Therefore, detailed models of the power system dynamical behaviour and the voltage control algorithms are required to assess whether voltage stability is maintained or lost, thus making co-simulation and system analysis suitable methods to assess such a consequence. Therefore, expert analysis and safety and security approaches have limited used to assess the severity of Lack of voltage stability, since they use high-level models of the system and cannot analyse properties of dynamical systems.

As the previous discussion indicates, the several consequence identification methods require different levels of infrastructure knowledge and are better suited for certain consequences than others. In the remainder of this section, a brief description of relevant consequence identification methods is given, along with an indication of the type of knowledge that is required to implement an analysis using the method.

6.2.1 Expert Analysis

Perhaps the most widely used approach to impact assessment is to make use of expert analysis, wherein a group of domain experts explore the potential consequences of a cybersecurity incident, often arranged into brainstorming sessions. Ideally, a multidisciplinary group of experts should be formed for an analysis of smart grid cyber-attacks, e.g., drawing on expertise in communication systems, information security and power systems engineering. Such analyses can be used to give indications of the potential physical consequences of cyber-attacks, e.g., that overvoltage may occur, based on the analysists’ experience from previous incidents and discipline-specific knowledge.

There are two well-understood shortcomings of this form of analysis, namely the potential for subjective bias and the influence of group dynamics (during brainstorming sessions) to result in inaccurate findings. To mitigate these aspects, techniques such as the Delphi method [48] can be applied, wherein a moderated group, which is answering questionnaires, iteratively moves toward an agreed consensus. Conversely, expert analysis has the benefit of being relatively quick to implement, e.g., a consensus may be formed about the potential consequences of cyber-attacks using a relatively small number of meetings. Additionally, an indication of consequences can be gained without the need for particularly detailed knowledge of a specific instantiation of a smart grid use case, in contrast to simulation studies, for example.

Of course, the findings from such an analysis should be treated as indicative, potentially forming the basis for further more rigorous assessment for scenarios that could result in a high impact for a set of stakeholders.

Infrastructure Knowledge Required

Due to the multidisciplinary nature of the group of experts, the required knowledge can span multiple layers of the SGAM model. Moreover, the indicative nature of the results does not need detailed knowledge of the SGAM model and its layers, as opposed to methods such as simulation studies. Therefore, one may argue that expert analysis mainly requires a high-level knowledge of the SGAM Business and Function Layers, which respectively specify the business context with relevant operational goals and the available smart grid functions and services. Some knowledge of the available devices at the SGAM Component Layer may also be of use to the expert analysis, since the
malfunction of a given device, e.g., a power transformer, provides insights into the corresponding impact and consequences.

### 6.2.2 Safety and Security Analysis

Given the cyber-physical nature of the smart grid, and the potential for safety-related incidents to occur because of cyber-attacks, it can be beneficial to build on analysis techniques that stem from the safety domain. A benefit of using these techniques is that safety-related expertise within an organisation may already exist; thus making the implementation of such studies more straightforward with existing skills sets. Three methods that can be readily applied in this context are event tree analysis [49], Failure Modes and Vulnerability Effect Assessment (FMVEA) [50], and Systems Theoretic Process Analysis (STPA) [51].

#### 6.2.2.1 Event-tree Analysis

Event-tree analysis [49] can be used to explore the potential physical consequences of an information asset being compromised in a structured manner. In summary, event-tree analysis is a structured analysis technique that can be used to inductively explore the potential outcomes associated with an initiating event that could have consequences to a system. 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. In this way, event trees can be used to support the enumeration of the different consequences of an information asset being compromised.

As a starting point for an analysis, one must identify the protection mechanisms that could be used to mitigate the impact of an information asset being compromised (an attacker goal). Here we do not consider cybersecurity mechanisms, such as firewalls or intrusion detection systems, but focus on power system protections that exist in the context of the use case under consideration. A set of example protection mechanisms for the VVO use case that is described in Section 4 is presented in Table 8.

<table>
<thead>
<tr>
<th>Protection Mechanisms</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bad Data Detection</td>
<td>A software component that checks the validity of the measurements that are used by control algorithms. 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. Studies have shown such bad data protection mechanisms can be effective in mitigating such issues [52].</td>
</tr>
<tr>
<td>Reactive Power Control</td>
<td>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.</td>
</tr>
<tr>
<td>DER Overvoltage Protection</td>
<td>Equipment associated with DERs, such as PV inverters, locally measure voltage levels; when they become too high, in such a way that there could be damage to equipment, they disconnect from the grid, thus protecting the DER equipment.</td>
</tr>
</tbody>
</table>

With an understanding of the protection mechanisms that are in place, one can deductively examine their capacity to mitigate the negative consequences of an initiating event — in this case, the compromise of an information asset. Figure 20 shows an event-tree for the VVO use case that explores the capacity for a number of protection mechanisms to mitigate an initiating event. In this example, the
event is distributed voltage measurements being spoofed to appear lower than they are in reality, a compromise of the integrity of this information asset. An attacker may choose to spoof measurements in this way to increase voltage levels on a distribution line to unsafe levels. Protection mechanisms may successfully mitigate an event or fail to do so, as indicated by the branches in the event-tree. Probabilities can be assigned to whether a mechanism is effective or not, based on modelling techniques, expert analysis or simulation, for example.

For each branch in the event-tree there is a success or failure outcome. A successful outcome occurs when a protection mechanism mitigates the initiating event, resulting in no negative consequences. In contrast, a failure outcome describes a situation in which there is some form of negative consequence, such as overvoltage on a power line in this example. In the example shown in Figure 20, if a bad data detection mechanism were to successfully identify that voltage measurements appeared to be bogus and, e.g., historical data is used as input to a control algorithm, a successful outcome occurs (Success Outcome A). If the bad data detection mechanism does not determine that a set of voltage measurements appear incorrect, then a number of failure outcomes (negative consequences) could occur, depending on the success or failure of further protection mechanisms.

Based on this short example, it can be seen how event-tree analysis, along with other consequence assessment methods, could be used to examine the potential physical consequences of information assets being compromised. For example, a combination of expert analysis that is supported by event-tree analysis (or vice versa) could indicate scenarios in which further more detailed analysis could be beneficial, for example, using co-simulation or more detailed systems analysis.

**Infrastructure Knowledge Required**

In order to implement an event-tree analysis, specific knowledge of the software and electro-mechanical power systems protection mechanisms are required, such as DER overvoltage protection sub-systems. In some cases, it may be beneficial to develop detailed models that describe the behaviour of specific mechanisms, such as bad data detection systems. However, an indicative understanding of potential consequences can be obtained with a high-level understanding of the operation of such mechanisms.

### 6.2.2.2 Failure Mode and Vulnerability Effect Analysis (FMVEA)

FMVEA [50] is a combined analysis method for safety and security. It is based on the Failure Mode and Effects Analysis approach, as described in IEC 60812 [53]. In the FMEA approach, each component of a system is analysed for potential failure modes. A failure mode is the manner in which the component fails [53] or which an occurred fault is observed [54]. Based on the level of detail and maturity of the design, components can be hardware or software modules, or functions. In the context
of an analysis for the smart grid, these entities will be described in the function and component layer of the SGAM-based use case description.

In the next step the effects (or consequences) of the failure mode on the system are identified. A failure mode could cause a component to cease to function and still only have a negligible effect on the functionality of the complete system. For example, a sensor may permanently fail, but under nominal conditions this has limited effects on the system behaviour. After the severity of the final effect is determined, potential causes are identified. Based on the causes, the probability of the failure mode is estimated. This process is repeated until every failure mode of the component and every component on the chosen analysis level is examined. A potential approach to scoping an analysis would be to consider the set of components that implement a common function e.g., expressed as part of a primary use case in the SGAM model.

FMVEA extends the FMEA approach with a security analysis. Components are not only examined for failure modes, but also for threat modes. While a failure mode describes how a system quality attribute [55] fails, a threat mode describes how a security attribute, e.g., in terms of confidentiality, integrity and availability, of the components fails (or is compromised). Causes for failing security attributes are vulnerabilities and threats. In order to estimate the frequency of threat modes, the techniques that are outlined in Section 5.3 on likelihood assessment can be applied. The results of a FMVEA are the failure and threat modes of a system, and their causes and consequences. In addition, based on a likelihood analysis, threat modes are evaluated in terms of probability.

**Infrastructure Knowledge Required**

To realise a FMVEA-based consequence analysis, it is necessary to have a design of the system that is being considered and their purpose. For example, this can be drawn from the SGAM Component Layer and Function Layers, respectively.

### 6.2.2.3 Systems Theoretic Process Analysis (STPA)

STPA [51] is an analysis technique that leverages control theory to determine the set of root causes of potential losses (consequences) and hazards that could occur in a system. In addition to the original goal of STPA – namely to perform a hazard analysis on existing complex systems – the findings from an STPA-based analysis can also be used to support the design of fault-tolerant systems. In contrast to event-tree analysis, STPA can be considered an inductive analysis technique, in that an analyst starts from a set of losses that could occur and determines their root cause. In this way, STPA is similar to the widely-known fault-tree analysis technique [56].

In summary, to realise an STPA analysis, one initially identifies the losses that could occur in a system, e.g., the loss of life or an injury, and the hazards that could lead to these losses, e.g., a microgrid connecting to the mains power supply out of phase, resulting in explosive damage to power equipment. With this understanding, an analyst then enumerates the control algorithms, actions they can perform and the variables in the target system that could lead to these hazardous states. Based on this, erroneous control behaviours are identified (using a template provided as part of STPA) that may result in the hazards occurring – for example, control signals arriving late or out of order, or control functions not behaving according to their design specification. STPA is not limited to the technical level, but aims to include the human factor of a system as represented by operators and corporations.

The assumption in the original version of STPA is that hazards are often caused by the complexity of modern systems. Rather than bad implementation, bad specification of interaction between subsystems or aging components not considered during system changes are the true reasons for losses that manifest in erroneous control behaviour. For cybersecurity purposes, erroneous control behaviour
could be the result of an attack that is identified as being possible by the attack graphs analysis that is described in Section 5. Therefore, we see the combination of the attack graph-based analysis that we propose, which can be used to identify the most likely threats, along with techniques, such as STPA, being useful to comprehensively analyse the cyber-physical consequences of cyber-attacks to smart grids.

**Infrastructure Knowledge Required**

To implement an STPA analysis, it necessary to understand the control functions that exist in a system, the actions that they can perform and interactions within the system, and the variables they act upon. These items may be derived from the Function and Information Layers of the SGAM framework, given these layers are modelled with sufficient detail.

### 6.2.2.4 Bayesian Networks

Bayesian Networks is a graphical methodology that captures causal and probabilistic dependencies among a set of random variables. Bayesian networks represent the set of variables as nodes in a directed acyclic graph and may correspond to measured variables, such as “power outage” (Node A), or may represent latent hidden states of the system that are not directly observable, e.g., “configuration of the voltage controller” (Node B). An edge from one node to another corresponds to a cause-and-effect relationship between variables. For instance, the probability distribution of a “power outage”, captured by Node A, depends on the nature of the voltage controller in Node B, which is represented by having a directed edge from Node B to Node A.

Each node also has a *node probability table* that summarizes the probabilities of the nodal event’s realization, which are conditioned on the realization of the events represented by parent nodes. Returning to the previous example, the node probability table of Node A includes the probability of mild and severe outages, conditioned on the correct or incorrect configuration of the voltage controller, as depicted in Table 9. Additionally, nodes without connecting edges are conditionally independent, while events corresponding to sink nodes without incoming edges (zero in-degree) only have prior probabilities.

<table>
<thead>
<tr>
<th>Node B (Configuration of Voltage Controller)</th>
<th>Incorrect</th>
<th>Correct</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severe</td>
<td>0.8</td>
<td>0.2</td>
</tr>
<tr>
<td>Mild</td>
<td>0.1</td>
<td>0.9</td>
</tr>
</tbody>
</table>

Bayesian networks naturally have some similarities to event trees, both being represented through directed acyclic graphs, and some event trees can, in fact, be viewed as Bayesian Networks [57]. Recalling the description of event trees earlier in this section, it is not surprising that Bayesian networks are also well suited for an inductive exploration of the consequence space. Furthermore, Bayesian networks may be used to identify and infer certain properties about latent nodes through training and Bayesian inference. Given their probabilistic nature, Bayesian networks can also provide additional information regarding the likelihood of certain consequences, which may be of use for the final assessment of risk.
Infrastructure Knowledge Required

In a similar manner to event tree analysis, knowledge of the different functions is required to perform consequence analysis. The probabilistic relationship between nodes in the network can be determined in a number of ways, including using expert knowledge through to detailed co-simulation. In this way, Bayesian networks provide some flexibility in the way a consequence analysis can be realised, whilst provide a structured approach.

6.2.3 Co-Simulation

The impact of certain consequences may be assessed through model-based co-simulation. Typical consequence categories that may benefit from a co-simulation approach include economic and quality of supply, since the impact of such consequences is assessed through performance objectives that involves physical variables of the power system, e.g., resistive power losses and lack of stability, as listed in the second column of Table 7.

A simulation is a virtual experiment which is executed in a controlled environment. A model describing the simulated environment is required. With this setting it is possible to perform several iterations of simulation and changing some of the input parameters each time. By that, the influence of certain parameters on the progress and result of the simulation can be evaluated. Also, different kind of attacks can be performed on the simulated environment in order to analyse their impact. Since a smart grid is a complex environment, dividing it into different domains is a valid approach to establish a useful simulation. A model is required for each domain. These models are then combined to a co-simulation. The two following kinds of co-simulations can be distinguished: hardware/software and software/software.

Interconnecting real world hardware with a virtual experiment is called a hardware/software co-simulation. This approach is used to analyse how hardware reacts to the occurring settings during a simulation run. In the case where two or more software based simulation frameworks are combined, this is called a software/software co-simulation. With this approach it is possible to make use of specialized tools for each domain, which are well-tested and established for their task in the community.

As part of ongoing research in the SPARKS project, we are developing a co-simulation environment for consequence analysis in the smart grid. In order to establish a co-simulation environment for a smart grid, the software/software approach was selected. The identified domains in a smart grid which require a suitable simulation frameworks as well as an according model to describe them are (1) the power grid and (2) the data network. The first one covers the electrical aspect of a smart grid with its transformers, power lines and consumers, whereas the second domain covers the communication aspects within the future smart grid where components exchange information and certain parts can be controlled through messages from the attached data network, e.g. be switched on or off.

Different tools are available to cover the power grid simulation, like GridLAB-D\(^9\) or Matlab in combination with Simulink\(^10\). There are also several tools available which cover the domain of data network simulation, like ns-2\(^{11}\), ns-3\(^{12}\) or OMNeT++\(^13\). For the co-simulation in SPARKS a

---

\(^9\) GridLAB-D: [http://www.gridlabd.org/](http://www.gridlabd.org/)

\(^10\) Simulink: [http://de.mathworks.com/products/simulink/?s_cid=wiki_simulink_2](http://de.mathworks.com/products/simulink/?s_cid=wiki_simulink_2)


\(^12\) ns-3: [https://www.nsnam.org/](https://www.nsnam.org/)

\(^13\) OMNET++ Discrete Event Simulator: [http://omnetpp.org](http://omnetpp.org)
combination of Gridlab-D to cover the power grid domain with OMNeT++ to address data network domain is used.

**Infrastructure Knowledge Required**

Co-simulation studies rely on a simulation environment that considers both the physical power grid and the data communication network. Therefore, detailed knowledge of the SGAM Function, Information, Communication, and Component Layers is required to retrieve models of the physical grid and communication infrastructure. Additionally, the SGAM Business Layer may also be used to define and prioritize scenarios that are aligned with the business goals.

### 6.2.4 System Analysis

As discussed in Section 6.2.1, given the feedback nature of the overall system where measurements are used to compute suitable set-points and steer the system, the impact assessment of physical consequences require models describing the behaviour of the physical power grid, the control algorithms, and the communication network. However, due to the high complexity of the overall smart grid, simulation-based impact analysis that considers detailed descriptions of the physical models, the control algorithms, and the communication networks is quite computationally demanding and, thus, often infeasible. Therefore, depending on the scope of the assessment, the type of stakeholder, and the available models of the system, the simulation-based impact assessment can be performed with varying degree of granularity. In particular, the analysis of large-scale smart grids is often performed at a coarser granularity level, relying on simplified or approximate models, while smaller systems may allow analysis with finer granularity.

Naturally, consequence identification exercises with higher levels of granularity also require the higher implementation efforts from the stakeholder. Therefore, in order to decrease the effort and time allocated to this exercise, it is desirable to begin with coarser levels of granularity to identify possible high-impact threats, which can then be studied in more detail through co-simulation approaches. Within the scope of power systems, theoretic system analysis is a suitable candidate impact assessment method with coarser granularity that is tailored to performance objectives that involve physical variables of the power system. In fact, system analysis has been widely used in planning and design of power systems at the transmission level [58].

Theoretic system analysis requires a mathematical description of the dynamical models describing the behaviour of the physical variables of the power system, such as voltage levels, frequency, and power flows, as well as the automatic control algorithms in place. Such models are often comprised of nonlinear differential-algebraic equations [58], which can be used to study important properties such as stability of frequency and voltage levels and maximum variations in the presence of attacks and disturbances, without resorting to computationally-demanding simulations.

**Infrastructure Knowledge**

As opposed to the co-simulation studies, system analysis only relies on mathematical models of the physical power grid and does not consider the data communication network. Hence, no information is needed regarding the SGAM Information and Communication Layers, while detailed knowledge of the SGAM Function and Component Layers is required to retrieve simplified models of the physical grid.
6.2.5 From System Analysis to Co-simulation: A Voltage Droop-Control Use Case

A brief example of how system analysis and co-simulation techniques may be integrated together is described below for a “Voltage Droop-Control” use case. Recently, Kang et al. [59] investigated the implementation of cyber-attacks against a common application-level protocol in smart grid applications, the IEC 61850 protocol. In the considered attack scenario, cyber adversaries built a custom tool to execute man-in-the-middle attacks and manipulate data transmitted to a photovoltaic power inverter, thus affecting the physical power system. To better understand the potential impact of such attacks on the distribution network, system analysis or co-simulation approaches may be used. Given the heavier computational efforts required for co-simulation, a first step is to perform system analysis of the attacked system using the available system models. Such an approach is detailed in [60], which is summarized below.

The power distribution system is considered to be a set of interconnected microgrids (MGs) that may be connected to the main grid through the feeder substation, where each MG may contain several inverter-based distributed energy resources (DER) and loads. The distribution system is depicted in Figure 21, wherein each MG is represented by a bus and the multiple DERs and loads within a given MG are grouped together and modelled as a single DER and load, respectively. Additionally, the DER devices are used to achieve voltage control capabilities through a standard approach known as voltage droop-control. Mathematical models describing the behaviour of such droop-controlled power distribution systems are readily available in the literature, see [60] and references within.

![Diagram of an inverter-based droop controller](image)

Figure 21: An inverter-based droop controller under (a1) a reference signal attack at bus i, where the adversary corrupts the corresponding voltage reference signal, and (a2) a measurement routing attack at bus i, where the adversary redirects the voltage measurement from bus j to the controller at bus i, as if it were a measurement from bus i.

Given the system model, relevant attack scenarios are then considered and their corresponding threat models are derived, based on which model-based consequence identification is performed. In particular, the attack scenarios in [60] consider cyber adversaries that may corrupt a few
measurements and reference signals, as depicted in Figure 21, which may degrade the system’s reliability and even destabilize the voltage magnitudes. For example, based on properties of the attacked system model, [60] shows that an attacker may destabilize the power system by merely redirecting measurements communicated through the communication network, without having substantial model knowledge. Additionally, the model-based consequence analysis also manages to identify which sets of attacked devices yield possibly higher impacts, thus indicating which threats may pose a high risk to the system.

Once a preliminary analysis has been carried out using system analysis, a more detailed and precise assessment is performed using co-simulation. The co-simulation environment is first defined by combining models of the relevant domains, namely the power grid and the data network. Then, the threats identified through the system analysis approach may be simulated, which results in a better characterization of the corresponding severity. Additionally, further threats that are not easily dealt with system analysis techniques may also be identified through simulations.

### 6.2.6 Assessing the Economic Consequences of Power Interruption

The economic consequences of power interruption can be placed into three categories [61]: (i) direct costs; (ii) indirect costs; and (iii) long-term costs of macroeconomic relevance. Typically, direct economic losses are of public attention. However, direct economic losses are usually limited and subordinate to indirect economic losses. They are a direct result of the power outages, e.g., repair costs for defective electrical infrastructure facilities.

To support the assessment of these costs, an open access software solution was developed in the FP7 SESAME project, called the Blackout Simulator (http://www.blackout-simulator.com/). The tool can be used to analyze the economic consequences of power outages, and focuses on indirect cost components. These indirect costs also arise as a consequence of power outages, yet they belong to the part of the total losses resulting from the absence of electricity supply in the aftermath of the power cut. Examples are the cost of production outages or lost value added due to inputs or logistics being unavailable. Through multiplier effects due to the marked dependence of some industries on the uninterrupted functioning of other industries, in particular these indirect costs make up a significant proportion of the total damages [62].

Long-term economic effects are understood to be the economically relevant changes in the behaviour of market participants, as a result of a perceived long-term change in the level of supply security. Part of this category of losses is, for instance, the influence on the choice of a place as a business location, the potential price rise for production facilities due to the increased need for backup-systems, or customer churn due to unreliability regarding delivery deadlines. As long-term economic effects cannot be assigned to individual events, they are not taken into consideration by the Blackout Simulator tool.

In terms of comparability of damage figures, various indicators for placing a monetary value on supply security exist. The *Value of Lost Load* (VoLL) is among the most used indicators and quantifies the economic losses per kWh of electricity not supplied. With respect to evaluation methods, three major paradigms for assessing supply security in monetary terms are frequently used:14

1. Proxy methods
2. Market-based valuation methods

---

14 These were suggested by Woo, Chi-Keung; Pupp, Roger L. (1992). Costs of service disruption to electricity consumers, Hong Kong.
3. Contingent valuation methods

Proxy methods rely on observable variables linked indirectly to supply security. Amongst them are expenditures on standby generating facilities, the monetary value of lost income, the costs due to production output decreases as well as other losses. Therefore, proxy methods are suitable in the cases where the losses anticipated can be expressed with sufficient precision by such observable variables. Market-based valuation methods rely on actual, observable consumer decisions and, as representatives of the revealed-preference approach, can deliver very robust data. However, for special cases with little market activity, such as grid-bound electricity supply, which is a natural monopoly, market-based assessments are not feasible. Conversely, contingent valuation methods, which are the cornerstone of the evaluation of households’ Willingness To Play (WTP), are typically included in outage assessments. They permit the valuation of power outage-related losses incurred from a customers’ (partly subjective) perspective. With this group of methods, customers themselves assign a value to the loss from power outages. As with any stated-preference method it is often employed for the monetary valuation of non-material losses such as stress, lost recreational amenities or more generally to assess households’ economic losses, taking into account the special nature of non-market goods.

Each of these three valuation paradigms focuses on different causes of losses. The relevance varies by consumer group. While a company experiences financial damage only, households suffer not solely from monetary losses but also a reduction in recreational benefits, inconvenience and mental stress, which occurs for instance if it is not known when electricity will be available again or as a result of a complete breakdown of communications. Here, the losses within the segment of non-households are represented by means of a method that maps the lost production value, while a contingent valuation method is used to value losses within the household segment.

6.3 Impact Assessment

Having identified the consequences of assets being compromised using the techniques that are outlined in Section 6.2, the next step is to map the identified consequences to a discrete set of impact levels (e.g., between Low (1) and Highly Critical (5)). This information will be used, along with the results from the likelihood assessment (see Section 5.3), to determine the overall risk level for an assessment. The first step in this process is to define a set of impact levels for the consequences that are relevant to the given stakeholder. This process should be driven by the (business) objectives of the stakeholder and the impact levels tailored accordingly.

Table 10 shows an example set of consequences and impact levels that are relevant for a small-to-medium sized Distribution System Operator (DSO). In this table, for example, an active power loss of less than 5 kW, e.g., caused by the loss of active power from a household photovoltaic, is considered to have a low impact on the organisation. In contrast, power losses greater than 5 MW are considered to be highly critical, and would result in significant impact to the organisation. Such losses could lead to regulatory penalties (not shown in the table) and serious reputational damage for the DSO. Note that this correlation of impacts does not always exist, e.g., highly critical power losses may not result in a safety-related impact.

The result of this mapping exercise is a set of (information asset, security objective, consequence, severity) tuples that can be ranked, e.g., based on impact level and the relative importance of different forms of consequence for an organisation, and considered alongside corresponding threats that can

---

15 Ultimately consumers are by definition not in a position to make market-based decisions in the case of natural monopolies.
result in the compromise of information assets. An example set of such tuples is shown in the table below.

<table>
<thead>
<tr>
<th>Information Asset</th>
<th>Objective</th>
<th>Consequence</th>
<th>Impact Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phase Angle Measurement</td>
<td>Integrity</td>
<td>Injuries and loss of life</td>
<td>Highly Critical</td>
</tr>
<tr>
<td>Voltage measurements</td>
<td>Integrity</td>
<td>Active Power Outage</td>
<td>Critical</td>
</tr>
<tr>
<td>Voltage measurements</td>
<td>Integrity</td>
<td>Frequency Variation</td>
<td>Critical</td>
</tr>
<tr>
<td>Consumption measurements</td>
<td>Confidentiality</td>
<td>Sensitive information disclosure</td>
<td>High</td>
</tr>
<tr>
<td>Consumption measurements</td>
<td>Confidentiality</td>
<td>Injuries and loss of life</td>
<td>Low</td>
</tr>
</tbody>
</table>

Throughout this consequence and impact assessment process, documentation should be maintained that describes the rationale behind the findings described in these tuples – this information is necessary to support the identification of suitable security requirements (during system design) and controls (during system implementation). This rationale could take the form of the results from a simulation exercise or be derived from the minutes of an expert analysis session.
Table 10: An example set of consequences and impact levels for a Distribution System Operator (DSO)

<table>
<thead>
<tr>
<th></th>
<th>Active Power Outages</th>
<th>Frequency variation</th>
<th>Voltage variation (over-/under-voltage)</th>
<th>Loss of trust</th>
<th>Injuries and loss of life</th>
</tr>
</thead>
<tbody>
<tr>
<td>HIGHLY CRITICAL (5)</td>
<td>&gt; 5 MW</td>
<td>&gt; 2%</td>
<td>&gt; 12% &gt; 230 V</td>
<td>&gt; 8% &lt; 230 V</td>
<td>Permanent loss of trust by &gt;50% of the population supplied by the DSO</td>
</tr>
<tr>
<td>CRITICAL (4)</td>
<td>500 kW - 5 MW</td>
<td>1% to 2%</td>
<td>10% to 12% &gt; 230 V</td>
<td>6% to 8% &lt; 230 V</td>
<td>Permanent loss of trust by &lt;50% or temporary loss of trust by &gt;50% of the population supplied by the DSO</td>
</tr>
<tr>
<td>HIGH (3)</td>
<td>50 - 500 kW</td>
<td>0.6% to 1%</td>
<td>5% to 10% &gt; 230 V</td>
<td>4% to 6% &lt; 230 V</td>
<td>Permanent loss of trust by &lt;33% or temporary loss of trust by &lt;50% of the population supplied by the DSO</td>
</tr>
<tr>
<td>MEDIUM (2)</td>
<td>5 - 50 kW</td>
<td>0.3% to 0.6%</td>
<td>2% to 5% &gt; 230 V</td>
<td>2% to 4% &lt; 230 V</td>
<td>Permanent loss of trust by &lt;10% or temporary loss of trust by &lt;33% of the population supplied by the DSO</td>
</tr>
<tr>
<td>LOW (1)</td>
<td>&lt; 5 kW</td>
<td>&lt; 0.3%</td>
<td>&lt; 2% +/- 230 V</td>
<td></td>
<td>Temporary loss of trust by &lt;10% of the population supplied by the DSO</td>
</tr>
</tbody>
</table>
7 Risk Treatment with Semantic Threat Graph Support

The purpose of a risk management process is not only to determine an appropriate risk level, but to derive a set of countermeasures to mitigate the risks to the system under consideration. Although there are many standards, best practices, and other catalogues for countermeasures and security recommendations, their linkage to the actual existing threats is mainly neglected for existing risk management cycles. In many standards, a set of high-level recommendations is made that are based solely on the final risk level. This completely neglects the results of a thorough threat analysis that has been performed, and might lead to the implementation of inappropriate countermeasures.

Therefore, for the SPARKS risk management process, we propose to use Semantic Threat Graphs (STGs) as a tool to precisely determine the necessary countermeasures for the identified threats. STGs are a variation of attack trees, which are extended in order to relate semantic information about security configuration with threats, vulnerabilities and countermeasures. Therefore, the analysis is on a technologically deeper level than threat identification based on attack trees, and requires knowledge about the actual technology that is deployed in the system under consideration.

In our approach, we start with a source node of the attack graph (see Section 5.2.1), which represents a high-level threat, and construct an STG for this node. STGs allow the refinement of an abstract threat into hierarchies. For this step, we can reuse information from precompiled hierarchies. The assets that are implicitly present in the attack tree are made explicit. Countermeasures and their effect on threats can be added again from catalogues. Additionally, relevant vulnerabilities can be added either as abstract classes or from specific sources, such as the NIST National Vulnerability Database (NVD)\(^\text{16}\). All four concepts related to each other in the graph.

STGs are represented in terms of Ontologies, which leads to a high re-usability of previously compiled graphs and gives access to a large number of implementation tools. Moreover, this formalization allows tool-based querying, and results in the necessary countermeasures being determined from a technologically precise perspective. By not implementing all available countermeasures but only those that are strictly necessary, costs can be reduced or the impact of security measures on the functionality of the system can be minimized.

7.1 Semantic Threat Graphs

An STG makes explicit the information that is typically implicit in an attack tree. An abstract model of a semantic threat graph that illustrates the concepts involved and their relationships is presented in Figure 22. Semantic threat graphs are constructed as an Ontology [63]. An Asset may have one or more hasWeakness relationships, which relate to individuals categorised in the Vulnerability concept. Individuals of the Vulnerability concept are exploitable (exploitedBy) by a threat or set of threats (the Threat concept). As a consequence, an asset that has a vulnerability is also threatenedBy a corresponding threat. A countermeasure mitigates particular vulnerabilities. Countermeasures are considered as assets and are thus defined as a subConceptOf Asset.

\(^{16}\) The NIST National Vulnerability Database (NVD): https://nvd.nist.gov/
Figure 22: The abstract semantic threat graph model

Figure 23 shows an example instantiation of an STG that represents the PSN to DER attack tree example that is presented in Section 5.2.3. As illustrated in Figure 10, the PSN and DER are interconnected. Figure 15 illustrates an example fragment of an attack tree that outlines a number of high-level threats to the DER, due to potential attacks that may come from a compromised PSN. In this example, the assumption is made that a DER PLC (instance of the concept DER Component \(\subseteq\) Asset) is protected (protects property relation) by a DER gateway firewall (an instance of concept DER Component \(\subseteq\) Asset) from external network connectivity.

A leaf node (A4.3) of Figure 15 outlines a particular kind of threat category (concept Manipulate Communication PSN to DER a subconcept of concept Threat) with respect to attacking the plc communication medium sourced at the PSN. The example STG further specialises the Manipulate Communication PSN to DER concept into manipulating the communication of PLCs with the DER (concept Manipulate PLC Communication) which in turn is further specialised to two Microsoft STRIDE [64] classifications (concepts) namely Information Disclosure and Denial of Service.

An information disclosure threat can be specialised, e.g., to the threat of Non–Authenticated Access, in which an instance of that concept may represent unapproved TCP Modbus read/write requests that are being used to probe a PLC. In this scenario, threat instance unapproved mbtcp rw access threatens the DER asset instance plc. This is because the Modbus protocol has no way to authenticate the source of such requests to the PLC. This is represented as an unauthenticated mbtcp command execution, an instance of the concept Vulnerability. As a consequence of the external DER command & control communication over Modbus to/from the PSN, the asset plc therefore hasWeakness vulnerability instance unauthenticated mbtcp command execution, which in turn isExploitedBy threat instance unapproved mbtcp rw access.

Considering Countermeasures, there are a number of possibilities that can be deployed. In this example, the Modbus enabled plc has no way of mitigating or reducing the threat of unauthenticated command & control access. However, the protecting firewall has a capability to perform this action on behalf of the plc. Having the firewall implement a particular firewall access control rule set (instance allow mbtcp pkts from trusted PSN Src IP) that is specialised to mitigate unauthenticated mbtcp command execution will resolve that particular threat of...
**Figure 23: An excerpt of the DER and firewall semantic threat graphs**

### 7.2 Attack Tree and Semantic Threat Graph Hybrid

Attack trees and STGs complement each other. While attack trees prove useful to identify, visualize and track attack vectors on relatively high levels of abstraction, they become unwieldy on device or implementation specific lower levels. In contrast, STGs are optimal for the evaluation of specific components and implementations on the lower levels, including identifying suitable countermeasures, but are not intuitively understandable and lack methods to model attack routes between different components. By combining attack trees (ATs) and STGs, the strengths of both techniques can be used to form an understandable overall map of potential attack paths, including detailed knowledge and protection strategies for the relevant components. As our new AT-STG hybrid enables alternative paths through a tree, it becomes a cyclic graph.

To create an AT-STG, each component is checked if it could be replaced by a corresponding STG. Thereby it must be kept in mind that – as is the case for each other component – an attacker must have a path to access an STG. This either requires the STG as the attack entry point or a logical AND combination of the access path and the STG. To be more precise, a sequential AND (SAND) operator could be used in order to highlight that an attacker first needs some sort of access before they could directly affect a component.

During tree creation and refinement, blocks with reoccurring pattern except a single parameter appear. Similar to the STG, each of these blocks could be swapped out into a new sub-graph with a reference at its former location and the parameter. Those links to a sub-graph are visualized by a triangle. While the initial high level attack tree is individual for each SUE, the sub-graphs form a pool of reoccurring patterns.
structures and known elements for future analysis. Although the instances of a sub-tree have an identical structure, their weight could differ and must be determined depending on the specific elements.

Figure 24 illustrates an AT-STG, which extends the one presented in Figure 15, whereby one of the leaf nodes is further examined with the threat’s explicit relationships to corresponding assets, vulnerabilities and countermeasures. Using this approach, it can be seen how countermeasures that relate to threats can be readily identified.

![Figure 24: A fragment of an attack tree and semantic threat graph hybrid](image-url)
8 Conclusion

With the introduction of new Information and Communication Technology (ICT) and Supervisory Control and Data Acquisition (SCADA) systems to enable advanced energy services in the smart grid, there is an increased cybersecurity risk. This increased risk has many facets, for example, a greater ICT component introduces new vulnerabilities, and the use of wide-area networks expands the surface available for attackers to gain entry into a smart grid system. Additionally, because these systems will be used to support services that are operationally critical, e.g., voltage control, the impact of their compromise can be significant; potentially resulting in equipment damage and in some cases safety-related incidents. Therefore, it is of utmost importance that a well-considered cybersecurity strategy is defined to address these risks, based on a structured risk management process.

In this deliverable, we present an approach to risk management for the smart grid, which includes an approach to threat identification and risk assessment. The process is based on the ISO/IEC 27005 information security risk management standard. Building on this standard, we provide specific guidance on how to perform a risk management exercise for the smart grid. We present overview implementation guidelines that highlight issues related to risk management for the smart grid, and point to how the further contributions in the deliverable can be applied. For example, we advocate the use of the SGAM framework to support the context establishment step of the risk management process, ensuring alignment with approaches to use case and architecture specification that have been proposed by CEN-CENELEC-ETSI in Europe. This should enable significant reuse of existing effort, and conform to related activities for smart grid development. Building on an SGAM-based description of a smart grid use case, we present an approach to the development of attack graphs – a means of threat identification – that uses the structured information in an SGAM model and attack patterns to develop well-formed attack graphs. A likelihood assessment can then be realised using the HMG IS1 standard. Identifying the consequences of an incident is an important step in a risk assessment – for the smart grid, there are many consequences of an attack, including reductions in quality of supply, safety-related incidents, regulatory penalties, and information disclosure. Guidelines are provided regarding which stakeholders may be interested in these different forms of consequence, and the techniques that can be used to identify them. With an understanding of the consequences of an incident, their impact needs to be assessed for an organisation; we provide guidance regarding how this can be achieved. Finally, we show how semantic threat graphs – a form of Ontology – can support the identification and traceability of appropriate security controls that are needed to address identified risks. We suggest that our approach to risk management for the smart grid can be applied to both existing operational systems and architectural concepts of proposed new smart grid use cases.

Future work will focus on two main activities: we will develop a suite of tools that can be used to support the implementation of the SPARKS risk management process. Specifically, we will develop a tool to support the specification of the SGAM-based use case description that includes the necessary attributes to support risk assessment. The outcomes from this specification can then be provided to others tools that we will develop, e.g., that support our approach to threat identification using attack graphs and the co-simulation tools. These tools will be made available at the end of March, 2016. Second, we will apply the risk management process in the context of the demonstrator sites that are available to the SPARKS project – this activity will focus on the Nimbus microgrid and the energy distribution network of SWW Wunsiedel GmbH. We anticipate the application of the process and tools, and the lessons learned from this exercise, will prompt us to revisit them for improvement.
References


Appendix A – An Introduction to Attack Trees

An attack tree (AT) is a hierarchical upside down tree structure with the attack goal as the root node at the top, different ways of achieving that goal as sub-goals and leaf nodes leading to this target as the bottom tasks. An attack tree is composed of a single root node that defines the primary threat to an asset. An attack may be decomposed into additional fine-grained sub-attacks, thereby forming a tree hierarchy. A threat/attack profile can be described as the path from a leaf node to the root node which represents a specific set of states involved in either achieving the primary threat or countering it. To express dependencies, the AT design includes AND (\(\land\)) and OR (\(\lor\)) operators to concatenate the sub-goals of a node. For sub-goals connected by an AND, all of them need to be fulfilled by the attacker to achieve their parent goal, whereas for OR connected sub-goals, only one of them need to be achieved. The process of splitting up nodes into sub-goals is repeated until a sufficient granularity is reached. The nodes at the lowest level in each branch are called leaf nodes. Figure 25 presents an example of such a tree, with the root node “A: Attack Goal”. In order to reach this goal, it is sufficient for the attacker to achieve either one of the OR connected sub-goals.

![Figure 25: Example of a simple attack tree with root node “A” followed by the operator OR (\(\lor\)) for four sub-goals where node “A.1” is further described by splitting it up in more sub-goals.](image)

Tree Creation

In order to establish an attack tree for a given System Under Evaluation (SUE), a detailed breakdown of the different components of this system, the available interfaces of each component and the functions provided by the system is necessary. The more information is available for this analysis, the more powerful becomes the tree to identify possible weak spots an attacker could make use of. The provided facts about the SUE are combined with expert knowledge about common attack patterns and typical weak spots in order to identify a set of assets which could be of interest to an attacker.

In order to identify assets which are of probable more interest to an attacker then others, further investigation for the identified assets is required. Therefore, each asset is treated as an attack goal an attacker would like to achieve. By splitting it up in sub-goals possible ways for an attacker are identified to reach this goal. These actions an attacker might perform to reach a certain goal are identified and registered in a tree structure. In Figure 25 node A.1 is split up and described more detailed with the sub-goals A.1.1 to A.1.3. Leaf nodes are those nodes, which do not have any children.
For each identified sub-goal the process of splitting it up in more sub-goals is repeated until a sufficient granularity is reached. Thereby, it is essential to assure that no potential path is missed, as this would lead to an unrecognized attack vector. After the tree is established with this method, one can use the tree to perform analysis on it to find the overall risk an attacker could reach the root node goal.

### Likelihood Assessment

Having the tree structure describing different paths an attacker could reach the attack goal in the root node, an evaluation on the tree is possible to find the overall risk for the root node. The nodes are weighted to describe the possibility an attacker can achieve what is described by this node. Usually a discrete scale is used to provide a clear distinction. In Figure 26 an example tree is presented where each leaf node is augmented with a value describing how difficult it is for an attacker to perform a certain action. For example the actions A.1.1 and A.1.2 listed in sub tree of A.1 are very unlikely to happen, because they are very hard for an attacker to perform, and so they are red. However, the action A.2 is very likely to happen and highlighted in green.

![Attack Tree Example](image)

**Figure 26: Example of an attack tree with the weight propagated to the root node.**

For the likelihood analysis, the scale represents how hard it is for an attacker to perform the individual action and is based on a combination of available security relevant values (like incidence, complexity, required knowledge, distribution, or reachability). An expert or group of experts should estimate the value for the leaf nodes. The values for their parent nodes is derived by the function represented by the operators AND and OR. In case the sub-goals are AND connected, the parent node is weighted with the highest value of its children, whereas if the sub-goals are OR connected, the smallest value is propagated to the parent node. By this processing the values are propagated from the leaf nodes to the root node, also highlighting possible ways an attacker could use to achieve this goal. The overall risk that an attack is capable of reaching the attack goal at Figure 26 is very likely due to the action introduced by node A.2.

### Attack Tree Drawbacks

Given a comprehensive description of the SUE, creating an according attack tree is a rather easy task. But establishing such trees also contains some problems which are briefly addressed here. For example, recoccurring actions along different paths or interchangeable actions at different levels could lead to inconsistency within the tree. In order to cope with them, they can be extracted into an independent sub-tree and referenced to from their former location. The interchangeable actions are further transformed to a directed acyclic graph (DAG). These sub-trees and DAGs are further
catalogued for reuse as common attack patterns for similar analysis. Introducing a new level by splitting up a node is different sub-goals there is the possibility of a state explosion. This is when rather simple goals are split up in a large subset of intermediate steps. A few of these cases could lead to a very big tree. In case the tree is getting to complex to be analysed properly, also the risk of missing potential attack vectors or entry points an attacker could use, increases. This is an inherent problem of attack trees. In Section 7.2 an approach is described to address this problem by combining attack trees with Semantic Thread Graphs (STG).
Appendix B – Likelihood Assessment Example

Here, we provide the remaining likelihood assessment (determination of threat levels) for the example attack tree that is presented in Section 5.3 (see Figure 17). The following threat levels were determined for three different TAs from HMG IS1, namely the handler (HAN), the indirect connected (IC) and the normal user (NU).

### Threat Actor Specific Leaf Node Rating

#### A 1.1.1 Exploit Vulnerability

The exploitation of a physical vulnerability using physical access requires a minimum of technical knowledge, like unplugging an internal cable.

<table>
<thead>
<tr>
<th>A1.1.1</th>
<th>Capability</th>
<th>Motivation</th>
<th>Threat Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>HAN</td>
<td>5</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>IC</td>
<td>1</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>NU</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>

#### A 1.1.2 Physical Access

A single DER component is considered to be installed at private premises, with minimal physical access protection like a case or a fence.

<table>
<thead>
<tr>
<th>A1.1.2</th>
<th>Capability</th>
<th>Motivation</th>
<th>Threat Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>HAN</td>
<td>5</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>IC</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>NU</td>
<td>4</td>
<td>5</td>
<td>5</td>
</tr>
</tbody>
</table>

#### A 1.2.1 Manipulate Service Device

Service devices for DER components (like diagnostic or programming laptops) are kept and maintained by the corresponding service personnel. These devices have no permanent network connection, but receive updates and other input via a temporary connection or by offline media like USB sticks.

<table>
<thead>
<tr>
<th>A1.2.1</th>
<th>Capability</th>
<th>Motivation</th>
<th>Threat Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>HAN</td>
<td>5</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>IC</td>
<td>2</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>NU</td>
<td>1</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

#### A 1.2.2 Manipulate OS or Running Software

The operating system and software running at the DER could provide local or remote access to the device. This access could be limited to a logical or privileged user group.

<table>
<thead>
<tr>
<th>A1.2.2</th>
<th>Capability</th>
<th>Motivation</th>
<th>Threat Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>HAN</td>
<td>3</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>IC</td>
<td>2</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>NU</td>
<td>4</td>
<td>3</td>
<td>4</td>
</tr>
</tbody>
</table>
A 1.3.1.1 Exploit Vulnerability in Webservice

Exploitation of a Webservice requires specific knowledge about the service, network security and access to the service.

<table>
<thead>
<tr>
<th>Capability</th>
<th>Motivation</th>
<th>Threat Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>HAN</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>IC</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>NU</td>
<td>3</td>
<td>2</td>
</tr>
</tbody>
</table>

A 1.3.1.2 Manipulate Connection PSN to DER

The connection between the PSN and DER is considered to be a PLC-based remote control technique.

<table>
<thead>
<tr>
<th>Capability</th>
<th>Motivation</th>
<th>Threat Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>HAN</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>IC</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>NU</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

A 1.3.2.1 Vulnerability in Another Service

Device and vendor specific services could have security issues.

<table>
<thead>
<tr>
<th>Capability</th>
<th>Motivation</th>
<th>Threat Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>HAN</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>IC</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>NU</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

A 1.3.2.2 Manipulate Connection PSN to DER

Manipulation of the connection between PSN and DER has already been evaluated as A 1.3.1.2.

**Threat Propagation**

As the evaluated branch contains no loops, the threat propagation is straightforward, for each threat level, starting at the bottom.

A 1.3.1 Manipulate Webservice

As the child nodes of this node are connected by a logical AND operator, the minimal threat level of each necessary child is adopted.

<table>
<thead>
<tr>
<th>Type: AND</th>
<th>Child node threat level (A1.3.1.1)</th>
<th>Child node threat level (A1.3.1.2)</th>
<th>Threat Level for A1.3.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>HAN</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>IC</td>
<td>5</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>NU</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

A 1.3.2 Manipulate other Service

As the child nodes of this node are connected by a logical AND operator the minimal threat level of each necessary child is adopted.
A 1.1 Physical Attack

As the child nodes of this node are connected by a logical AND operator the minimal threat level of each child is adopted.

<table>
<thead>
<tr>
<th>Type: AND</th>
<th>Child node threat level (A1.1.1)</th>
<th>Child node threat level (A1.1.2)</th>
<th>Threat Level for A1.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>HAN</td>
<td>4</td>
<td>6</td>
<td>4</td>
</tr>
<tr>
<td>IC</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>NU</td>
<td>3</td>
<td>5</td>
<td>3</td>
</tr>
</tbody>
</table>

A 1.2 Local Attack

As the child nodes of this node are connected by a logical OR operator the maximal threat level of each child is adopted.

<table>
<thead>
<tr>
<th>Type: OR</th>
<th>Child node threat level (A1.2.1)</th>
<th>Child node threat level (A1.2.2)</th>
<th>Threat Level for A1.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>HAN</td>
<td>4</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>IC</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>NU</td>
<td>1</td>
<td>4</td>
<td>4</td>
</tr>
</tbody>
</table>

A 1.3 Remote Attack

As the child nodes of this node are connected by a logical OR operator the maximal threat level of each child is adopted.

<table>
<thead>
<tr>
<th>Type: OR</th>
<th>Child node threat level (A1.3.1)</th>
<th>Child node threat level (A1.3.2)</th>
<th>Threat Level for A1.3.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>HAN</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>IC</td>
<td>4</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>NU</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

A1 Manipulate DER Component

As the child nodes of this node are connected by a logical OR operator the maximal threat level of each child is adopted.

<table>
<thead>
<tr>
<th>Type: OR</th>
<th>Child node threat level (A1.1)</th>
<th>Child node threat level (A1.2)</th>
<th>Child node threat level (A1.3)</th>
<th>Threat Level for A1</th>
</tr>
</thead>
<tbody>
<tr>
<td>HAN</td>
<td>4</td>
<td>4</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>IC</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>NU</td>
<td>3</td>
<td>4</td>
<td>1</td>
<td>4</td>
</tr>
</tbody>
</table>