World Academy of Science, Engineering and Technology
International Journal of Energy and Power Engineering
Vol:16, No:5, 2022

Combined Safety and Cybersecurity Risk Assessment for Intelligent Distributed Grids

Anders Thorsén, Behrooz Sangchoolie, Peter Folkesson, Ted Strandberg

Abstract—As more parts of the power grid become connected to the internet, the risk of cyberattacks increases. To identify the cybersecurity threats and subsequently reduce vulnerabilities, the common practice is to carry out a cybersecurity risk assessment. For safety classified systems and products, there is also a need for safety risk assessments in addition to the cybersecurity risk assessment to identify and reduce safety risks. These two risk assessments are usually done separately, but since cybersecurity and functional safety are often related, a more comprehensive method covering both aspects is needed. Some work addressing this has been done for specific domains like the automotive domain, but more general methods suitable for, e.g., Intelligent Distributed Grids, are still missing. One such method from the automotive domain is the Security-Aware Hazard Analysis and Risk Assessment (SAHARA) method that combines safety and cybersecurity risk assessments. This paper presents an approach where the SAHARA method has been modified to be more suitable for larger distributed systems. The adapted SAHARA method has a more general risk assessment approach than the original SAHARA. The proposed method has been successfully applied on two use cases of an intelligent distributed grid.

Keywords—Intelligent distribution grids, threat analysis, risk assessment, safety, cybersecurity.

I. Introduction

INTELLIGENT Distribution Grids (IDG) is an emerging concept that allows connecting different segments of the grid, as we move towards the era of Internet of Things (IoT) and smart cities. Connectivity between grid segments, that previously only used Local Area Network (LAN) for internal communications enables monitoring and controlling energy consumption in a wider perspective. The increased connectivity can be used in commercial- and industrial buildings or smart homes as well as energy distribution through power stations and wind/solar farms [1] and gain better "situational awareness" of utilities regarding the state of the grid [2].

Compared with traditional grids, an Information and Communication Technology (ICT) part has been added which increases the exposure for cybersecurity threats. The new risks introduced by the additional communication channels must be handled to maintain the desired behaviour. Moreover, depending on what the intelligent grid is allowed to do, malfunctions in the system may be hazardous and this needs to be analysed from a functional safety perspective.

The work has been supported by the European Community's Horizon 2020 Framework Programme through the UNITED-GRID project under grant agreement 773717.

Anders Thorsén, Behrooz Sangchoolie, Peter Folkesson, and Ted Strandberg are with the Department of Electrification and Reliability, Safety and Transport, RISE Research Institutes of Sweden, Box 857, SE-501 15 Borås, Sweden (e-mail: firstname.lastname@ri.se).

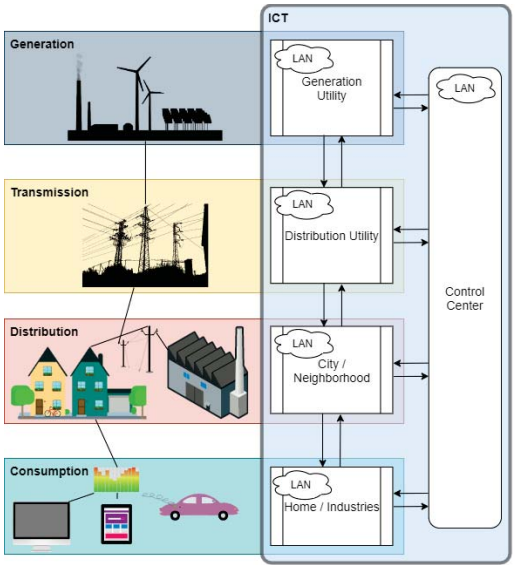

Fig. 1 Intelligent distribution grid architecture (based on [2])

Cybersecurity and functional safety are disciplines for which methods have been developed in other domains. Mostly these are separate methods, but there is a need for combined approaches covering both cybersecurity and functional safety. One such method is the Security-Aware Hazard and Risk Analysis (SAHARA) method [3]–[5] developed for the automotive domain. This paper presents an adaption of the SAHARA method to make it more general and suitable for other domains. The method is evaluated on the *advanced measurement solution* and *setting-less protection* use-cases from the UNITED-GRID project [6]–[9]. The results show that for each of these two uses cases from the IDG domain, the adapted SAHARA method is able to identify the most critical assets and threat scenarios.

The remainder of the paper is organised as follows: Section II provides background information. Section III describes the SAHARA method while Section IV describes the adaption made to the SAHARA method to support the IDG domain. Section V presents the results of applying the adapted SAHARA method on two UNITED-GRID use-cases. Finally, concluding remarks on this study are given in Section VI.

II. Background

A. Intelligent Distribution Grids

An IDG with its components is schematically illustrated in Fig. 1. The four traditional grid components shown on the left

side of Fig. 1 are connected by an *ICT* architecture shown on the right side. The ICT architecture enables communication between the LANs of each grid component and to add a control centre allowing new advanced intelligent functionality. The traditional grid components are explained below:

- *Generation* transforms primary energy sources to electric power. The bulk power contribution still comes from centralized production, but small-scale distributed generation is increasing in volume [10].
- *Transmission* distributes the electric power using high voltage infrastructure from production sites, via substations, to cities and neighbourhoods. Important parts include mechanisms to interrupt any short circuits or overload currents that may occur on the network.
- *Distribution* transforms high voltage power used in transmission lines to lower voltage power for distribution to residential homes and businesses. There is also functionality to calculate the difference between actual energy consumption in each individual house and consumption estimated based on historical consumption data and the climate conditions in the area.
- *Consumption* concerns the usage of electricity in residential areas as well as industrial and commercial areas. Smart appliances and smart meters are used to manage and optimize the energy consumption.

B. Cybersecurity and Functional Safety

The ICT architectures in IDGs increases the exposure of cybersecurity related threats and risks compared with traditional grids. Apart from increasing financial, operational and privacy concerns, the interplay between cybersecurity and functional safety becomes more relevant [11], [12].

- *Cybersecurity* deals with threats to the system or equipment from the outside world causing system compromises through unintentional or intentional attacks; and
- *Functional safety* is about protecting people, processes, systems, and environments from hazards due to the system or equipment not operating correctly.

A view of the relationship between cybersecurity and functional safety is shown in Fig. 2. Cybersecurity weaknesses may cause systems or equipment to be a hazard to the outside world and hence considered to be a safety issue [13].

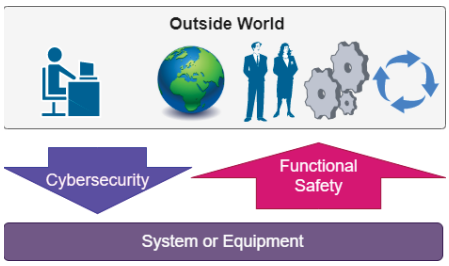

Fig. 2 A view of the relationship between cybersecurity and functional safety

C. Dependability Attributes

Dependability is an important concept for both cybersecurity and functional safety. A taxonomy of dependable and secure computing and communication is presented in [14], which defines dependability as "*the ability to avoid service failures that are more frequent and more severe than is acceptable*". Dependability encompasses several attributes. The following six attributes are considered to be the primary ones:

- *Reliability* - the continuity of correct service.
- *Safety* - the absence of catastrophic consequences on the user(s) and the environment.
- *Maintainability* - the ability to undergo modifications and repairs.
- *Confidentiality* - the absence of unauthorized disclosure of information.
- *Integrity* - the absence of improper system alterations.
- *Availability* - the readiness for correct service.

The attributes in the CIA triad (Confidentiality, Integrity, and Availability) are the primary ones for addressing cybersecurity. For IDG's, these attributes must be considered at least in the sense of availability of the service, integrity of transmitted data and confidentiality of the consumer's data.

In addition to primary attributes, there are several secondary attributes for addressing cybersecurity, e.g., [15], [16]:

- *Authenticity* - the property that an entity is what is claims to be.
- *Authorization* - enforces means to ensure access rights for entities in relation to assets (i.e., physical, or digital entities that have value to individuals, organizations, or governments [17]).
- *Non-repudiation* - to be able to prove the occurrence of an event or action and its originating entities to ensure that an entity cannot deny that the event or action was actually performed by the entity.
- *Privacy* - to ensure that the relation between an entity and a set of information is confidential with respect to authorized entities.
- *Freshness* - specifies that the specific information received by an authorized entity at a given time is not a copy of the same information received at an earlier time by the same or another entity.

D. Risk and Threat Analysis

Risk analysis is fundamental in the functional safety domain, as is threat analysis in the cybersecurity domain. In both these there are several terms that is frequently used.

For the functional safety domain commonly used terms in the context of risk assessments includes [18]:

- *Risk* - the combination of the probability of occurrence of harm and the severity of that harm.
- *Harm* - injury or damage to the health of people, or damage to property or the environment.
- *Hazard* - potential source of harm.
- *Risk analysis* - systematic use of available information to identify hazards and to estimate the risk.

- *Tolerable risk* - level of risk that is accepted in a given context based on the current values of society.
- *Risk evaluation* - procedure based on the risk analysis to determine whether tolerable risk has been exceeded.
- *Risk assessment* - overall process comprising a risk analysis and a risk evaluation.

Similar, in the cybersecurity domain there are also a number of terms used in the context of threat analysis [19], [20]:

- *Threat* - potential cause of unwanted incidents that may result in harm to a system or organization.
- *Vulnerability* - weakness of an asset or control that can be actively exploited by one or more threats.
- *Threat action (attack)* - the active exploitation of vulnerabilities by one or more threats.

E. Assessment Methods Combining Safety and Security

There are few methods combining cybersecurity analyses with safety analyses of systems, but some have recently been developed within the automotive domain: The *HEAVENS Security Model* [21] focuses on methods, processes and tool support for threat analysis and risk assessment with respect to the vehicle Electrical and/or Electronic (E/E) systems. The *EVITA (E-Safety Vehicle Intrusion Protected Applications) method* [21] adopts an attacker-centric approach to risk analysis identifying four high-level security objectives: operational, privacy, financial and safety. The *SECTRA model* [16] is an asset-centric model which defines required strength levels for security mechanisms needed to protect assets. It classifies the impact level of attacks with respect to safety as well as privacy, operation, and financial aspects. The *SAHARA method* [3]–[5] combines cybersecurity evaluation with automotive hazard analysis and risk assessment according to the automotive functional safety standard ISO 26262 [22].

This paper focuses on the SAHARA method due to its simplicity compared with some of the other methods allowing for a relatively straightforward adaption to the IDG domain.

III. The SAHARA Method

The SAHARA method combines cybersecurity evaluation, using the STRIDE approach developed at Microsoft [23]–[25], with functional safety evaluations using the automotive HARA (Hazard Analysis and Risk Assessment) defined in ISO 26262-3:2018 [22]. This allows the impact of security threats on system safety to be analysed early at the concept-phase of system development. The aim of the method is to classify the probability of security threats and to determine the countermeasures needed. The SAHARA method is composed of two parts that are explained in the remaining of this section.

1) SAHARA Part 1: This part quantifies cybersecurity threats according to the STRIDE security threat model, i.e., threats are grouped based on the goals and purposes of the attacks. A working knowledge of these groups of threats helps to organize a security strategy to plan responses to threats. The term STRIDE stems from the initial letters of the six different possible types of threats:

- *Spoofing* - Attackers pretend to be someone or something else. The main security attribute targeted is authenticity.
- *Tampering* - Attackers change data in transit or in a data store. The main security attribute targeted is integrity.
- *Repudiation* - Attackers perform actions that cannot be traced back to them, thus mainly targeting non-repudiation (or in some cases freshness).
- *Information disclosure* - Attackers get access to data in transit or in a data store, thus mainly targeting confidentiality and/or privacy.
- *Denial of service (DoS)* - Attackers interrupt a system's legitimate operation, thus mainly targeting availability.
- *Elevation of privilege* - Attackers perform actions they are not authorized to perform, thus mainly targeting authorization.

The STRIDE model could be considered as threat-centric or attacker-centric since each threat is associated with a particular asset from the attacker's perspective.

Threat modelling using STRIDE can be seen as a cybersecurity equivalent to the functional safety hazard and risk analysis [5]. In functional safety standards such as IEC 61508 [26] and its derivative IEC 61511 [27] for the process industry, safety integrity levels (SIL) are calculated as a measure of reliability and/or risk reduction. In SAHARA part 1, the Security Level (SL) is determined in a corresponding way by quantifying the cybersecurity threats according to (see also Table I):

- *Level of Knowledge (K)* concerns knowledge of the target system specifically (not knowledge in general) and is rated from 0 to 2. Level 0 denotes that no prior knowledge of the target system is needed, i.e., a black box approach can be used, while Level 2 denotes that domain knowledge needed, i.e., person with technical training and focused interests having knowledge of the internals of the target system is needed to perform an attack.
- *Required Resources (R)* concerns hardware tools required for targeting the system with attacks and is rated from 0 to 3. Level 0 refers to when no additional tools are required; Level 1 means commonly-used tools are available (e.g., screwdriver, PC with commonly available tools etc.); Level 2 means limited availability of tools (e.g., sniffer, oscilloscopes, SDR, OBD hacking tools etc.); and Level 3 means advanced tools adapted for the target systems (e.g., debuggers, flashers, simulators specifically developed for the target system, etc.) are required.
- *Threat Criticality (T)* concerns the impact of the attack on security and safety rated from 0 to 3. Level 0 means that there is no impact; Level 1 that there is some impact such as reduced availability or service; Level 2 that there is significant impact, e.g., on the delivered service or intrusion on privacy; and Level 3 is the highest impact level (e.g., life-threatening) where safety is affected in addition to security.

After determining K, R and T, Table II is used to determine the SL of each threat from the scale 0-4. The SL measures the risk associated with the threats based on impact and likelihood parameters according to the SAHARA model.

TABLE I
SAHARA LEVEL OF KNOWLEDGE (K), REQUIRED RESOURCES (R) AND THREAT CRITICALITY (T) [4]

#	Level of Knowledge (K)	Required Resources (R)	Threat Criticality (T)
0	No prior knowledge (black-box approach)	No additional tool or everyday commodity	No security impact
1	Technical knowledge (gray-box approach)	Standard tool	Moderate security relevance: *Annoying manipulation, partial reduced availability of service*
2	Domain knowledge (white-box approach)	Simple tool	High security relevance: *Damage of goods, invoice manipulation, non-availability of service, privacy intrusion*
3	-	Advanced tools	High security and/or possible safety relevance: *Maximum security impact and life-threatening abuse possible*

2) SAHARA Part 2: The second part is to perform an automotive HARA according to ISO 26262. The HARA analysis is limited to identifying events caused by malfunction behaviour of the system. Thereafter safety goals with corresponding Automotive Safety Integrity Levels (ASILs) are formulated related to the prevention or mitigation of the identified hazardous events to avoid unreasonable risks. The ASIL is determined by considering severity, probability of exposure and controllability.

All threats identified in SAHARA part 1 having a threat criticality (T) larger than 2 may have an impact on system safety. These threats shall be analysed from a functional safety perspective using the HARA approach formulating safety goals and corresponding ASILs. These are added to the result from the already performed HARA to give a complete set of functional safety goals also covering cybersecurity threats.

IV. ADAPTION OF THE SAHARA METHOD

To make the SAHARA method more general and suitable for combined cybersecurity and functional safety assessments in other domains that automotive, some adaptations are needed. In this section, we present an overview of the adapted SAHARA method (see Fig. 3) with special focus on the IDG domain.

A. Asset and Communication Channel Analysis

A common practice in identifying potential cybersecurity attack surfaces is to identify all assets in the system and define appropriate countermeasures [28]. For the IDG domain, this includes handling a distributed system with assets belonging to different grid components and possible organizations. Moreover, the communication conducted within IDGs may be performed using different channels that could partly be physical channels that are outside the analysed system (such as Ethernet). This motivates adding a communication channel analysis as a separate activity besides the asset analysis. In the IDG case, it is also likely that the analysed system is only a sub part of the complete power grid that communicates with external assets outside the analysed system.

Proposed information to include in the two analyses are listed in Table III. Some information is overlapping to ensure not missing any assets or communication channels. All communication channels listed during the asset analysis shall be included in the communication channel analysis and all endpoints listed in the communication channel analysis shall be include in the asset analysis unless belonging to an external endpoint.

TABLE II
SAHARA SECURITY LEVEL (SL) DETERMINATION MATRIX

Required Resources (R)	Level of Knowledge (L)	Threat Criticality (T) 0	1	2	3
0	0	0	3	4	4
	1	0	2	3	4
	2	0	1	2	3
1	0	0	2	3	4
	1	0	1	2	3
	2	0	0	1	2
2	0	0	1	2	3
	1	0	0	1	2
	2	0	0	0	1
3	0	0	0	1	2
	1	0	0	0	1
	2	0	0	0	1

B. Cybersecurity Threat Analysis

1) STRIDE Analysis: The cybersecurity analysis follows the STRIDE method as described in Section III-1. It is adopted for the IDG domain such that the results obtained from the asset and communication channels analysis in Section IV-A are used as input. For each asset, the relevance of each STRIDE threat type and the scenarios are described. It is important to include all relevant communication channels in the analysis.

2) Adapted SAHARA Part 1: Based on the threat types and attack scenarios identified in Section IV-B1, the STRIDE security threats are quantified according to the

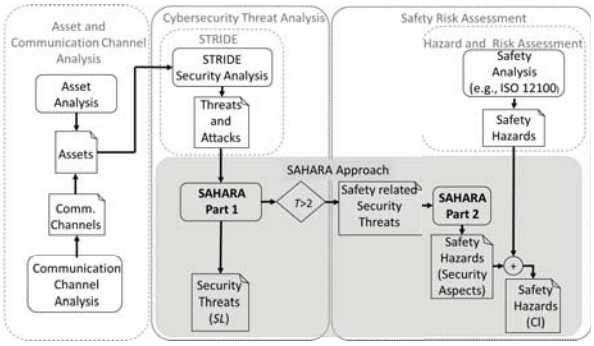

Fig. 3 The SAHARA method adapted for the power grid domain

TABLE III
LIST OF INFORMATION DOCUMENTED FOR THE ASSET AND COMMUNICATION CHANNELS ANALYSIS

Asset analysis	Communication channel analysis
ID	ID
Asset name	Communication channel
Type	Endpoint from
Location	Endpoint to
Description	Description
Important functions	Protocol
Inbound communication channels	Format
Outbound communication channels	Important features
System level dependability attribute possible affected by the asset	System dependability attribute possible affected by the communication channel

SAHARA part 1 approach described in Section III-1. Though the original SAHARA is based on ISO 26262 with its specific ASIL definition for calculation of Security Level (SL), the SL definition is considered applicable also for the majority of other functional safety standards. Level of Knowledge (K), Required Resources (R) and Threat Criticality (T) are quantified according to Table I followed by determining the SL according to Table II.

C. Security and Safety Risk Assessment

1) Safety Risk Assessment: Risk analyses and risk assessments are fundamental in the functional safety domain and are performed in parallel with the SAHARA cybersecurity threat analyses.

The original SAHARA is based on ISO 26262 with its rather narrow definition of functional safety as "Absence of unreasonable risk due to hazards caused by malfunctioning behaviour of Electrical/Electronic systems". For the proposed adapted SAHARA method, the risk assessment method needs to comply with the more general functional safety definitions given in Section II-B. IEC 61508 Part 5 [26] lists a number of risk assessment methods suitable with the safety integrity level concept. One method is the risk graph qualitative method used extensively in the machinery sector, see Annex A of ISO 13849-1 [29] and ISO/TR 14121-2:2012 [30]. The latter document gives practical guidance on conducting risk assessment for machinery in accordance with ISO 12100:2010 [31] providing designers with a framework and guidance for decision-making during the development of machinery.

In this paper, we perform the safety risk assessment using the *quantitative risk graph method* described in ISO/TR 14121-2:2012 [30]. The method focuses on protecting people from hazards due to the system, or equipment not operating correctly, a concept suitable to expand to also cover processes, systems, and environments. The first step of the assessment is to quantify the following factors (see also Table IV):

- *Severity of possible harm (Se)* - estimate of the severity of the injuries or damage to health, and the extent of harm. Scored from 1 (least severe harm) to 4 (most severe harm).
- *Frequency of exposure and its duration (Fr)* - estimate of the exposure to the hazard. All modes of operation of the machinery and methods of working shall be taken into consideration, including long-term damage to health. Scored from 2 (lowest frequency) to 5 (highest frequency).
- *Probability of occurrence of a hazardous event (Pr)* - estimate of the probability that a person, property or environment is exposed to harm. Factors to consider include the need for access to the hazard zone, the nature of access, time spent in the hazardous zone, the number of persons requiring access and the frequency of access. Scored from 1 (lowest probability) to 5 (highest probability).
- *Possibility of avoiding or limiting harm (Av)* - factors to consider are persons (skilled or unskilled) that can be exposed to the hazards, how quickly the hazardous situation can lead to harm, awareness of risk, the human ability to avoid harm and practical experience and knowledge. Scored as 1 (likely), 3 (possible) or 5 (impossible).

Following the quantification, a risk class (Cl) is calculated as the sum of Fr, Pr and Av. Finally, using Table V, the resulting risk is measured as low (L), medium (M) or high (H).

2) Adapted SAHARA Part 2: Similar to the original SAHARA, all threats with 'Threat Criticality'$>$ 2 from SAHARA part 1, are analysed using the quantitative risk graph method described in Section IV-C1. The result is a number of security-related safety goals that are added to the safety goals from the already performed safety risk assessment.

V. USE-CASE EVALUATION FROM THE UNITED-GRID PROJECT

The adapted SAHARA method has been used to evaluate and quantify the cybersecurity and safety of the ICT part of the IDG architecture used in the UNITED-GRID project [6]. The architecture comprises of sensing, protection and control tools in any smart-grid utilising an open cross-platform (OCP) middleware at the boundary of the smart-grid. The idea is that the OCP is delivered as a tool-box possible to connect to existing Distribution Management Systems (DMS) for advanced energy management, grid-level control, and protection. The project evaluates several use cases using simulations, in laboratories or at demo sites including the Strijp-S living-lab [8] and the Chalmers Campus testbed [7].

This section first presents two of the project use cases (see Sections V-A and V-B) and then conduct an evaluation of these use cases in Section V-C using the proposed adapted SAHARA method presented in Section IV.

A. Use Case 1: Advanced Measurement Solution

The first use case, the advanced measurement solution, is important for IDGs and many of the UNITED-GRID project use cases relies on its provided functionality. The solution is based on SST's Low Voltage smart sensors [32], [33] that are used to gather data and events at a medium frequency. It consists of a time beacon for synchronisation, voltage-

TABLE IV
RISK ANALYSIS QUANTIFYING, ADOPTED FROM ISO/TR 14121-2:2012 [30]

#	Severity of possible harm (Se)	Frequency of exposure and its duration (Fr)	Probability of occurrence of a hazardous event (Pr)	Possibility of avoiding or limiting harm (Av)
1	Reversible, first aid	-	Negligible	Likely
2	Reversible, medical attention	t≥1y	Rarely	-
3	Permanent, e.g., losing fingers	2w≤t<1y	Possible	Possible
4	Death or permanent disability, e.g., losing an eye or arm	24h≤t<2w	Likely	-
5	-	t<24h	Very high	Impossible

and current-sensors, and an embedded computer acting as a smart node running the advanced function. In addition, the embedded computer runs a docker container of the Atos developed UNITED-GRID toolbox as one smart node and with another instance as master smart node in a cloud service. The latter also includes a sftp server. Communications between the nodes in the Toolbox is done through a MQTT broker for the advanced function management and using text files over sftp to the cloud smart node. ZeroMQ is used for sensor communication. In Fig. 4 the target architecture is shown highlighting the parts belonging to the UNITED-GRID toolbox.

B. Use Case 2: Setting-Less Protection

The second use case, the setting-less protection use case, has the purpose to demonstrate a Dynamic State Estimation (DSE) [34], [35] based protection scheme. It is an extension of the advanced measurement solution described in Section V-A. Same type of SST's Low Voltage smart sensors are used, but the DSE algorithm (or Real Time algorithm) runs on the local smart node and controls the trip signals to the circuit breakers. In addition to the advanced measurement solution use case, this use case performs active actions based on measurement data from the SST sensors.

C. Results of SAHARA Analysis

The analyses of the use cases identified the assets with negative effects on dependability and security related attributes. The assets for which security may be affected negatively were selected for SAHARA analysis. In this section, we summarize the results of the SAHARA cybersecurity analyses conducted.

Fig. 5 summarizes the results for the *advanced measurement solution*. In total, 58 threat scenarios were identified. There are four threat scenarios with a threat criticality level T $>$ 2 and no threat scenarios with a security level SL $>$ 2. The most critical asset is the UNITED-GRID toolbox *sftp server* with the threat criticality T $>$ 2 for threat scenarios involving tampering, spoofing, repudiation, and elevation of privilege threats. However, since several security protection mechanisms are already in place, the security level SL is equal to 1 for these scenarios. For the denial-of-service threat scenario on the sftp server, safety is not affected, however the security level SL = 2 since the denial-of-service attacks may be performed using comparatively low resources and knowledge of the system. Among the 58 threat scenarios of the advance measurement solution, 12 scenarios have a security level SL = 2 but none of those have threat critically above 2.

For the *setting-less protection* use case, 36 threat scenarios were identified, see Fig. 6. There are 17 threat scenarios with a threat criticality T $>$ 2 and 11 threat scenarios with a security level SL $>$ 2. In the remaining of this section, we present the analysis results obtained for the most critical assets:

- *SST smart node*: The most critical asset of this use case is the local SST smart node. The threat scenario involving denial of service threats is the most critical one with a security level SL = 4. Moreover, tampering, repudiation and elevation of privilege threats are critical with SL = 3. Since the threat critically T $>$ 2 for these scenarios, safety requirements may be violated if attacks are successful. Spoofing threats also have a T $>$ 2 which may result in the safety requirements to be violated, but due to the significant knowledge needed to spoof the smart node, the security level is lower (SL = 2).
- *DSE algorithm*: The DSE algorithm running on the local

TABLE V
RISK ANALYSIS SAFETY CLASS (CL) DETERMINATION MATRIX [30]

Severity	Class Cl = Fr+Pr+Av				
	4	5-7	8-10	11-13	14-15
4	M	H	H	H	H
3	L	M	H	H	H
2	L	L	M	H	H
1	L	L	L	M	H

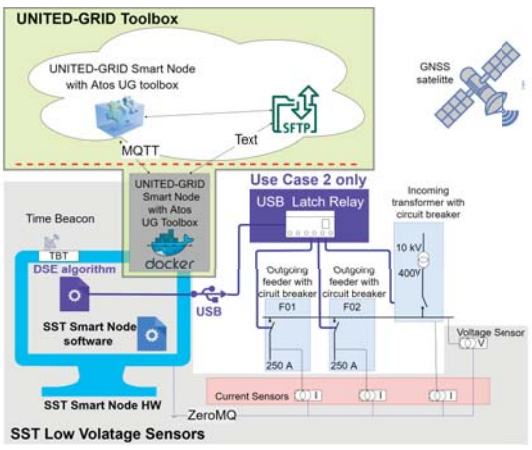

Fig. 4 Illustration of the evaluated UNITED-GRID use cases

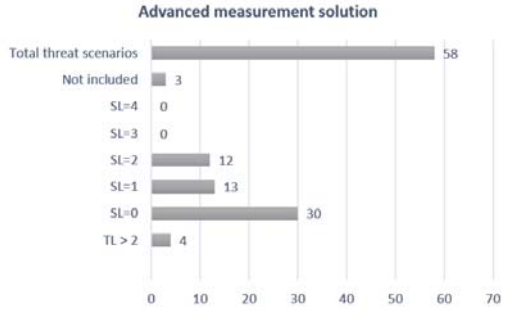

Fig. 5 Number of threat scenarios identified by SAHARA for the Advanced measurement solution use-case

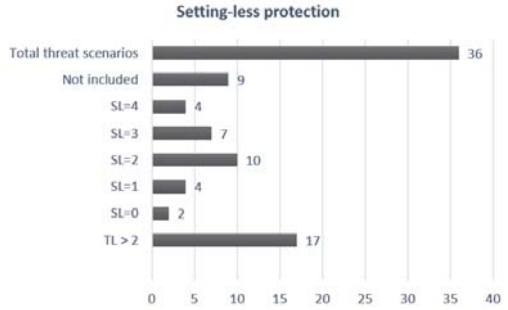

Fig. 6 Number of threat scenarios identified by SAHARA for the Setting-less protection use-case

SST smart node is another critical asset. The threat scenario involving denial of service threats is the most critical with a security level SL = 4. Also tampering threats are critical with SL = 3. Since the threat critically T $>$ 2 for these threat scenarios, safety requirements may be violated if attacks are successful.

- *SST low voltage (LV) sensor*: The threat scenario involving denial of service threats is the most critical one with a security level SL = 3. Moreover, tampering and elevation of privilege threats may be critical for the low voltage sensor with SL = 2. Since the threat critically T $>$ 2 for these threat scenarios, safety may be affected if attacks are successful. Repudiation threats also have a T $>$ 2 which may result in the violation of safety requirements, however due the significant knowledge and equipment required to attack the SST LV sensor, the security level is lower (SL = 1) for the repudiation threat scenario.
- *USB Latching relay module*: The USB latching relay modules (not visible in Fig. 4) are used for connecting the local smart node to the circuit breakers. For these, the threat scenario involving denial of service threats is the most critical one with a security level SL = 4. Tampering and repudiation threats may also be considered critical with SL = 2. Since the threat critically T $>$ 2 for these threat scenarios, safety requirements may be violated if attacks are successful.
- *Circuit breaker*: The threat scenario involving denial of service threats is the most critical scenario for the circuit breaker with a security level SL = 4. Tampering and repudiation threats are also critical with SL = 3. Since the threat critically T $>$ 2 for these threat scenarios, safety requirements may be violated if attacks are successful.

VI. Conclusions

In this paper, we presented a methodology to assess the level of cybersecurity and safety required for ICT architectures used in Intelligent Distribution Grids (IDG). Our method for evaluating ICT architectures of IDGs is based on the SAHARA (Security-Aware Hazard and Risk Analysis) method originally proposed for the automotive domain. The first step in our method is to perform an asset analysis including all relevant parts of the system. Moreover, a communication channel analysis is performed including all communication channels with endpoints among the assets in the previous step. After that follows the SAHARA analysis, which is divided into two parts; (1) evaluate the cybersecurity for each cybersecurity-relevant asset by quantifying the security threats defined by the STRIDE security model according to the Level of Knowledge (K), Required Resources (R) and Threat Criticality (T); (2) a safety risk assessment using a risk graph qualitative method for each safety-related asset. The safety risk assessment shall include all identified cybersecurity threats with possible functional safety relevance, i.e., threats with threat criticality levels higher than 2 derived in part 1.

The method has been used to evaluate safety-related cybersecurity threads of the ICT architecture used in the UNITED-GRID project with special focus on two use cases, namely, *advanced measurement solution* and *setting-less protection*. For *advanced measurement solution* use case, the most critical asset is the UNITED-Grid toolbox sftp server for threat scenarios involving tampering, spoofing, repudiation, and elevation of privilege threats, but due to the several security protection mechanisms already in place, the security level is kept on acceptably low levels. For the *setting-less protection* use case, there are several threat scenarios identified with high threat critically and/or high security level. The most critical threat is denial of service attacks that may target the local Smart Node (SN) and the RT Algorithm running on it, the LV sensor, the USB latching relay module, and the circuit breakers. Tampering is critical for all these assets; repudiation is critical for the SN, the USB latching relay, and the circuit breaker; and elevation of privilege is critical for the SN and the LV sensor. In all these scenarios, safety requirements may be violated if attacks are successful. For the SN, spoofing threats may also result in the violation of safety requirements. However, due to the significant knowledge needed to spoof the SN, the security level is lower for the spoofing thread scenarios. Similar reasoning and conclusions could be drawn for repudiation threats on the LV sensor.

As part of the future work, the plan is to further enhance the method to be able to apply it on active IDG implementations already operating in the field. Moreover, parts of the method should be automated, e.g., by incorporating the Microsoft Threat Modelling Tool to identify threat scenarios in the SAHARA part 1 analysis. There are also plans to extend the method to be used in other domains, e.g., by incorporating safety and cybersecurity analyses commonly used in other domains, with the goal of developing a more generic method.

ACKNOWLEDGMENT

The authors would like to thank David Steen and Ankur Srivastava from Chalmers University of Technology, Dennis Bijwaard and Omar Mansour from SmartStateTechnology and Lucile Lemius and Emmanuel Zychla from Atos for their aid in the evaluation of the UNITED-GRID use-cases. Special thanks also to Alexis Leikidis for his help with preparing the background material for this paper.

REFERENCES

[1] ScienceTech. A Green Future for Electrical Networks. Think Magazine. [Online]. Available: https://www.um.edu.mt/think/a-green-future-for-electrical-networks/

[2] Y. Mo, T. H.-J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, "Cyber–Physical Security of a Smart Grid Infrastructure," in *Proceedings of the IEEE*, vol. 100, no. 1, pp. 195–209.

[3] G. Macher, E. Armengaud, E. Brenner, and C. Kreiner, "Threat and Risk Assessment Methodologies in the Automotive Domain," *Procedia Computer Science*, vol. 83, pp. 1288–1294.

[4] G. Macher, H. Sporer, R. Berlach, E. Armengaud, and C. Kreiner, "SAHARA: A security-aware hazard and risk analysis method," in *2015 Design, Automation Test in Europe Conference Exhibition (DATE)*, pp. 621–624.

[5] G. Macher, A. Höller, H. Sporer, E. Armengaud, and C. Kreiner, "A Combined Safety-Hazards and Security-Threat Analysis Method for Automotive Systems," in *Computer Safety, Reliability, and Security*, ser. Lecture Notes in Computer Science, F. Koornneef and C. van Gulijk, Eds. Springer International Publishing, vol. 9338, pp. 237–250.

[6] Solutions for intelligent distribution grids. UNITED-GRID. [Online]. Available: https://united-grid.eu/

[7] K. Antoniadou-Plytaria, A. Srivastava, M. A. F. Ghazvini, D. Steen, L. A. Tuan, and O. Carlson, "Chalmers Campus as a Testbed for Intelligent Grids and Local Energy Systems," in *2019 International Conference on Smart Energy Systems and Technologies (SEST)*, pp. 1–6.

[8] R. Fonteijn, M. Roos, P. Nguyen, J. Morren, and J. Slootweg, "The Strijp-S living-lab: Testing innovative solutions for fault protection, self-healing, congestion management, and voltage control," in *2018 53rd International Universities Power Engineering Conference (UPEC)*, pp. 1–6.

[9] M. Roos, R. Fonteijn, P. Nguyen, J. Morren, and H. Slootweg, "The Strijp-S living lab for embedded microgrid studies," in *2018 CIRED Workshop*.

[10] Generation. [Online]. Available: https://www.itc-holdings.com/a-modern-power-grid/about-the-national-power-grid/generation

[11] Breaking Down Cybersecurity and Functional Safety Requirements for Industrial Control Systems. Totally Integrated Automation. [Online]. Available: https://www.totallyintegratedautomation.com/2019/06/breaking-down-cybersecurity-and-functional-safety-requirements-for-industrial-control-systems/

[12] J. K. von Wedel and P. Arndt, "Safe and Secure Development: Challenges and Opportunities," in *SAE Technical Paper*, vol. 2018-01-0020. SAE.

[13] L. Piètre-Cambacédès and C. Chaudet, "The SEMA referential framework: Avoiding ambiguities in the terms "security" and "safety"," *International Journal of Critical Infrastructure Protection*, vol. 3, no. 2, pp. 11–33.

[14] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," *IEEE Transactions on Dependable and Secure Computing*, vol. 1, no. 1, pp. 11–33.

[15] Y. Cherdantseva and J. Hilton, "A Reference Model of Information Assurance Security," in *2013 International Conference on Availability, Reliability and Security*, pp. 546–555.

[16] Aljoscha Lautenbach and Mafijul Islam, "Deliverable D2.0, Security models, HEAVENS (HEAling Vulnerabilities to ENhance Software Security and Safety), Project deliverable." [Online]. Available: https://autosec.se/holisec-results/

[17] IEC 60050 - International Electrotechnical Vocabulary - Details for IEV number 741-01-04: "Asset". [Online]. Available: https://www.electropedia.org/iev/iev.nsf/display?openform&ievref=741-01-04

[18] ISO/IEC, *ISO/IEC Guide 51:2014 Safety Aspects-Guidelines for their Inclusion in Standards.*

[19] R. Shirey, "Internet Security Glossary, Version 2," vol. RFC4949.

[20] ISO/IEC, *ISO/IEC 27000:2018 Information technology-Security techniques - Information security management systems—Overview and vocabulary.*

[21] SAE Vehicle Cybersecurity Systems Engineering Committee, *Cybersecurity Guidebook for Cyber-Physical Vehicle Systems*, no. J3061.

[22] ISO, *ISO 26262:2018 Road Vehicles : Functional Safety*.

[23] F. Swiderski and W. Snyder, *Threat Modeling*. Microsoft Press.

[24] L. Kohnfelder and P. Garg, "The threats to our products," *Microsoft Interface*. [Online]. Available: https://adam.shostack.org/microsoft/The-Threats-To-Our-Products.docx

[25] A. Shostack. "Experiences Threat Modeling at Microsoft". [Online]. Available: https://adam.shostack.org/modsec08/Shostack-ModSec08-Experiences-Threat-Modeling-At-Microsoft.pdf

[26] IEC, *IEC 61508:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems.*

[27] IEC, *IEC 61511:2010 Functional safety - Safety instrumented systems for the process industry sector.*

[28] ISO, *ISO - ISO/IEC 27001:2013 — Information Security Management*.

[29] ISO, *ISO 13849-1:2015 Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design.*

[30] ISO, *ISO/TR 14121-2: 2007 Safety of Machinery-Risk Assessment-Part 2: Practical Guidance and Examples of Methods*.

[31] ISO, *ISO 12100:2010 Safety of Machinery–General Principles for Design–Risk Assessment and Risk Reduction*. CEN.

[32] Smart State Technology. [Online]. Available: https://www.smartstatetechnology.nl/

[33] G. Hoogsteen, M. E. Gerards, J. L. Hurink, G. J. Smit, O. Mansour, and D. Bijwaard, "Combining distributed synchronized high frequency measurements with a control system for smart low voltage grids," in *Proceedings of the 25th International Conference on Electricity Distribution (CIRED 2019)*. CIRED.

[34] R. Fan, A. P. S. Meliopoulos, L. Sun, Z. Tan, and Y. Liu, "Transformer inter-turn faults detection by dynamic state estimation method," in *2016 North American Power Symposium (NAPS)*.

[35] A. P. S. Meliopoulos, G. J. Cokkinides, Z. Tan, S. Choi, Y. Lee, and P. Myrda, "Setting-Less Protection: Feasibility Study," in *2013 46th Hawaii International Conference on System Sciences*, pp. 2345–2353.