Threat Analysis in Systems-of-Systems: An Emergence-Oriented Approach

ANDREA CECCARELLI and TOMMASO ZOPPI, University of Florence

ALEXANDR VASENEV, University of Twente

MARCO MORI, University of Florence

DAN IONITA and LORENA MONTOYA, University of Twente

ANDREA BONDAVALLI, University of Florence

Cyber-physical Systems of Systems (SoSs) are large-scale systems made of independent and autonomous cyber-physical Constituent Systems (CSs) which may interoperate to achieve high-level goals also with the intervention of humans. Providing security in such SoSs means, among other features, forecasting and anticipating evolving SoS functionalities, ultimately identifying possible detrimental phenomena that may result from the interactions of CSs and humans. Such phenomena, usually called *emergent phenomena*, are often complex and difficult to capture: the first appearance of an emergent phenomenon in a cyber-physical SoS is often a surprise to the observers. Adequate support to understand emergent phenomena will assist in reducing both the likelihood of design or operational flaws, and the time needed to analyze the relations amongst the CSs, which always has a key economic significance. This article presents a threat analysis methodology and a supporting tool aimed at (i) identifying (emerging) threats in evolving SoSs, (ii) reducing the cognitive load required to understand an SoS and the relations among CSs, and (iii) facilitating SoS risk management by proposing mitigation strategies for SoS administrators. The proposed methodology, as well as the tool, is empirically validated on Smart Grid case studies by submitting questionnaires to a user base composed of 3 stakeholders and 18 BSc and MSc students.

CCS Concepts: • **Software and its engineering** → **Risk management**; • **Security and privacy** → *Software security engineering*; • **Applied computing** → *IT architectures*; • **Computer systems organization** → *Embedded and cyber-physical systems*;

Additional Key Words and Phrases: Emergent properties, systems-of-systems, cyber-physical systems, threat analysis, security, evolution, user assessment

ACM Reference format:

Andrea Ceccarelli, Tommaso Zoppi, Alexandr Vasenev, Marco Mori, Dan Ionita, Lorena Montoya, and Andrea Bondavalli. 2018. Threat Analysis in Systems-of-Systems: An Emergence-Oriented Approach. *ACM Trans. Cyber-Phys. Syst.* 3, 2, Article 18 (October 2018), 24 pages.

<https://doi.org/10.1145/3234513>

This work has been partially supported by the Joint Program Initiative (JPI) Urban Europe via the IRENE project and has received funding from (i) the European Union 7th Framework Programme (FP7/2007-2013) under grant agreement n° 318003 (TREsPASS), (ii) the “Ente Cassa Di Risparmio di Firenze”, Bando per progetti 2016, and (iii) the REGIONE TOSCANA POR FESR 2014-2020 SISTER “Signaling & Sensing Technologies in Railway application” project.

Authors’ addresses: A. Ceccarelli, T. Zoppi, M. Mori, and A. Bondavalli, University of Florence, Viale Morgagni 65, Firenze, Italy; emails: {andrea.ceccarelli, tommaso.zoppi, ma.mori, andrea.bondavalli}@unifi.it; A. Vasenev, D. Ionita, and L. Montoya, University of Twente, Drienerlolaan 5 7522 Nb Enschede, the Netherlands; emails: {a.vasenev, d.ionita, a.l.montoya}@utwente.nl.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

© 2018 Copyright held by the owner/author(s). Publication rights licensed to ACM.

2378-962X/2018/10-ART18 \$15.00

<https://doi.org/10.1145/3234513>

1 INTRODUCTION

In the cyber-physical System-of-Systems (SoS) paradigm [1, 18, 21], an SoS consists of the integration of independent, autonomous Constituent Systems (CSs), which are networked together to satisfy a global high-level goal under certain rules of engagement. Concisely, domain experts usually identify (i) a micro-level, where CSs operate by themselves and (ii) a macro-level, which describes behaviors that can be achieved only by cooperating CSs.

The role of security is gaining a predominant relevance in modern cyber-physical SoSs [1]. In this article, we focus on *threat analysis*, which is typically carried out as part of the risk assessment process to identify threats, their impact, and mitigations, at an early stage of system implementation [10]. Acknowledged approaches to security, applied also by standardization bodies [10] or governmental agencies [49, 50], carry out threat analysis of systems that are usually seen as static, with no relevant changes to their functional and non-functional requirements during their life. In this context, security properties rarely change during system life and their achievement is supported by identifying threats and corresponding mitigation strategies that typically do not need to be revised.

On the contrary, SoSs pose new constraints to the threat analysis processes [2], especially regarding their (i) *evolutionary* nature and (ii) *emergent* properties. *Evolution* refers to long-term changes required to accomplish variations to the requirements in light of an always-changing environment [3]. *Emergence* is a phenomenon that appears at the macro level of an SoS and it is new with respect to the non-relational phenomena of any of its proper parts at the micro level (CSs). Emergent phenomena can be of a different nature: either beneficial or detrimental [18, 14]. A typical example of detrimental emergence can be observed in automotive complex systems composed by cars that may decide to take the same highway to reach their destination, thus leading to traffic jams. If we only look at the single CSs without considering their relational phenomena we cannot be aware of the potential negative consequences. To this end, it is required to identify not only the misbehavior of individual or coordinated CSs, but also the detrimental behaviors described by emergent phenomena that appear at the macro-level of the SoS after an evolution step of the SoS. Lastly, threats should be associated with appropriate mitigation strategies in order to support the dynamic achievement of the security properties. Further, emerging phenomena are at the same time leveraging on the exploitation of composable [51] properties of SoS, and promoting such properties, especially for the service and architectural levels of abstractions. Freedom in composition allows for self-organized system reconfiguration such that the system is able to perform optimally in case new functionalities become available and previously existing one become unavailable. The existence of emergence itself is favored by such loose composition, while being able to manage emergence may allow predicting the effects of composition on dependability, safety, security, availability [18]. Additionally to the above observations, emergence may also break the expected rules for compositionality [52]; especially, unexpected emergence phenomena may change the meaning of system parts, or the syntactic rules by which system parts are combined, which determine system compositionality.

As a result, most of the existing threat analysis processes as [10] do not fit into SoS requirements because they are not able to capture the variations to the security requirements which have to be met in order to achieve safe and secure SoS evolutions. In addition, classical approaches do not primarily focus on risks associated with how autonomous CSs may interact with each other, leading to emergent phenomena. Such classical approaches generally fail to adequately capture the complex relations between SoS evolution, emergence phenomena and security requirements. Such challenges are already partially tackled in [5, 6, 7, 8], where the authors proposed risk assessment approaches devoted to evolving systems.

More specifically, in this article, we present a methodology which supports an *evolutionary threat analysis* by focusing on emergent phenomena originating in an evolving cyber-physical SoS. Detecting and analyzing emerging properties of an SoS may lead to identifying future threats to the achievement of existing security properties. Our methodology allows us to (i) identify threats arising from the planned SoS evolution and (ii) propose adequate mitigation strategies to SoS administrators. Such methodology is supported by a tool that encodes: (i) a mapping between both cyber and physical threats and the system evolutions and (ii) the behavior or the amount of CSs constituting the targeted SoS. By automatically detecting emergent behaviors and consequently identifying novel threats, the tool aims at reducing the *cognitive load*—or rather the total amount of mental effort being used in the working memory [28]—required from the *Risk Assessment* (RA) analyst.

The methodology and the supporting tool are evaluated by considering power grids as a specific category of SoS: (Smart) power grids are an ensemble of electric components, communication nodes, critical infrastructures, and human-made policies that are networked together to achieve high-level goals such as the continuous provision of energy to all the grid components. Analyzing effects of the interconnection among these components is often complex. RA experts need significant amounts of time and efforts (including *cognitive load*) to complete such tasks. We first submitted an evolving Smart Grid SoS scenario to a group composed of 18 BSc and MSc students and we tasked them to perform several security-related analyses either with or without our methodology and the supporting tool. Then, we conducted a separate gaming session with three stakeholders, namely a *City Planner*, a *Distributed Network Operator*, and a *Citizen&Business Representative*. In both sessions, we asked participants to fill out questionnaires aimed at evaluating the difficulties they encountered in completing the tasks above. In addition, the questionnaires aimed at measuring usability factors, such as efficiency and difficulty, which are indicators of the cognitive load [29, 30]. Results show that applying our tool for identifying threats was perceived well, while students critically reflected on its strengths and weaknesses and stakeholders discussed the market opportunities and future improvements of the tool.

This article starts with basics on SoSs and SoS security in Section 2. Section 3 instead presents related work to threat analysis in complex systems and SoSs, and positions our article with respect to the surveyed works. In Section 4, a motivating Smart Grid scenario, inspired to the campus of the University of Twente in the Netherlands, is presented, and it will be used as running example to explain the methodology. The methodology is discussed in Section 5 and Section 6. The supporting tool is presented in Section 7, while the results of the users' base assessment are described in Section 8. Finally, in Section 9, we conclude the article.

This article extends our preliminary work [21] on a methodology for threats assessment that captures the relations between security and emergence in an SoS. The novel contributions we introduce in this article lie in (i) the introduction of cognitive load as dimension of analysis, (ii) a revision of the methodology, (iii) its application to a different and more relevant case study, i.e., investigating the power grid underlying the campus of the University of Twente (Section 4), (iv), an elaborated description of the tool features (Section 7), and (v) a validation phase with the involvement of both expert and non-expert users (Section 8).

2 BASICS ON SYSTEMS OF SYSTEMS AND SECURITY

2.1 Systems of Systems

We adopt the definition of SoS from [1]: An SoS is an integration of a finite number of constituent systems (CS) which are independent and operable and which are networked together for a period of time to achieve a certain higher goal. In this article, we refer to cyber-physical SoSs; for readability, we will often omit the term “cyber-physical”, whenever it is clear from the context. An SoS is

composed of both hardware and software systems, communication systems, physical machines, and humans.

It defines the structure of its composition and the behavior to help reduce the *cognitive complexity* of the system, or rather the mental effort required in order to understand a given scenario for the given purpose by an identified user. The time it takes for an average representative from the intended user group to understand the system is linked to its cognitive complexity [28, 29]. The understanding and analysis of the immense variety of items and their behaviour in the non-living and living world surrounding us requires appropriate modeling structures that must limit the overall complexity of a single model and support the step-wise integration of a multitude of different models. One such widely identified modeling structure is the *multi-level hierarchy*, where each level of a hierarchy possesses its unique set of laws. A multi-level hierarchy is a recursive structure where a system, the *whole* at the level of interest (the *macro-level*), can be taken apart into a set of constituent sub-systems that interact statically or dynamically at the underlying level (the *micro-level*). Each of these sub-systems can be viewed as a system of its own when the focus of observation is shifted from the level above to the underlying one, while this recursive decomposition ends when the internal structure of a sub-system is of no further interest. As a remark, it is acknowledged that if there are important systems in the world that are complex without being hierarchic, they may to a considerable degree escape our observation or understanding [47].

One key characteristic integrated in the paradigm of SoSs is their evolution. Evolution can be defined as the gradual and progressive process of change or development, resulting from changes in its environment (primary) or in itself (secondary) [22]. Evolution includes all the changes that have been introduced to accommodate modified or brand new requirements by means of including, removing or updating system functions [17]. Large scale Systems-of-Systems (SoSs), such as those related to infrastructures, e.g., chemical plants, railways, and power grids, tend to be designed for a long period of usage, e.g., 10 or more years. Over time, the demands and the constraints put on the system will likely change, as well as the environment in which the system operates [22].

Another fundamental phenomenon of an SoS is *emergence* [18, 19]. From [18], we define that a phenomenon of a whole at the macro-level is *emergent* if and only if it is of a new kind with respect to the non-relational phenomena of any of its proper parts at the micro level (e.g., the CSs). An emergent phenomenon manifests when CSs act together, and it is not observable by looking at single CSs separately, and [46] is always associated with levels of a multi-level hierarchy as expanded above. When it is possible to apply strict verification and validation processes to an SoS, the amount of emerging phenomena is expected to be very low or even null [48]. In general, in these SoS, all participating CSs and interactions are well known before the SoS is put into operation. An example would be the set of control systems in an unmanned rocket, that is a *directed* SoS, i.e., an SoS with a central managed purpose and central ownership of all CSs [22]. Instead, in *evolutionary* SoSs CSs are collaborating without strict rules or without a single coordinator. Therefore, it is not easy to perform a satisfactory verification and validation at the macro-level, and emerging phenomena may arise [46]. This is most likely in *acknowledged* SoSs, where there are independent ownership of the CSs (but cooperative agreements among the owners to an aligned purpose), and *collaborative* SoSs, that are characterized by the voluntary interactions of independent CSs to achieve a goal that is beneficial to the individual CS [53].

As an example of emergence, let us consider that in today's electronic financial markets, an electronic trader can execute more than 1,000 trading operations in a single second. The actions of a multitude of human traders and automated trading systems at the micro-level cause the valuation of the assets at the macro level which in turn influences the actions of the human traders and the algorithms of the automated trading systems, thus forming causal loops and cascade effects that can result in emergent misbehavior. In [40], the authors report about such a misbehavior of the

stock market, called the Flash Crash on May 6, 2010: "... in the span of a mere four and half minutes, the Dow Jones Industrial Average lost approximately 1,000 points."

The purpose of building a System-of-Systems out of its CSs is to realize new services that go beyond the services provided by any of the isolated CSs. Emergence is thus at the core of SoS engineering [18]. Emergent phenomena can be of a different nature, either *beneficial* or *detrimental*. Managing emergence is important to realize *beneficial* emergent phenomena, being usually the higher goal of an SoS [19]. At the same time, managing emergence is essential to avoid undesired, possibly unexpected situations generated from CSs interactions that is, *detrimental* emergent phenomena. For example, when novel evolution or emergent phenomena arise [20], an SoS may be exposed to new *security* threats [21]. Summarizing, it is necessary to identify detrimental emergence phenomena in a timely manner, such that proper countermeasures, including security-related, can be planned.

2.2 Threats Classification in Cyber-Physical Systems of Systems

The CS of an SoS may be subject to hazards and threats that are typical for the specific CS class. When a CS becomes part of an SoS and it is coupled with other CSs, it can be exposed to a growing number of hazards and threats. Indeed, exposing an interface to participate in the SoS may introduce new security concerns since it exposes the CS to additional attacks achievable through the interdependencies [16] among the interconnected and cooperating CSs. Consequently, it is necessary to understand potential failure propagation, attack paths and the impact of security violations on the connected CSs.

Thus, exposure to security threats in cyber-physical SoS constitutes a challenging topic [35]. When dealing with critical systems or infrastructures, the exploitation of security weaknesses may lead to serious consequences. There are several examples in recent literature. Just to mention a few, new generation TVs—*Smart TVs*—integrate an operating system and an Ethernet connection, allowing them to offer more features to the users. The embedded operating system may contain vulnerabilities that could be exploited by an attacker [41], compromising the whole *Home Area Network*—the macro-level—or other *Smart Appliances* that are connected to the Smart TV, which instead represents the micro-level of such SoS. Biomedical researchers were able to hack defibrillators, reprogramming the compromised device to shut down intermittently, and to deliver potentially fatal levels of electricity [37], while outages in power grids are often due to malicious activities [38].

Thus, taking into account malicious actions as intrusions into communications and control systems becomes a critical step during both the design and the assessment of cyber-physical SoS, especially when they provide critical services [36]. To such extent, several threat analysis and risk assessment approaches were proposed, providing methodologies and tools to support the identification of risks also considering their societal impact [39]. Threats—and consequently *risks*, which are a function in the degree of likelihood and impact of a threat [10]—can be classified in two different groups, depending on the way they threaten a system. In more detail, we propose a distinction between *emerging* threats, and *structural* threats. Emerging threats are events originated by malicious attackers who exploit interactions among different subsystems constituting the cyber-physical SoS. Examples include, but are not limited to, communication interception (e.g., man in the middle), device compromise, and *tunneling* attacks that are made possible by the introduction of new components or new functionalities, that create novel ways of interaction within the SoS. Structural threats, instead, refer to the attacks that target a specific component without considering its interaction with other entities of the SoS. Examples may include a physical attack on a component (e.g., sensors tampering), or exploiting a firewall vulnerability to penetrate the internal network of a company.

3 RELATED WORK

Most of the approaches supporting the achievement of security requirements aim at conducting threat analyses focusing only on *static cyber-physical systems*. Depending on the specific system, available standards lack strict guidance that domain experts should follow when dealing with evolving SoS and, therefore, with possible emergent behaviors. As example, in the Smart Grid domain, IEC and NIST respectively defined a roadmap [24] and a guideline document [25] but they do not provide any standard methodology for conducting cyber-threat analysis of energy control systems. In addition, the NIST 800-30 standard for conducting risk assessments [10], along with the NISTIR 7628 [11] standard on Smart Grids, provide a consolidated background to such type of analysis but they do not provide guidelines or methodologies amenable for supporting evolution and emergent SoS properties.

3.1 Switch in Threat Analysis Focus

It is generally acknowledged that, depending on the specific system or scenario, the focus of the threat analysis might vary over time. As [4] points out, both the threat landscape and the assets to be protected can change. Previously, the topic of considering the threat landscape was addressed from the attack perspective. For instance, the *TREsPASS* project constructed the attack navigator map as an approach to reduce the complexity of systems [13]. Specifically, this constitutes an effort to bridge the gap between complexity of real systems and the limits of human perception by using a concept familiar to all of us, namely spatial navigation. Key features aiming to reduce complexity are attacker profiles and *attack pattern libraries* (APL).

3.2 Threat Analysis in Evolving Cyber-Physical Systems

Even though some approaches do consider evolving scenarios and aim at providing different type of assurances, they often do not consider (safety and) security. For instance, the approach presented in [5] considers evolving scenarios in detecting recurring software failure patterns. The authors show the utility of considering evolution concerns in the detection process. However, that approach does not concentrate on how the system evolves and how this may affect the process of detecting threats and corresponding mitigation strategies. Evolution properties are considered in [42], where authors explore potential sources of systemic risks in complex SoS by analyzing unique failure modes in a nonlinear dynamic multi-objective sequential decision-making process. The main focus of [42] is to ignore the decisions that may reduce the safety margin of a specific CS within the SoS to withstand unexpected external perturbations due to the interdependencies among CSs. Additionally, in [32], the author lists seven issues and recommendations for companies willing to adopt risk management mechanisms in their SoS-based systems.

However, other solutions do assist the analysis of security threats in evolving scenarios but they do not support the complete threat analysis process [6, 7]. The approach in [6] provides security-based assurances in case of evolution of the basic system functionalities. A monitoring infrastructure alerts users in case they are working in an unsafe zone by applying run-time monitoring system properties, ultimately estimating an acceptable probability of the system operating satisfactorily. However, the latter does not support the enactment of security requirements according to the monitored security threats. The approach presented in [7] supports modeling and analysis of complex networks to mitigate security threats by also enabling the application of security measures. Differences among network states are detected to reveal points of variations, thus triggering updates of both threat lists and corresponding security policies. In [8], the authors present a process for threat analysis of evolving systems by specializing the risk management principles and guidelines of the ISO 31000 standard [31]. Traceability between risk and target system models

is kept to manage evolving security requirements. Nevertheless, the evolutionary threat analysis approaches as [7, 8] are not thought of as SoSs since they do not explicitly consider emergent phenomena originated by evolutions, thus they cannot primarily focus on risks associated on information flows and control among autonomous and interacting CSs.

3.3 Our Contribution

Within the community of experts in power system security, the problems arising from system interdependency stressed the need to extend the power system transient analysis with new approaches able to deal with cascading contingency chains [26]. The intensive networking at the core of advanced grid control favors the occurrence of cascading phenomena in the power system, which emerge from the relation among different grid components. Thus, novel approaches tailored to identify and analyze such emerging phenomena constitute one of the frontiers that are currently requiring attention. This acquires relevance when dealing with threat identification and risk assessment processes, since emerging phenomena may expose the system to novel threats that are not easily detectable otherwise.

This article contributes by reducing the gaps we identified to threat analysis process for evolving systems, considering Smart Grids as a case study for both qualitative and quantitative evaluations. With respect to the state-of-the-art works listed above, we state how to generate automatically lists of threats for a complex and evolving cyber-physical SoS by emphasizing the identification of emergent phenomena and related threats. This is intended to fill the lack of details on evolutionary threat analysis processes and support we noticed by examining both risk assessment and Smart Grid standards [10, 11] and research papers discussing on threat analysis approaches for evolving systems [5, 6]. By providing a tool-supported methodology to SoS threat analysis, we aim at reducing the cognitive load required from SoS administrator, consequently leading to (i) performance improvement [29] and (ii) reduction of potential manual errors [30].

4 MOTIVATING SCENARIO: SMART GRID

As discussed in the Introduction, we consider *Smart Grids* as reference SoS for evaluating our methodology and the supporting tool. Smart Grids are power grids which integrate in a cost-efficient way the behavior and actions of all users connected to it—producers, consumers and those that do both—in order to ensure a sustainable power system with high levels of quality, safety, and security of supply [12]. These systems are subject to topology or policy updates, or rather *evolutionary steps*, which evolve functional requirements possibly leading to expose novel security breaches that can be exploited by malicious attackers. Once an evolutionary step is defined, city planners or stakeholders have to deal with the novel threats introduced by that topology or policy changes.

Our case study investigates the grid underlying an area of the campus of University of Twente in Enschede, the Netherlands. We used this grid as the case study since most of the students who participated in our experiments (Section 8) attended courses at that university. The students suggested possible future evolutions of an existing grid model, acting the role of a city planner who is tasked to figure out how the campus will develop in the next few years. To assist them in this process, the students were introduced to the idea that the future grid can be characterized by two aspects: (i) *smartness*, if the grid incorporates many smart components or not and (ii) *regulations*, whether the grid operates under strict regulations or not (highly regulated/low regulated). Figure 1.S1 represents a high-level model of the current campus grid topology. This *Initial Scenario* consists of a power grid supporting the *Smart Homes (SH)* energy consumption, their internet connectivity through a shared *Access Point (AP)*, the functional activities of an *Office (O)*, a *Data Centre (BDC)*, and a *Hospital (H)*, all requiring energy, and finally a *Carbon Power Plant (PP)* producing the energy required for the other constituent systems. A *Mid-Low Voltage Substation (SS)* supplies

Fig. 1. First (S1), second (S2) and third (S3) evolutionary steps for the motivating Smart Grid scenario of the campus of University of Twente.

low voltage to *SH*. The data connection (line connected to the AP in Figure 1) exists between few buildings, enabling smart controls such as the advanced monitoring of energy consumption.

Based on the *Initial Scenario*, the students suggested the two possible subsequent evolutionary steps we depicted in Figure 1.S2 and Figure 1.S3. Since the number of university employees is expected to increase, the students suggested *Adding Resources* (see Figure 1.S2), or rather new *SH* components representing more housing facilities for students. This also implies a greater energy demand, which is balanced by adding a *Photo Voltaic Generation (PVG)* source within the campus. The usage of green energy, which is encouraged by local authorities in the Netherlands, motivated also the last evolution step (*Decarbonisation* in Figure 1.S3), where the carbon power plant was replaced with another PV source.

We consider the employed grid model to be a motivating example, which we built with the aid of both students and technical personnel working at the University of Twente. Certainly, both students and technical personnel did not know all the insights of the grid topology, ultimately leading to building a grid model containing several high-level approximations. This motivating scenario is used as a case study to validate the methodology proposed in this article.

5 PROPOSED THREAT ANALYSIS FOR AN EVOLVING SOS

In order to provide safety and security requirements for SoSs, it is essential to analyze the interdependency regulating the flow of information among entailed CSs. As remarked in Section 3.3, interactions among CSs may generate emerging phenomena, which represent possible security threats and damages.

Fig. 2. Methodology for evolutionary threat analysis.

The methodology for the evolutionary threat analysis proposed in this article adopts the guidelines defined from NIST in the SP 800-30 [10] regarding both the approach to be followed and the main steps to be performed for validating the threat analysis. In particular, we exploited an *asset-oriented* approach as defined in the NIST standard by identifying (i) first, critical or updated assets of the SoS and then (ii) the related threat events, i.e., the internal behavior of a CS and their possible interactions. In contrast to the NIST standard, we supported an incremental threat identification process carried out after the SoS evolution through evolutionary steps. The methodology uses a threats list and a set of mitigations, which need to be instantiated depending on the specific target system.

5.1 The Methodology

Considering each evolution step as a set of addition, removal, or change of assets, our approach identifies the threats which can arise due to this scenario's evolution. Consequently, the mitigation strategies to apply/remove are identified according to their threats traceability. The steps of our methodology (see Figure 2) are:

- *Setup/Evolve the Scenario.* The initial scenario (1.A) or the evolution step (1.B) is loaded and merged with the previous scenario (if any). The current scenario is then analyzed to detect new or removed assets, e.g., the addition of SH and PVG in the “*Adding Resources*” scenario in Figure 1.S2;
- *Identifying Structural Threats.* Considering only the updated assets, we look at the considered threats list to understand if the updated assets carry one or more intrinsic (*structural*) threats, which are introduced in the scenario with the addition of the new assets;
- *Identifying Emerging Threats.* Here we investigate the interactions between the novel or removed assets and the others in the scenario, identifying threats due to complex emerging behaviors, e.g., two components of a power grid competing against each other for acquiring energy;
- *Merge and Mitigate.* The novel structural and emerging threats are merged and added to the partial results of the process. Following this, each threat is linked to its corresponding mitigations.

Once all the evolution steps are analyzed, all the results coming from each iteration of the process are merged and added to the *identified threat* list, which contains information about threat

Table 1. Threats Identified by Applying the Methodology to the Motivating Smart Grid Scenarios

Threats				Mitigations	
#	Name	Type	CS	Motivation	# Names
14	Compromise software of organizational critical information systems.	ST	PP	Adversary inserts malware or otherwise corrupts critical internal organizational information systems.	4, 5, 19 Security Assessment and Authorization, Configuration Management, Smart Grid Information System and Information Integrity
32	Earthquake at primary facility	STR	SS	Earthquake of organization-defined magnitude at primary facility makes facility inoperable.	-
18	Conduct Denial of Service (DoS) attacks	EM	AP, H	Adversary attempts to make an Internet-accessible resource unavailable to intended users, or prevent the resource from functioning efficiently or at all, temporarily or indefinitely.	4,6,10 Security Assessment and Authorization, Continuity of Operations, Smart Grid Information System Development and Maintenance

events concerning (i) the threat type, (ii) its nature, either structural or emerging, (iii) affected CSs, and (iv) corresponding mitigations strategies.

It is worth noting that since it is very difficult to link a threat event with a reasonable quantitative evaluation of its impact and likelihood in such a generic context, we will not weigh the degree of harm and likelihood of threats' occurrences. These quantities can be added by the security experts that examine a specific scenario, knowing all its assumptions and the critical factors that are contributing to the occurrence of the threats. As a result, our focus in this study is not on risks; instead, we focus on the identification of threats and their corresponding mitigation strategies.

5.2 Applying the Methodology to the Smart Grid Scenario

Based on the Smart Grid scenario, we show how the methodology can be applied to support threat analysis of an SoS. As reference threat and mitigation lists, we considered the work done in the context of the IRENE project [34]. Here the authors of the cyber-security analysis of smart grids [12] derived a list of 38 threats to the urban grid mainly due to cyber-security (i.e., 29 cyber-security threats and 9 related either to environmental and accidental threats) based on the NIST 800-30 [10] guidelines. We chose to adopt this reduced list instead of the original one since at such high abstraction level it is not necessary to have detailed information about specific categories of threats, e.g., we cannot distinguish between a *Denial of Service* (DoS) attack and a *Distributed DoS*. Moreover, in IRENE, each threat is mapped with a set of possible mitigations, which are extracted from the NISTIR 7628 [11] security requirements. This set of mitigations is particularly suitable in the cyber domain; depending on the specific focus of the threat analysis (e.g., human faults, environmental), the set of mitigations can change.

As an example, Table 1 shows a partial outcome of applying the proposed methodology to the scenarios presented in Section 4. Each row shows a numeric identifier of the threat as shown in the IRENE threat list [12], the name, the type (either structural or emerging), the involved CSs, a textual motivation and several linked mitigations with their identifiers. Two of the threats presented in the table are intrinsic to *PP* and *SS*; therefore are classified as structural (ST), differing from the last one that is classified as emerging (EM). The “DoS” threat, which emerges from the interconnection

between two components, represents an attacker that uses the public AP—which is networked with other components—to conduct such an attack against the hospital (H). We can also notice how the “*earthquake*” threat affecting the SS component is not linked to mitigations. Since this is an environmental threat, we could not match it with any of the available mitigations since these are explicitly directed to cyber-security threats.

6 MODEL FOR THREAT ANALYSIS

Following a feature engineering perspective [15], we describe an evolving SoS as one which provides a set of features at each evolutionary step. A feature is defined as $f = (CS, T, M)$, where

- CS is the set of required constituent systems to provide the functionalities. In a given scenario S , each element $cs \in CS$ contains a set of structural threats defined as $cs.T^S$;
- T^ϵ entails the set of emerging threats;
- M is the set of mitigation strategies which have to be activated in a given scenario S_i to mitigate the threats in $(\cup_{x \in CS} x.T^S) \cup T^\epsilon$.

We define the set of scenarios $S = \{S_0, S_1, \dots, S_n\}$, each represented as a combination of features that have to be provided by the SoS. A set of emerging threats $T_{S_x}^\epsilon$ arising among CSs belonging to multiple features, corresponds to each scenario S_x .

6.1 Evolutionary Threat Analysis

The SoS evolution process is started by the SoS administrator who desires to change a set of features to satisfy modification in the user needs. This process is formalized by Algorithm 1 describing the evolutionary threat analysis from the current to the target scenario. The algorithm determines the current set of threats affecting the evolved SoS and it determines their corresponding mitigation strategies. The first step consists of computing the set of features to be added (line 1) and to be discarded (line 2). Following this, it computes the set of threats that arise in the evolved scenario by considering structural T_{target}^S (lines 4–6) and emerging T_{target}^ϵ (line 7) threats and it collects their corresponding mitigations M_{target} (line 8). For each feature to be added, it collects the set of structural $T^{S,+}$ (lines 11–13) and emerging threats $T^{\epsilon,+}$ (line 14) by neglecting the ones that have been already mitigated in the current scenario, i.e., T_{curr}^S and T_{curr}^ϵ . For each feature to be deleted, the algorithm computes the set of structural $T^{S,-}$ (lines 17–19) and emerging $T^{\epsilon,-}$ (line 20) threats that are no longer present by neglecting the ones which are still in the target scenario T_{target}^S and T_{target}^ϵ . The next step consists of updating the already computed emerging threats to be added and deleted with the ones arising from the features interactions, i.e., $T_{S_{target}}^\epsilon$ (lines 22–23). Finally, the algorithm applies function *Mitigate*: $2^T \rightarrow 2^M$ which, taking as input the set of threats in T , determines the corresponding mitigation strategies to be applied among the ones in M . To compute the required strategies, we consider those necessary for the additional set of structural $T^{S,+}$ and emerging $T^{\epsilon,+}$ threats, by neglecting the ones already implemented in the current scenario M_{curr} (line 24). The mitigations to be discarded are computed as those required by threats in $T^{S,-}$ and $T^{\epsilon,-}$ by neglecting those that have to be included in the target scenario M_{target} (lines 25–26).

6.2 Analyzing the Smart Grid Scenario

Based on the “*Initial*” scenario in Figure 1.S1, we identified, among others, the following set of features. $F_{Household}$ is the household energy consumption, $F_{Internet}$ provides the household internet connectivity, F_{Office} represents the working activity of the office, and finally $F_{CarbonProd}$ is the carbon energy production due to the power plant. Table 2 reports for each feature the set of required CSs, their affecting threats, both structural and emergent, and the amount of corresponding mitigation

Table 2. Threats Related to Features of “Initial” Scenario

Feature	CSs	#Threats	Threat Listing	#Mitigations
F _{Household}	SH	12	{1,3,4,6,9,11,15,23,24,29,30,33}	37
F _{Internet}	SH, AP	14	{4,9,11,14,16,18,19,23,24,29,30,31,33,37}	44
F _{Office}	O	23	{2,3,4,5,7,8,9,12,13,14,19,20,22,23,25,26,29,30,32,33,34,35,37}	51
F _{CarbonProd}	PP	16	{3,5,6,7,8,14,19,22,26,27,28,30,32,33,34,35}	38

ALGORITHM 1: Evolutionary Threat Analysis

Require: The current scenario S_{curr} affected by the structural T_{curr}^S and emerging T_{curr}^ϵ threats, their corresponding mitigation strategies M_{curr} and the scenario to achieve S_{target}

Ensure: The mitigation strategies to add M^+ and remove M^-

```

1:  $\delta_F^+ = S_{target} - S_{curr}$ 
2:  $\delta_F^- = S_{target} - S_{curr}$ 
3: for all feature  $f \in S_{target}$  do
4:   for all  $cs \in f.CS$  do
5:      $T_{target}^S = T_{target}^S \cup cs.T^S$ 
6:   end for
7:    $T_{target}^\epsilon = T_{target}^\epsilon \cup f.T^\epsilon$ 
8:    $M_{target} = M_{target} \cup f.M$ 
9: end for
10: for all feature  $f \in \delta_F^+$  do
11:   for all  $cs \in f.CS$  do
12:      $T^{S,+} = T^{S,+} \cup (cs.T^S - T_{curr}^S)$ 
13:   end for
14:    $T^{\epsilon,+} = T^{\epsilon,+} \cup (cs.T^\epsilon - T_{curr}^\epsilon)$ 
15: end for
16: for all feature  $f \in \delta_F^-$  do
17:   for all feature  $cs \in f.CS$  do
18:      $T^{S,-} = T^{S,-} \cup (cs.T^S - T_{target}^S)$ 
19:   end for
20:    $T^{\epsilon,-} = T^{\epsilon,-} \cup (f.T^\epsilon - T_{target}^\epsilon)$ 
21: end for
22:  $T^{\epsilon,+} = T^{\epsilon,+} \cup T_{target}^\epsilon$ 
23:  $T^{\epsilon,-} = T^{\epsilon,-} \cup (T_{curr}^\epsilon - T_{target}^\epsilon)$ 
24:  $M^+ = Mitigate(T^{S,+} \cup T^{\epsilon,+}) - M_{curr}$ 
25:  $M_{target} = M_{target} \cup Mitigate(T_{target}^\epsilon)$ 
26:  $M^- = Mitigate(T^{S,-} \cup T^{\epsilon,-}) - M_{target}$ 

```

strategies. For example, regarding $F_{CarbonProd}$, threat 14 consists of unauthorized access to the critical control software of the PP (see Table 1). The corresponding mitigations are the management of configuration (mitigation 5 in [12]), monitoring facilities, and malware detection policies, i.e., mitigations 4, 19. Emergent threats may involve features $F_{Internet}$ and F_{Office} , considering that employees can get access to their organizational data from home. Under this assumption, attackers can perform sniffing (threat 6 in [12]), communication interception, e.g., threat 15, 21 (*Man in the*

Table 3. Threats and Novel Features of “AddingResources” Scenario

Feature	CSs	# Threats	Threat Listing	# Mitigations
$F_{GreenProd}$	PVG	16	{3,5,6,7,8,14,19,22,26,27,28,30,32,33,34,35}	38

Table 4. Evolutionary Threat Analysis (Smart Grid scenario)

Evolution Step	#F ⁺	#F ⁻	#T ⁺	#T ⁻	#T ^{ε,+}	#T ^{ε,-}	#M ⁺	#M ⁻
(Baseline) Initial	6	-	194	-	75	-	578	-
Initial → AddingResources	3	0	77	0	53	0	139	0
AddingResources → Decarbonisation	1	1	23	23	5	5	47	47
Initial → Decarbonisation	4	1	100	23	58	5	186	87

Middle - MiM) or they can exploit tunnels or unexpired sessions that the employee did not close properly (threat 10). A possible mitigation to these attack is to implement mitigation 18 “*Smart Grid Information System and Communication Protection*”, aimed at defining specific policies or protocols to close all unused connections.

Switching from “Initial” to “AddingResources” scenario by implementing the evolution step requires an additional set of features to be considered. We report in Table 3 the novel features to be added. This includes the $F_{GreenProd}$ feature, which describes the renewable energy production and it is the unique novel feature arising from the current scenario. It can be noted that, considering the threats list we adopted, the threats related to the $F_{CarbonProd}$ feature are the same of the $F_{GreenProd}$ feature. Both features are related to components (PP and PVG) that provide energy to the connected buildings, and they are exposed to the same subset of threats. In addition, this evolution step describes an increasing number of students, which results in the building of more houses. This is described with the $F_{Household}$ feature, which we summarized in Table 2. In this case, threats related to $F_{Household}$ are duplicated, since they refer to different SH components. The last evolution step completes the “Decarbonisation” of the area of the campus described in our Smart Grid scenario. More detailed, the carbon power plant is replaced by a PV power plant, meaning that a $F_{GreenProd}$ feature replaces an existing $F_{CarbonProd}$ one. This completes the 2-step evolution of the initial scenario that we analyzed using our methodology.

Lastly, Table 4 summarizes how the sets used in Algorithm 1 change through the application of the methodology to the scenarios we used as case study. In the table, we can see how the features (sets F⁺, F⁻) related to the scenarios are evolving, by impacting both the amount of structural (T⁺, T⁻) and emerging (T^{ε,+}, T^{ε,-}) threats and the linked mitigations (M⁺, M⁻ sets). As mentioned before, by switching from “AddingResources” to “Decarbonisation” scenario, we are removing the $F_{CarbonProd}$ feature and adopting the $F_{GreenProd}$ one, which have the same amount of related threats (16) and mitigations (38). In Table 4, we can observe that this change leads to the removal of and consequently to the addition of 23 structural threats, 5 emerging threats, and 47 mitigations. These amounts, e.g., 47 mitigations, are higher than the ones related to single features since removing or adding a feature involves the removal or the addition of electric circuitry, e.g., wires, that are used to connect buildings to the existing grid. These components, along with the buildings, can be targeted by cyber-attacks and therefore have their related threats and mitigations, affecting the size of the T and M sets.

6.3 Scenario-Based Analysis of Threats Distribution

Given the set of input scenarios that are affected by the set of structural and emerging threats, we are interested in exploring the distribution of such threats across the scenarios. It is important

Fig. 3. Threats' distribution in the Smart Grid scenario.

to detect which threats affect all the input scenarios and which are very specific since they only affect just a few possibly evolutionary scenarios. Having such information, an SoS administrator is able to evaluate the relevance of threats thus having a decision-making support to drive the SoS evolution. To this end, we propose to apply the *Formal Concepts Analysis* (FCA) [9] in order to identify groups of objects sharing common attributes. FCA supports the definition of a formal context $C = (Obj, Att, Rel)$ where Obj is the set of objects, Att is the set of attributes and $Rel \subseteq Obj \times Att$ is the relation between objects and attributes. In our case, objects are the scenarios, while corresponding attributes are the set of relevant threats in each scenario. By adopting an FCA analysis we can easily know which are the scenarios affected by a certain threat and consequently detecting if some threats are very frequent, i.e., appearing in almost all the scenarios, or not, i.e., appearing just in a few scenarios. This implies two important facts. First, scenarios can be put in a hierarchical relationship depending on the impacting threats: a scenario is a child of another scenario if all the threats affecting the father scenario are affecting also the child. Another implication regards a possible association of costs to the implementation of mitigations. Having such a FCA structure allows the identification of which threats are changing from a scenario and another, and consequently how much money is required to implement new mitigations in order to avoid or mitigate novel threats.

The FCA output resulting from the application of our methodology to the scenarios in Section 4 is depicted in Figure 3 and expanded in Section 7.2.

7 TOOL SUPPORT

The methodology presented in this paper has been implemented in a supporting tool along with the proposed algorithm determining the variation of mitigation strategies and the scenario-based distribution analysis. It makes use of the *Colibri-Java* FCA API¹ to analyze the distribution of threats. The tool takes as input the evolutionary scenarios defined in terms of features and the mapping between threats and their corresponding required mitigation strategies. A list of structural threats related to each component is also provided as input, along with information regarding threats that may emerge in the grid. For example, an attacker that may want to get into a network may need to access a public access point (see AP component in Figure 1), and use this component as a starting point to exploit vulnerabilities and conduct *tunneling* or *MiM* attacks. Such information, if exists, is linked to each threat in our list, and is used by the tool to identify possible emerging threats by analyzing the grid scenario that is given as input. As a remark, the tool is meant to discover possible emerging threats that will impact the grid scenario, while the structural threats are given as input and simply reported in our analysis for completeness.

¹<https://code.google.com/archive/p/colibri-java>.

Lastly, according to the methodology it implements, the tool outputs a list of threats that may arise at each evolutionary step, in association with a suggested set of mitigations the SoS administrator may want to apply.

7.1 Tool Characteristics

Inputs. The tool requires the following inputs: (i) a list of threats, (ii) a list of threat categories, (iii) a list of mitigations, (iv) a list of grid components, (v) the mapping between components and structural threats, (vi) information about emerging threats, and (vii) a (set of) scenario including a grid topology. Concisely, the *list of threats* and *threat categories* define the threat model, or rather the threats that the user is taking into account for the specific study, e.g., cyber-security or environmental. The *mitigations* are a set of strategies that can be instantiated and implemented on a specific grid to mitigate or avoid the detrimental effects of threats. This information is therefore used to analyze a *grid scenario*, which can be either brand new or an evolution of a previously analyzed one. In both cases, the grid scenario is defined as a grid topology that is composed of the components in the *components list*, complemented with several assumptions about the city scenario under investigation, e.g., seismic zone, prone to terrorism.

Outputs. The output of the tool is provided both in terms of a list of identified threats and a FCA file. In particular, some files listing the threats identified in each grid scenario given as input are provided, with several mitigations that can be applied to each of the identified threats. Moreover, consider threats happening in a scenario as a formal relation between two components, i.e., threats and scenarios allow viewing the results of the threat analysis as a FCA structure. This helps define a hierarchy for the involved grid scenarios. The hierarchy is based on the threats that can arise in each scenario: a grid scenario is an ancestor of another one if its possible threats are a subset of threats that occur in the child scenario.

Code, Language, and Interfaces. We chose Java as reference platform since it is not OS dependent and since other tools in the IRENE [34] toolset were developed with the same language. Nevertheless, the tool doesn't have a graphical interface since it is intended to be used in cooperation with other tools by the toolset above that offer a graphical user interface. However, the tool can be considered as a standalone resource that has its inputs and outputs into text files. This allows a simple integration with other tools that can read and write the input and output files to tune the preferences of the threat analysis tool according to their actual needs. Code quality was checked using FindBugs [27], which was tuned to identify the following bug categories: *security flaws*, *bad practices*, *dodgy code*, and *multi-threading correctness*.

Computational Complexity. The tool implements a simple methodology; consequently, the complexity of the tool itself does not require deep performance analysis. However, during the CPU-intensive phase—while threats for each evolution step are listed—the tool executes the most expensive tasks in dedicated threads, to not lock the main thread responsible to collect the outcomes of the created threads. This will increase the performances of the tool in workstations where several (physical or virtual) CPUs are available. The management of such threads is left to the Java scheduler, which runs a preemptive priority-based algorithm. Summarizing, the tool performs satisfactorily with the scenario's inputs, given that it is polynomial with respect to the inputs. Consequently, we expect to have an acceptable scalability to larger scale Smart Grids.

7.2 Executing the Tool

We applied the tool to the Smart Grid scenario introduced in Section 4. In particular, Figure 3 represents the distribution of threats across the scenarios of our case study. Each node of the

figure represents parts of scenarios sharing the exact same set of threats. The upper-level node contains the threats affecting all the scenarios, i.e., the ones that should be always mitigated. On the contrary, the lower-level node contains all the threats that are affecting at least one scenario. In our case, 56.4% of threats affect all the three scenarios. “Decarbonisation” scenario contains 93.4% of threats among which 86.8% are also present in “AddingResources” scenario. “Initial” scenario contains the 63.0% of threats, thus it is the scenario affected by the lower number of threats. Further details on the tool can be found in [43].

8 USER ASSESSMENT

The validation of the proposed methodology and the tool was first performed during a risk management workshop at the CuriousU summer school at University of Twente, and then during a stakeholder workshop conducted at Power Networks Demonstration Centre (PNDC) in Glasgow, Scotland. Students attending the first workshop (student workshop) are not experts in the field. However, as can be seen later, the questionnaires are mainly directed to assess features such as perceived difficulties in key steps of the process, clarity of the overall process, and perceived usefulness of the overall process. Since we expect RA results being shared with other non-domain experts, e.g., city planners, to progress with the process of collaborative planning, these aspects need to be very clear to everyone, motivating the choice of non-expert people as user-base of our assessment. Differently to student workshop, the stakeholder workshop was focused on gaming simulations. The goal of this workshop was to assess scalability of the methods and tools developed in the IRENE project (including the threat analysis tool described in Section 7) by taking advantage of the expertise of the three stakeholders who attended the workshop.

8.1 Student Workshop

In the student workshop, we asked participants to rate and discuss: (i) the structure and possible evolutions of the power grid underlying the university campus (related to Step 1 of the methodology in Figure 2) and (ii) the emerging threats identified by the Evolutionary Threat Analysis tool, which are targeted by Step 3 of our methodology.

The novelty of our methodology does not regard the identification of structural threats, i.e., Step 2 of our methodology, as this research topic is already quite advanced. In addition, we did not concentrate on mitigations, i.e., Step 4 of the methodology, as mitigations are domain-specific and they can be evaluated only by experts in a given city scenario. In our experiments, we concentrated on (i) assessing the proposed methodology, i.e., Step 1-related and Step 3 of the methodology and (ii) studying the cognitive load requested to fulfill the task with and without using the associated automated threat identification tool.

In order to assess the methodology, we asked participants to rate the perceived difficulty of defining a grid evolution step, in terms of difficulty to select a future grid scenario and of difficulty to select future grid components, as well as rating the perceived agreement with the evolved grid produced. We asked those questions in questionnaire Q1. In addition, in questionnaire Q3, we asked students to (i) rate the clarity of the overall process and (ii) report the perceived usefulness of the overall process. We describe below the object of study, treatment details and measurement design, finally discussing the results we obtained.

8.1.1 Object of Study. Our population consisted of 18 BSc and MSc students. The students had mixed backgrounds, but shared interest in risk assessment. It is worth noting that skills and experience of these students can be hardly compared to the expected expertise of users of this tool, e.g., security experts or decision makers. However, several similarities allow us to consider the experiment to be relevant to the study. Specifically, students and real decision makers might not be

familiar with our approach in particular or practices of cybersecurity risk assessment in general. In addition, underlying cognitive mechanisms and group dynamics are shared. Furthermore, the students will also allow assessing features related to the clarity of the process and results. Since we expect RA results to be shared with other non-domain experts, e.g., city planners, for the purposes of collaborative planning, it is important that the outputs of the threat analysis are easily understood.

The students were not pre-selected, neither did they choose to follow one treatment or the other. All participants were exposed simultaneously to the same treatment, which is described next.

8.1.2 Treatment Design. The validation session was performed as part of a full-day cybersecurity workshop at University of Twente. During the workshop, participants were first introduced to the topic of information security risk assessment and cyber-threats to urban grids. Afterwards, a simplified model of the grid (see Figure 1.S1) underlying the campus of University of Twente was demonstrated.

Participants were asked to work on the first step of our methodology: evolve the grid. To do so, they discussed possible future grid scenarios and then suitable grid components, finally agreeing on the evolutionary scenarios depicted in Figure 1.S2 and Figure 1.S3. At the end of the grid evolution exercise, each participant received a questionnaire about the task they just performed, i.e., questionnaire Q1 in the next subsection. Following that, the participants were introduced to an informal qualitative risk assessment tool *ArgueSecure* [23]. The goal of this step was to encourage them to identify risk on their own and familiarize themselves with the topic of risk identification. The participants then filled in a questionnaire on usability and utility of the *ArgueSecure* tool, i.e., questionnaire Q2, which is less relevant to this work and is mentioned for the completeness of this subsection. Therefore, the collected data are not reported in this article.

Following that, workshop participants were introduced to the tool described in Section 7. The performance of the tool for analyzing the same evolved campus grid depicted in Figure 1 was demonstrated. In addition, an overview of the emerging threats identified by the tool was given. Furthermore, workshop participants rated the tool according to their impression and resulting risks (questionnaire Q3). Finally, they documented perceived differences between conducting and informal risk assessment (on the example of *ArgueSecure*) and using an automated threat identification tool, such as the tool described in this article (questionnaire Q4). The design of the questionnaires and their results obtained are described and discussed in the following subsections.

8.1.3 Measurement Design and Data Collected. We operationalized the cognitive load required to use our tool in terms of the following indicators: perceived difficulty of using the tool and perceived duration of using the tool. In addition, we focused on perceived quality of the results, measured via Q3. Quality of the results is further decomposed into perceived understandability, correctness and completeness, also measured via Q3. All of the indicators listed above were rated on a 5-point semantic Linkert [33] scale, i.e., ‘Very Easy’, score 1, to ‘Very Hard’, score 5. The participants filled-in each questionnaire individually. Lastly, participants were asked to describe—using free text—how they would improve upon the proposed methodology, as well as discuss how the proposed methodology compares with performing an informal risk assessment with *ArgueSecure* (see Q4).

After the first round of experiments, 17 participants returned Q1 questionnaires. Details of questions are described in Section 8.4, while answers are shown in Table 5 (we numbered Q_{x.y} questions corresponding to *x* questionnaire with cumulative numbering *y* of the question itself). In total, 18 questionnaires were collected after Q3. The answers are described in Table 6.

The open question of Q4.21 (*What do you think are the strengths and weaknesses of each of the two presented approaches*) resulted in the following remarks:

Table 5. Answers to Questionnaire Q1. Q1.1, Q1.2, Q1.3, Q1.5 are scored from 1 - Completely Disagree - to 5 - Completely Agree, while Q1.4 and Q1.6 are Open Questions

Code	Question Text	Answers
Q1.1	<i>Agreement with the future grid</i>	Average (Avg) 3.52, Standard Deviation (Std) 0.51
Q1.2	<i>Difficulty of selecting a future grid scenario using smartness/regulations categories</i>	Avg 3.35, Std 0.61
Q1.3	<i>Are there more scenarios than smartness/regulations categories</i>	7 Yes, 10 No
Q1.4	<i>Remarks about scenario, if question 3=T:</i>	'Culture' (Participant P.1) 'Building energy efficiency' (P.8) 'Considering feasibility (economic) and social acceptability' (P.9) 'Intermediate one, not only low-high' (P.12) '+ houses; electric cars; solar panels' (P.13) 'users (traffic? industry? household?)' (P.16)
Q1.5	<i>Difficulty to select grid components based on the scenario</i>	Avg 2.47, Std 0.94
Q1.6	<i>If the difficulty ≥ 3, please explain why (Open question):</i>	'due to technology policy' (Participant 1) 'very unpredictable' (P.9) 'not aware of the progress of current technologies' (P.10) 'by analysis of recent trends this components are the most expected' (P.13) 'I think any of these can be different from country to country, e.g., politics and economics. Especially for 'solar' solution, I'm not that optimistic, as it brings in a lot of pollution during production' (P.16)

Table 6. Answers to Questionnaire Q3

Code	Question Text	Answers
Q3.14	Difficulty to identify threats with the developed tool	Avg 3.28, Std 1.02
Q3.15	Time needed for a formal RA	3.61, 0.78
Q3.16	Understandability of the result	3.28, 0.96
Q3.17	Correctness of the result	3.67, 0.49
Q3.18	Completeness of the result	3.83, 0.71
Q3.19	How would you improve the tool	'Easier' (Participant 12); 'Consideration of external factors, showing the level of threat of a particular entity' (P.13); 'The language was technical for non-expert in the matter, should be given in customers language not experts language. We know basic stuff' (P.15); 'Introduce a standard procedure that can be applied to different system' (P.16)
Q3.20	Consider a 3-step process: construct grid model; select future components; identify emerging threats	
Q3.20a	Process is clear	Avg. 3.5, Std 0.86
Q3.20b	Process is useful	3.83, 0.99

- “[the tool] may find more risks than [informal risk assessment]”;
- “Weakness: A lot of clarity needs to be laid on how Structural and Emerging Threats are depicted. Strength: Effective in terms of time, cost, and effort”;
- “Weakness: (1) No way to rank threats, (2) Does not consider external factors. Strength: (1) Shows all possible connections, (2) Shows new ideas”;
- “Weakness: Not easily interpretable. Strength: Precise calculation, more computational (more component?)”;
- “[formal assessment using the tool is] more concrete and systematic but covers some of the unseen but possible risks.”

8.1.4 Summary of Results and Discussions. The data reported above reflect Q1, which is related to Step 1 of the methodology in Figure 2, and Q3, which focuses more on the tool and on the identification of threats. Answers related to Q1 indicate that participants agreed with the design of the future campus grid they constructed (participants marked ‘completely agree’ in Q1.1). This can be interpreted as no significant objections against both the initial and the evolved grid configurations being raised. Therefore, we assume that due to the lack of possible objections, such potential disagreement did not heavily influence other answers. Participants indicated some difficulty to choose a particular scenario (Q1.2) and they felt that some aspects of the future might be accounted in addition to smartness and regulatory dichotomies that are described in Section 4 (see Q1.3 and Q1.4). The task of selecting grid components was perceived as being relatively easy (rated as 2.47 out of 5, as shown in Q1.5 and Q1.6). Together, answers to questionnaire Q1 suggest that selecting grid components based on an identified future grid context is feasible, although not free from contradictions.

Answers to Q3 show that the result of applying the tool for identifying threats was perceived well. The result was seen as rather complete (3.83 out of 5, Q3.18) and correct (3.67, Q3.17). The understandability was rated as 3.28 out of 5 (Easy to understand), as the answer to Q3.16 shows. Still, the time needed for a formal RA was quite high 3.61 (when 5 is Very long) and a bit difficult (3.28 out of 5 being Very hard, Q14). Possibly, the participants did not account for re-usability of the tool. The process was perceived to be useful (3.83), and rather clear (3.5). The workshop participants might have understood the process and were able to position the tool within it, although they found it a bit difficult to use. Given that the system analysis is a complex topic, we see the overall results as positive.

From the Q4.21 remarks we can conclude that workshop participants reflected on strong and weak aspects of the formal modeling using our tool. The reflection (i) indicates the need to clearly introduce important constructs, (ii) ensures that interactions with the tool are simplified, and (iii) identifies a way to communicate results with the users in an understandable format. It is worth noting that while the task can be conducted collaboratively, it might require some effort and time to resolve possible misinterpretations and contradictory views. We anticipate that further explanation of scenarios and of the underlying aspects might be needed to make the choice of future scenarios easier.

Finally, we anticipate that the time needed for a formal Risk Assessment was considered in connection to a complete exercise, which includes the grid evolution, configuring the tool input, and interpreting the result. The issue of the tool being able to re-run with slight configuration changes was possibly omitted in the replies.

8.2 Stakeholder Workshop

The *stakeholder workshop* was organized by the IRENE researchers to assess the use of the IRENE methods. Three stakeholders participated in the workshop taking over the roles of City Planner,

Fig. 4. Baseline Scenario for Stakeholder Workshop.

Distributed Network Operator, and Citizen&Business Representative. The stakeholders had extensive expertise with security, private public relations, and consultancy on relevant topics. Software tools were introduced to the stakeholders and it was clarified how modeling tools are intended to improve the resilience of the overall grid. Exercise handouts were given to stakeholders, who collaboratively decided how to introduce new components or modify existing components to improve robustness of a baseline grid scenario (see Figure 4). This scenario was built on the idea of the IEEE 14-nodes grid [45]. The analysis of the three-step evolution of the grid proposed by stakeholders is expanded in the next section, while additional details on the scenarios used in the experiments can be found in [44].

8.2.1 Evolutionary Threat Analysis. According to the methodology in Section 5, we first analyzed the baseline scenario in Figure 4. In particular, the baseline scenario represents a basic setup and, consequently, all the components, i.e., 34 buildings and 33 connections, are considered as newly added. Our ETA tool identifies 1220 threats from the IRENE threat list that can impact the grid. 69.9% are structural threats, while the remaining 30.1% emerge due to interconnections among different components of the grid. Considering the evolution of the “Baseline” suggested by the stakeholders, our tool pointed out that 54 and 59 structural threats are removed, while 81 and 36 are, respectively, added to that scenario due to the inclusion of the PV and the wind farm in Node 2, the inclusion of a new battery in Node 1, the removal of one distributed generator each from Node 1 and Node 2, and the related connections. A similar trend can be observed looking at the 2nd Scenario, where a battery is removed from Node 3, while a generator is added to the same node of the grid. Here the total amount of threats decreases, despite the number of components being exactly the same. This means that the novel component (generator) is affected by a smaller amount of threats with respect to the removed one (battery). Overall, in its last evolution stage, the grid can be targeted by 1210 threats. Compared to the overall number of baseline threats, we can assert that these evolutions lowered the total number of threats that affect our grid scenario. A detailed report of such analysis is available in [44].

8.2.2 Stakeholders’ Answers and Feedbacks. Among all the feedback received by stakeholders, we next summarize the ones that are closely related to our methodology and the associated tool for evolutionary threat analysis.

- How would you rate the level of easiness in using the tool?
 - a. (From 1 – Very Low to 7 – Very High) Answers: {4, 5, 6}
- How strongly do you agree the tool is fast in providing simulation results for urban electricity networks?
 - b. (From 1 – Completely Disagree to 7 – Completely Agree) Answers: {5, 6, 6}
- How strongly do you agree that the tool is suitable for urban electricity networks?
 - c. (From 1 – Completely Disagree to 7 – Completely Agree) Answers: {4, 5, 6}
- (Open Question) Applicability and practicability of the tool
 - d. Stakeholder#1: I felt the tool was almost immediately applicable, but I do think there needs to be recognition that cross connections will also exist in addition to the vertical hierarchy shown in the scenario. As a tool that may allow to explore islanding, it will need to additionally consider the transition from grid to microgrid and back again.
 - e. Stakeholder#2: Based on my understanding I see opportunity in the ongoing development of the tool. From my perspective the ability of the tool to assist with network congestion– and related security aspects–is a very important aspect and should be of value to utility companies. I understand there is an aspiration for the tool to be of value to city planning departments. I think this is possible.
- (Open Question) Efficiency of the tool
 - f. Stakeholder#1: I feel the tool has a lot to offer but needs further development, essential will be the facility to save configured networks so they can be reloaded and returned to at a later date. Usability also needs to be improved, it was apparent at the workshop that considerable familiarity with the tool was needed to use it in its current form, it will be important that a user with domain knowledge but little else be able to use the tool.
- (Open Question) Market opportunity for the tool
 - g. Stakeholder#1: I think there is a commercial use for the tool, but only once it has been enhanced after further testing. This was supported by Stakeholder #2 (who can be considered independent). The tool could be marketed as a basic system arrangement capture and documentation tool, the later may be of particular interest to city planners and DNO/DSO seniors that may not understand the detailed technical information on existing diagrams (where they exist).
 - h. Stakeholder #2: I see an immediate benefit if the tool were to be road tested with some utility companies so that the concept can be proved and validated. This would help define the next steps of activity and help make the product adaptable to a range of potential market sectors.

8.2.3 Summary of Results and Discussions. The stakeholders made remarks on usability and the targeted use of the tool. In connection to “Efficiency of the tool”, Stakeholder#1 highlighted that the tool in its current stage needs a more intuitive interface to improve usability. This also impacts the “Market opportunity for the tool” answers. Stakeholders highlighted that the tool is based on a methodology with a potential. They also pointed out its applicability as enterprise software, but it would require further validation and verification with utility companies according to their specific interests.

Before the end of the workshop, stakeholders suggested several ideas in improving the tool, where the tool should integrate flexibility to allow for city configurations, a better user-friendly interface that is simpler to operate, and also a saved output parameters for comparisons based on different component alterations. Moreover, one of the stakeholders (*Citizen&Business* representative) argued that specialized industry knowledge is required in order to fully determine the inputs

of the tool, highlighting the need for a domain expert for several input parameters, e.g., identifying the threat list.

Taking into account all opportunities for improvement, the stakeholders found the tool usable for urban electricity network modeling, fast in providing results, and relatively easy to use, if initial data are entered and relevant knowledge is available.

9 CONCLUSION

This article presented an emergence-oriented approach to threat analysis for evolving cyber-physical SoSs. The methodology is supported by a tool, which allows us to (i) identify threats and propose suitable mitigation strategies for evolving SoSs and (ii) reduce the cognitive load required to ease the understanding of an SoS by capturing the possibly dangerous CSs interactions. The tool provided means to automatically identify emerging threats related to interacting CSs by tracing their corresponding evolutions. Moreover, with the support of current practice technologies, the tool supported the analysis of threats' distribution among time by automatically identifying mitigation strategies to be implemented, ultimately achieving a safe and secure SoS evolution. The presented methodology and the supporting tool have been applied to a Smart Grid SoS scenario based on which results of an evolutionary threat analysis have been reported.

Finally, both the methodology and the supporting tool have been empirically validated on a Smart Grid case study based on the power grid underlying the campus of an area of University of Twente. The validation process was based on questionnaires submitted to students in order to test—among others—how the tool allowed non-expert people to reduce the cognitive load required for identifying threats in evolving scenarios with respect to a manual identification. Moreover, another workshop session with stakeholders (City Planner, Distributed Network Operator, and Citizen&Business Representative) gave us interesting feedback from a business-oriented point of view.

Overall, both students and stakeholders agreed that the tool helps in reducing the cognitive load required to capture interactions among grid components in complex systems. We are aware that the strategy is not mature enough to have concrete market opportunities, but most of the workshop attendees confirmed that our methodology and the associated tool clearly supported the threat identification process.

As future work, we plan to (i) extend the methodology with means to rank identified threats with respect to their corresponding mitigation costs also considering the specificity of the evaluated SoS and (ii) improve the usability of the associated tool. Ultimately, this will allow the user of the tool to plan the evolution of an SoS by also considering the cost related to secure it.

REFERENCES

- [1] M. Jamshidi, Ed. 2009. *System-of-Systems Engineering - Innovations for the 21st Century*. J. Wiley & Sons.
- [2] A. Waller and R. Craddock. 2011. Managing runtime re-engineering of a system-of-systems for cyber security. In *6th International Conference on System of Systems Engineering (SoSE)*. 13–18.
- [3] S. A. Selberg and M. A. Austin. 2008. Toward an evolutionary system-of-systems architecture. In *INCOSE*, 2008.
- [4] S. Bleikertz, J. W. Bullée, M. Ford, D. Ionita, H. Jonkers, L. Montoya, S. Saraiva, A. Tanner, A. S. Yesuf, J. Willemson, C. W. Probst. 2015. D1.3.3. Dynamic features of socio-technical security models. *TRESPASS Project*, 2015.
- [5] Hussein A. Abbass, Sameer Alam, and Axel Bender. 2009. MEBRA: Multiobjective evolutionary-based risk assessment. *IEEE Computational Intelligence Magazine* 4, 3 (2009), 29–36.
- [6] Kip Morison, Wang Lei, and Kundur Prabha. 2004. Power system security assessment. *Power and Energy Magazine*, 2, 5 (2004), 30–39.
- [7] A. Najgebauer, R. Antkiewicz, M. Chmielewski, and R. Kasprzak. 2008. The prediction of terrorist threat on the basis of semantic association acquisition and complex network evolution. *Journal of Telecommunications and Information Technology*. (2008), 14–20.
- [8] Lund Mass Soldal, Bjørnar Solhaug, and Ketil Stølen. 2011. Risk analysis of changing and evolving systems using CORAS. *Foundations of Security Analysis and Design VI*. Springer, Berlin, 231–274.

- [9] B. Ganter, R. Wille, and R. Wille. 1999. *Formal Concept Analysis*. Springer, Berlin.
- [10] NIST. 2012. *Guide for Conducting Risk Assessments*. NIST Special Publication 800-30, Sep (2012).
- [11] NIST. 2010. Introduction to NISTIR 7628 *Guidelines for Smart Grid Cyber Security*. Guideline, Sep (2010).
- [12] IRENE. 2015. D2.1: Threats identification and ranking, 2015. Retrieved from <http://www.ireneproject.eu>.
- [13] W. Pieters, D. Hadžiosmanović, A. Lenin, L. Montoya, and J. Willemson. 2014. TREsPASS: Plug-and-play attacker profiles for security risk analysis (poster). In *35th IEEE Symposium on Security and Privacy*. IEEE Computer Society.
- [14] M. Mori, A. Ceccarelli, P. Lollini, A. Bondavalli, and B. Frömel. 2016. A holistic viewpoint-based SysML profile to design systems-of-systems. In *Proceedings of the IEEE International Symposium on High Assurance Systems Engineering (HASE)*. 276–283.
- [15] K. Pohl, G. Bockle, and F. van der Linden. 2005. *Software Product Line Engineering: Foundations, Principles and Techniques*. Springer, Berlin, 2005.
- [16] S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly. 2001. Identifying, understanding, and analyzing critical infrastructure interdependencies. *Control Systems, IEEE*, 21, 6 (Dec 2001), 11–25.
- [17] Stephan Murer and Bruno Bonati. 2010. *Managed Evolution: A Strategy for Very Large Information Systems*. Springer Science & Business Media, 2010.
- [18] H. Kopetz, A. Bondavalli, F. Brancati, B. Fromel, O. Hoftberger, and S. Iacob. 2016. Emergence in cyber-physical systems-of-systems (CPSoSs). In *Cyber-Physical Systems of Systems. Foundations – A Conceptual Model and Some Derivations: The AMADEOS Legacy*. Lecture Notes in Computer Science, vol. 10099, Springer, Berlin.
- [19] Jeffrey C. Mogul. 2006. Emergent (mis) behavior vs. complex software systems. *ACM SIGOPS Operating Systems Review*, 40, 4 (2006), 293–304.
- [20] Virgil Gligor. 2004. Security of emergent properties in ad-hoc networks (transcript of discussion). In *Security Protocols*. Springer, Berlin, 2004, 256–266.
- [21] Marco Mori, Andrea Ceccarelli, Tommaso Zoppi, and Andrea Bondavalli. 2016. On the impact of emergent properties on SoS security. In *IEEE System-of-Systems Engineering (SoSE'16)*.
- [22] Andrea Ceccarelli, Andrea Bondavalli, Bernhard Froemel, Oliver Hoeffberger, and Hermann Kopetz. 2016. Basic concepts on systems of systems. In *Cyber-Physical Systems of Systems. Foundations – A Conceptual Model and Some Derivations: The AMADEOS Legacy*. Lecture Notes in Computer Science, vol. 10099, Springer, Berlin.
- [23] D. Ionita, R. Kegel, A. Baltuta, and R. Wieringa. 2016. ArgueSecure: Out-of-the-box security risk assessment. In *3rd Evolving Security & Privacy Requirements Engineering Workshop: co-located with 24th IEEE International Requirements Engineering Conference (RE'16)*. Beijing, Springer.
- [24] SMB Smart Grid Strategic Group SG3, IEC Smart Grid Standardization RoadMap, Ed 1.0, June 2010, http://www.iec.ch/smartgrid/downloads/sg3_roadmap.pdf [last accessed 1st February 2016].
- [25] George Arnold and Ralph Sporer. 2016. “White Paper on Standardization of Smart Grids”, [Online]. <https://www.nist.gov/sites/default/files/documents/smartgrid/eu-us-smartgrids-white-paper.pdf> [last accessed 1st February 2016].
- [26] Mladen Kezunovic, Hongbiao Song, and Nan Zhang. 2005. “Detection, prevention and mitigation of cascading events, Final Report, Part I, October 2005 [Online]. Retrieved from <http://www.pserc.org>.
- [27] N. Ayewah, W. Pugh, J. D. Morgenthaler, J. Penix, and Y. Zhou. 2007. Using findbugs on production software. *Companion to the 22nd ACM SIGPLAN Conference on Object-Oriented Programming Systems and Applications*. ACM, 2007.
- [28] John Sweller. 1994. Cognitive load theory, learning difficulty, and instructional design. *Learning and Instruction* 4, 4 (1994), 295–312.
- [29] Paul A. Kirschner. 2002. Cognitive load theory: Implications of cognitive load theory on the design of learning. *Learning and Instruction* 12, 1 (2002), 1–10.
- [30] Paul Chandler and John Sweller. 1992. The split-attention effect as a factor in the design of instruction. *British Journal of Educational Psychology* 62, 2 (1992), 233–246.
- [31] ISO 31000. 2009. *Risk Management – Principles and Guidelines*. Retrieved from http://www.iso.org/iso/catalogue_detail?csnumber=43170.
- [32] Edmund H. Conrow. 2005. Risk management for systems of systems. *CrossTalk* 18, 2 (2005), 8–12.
- [33] Oddgeir Friberg, Monica Martinussen, and Jan H. Rosenvinge. 2006. Likert-based vs. semantic differential-based scorings of positive psychological constructs: A psychometric comparison of two versions of a scale measuring resilience. *Personality and Individual Differences* 40, 5 (2006), 873–884.
- [34] O. Jung, S. Bessler, A. Ceccarelli, T. Zoppi, A. Vasenev, L. Montoya, T. Clarke, and K. Chappell. 2016. Towards a collaborative framework to improve urban grid resilience. In *2016 IEEE International Energy Conference (ENERGYCON)*. IEEE, 1–6.
- [35] Cardenas Alvaro, Saurabh Amin, Bruno Sinopoli, Annarita Giani, Adrian Perrig, and Shankar Sastry. 2009. Challenges for securing cyber physical systems. In *Workshop on Future Directions in Cyber-physical Systems Security*, 5 (2009).
- [36] Robert L. Flood and Michael C. Jackson. 1991. *Critical Systems Thinking*. Wiley, Chichester.

- [37] D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. H. Maisel. 2008. Pacemakers and implantable cardiac defibrillators: Software radio attacks and zeropower defenses, SP 2008. In *IEEE Symposium on Security and Privacy*, 2008.
- [38] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong. 2017. The 2015 Ukraine blackout: Implications for false data injection attacks. *IEEE Transactions on Power Systems* 32, 4, 3317–3318.
- [39] Ik Jae Chung. 2011. Social amplification of risk in the Internet environment. *Risk Analysis* 31, 12 (2011), 1883–1896.
- [40] E. M. Aldrich, J. Grundfest, and G. Laughlin. 2016. The flash crash: A new deconstruction. DOI: <http://dx.doi.org/10.2139/ssrn.2721922>
- [41] Y. Bachy, F. Basse, V. Nicomette, E. Alata, M. Kaâniche, J. C. Courrage, and P. Lukjanenko. (2015). Smart-TV security analysis: Practical experiments. In *2015 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*. IEEE (June 2015), 497–504.
- [42] Guo Zhenyu and Yacov Y. Haimes. 2017. Exploring systemic risks in systems-of-systems within a multiobjective decision framework. *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 47, 6 (2017), 906–915.
- [43] T. Zoppi, A. Ceccarelli, and M. Mori. 2017. A tool for evolutionary threat analysis of smart grids. In *Smart Grid Inspired Future Technologies*. Springer, Berlin, 205–211.
- [44] IRENE. D5.2: Evaluation method design, evaluation of IRENE methods, collaboration framework and modelling tool, 2017 [Project Report]
- [45] R. D. Christie. 1999. Power Systems Test Case. <http://www.ee.washington.edu/research/pstca/>.
- [46] H. Kopetz. 2011. *Real-Time Systems: Design Principles for Distributed Embedded Applications*. Springer Science & Business Media.
- [47] H. A. Simon. 1996. *The Architecture of Complexity*. MIT Press, Cambridge, MA, 219.
- [48] A. Bondavalli, A. Ceccarelli, P. Lollini, L. Montecchi, and M. Mori. 2016. System-of-systems to support mobile safety critical applications: Open challenges and viable solutions. *IEEE Systems Journal*.
- [49] National Cyber Security Center, Information Risk Management: HMG IA Standard Numbers 1 & 2, 2015. Retrieved from <https://www.ncsc.gov.uk/>.
- [50] Gov. of Canada, All Hazards Risk Assessment Methodology Guidelines 2012-2013. Retrieved from <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/ll-hzrds-ssssmnt/index-en.aspx#iap>.
- [51] Peter G. Neumann. 2004. Principled assuredly trustworthy composable architectures. *Final report for Task 1* (2004).
- [52] Emiliano Guevara. 2011. Computing semantic compositionality in distributional semantics. In *9th International Conference on Computational Semantics (IWCS'11)*. Association for Computational Linguistics, Stroudsburg, PA, 135–144.
- [53] J. S. Dahman and K. J. Baldwin. 2008. Understanding the current state of US defense systems of systems and the implications for systems engineering. In *2nd Annual IEEE Systems Conference*, IEEE Press, 2008.

Received September 2017; revised April 2018; accepted June 2018