A conceptual redesign of a modelling language for cyber resiliency of healthcare systems

Myrsini Athinaiou[1], Haralambos Mouratidis[1], Theo Fotis[1] and Michalis Pavlidis[1]

[1] University of Brighton, Brighton, BN2 4GJ, UK

Abstract. Security constraints that enforce security requirements characterize healthcare systems. These constraints have a substantial impact on the resiliency of the final system. Security requirements modelling approaches allow the prevention of cyber incidents; however, the focus to date has been on prevention rather than resiliency. Resiliency extends into the detection, mitigation and recovery after security violations. In this paper, we propose an enhanced at a conceptual level that attempts to align cybersecurity with resiliency. It does so by extending the Secure Tropos cybersecurity modelling language to include resiliency. The proposed conceptual model examines resiliency from three viewpoints, namely the security requirements, the healthcare context and its implementational capability. We present an overview of our conceptual model of a cyber resiliency language and discuss a case study to attest the healthcare context in our approach.

Keywords: Security, Resiliency, Modelling language, Healthcare.

1 Introduction

Security covers an increasingly broad range of domains that rarely interplay in other contexts. For example, a healthcare system's security design should address, not just hardware and software vulnerabilities, but also other issues, such as equipment failures, human errors, dependencies of healthcare services. In this sense, it essential to provide a common language to address and manage this heterogeneity within the security context. Such a language will allow the specification of a broad range of security requirements of different stakeholders within the healthcare setting. Moreover, it can allow the analysis of their resiliency as part of their security requirements elicitation, meaning as early as possible in their design.

Healthcare systems stand for the organization of interacting elements arranged to accomplish one or more healthcare purposes (based on [1]). Examples of healthcare systems are implantable cardiac medical devices; medical ventilator and robotic X-ray. Long life-cycles characterize healthcare systems. Over the usable lifespan of healthcare, their design and development methods change [47]. While an understanding of the preventive security aspects of healthcare systems' design is essential, issues associated with other requirements and constraints when incidents occur are of more significant concern for life-critical and context-aware systems. Healthcare systems are

increasingly networked, interconnected and software-dependent. With limited resources and an ever-evolving threat landscape, any new insight into the cyber resiliency of healthcare systems and their design and implementation becomes crucial [22].

Cyber resiliency (also termed resilience) stands according to NIST SP 800-160, V.2. for "*the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources*." [40]. Based on the context (e.g., supply chain, environmental, psychological, technological) with which it associates, resiliency can approach different types of problems. In this paper, we focus only on cybersecurity resiliency, excluding other contexts of resiliency.

One approach to allow the by-design cyber resiliency of maintaining security requirements is the Model-driven engineering (MDE) [10, 47]. For healthcare systems that have the patient-in-the-loop, model-based frameworks that explicitly model an MCPS's interaction with the environment and with the patient can contribute towards safer development [5]. Similarly, modelled-based security approaches have shown the benefits of considering security requirements from the early stages of systems development [34, 32]. Such modelling approaches can potentially facilitate the development of healthcare systems that consider the full cyber resiliency life-cycle (i.e., preparation, identification, containment, eradication, recovery, lessons learned) [13].

Many security requirements modelling approaches are based on *Goal-oriented Requirements Engineering* (GORE). Typically, they analyze a system considering its organizational, operational and technical environment; to identify issues and opportunities. High-level goals are then modelled refined to address such issues and meet the opportunities [20, 15]. In Security Requirements Engineering (SRE), relevant requirements are then elaborated to meet those goals [32, 2, 34]. MDE and SRE may be used in combination to support the resilience of healthcare systems and in particular, to improve the awareness of redesign and reconfiguration capabilities of a healthcare system, before its actual construction. After all, any of such activities, if not well studied in advance, can harm the patients. Such cases contradict with the fundamental medical goal of "at least not harm" [5], and hence, they should not be ignored in healthcare systems engineering.

The main aim of this paper is to explore the consideration of cyber resiliency under conditions of uncertainty where incidents challenge the achievement of a healthcare system's goals. In this paper, we present the first step towards the modelling language, which will be part of a framework: redesigning a metamodel. Notice that we do not offer a modelling language, but we do present underlying conceptual considerations that led to the redesign of the language.

The research outcomes presented here aim to enhance the resilience management of cybersecurity by proposing a cybersecurity-resilience unified model. Mainly, the contribution of this paper comprises of:

- a combination of resiliency in the cybersecurity domain, extending the Secure Tropos approach to cover resiliency concepts. We focus on the design of systems considering cyber resiliency from the stage of requirements engineering;

- the proposed conceptual model presented as a UML class diagram, useful for the development of other cybersecurity artefacts that support cyber resiliency. Such artefacts can include processes, algorithms and tools. Such artefacts can support the semi-automation of a cyber resiliency analysis;
- the demonstration of the pertinence of the conceptual model in regard to the healthcare context, through a case study.

2 Background

Existing research indicates areas where more domain-specific research is needed. It is possible to form a structured approach for cyber resiliency with the current technical means. But validation and evaluation approaches for the assessment of resiliency plans and their resilience capability is limited [44][14][16][18][12]. Restrictions in the form of time, security capabilities, actors' skills, responder's motivation, financial resources and heterogeneity among systems are also addressed [14][45][11][21][18][30] showing the need for a holistic approach. The technological heterogeneity that introduces complexity associated with the healthcare context yields a technical conflict [7][23]. Specifically, security mechanisms exist for security [44], but research related to their cyber resiliency, let alone in regard to healthcare systems is very limited [23]. This is coupled with the challenges of incident quantification [17] and cyber resiliency assessment [14], enforcement of resiliency plans and security practices during response [44][18]. Additionally, the lack of cybersecurity expertise results in outsourced resilience that does not correspond to healthcare contextual needs [14][21]. Hence more research is required in the field where cybersecurity, resiliency and healthcare intersect.

2.1 Healthcare cyber resiliency

Concerning healthcare and cyber resiliency, Jalali et al. conducted a systematic review of journal articles that focus on cyber resiliency in healthcare [23]. They identified the need to evaluate and improve incident response strategies. The existing literature, in regard to the different phases of resiliency offers some guidance. For example, for preparation phase of cyber resiliency in healthcare, the literature addresses the need for more resources referring not only to financial but also to other types such as human availability and systems' redundancies [44][14][16]. It also identifies the need for security policies [44][16][12], identification capability of critical information, systems, actors and the dependencies among them [44][45][43].

The literature related to the cyber resiliency phase of detection and analysis, shows that independently from preparedness and preventive security mechanisms, incidents can still occur. When that happens a root cause analysis (RCA)is suggested [14][11] to guide incident categorization [16][17][21]. When an incident does occur, existing works are concerned with the need of healthcare organizations to maintain communication with internal and external parties, which will be also used for compliance with legally required notifications [14][16][17][18][23]. Forensic analysis is essential at all phases and at this phase it supports incident classification, prioritization and damage assessment of the affected entities [16][23][12].

At the phase of containment, eradication and recovery, according to the literature, incident response teams (IRTs) need to contain an incident initially. Containment requires the availability of relevant technical and legal expertise [14]. At this phase incident, IRTs want to eliminate any further damage [16]. They can achieve that through a diverse set of control mechanisms to initially neutralize an attack, using incident response systems, segmentation of networks, disconnection of affected devices and algorithmic recovery support to name a few [11][23]. These are all relevant with downtime procedures, vulnerabilities patching and forensic evidence preservation [16][23].

For the implementation of these controls and activities, what seems to be essential is the way with which IRTs prioritize restoration activities [17]. This prioritization seems in case studies to be a straight forward ability, and current ad hoc practices seem to indicate that [14]. However, within healthcare organizations, there are various people, processes and technologies that are prioritized differently under different circumstances [14][16]. Thus an ad hoc mentality is not optimal as attacks are sophisticated, and they can introduce delays and further vulnerabilities that can allow more attacks, more significant impact or increased costs [14][11].

Lastly, at the phase of post-incident activity that follows the demobilization of the emergency operations command center, healthcare organizations need to take actions to prevent an incident's recurrence [17][43]. Regulatory oversight might be necessary in cases of health sector-wide digital changes, following an incident [18]. To list and initiate the necessary changes as well as to determine how wide they need to be, the identification of what went wrong is necessary. After debriefing takes place based on reports of incident occurrence and severity resulted from the previous phases, assessments are conducted [44][14].

After this knowledge has been collected, it needs to be redistributed back to the healthcare organization [21][23]. Essential part of this process is the documentation of the recommendations and lessons learned that commonly take the form of a after action report (AAR) [14][16][17][23].

2.2 Security-oriented modelling languages

There are plenty of existing security-oriented modelling languages. Each one of the addresses relevant concerns from a different viewpoint. Usually, they extend existing modelling languages to cover security concerns. For example, Misuse Cases [42] and Abuse Cases [29], extend the use case diagrams, to elicit threats and vulnerabilities that adversaries could target. SecureUML [28] also extends UML diagrams centering on authorization constraints for access control goals. UMLsec [24] is another approach that extends UML, providing security data to UML diagrams. SecureUML and UMLsec address security at the design level and they do not concentrate on assets and early security requirements.

Other examples are extensions of the i* goal-oriented approach [46], an extension of Tropos [19]. KAOS, which is also goal-oriented, addresses security concerns by perceiving attacks as anti-goals [26]. Anti-goals stand for adversarial purposes that obstruct security goals. Abuse Frames have also been used to frame a security

problem's scope with anti-requirements and their usage to aid the formation of security requirements and the examination of relevant vulnerabilities and threats [27].

The Secure Tropos [34] approach is also an extended Tropos [9] version, which provides means to elicit and analyze security requirements. It allows the expression of a wide range of security, privacy and trust requirements in the form of constraints. Secure Tropos is well-known for being a robust language for defining secure systems at the organizational level. Its organizational approach to security allows its extension to cover the healthcare context considering attacks that can have beyond cyber also physical impact. Furthermore, existing automatic tools (i.e., SecTro [36]) ease the design activities using this metamodel and can also be extended accordingly.

3 Redesign decisions and challenges

The Secure Tropos metamodel inspired the first design attempt of a cyber resiliency modelling language for healthcare [34]. The initial design of the metamodel can be found in [6]. The decision of a redesign stemmed from interviews with experts from the Brighton and Sussex University Hospitals and MedStar Health as well as the application of small case studies. From there, it became apparent that the metamodel needed some enhancements. As a group, we agreed into three main redesign enhancements: the incident, the healthcare context and the inclusion of constructs related to resiliency. These enchantments led to the design of a second version of the metamodel, presented in Fig. 1. The following subsections report on how this metamodel was redesigned.

3.1 Justification for the use of Secure Tropos

We consider that the Secure Tropos metamodel is suitable to achieve the following purposes that relate to our research:

1. Supports the analysis and design activities in the software development process, capturing early and late requirements, modelling the environment of the system and the system itself respectively. Hence it can be used for healthcare systems representing the unique environment in which they operate.
2. It takes into account the relationship between security controls and security requirements [38]. This aspect forms an important base for the assessment of a security design when controls fail to achieve security requirements (i.e., when successful attacks do occur).
3. It is based on the principle that security should be taken into consideration from the early stages of the software system development process instead of been added as an afterthought. Resiliency also needs to be considered from early development stages, and a relevant conceptual extension might be useful.
4. Provides a modelling language, a process and a set of reasoning automation to support security analysis. The overall approach is well known and peer-reviewed, and any extension does not need to establish fundamental constructs but focus only to those constructs that are related to cyber resiliency and are not currently covered.

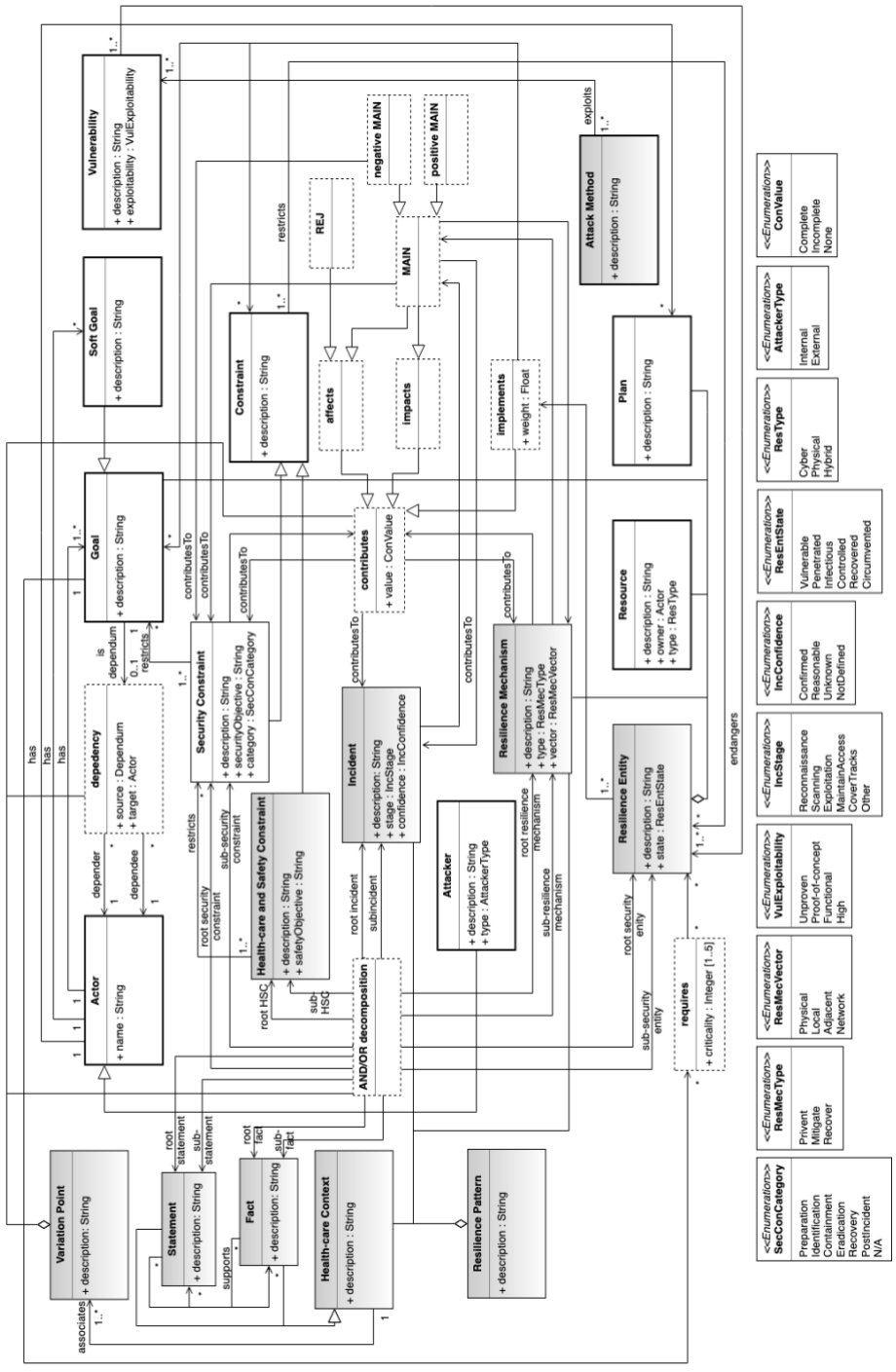

Fig. 1. Redesigned metamodel.

5. Secure Tropos, has been already extended to cover different types of systems (e.g., cloud security requirements [33], trust [37], business processes [4]). Following this paradigm, an extension can take place addressing the unique characteristics of healthcare systems in relation to their cyber resiliency.

Having identified some of the advantages of extending Secure Tropos, coincide with other security requirements approaches (e.g., KAOS [25], CORAS [8], SQUARE [31], GBRAM [3]). However, these approaches tend to focus on the preventive aspect of security. Resiliency stands for the ability to prepare for, respond to and recover from cyber incidents. It helps a healthcare infrastructure to prepare for incidents, defend against, limit their severity and ensure the continuation of operations despite an incident. Cyber resiliency has emerged as traditional cybersecurity measures are challenged, especially in the case of APTs [35]. When incidents do occur, the systems need to be able to keep up with the changes and continue to pursue critical goals and functions.

3.2 Redesign challenges

The redesign of the modelling language with resiliency in the healthcare context is a challenging and critical task. Typically, cybersecurity languages are well structured and technical. Requirements engineers and technology-oriented stakeholders use the same vocabulary having a technological focus. They can follow deterministic approaches using security models as the technological interdependencies are known. However, the healthcare context introduces unique challenges for a language redesign. Such a redesign requires a way to capture the healthcare aspect to be able to express relevant processes and services. However, this is not enough. It also needs to show how cybersecurity and resiliency affect and are affected by it too. There classical deterministic approaches do not suffice. Because on the one hand, incidents cannot be easily analyzed and managed, nor cyber resiliency engineering is yet well studied and understood to be able to determine with certainty responses and their negative impact on infrastructure's operational or security capability.

Semantic level differences intensify these difficulties as the language has a multidisciplinary focus. Different interpretations of the same term or different terms with the same meaning are common, which the literature review indicates. Nevertheless, the language needs to ensure that all the involved stakeholders share and understand the terminology used. However, this terminology expands far beyond the technology constructs commonly applied for the conceptualization of cybersecurity and resiliency. Social aspects integrated into the healthcare context demand from a language to also consider the values that underpin a diverse set of stakeholders that holds them might prioritize and appreciate them differently. For example, healthcare stakeholders commonly focus on systems functionalities that enhance the health and wellbeing of patients and do not cause harm. Naturally, they prioritize safety over security and understand the necessity for cyber resiliency differently from security and resiliency engineers. For example, they prioritize availability over maintenance and practice with medical equipment over participation in the incident response capability testing of their

department. To redesign a language that combines cybersecurity features with resiliency, we realized that there was a need to form constructs that support their unification. Though, there was no clear way derived from the literature to support us into making such a decision. Consequently, to face this obstruction, we plan to involve practitioners for validation of the redesigned language.

3.3 Healthcare cyber resiliency challenges

Healthcare services are dependent not only to computer systems and hospital equipment but also to devices attached to or even implemented in the human body. Thus, the healthcare context introduces unique challenges in the design of a language. For cybersecurity and resiliency, this means that any configuration can have not only cyber impact but also kinetic. This context sets implementational barriers of conventional cybersecurity approaches. For example, the time and duration of security and resiliency are affected. They need to consider what healthcare processes are ongoing when an incident occurs and how they can pursue security requirements attainment even when an attack has successfully compromised other healthcare systems of the same infrastructure (e.g., hospital, biomaterials facility).

Moreover, healthcare systems are diverse and have different challenges and limitations based on their type. For instance, the security challenges for a healthcare system where the user has device control capabilities, raise cybersecurity challenges related to the design of an interface that recognizes cases of patient's misuse [39]. However, in healthcare systems that sense and actuate without user involvement, the challenges are different and not user-related. They relate to the systems decision process design, the establishment of secure communications among system's components given hardware limitations, and even the alert system that will inform that security configurations are undertaken and can change the system's behavior and are within the patient's body [39]. It becomes clear through these simple examples that healthcare challenges cannot be excluded from the cyber resilience design because that can cause much more than just systems malfunctions. The patient is in the loop of this system, along with all the other users of such devices and ultimately the society as a whole. Please note that the first paragraph of a section or subsection is not indented. The first paragraphs that follows a table, figure, equation etc. does not have an indent, either.

3.4 Conceptual metamodel redesign

The basic idea of redesigning a metamodel is that the initial metamodel is the source that produces the redesigned metamodel. Before presenting an overview of the redesigned model, let us clarify that we have a model engineering perspective. In other words, we want to elaborate redesign decisions with the help of metamodels. Model engineering suggests that we have to start by identifying an existing metamodel for a redesign. Such a metamodel abstracts and collects the changes. In our redesign, we use the UML class diagram for the formulation of redesign models. Consequently, the redesigned model is a UML model. The class diagram in Fig. 2 presents the three parts

of the redesigned model. Incident constructs are in the middle, healthcare constructs in the left, and resiliency constructs in the right. The model also expresses generalization and associations among the various constructs.

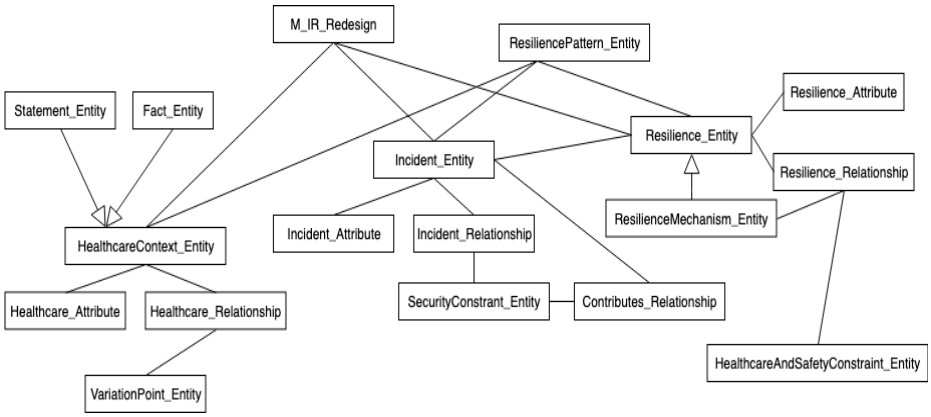

Fig. 2. Early version of the redesigned metamodel of Secure Tropos.

The main semantic changes reflected in the three parts of the redesigned model resulted from a systematic review of the scientific and standardization literature. The purpose of the review was the sound derivation of a conceptual model. Here we cannot present in detail the review process, but we discuss the main findings that resulted in the redesign of the modelling language at a conceptual level. Every construct has a variety of functions and implications, which can change over time and context. The conceptual unification of cybersecurity and resiliency starts with the identification of the basic constructs of the problem to be treated. The common terms identified in the relevant literature are incident, healthcare, response and security. We briefly present how they have been interpreted, offering useful components for the design of a conceptual model of a modelling language.

The set of collected papers interprets the term incident in four different ways. The majority of papers (7) consider an event such as updates, hardware failures, emergencies, human errors, natural disasters, misuse and abuse cases as occurrences of incidents [44][14][45][17][21][30][12]. In 4 papers an incident interpreted as a cybersecurity attack like hacking, ransomware and advanced persistent threat (APT) [11][43][7][12]. Two (2) papers use the NIST SP 8000-61 definition either explicitly or implicitly [16][23] and 1 paper focuses on the effects of an occurrence on systems functions and society as an incident [18]. Here it seems that an incident definition exists, and each study chooses to focus on an aspect of an incident. Other studies seem to choose a wider scope, that of event that also includes incidents and subsequently cybersecurity incidents.

Healthcare overall appeared to have five different meanings. In 3 papers coincides with the term hospital [44][16][17], in 6 papers with a form of a system, including medical cyber-physical systems, electronic medical records systems and healthcare information systems [14][45][11][43][7][30], in 3 papers as a healthcare critical infrastructure or a particular type (e.g. NHS) [45][7][18], in 2 papers addressed

healthcare organizations in general [21][23] and 1 was focusing on healthcare information [12]. From the above, it can be observed that the majority of papers interpret the term healthcare as a type of healthcare system. It is important here to clarify, that the reason the number of papers corresponding to meanings (15) is greater than the set of papers collected (13) is that in some papers the same term is used but is given multiple meanings. The same holds for the rest of the terms and the corresponding number of papers with similar interpretations.

When it comes to response, 4 papers address specific aspects/phases like detection, forensics and post-incident activities [7][21][30][12], 3 papers refer to all the phases of incident response [14][16][43], 2 papers analyze response overarching manner ranging from reactive on the one end and on the other to proactive adaptable responses to incident characteristics [44][11], in 2 papers response is studied within the planning context in the form of an incident response plan (IRP) along with other types of plans like emergency plan and business continuity plan [17][23]. Response is also considered closely associated with resilience and recovery in [45] and with management in [18]. The selected set of papers studies response from many aspects, usually related either with its phases individually or as a whole and in other studies as broader positioning of response within healthcare organizations.

The concept of security is one that is commonly associated with safety. Within this set of papers that was the case only in [16] and even there, the proposed security approach adjusts to feet cybersecurity needs. Examining relevant papers, it also seems that security mostly in the past but also in the present focuses on information security and confidentiality, integrity and availability properties [44][45][16][21][30][12]. However, in more recent studies, cyber-physical aspects are studied as well as moving from information technology-security to what is referred to in the broader literature as operational technology-security [7][18].

Specific aspects of security are also studies in the relevant literature. The conceptualization of security as vulnerable [45], the adaptability of security [45][11] are two such examples. Moreover, security is addressed from a socio-technical perspective [43], as organization wide [14][17]. In some cases, defense [44] and forensics [12] as important elements of security are studied based on risk plans [23]. Thus, security evolves as cyber risks do. The cyber risks become more sophisticated and dynamic, and security interpretations and understanding reflect these changes.

3.5 Incident redesign

While most people have an intuitive idea of what an incident is when asked to define it explicitly, there are large numbers of correct answers. From early incident response research, we learn that incidents have typically been defined as including the concepts of a set of security constraints imposed to goals within an infrastructure, that are impacted from actual attacks or are exposed to potential threats. An incident has been defined from NIST SP.800-61r2 as "*a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.*" [13]. Based on the above definitions and our interviews with experts an incident stands

for a negative occurrence that happens or is thought of as happening and leads to the failure of security constraints maintenance.

This definition similar to NIST SP.800-61r2 is quite subtle because it not only allows that an incident can be something that actually happened in the real world, but also that it can be imaginary and does not really occur. The example of a false positive alarm of an intrusion detection system can be treated as an incident even though it did not occur. The second meaning describes incidents that occur in computer systems. In this way, the term incident corresponds to incidents as a threat or as an actual attack.

An incident can be better understood through its likelihood and severity. In our framework, we consider likelihood as evidence that maintains or rejects the occurrence of an incident (MAIN and REJ). For example, the resilience entity *all the actions the surgeon takes should be recorded with nonrepudiation capability* in the telesurgery robotic system will help to enforce (MAIN) the security constraint *protect against any reasonably anticipated uses or disclosures of patient's health-care data* and discard (REJ) the incident *modify messages while packets are in-flight*.

On the other hand, severity is introduced as the influence of an incident to a security constraint. This relation allows us to model situations where a single incident impacts on more than one security constraints. The occurrence of an incident contributes to security constraint maintenance. In other words, a system under normal circumstances achieves a security constraint. When an incident occurs, the system wants to maintain security constraint achievement. The occurrence of an incident contributes to a security constraint's negatively in regard to its maintenance. Since the severity of an incident restrains a security constraint when it occurs, in our model, we use only MAIN relations between an incident and security constraints. This relation stands for the maintenance of an incident and can result in a positive or negative contribution to a security constraint's maintenance.

On the other hand, a *resilience mechanism* is a tool or technique that can be adopted in order to either prevent, mitigate or recover from an incident or is meant to implement a security constraint. A resilience mechanism might operate by itself, or with others, to provide a particular service. When an incident stands for a threat, then the preventive aspect of a resilience mechanism is meaningful, whereas in cases where an incident is an actual attack, then the mitigating and recovery aspects are relevant.

A *healthcare and safety constraint* (HSC) is a safety condition that the system has to achieve and restricts a security constraint in order not to endanger a patient's health and/or well-being. In the modelling process, HSC constraints are modelled as variation points of a resiliency plan. They are imposed by a healthcare actor that restricts the achievement of a security constraint. HSC constraints are within the control of an actor. This association with actors means that, differently than security constraints, HSC constraints are conditions that an actor wishes to introduce to protect the patient in the loop that characterizes healthcare systems. However, HSC constraints are examined based on how they affect security entities and thus contribute towards the analysis of resilience security requirements. HSC constraints can also be grouped according to the safety objective towards the achievement they contribute. Safety objectives are broader descriptions of safety principles or rules such as sterilization, calibration and interoperability.

3.6 Healthcare redesign

Healthcare services are dependent not only to computer systems and hospital equipment but also to devices attached to or even implemented in the human body. Thus, the healthcare context introduces unique challenges in the design of a language. For cybersecurity and resiliency, this means that any configuration can have not only cyber impact but also kinetic (e.g., physical harm to a patient). This context sets implementational barriers of conventional cybersecurity approaches. For example, the time and duration of security and resiliency are affected. They need to consider what healthcare processes are ongoing when an incident occurs and how they can pursue security requirements attainment even when an attack has successfully compromised other healthcare systems of the same infrastructure (e.g., hospital, biomaterials facility).

Moreover, healthcare systems are diverse and have different challenges and limitations based on their type. For instance, the security challenges for a healthcare system where the user has device control capabilities, raise cybersecurity challenges related to the design of an interface that recognizes cases of patients' misuse [39]. However, in healthcare systems that sense and actuate without user involvement, the challenges are different and not user-related. They relate to the systems decision process design, the establishment of secure communications among system's components given hardware limitations, and even the alert system that will inform that security configurations are undertaken and can change the system's behavior and are within the patient's body [39]. It becomes clear through these simple examples that healthcare challenges cannot be excluded from the cyber resilience design because that can cause much more than just systems malfunctions. The patient is in the loop of this system, along with all the other users of such devices. text can be associated with AND/OR decomposition, contribution and dependency.

3.7 Resiliency redesign

Resilience mechanisms are central to the process of determining the impact of an incident on the security constraint satisfaction. For instance, the incident *ransomware attack* can obstruct the satisfaction of the security constraint *patients' data availability*. However, the severity of this incident can be reduced with the use of the resilience mechanisms *use different credentials for backup storage*, *maintain complete visibility of healthcare IT infrastructure* and *leverage different file systems for backup storage*. The vulnerability is a critical component that defines the weakness of the designed healthcare system or the structure that can be exploited from one or more attack methods (e.g., unpatched equipment, insecure communication protocols). Attack methods are needed to distinguish between the ways an attacker can utilize to harm the system and how this harm is manifested. For example, a social engineering attack method manifests as an information breach threat. Each attack method is linked to one or more system vulnerabilities.

Another relevant construct to an incident is the *resilience entity* that represents any resilience-related goal, soft goal, plan, resource, resilience mechanism of the system. We extend the meaning of the security entity to cover resilience. For that purpose, we

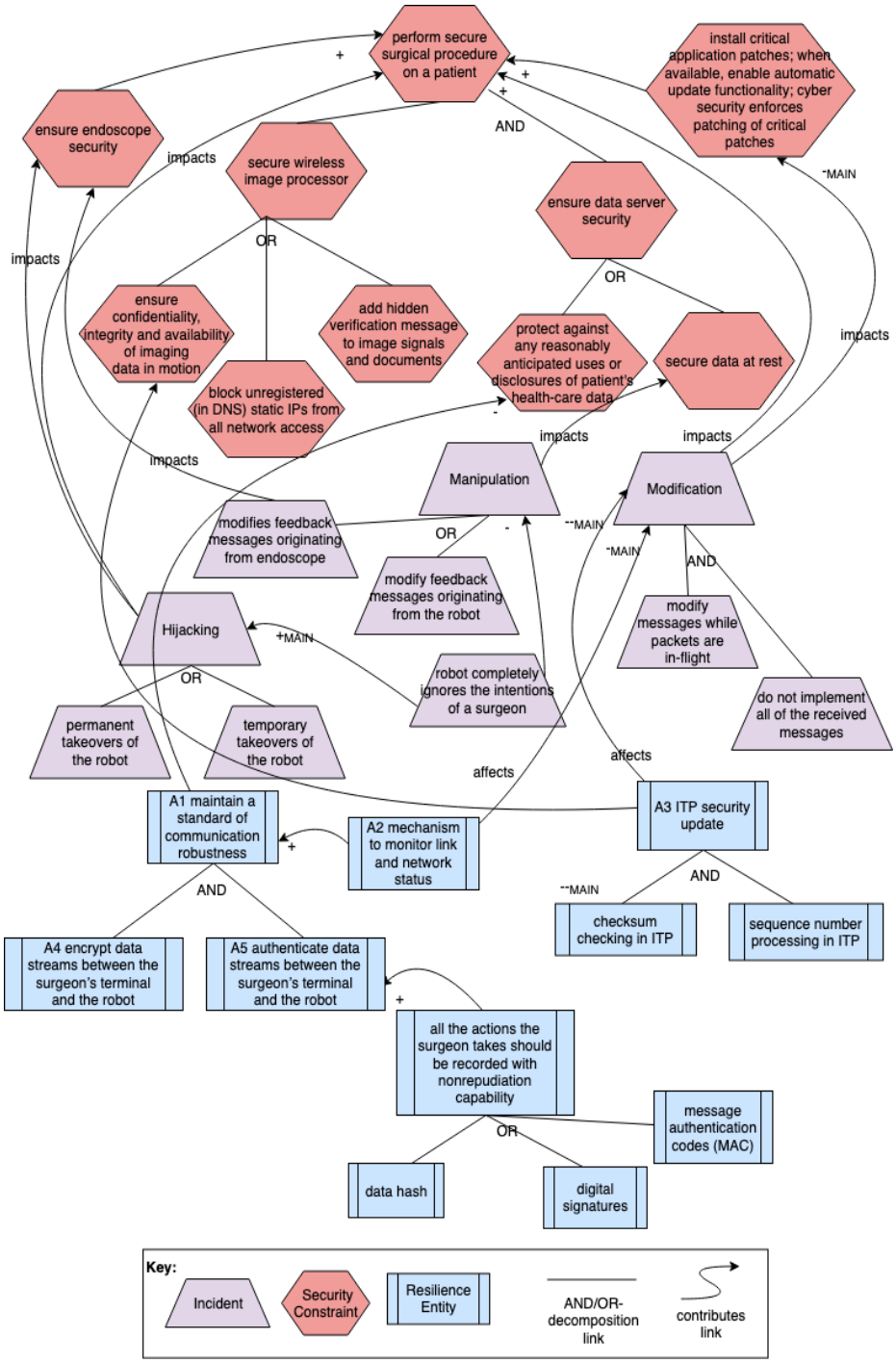

Fig. 3. Example of security model.

use the concept as an overarching term to cover especially decomposition, requires and endangers relations.

We understood that detecting simple mishandling incidents is a critical issue. However, heading off incidents before they occur requires detecting patterns as they are happening. Patterns of resilience can be used to detect situations where resilience is likely to result in an unwanted impact. A *resilience pattern* can be extracted based on the pattern definition given from Schumacher [41]. In general terms, a *Resilience pattern* is a template that specifies resilience objects called instances of the pattern. According to a security ontology introduced from Schumacher [41] a security pattern aggregates the concepts: context, problem and solution. In our modelling language following the same pattern ontology, we aggregate under a resilience pattern the concepts: health-care context, incident and resilience mechanism as defined in this document. The construct incident stands for a specific and observable adversarial action that violates or poses an imminent threat of violation of security constraints (based on NIST SP.800-61r2 [13]) It is a negative occurrence that happens or is thought of as happening.

The general structure of resilience patterns is identical to traditional patterns. They have a descriptive name, a context, a problem and a solution. There are relations to other resilience patterns as well. Nevertheless, specific resilience concepts can be assigned to these structural pattern elements. An example of such a pattern is teleoperation that is subject to hijacking and to be resilient for such attacks it is designed with non-persistence (i.e., generating and retaining resources within needs and time constraints).

4 Case study

We take a scenario where a surgical system performs a surgical procedure (e.g., biopsy) on a patient with manipulators and an endoscope. An endoscope is a long, thin, flexible tube that has a light source and camera at one end. In our scenario, the surgical system comprises a surgical robot, including a station, four robot arms mounted on the station and a console for controlling the surgical robot. The surgical system also comprises a data server for storing information from diagnostic imaging modalities (e.g. MRI, CT, X-ray) which have been captured from a patient with the use of an ultrasonic diagnostic device mounted on the distal end of a robot arm and a display unit. The display unit simultaneously displays an endoscopic image and acquired from the endoscope and an ultrasonic image acquired by the ultrasonic diagnostic device. This scenario provides a simplified view of the stakeholders in the surgical system, the healthcare services supported, and the concepts involved when a healthcare service is provided.

Due to space limitations in Fig.3 and Fig.4 we present a partial view that captures the security and healthcare context, respectively. Particularly Fig.4 depicts the healthcare context along with goals, security constraints and resilience entities. The process starts taking the security constraints from Secure Tropos and forming a conjunctive security constraints tree (where the relation between sub-security

constraints represents conjunctive or disjunctive sub-security constraints). We have developed a simple security constraints structure with parent goal "perform surgical procedure on a patient" that has an AND decomposition (both of them need to be achieved for the parent goal to be achieved) with the sub-goals "use console to control the surgical robot" and "utilize patient data from the data server". From the high-level security constraint "perform a secure surgical procedure on a patient", we can also extract leaf security constraints that must be satisfied by resilience entities within the system. In our example, we prefer to keep simplicity at this point, because the AND/OR decomposition are well known in the existing literature.

Given ongoing attacks and expected incidents, we derive what security constraints are relevant to these incidents and consequently, what are the security entities that we need to consider. These considerations take the form of a three-layered incident model that connects security constraints, incidents and resilience entities, as shown in Fig.3. This model is then used as input for the instantiation of Fig 4. Moreover, by reviewing healthcare process documents and relating them with resilience entities, different points where a response will need to adjust to the ongoing conditions are specified. In our example, some of such points are "ergonomic settings", "laparoscopic procedure" and "change device settings". Taking one of these points, let us say "laparoscopic procedure" a security practitioner that considers implementing a resilience entity such as "encrypt data streams between the surgeon's terminal and the robot" has to consider if a laparoscopic operation is taking place at the same time. If so, the overhead or other complication that encryption might result from having to be valued in relation to the potential impact the response can have to the ongoing healthcare process and ultimately, the patient.

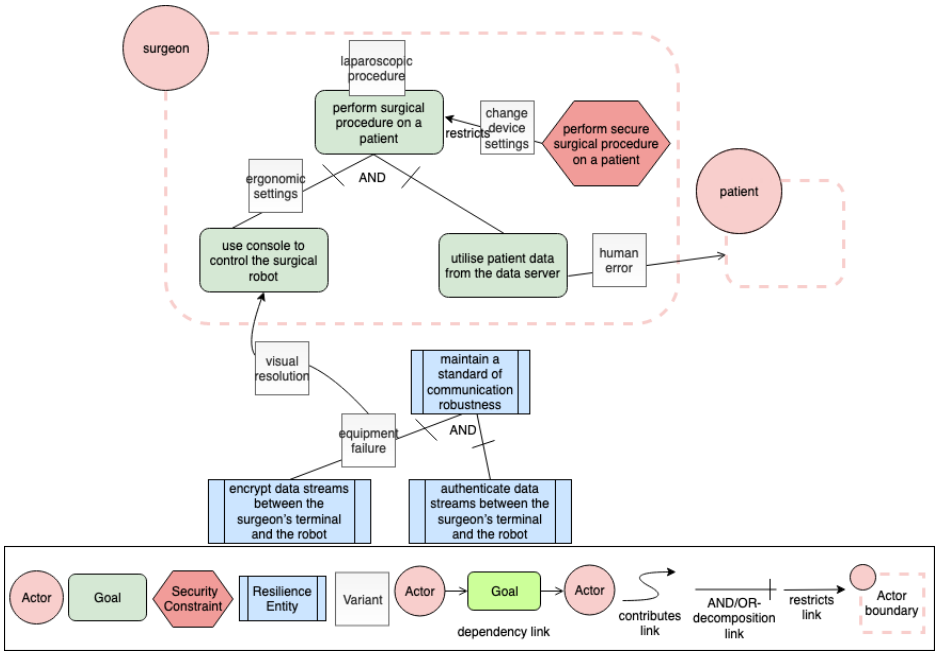

Fig. 4. Example of healthcare context variations model.

With this simple case, we were able to demonstrate one of the additional capabilities that the enhanced design can offer to cybersecurity practitioners of healthcare environments. In particular, we looked at the constructs that relate to the healthcare context and described at a high-level process through which such models can be instantiated.

5 Conclusions

This paper focuses on cyber resiliency in relation to incidents that have recently arisen or may arise for healthcare systems. The critical result of this revision of the modelling language was the update of the metamodel to define more accurately the constructs related to incidents, healthcare and resiliency. These enhancements were made to allow security engineers to define a structure to support the resiliency of specific applications relevant to their healthcare systems and incident conditions they face or prepare to manage. In a case study for a robotic surgical system, we were able to demonstrate one aspect of the application of the modelling language extensions. A detailed validation needs to take place in future work. Because of the wide variety of physical and digital capabilities of healthcare systems along with the potential impact they can have, we believe that their cybersecurity needs to be studied further.

References

1. ISO/IEC/IEEE 15288:2015, https://www.iso.org/standard/63711.html, last accessed 2019/07/12.
2. Frank, U., Loucopoulos, P., Pastor, O., Petrounias, I., Li, T., Horkoff, J., Mylopoulos, J. (eds.): Integrating Security Patterns with Security Requirements Analysis Using Contextual Goal Models. In: Lecture Notes in Business Information Processing. Lecture notes in business information processing, vol. 197, pp. 208–223. Springer, Manchester, UK (2014).
3. Antn, A.I., Earp, J.B.: Strategies for Developing Policies and Requirements for Secure and Private Electronic Commerce. In: Ghosh, A.K. (ed.) E-Commerce Security and Privacy, vol. 2, pp. 67–86. Springer US, Boston, MA (2001).
4. Argyropoulos, N., Mouratidis, H., Fish, A.: Advances in Conceptual Modeling. Springer International Publishing, Cham (2015).
5. Arney, D., Pajic, M., Goldman, J.M., Lee, I., Mangharam, R., Sokolsky, O.: Toward patient safety in closed-loop medical device systems. In: Proceedings of the 1st ACM/IEEE International Conference on Cyber-Physical Systems - ICCPS '10. pp. 139-148. ACM Press, Stockholm, Sweden (2010).
6. Athinaiou, M., Mouratidis, H., Fotis, T., Pavlidis, M., Panaousis, E.: Towards the Definition of a Security Incident Response Modelling Language. In: Trust, Privacy and Security in Digital Business - 15th International Conference, TrustBus 2018, September 5-6, 2018, Proceedings. pp. 198–212. Regensburg, Germany (2018).
7. Boddy, A., Hurst, W., Mackay, M., Rhalibi, A.E.: A study into data analysis and visualisation to increase the cyber-resilience of healthcare infrastructures. In: Proceedings

of the 1st International Conference on Internet of Things and Machine Learning - IML '17. pp. 1–7. ACM Press, Liverpool, UK (2017).
8. Den Braber, F., Hogganvik, I., Lund, M.S., Stlen, K., Vraalsen, F.: Model-based security analysis in seven steps a guided tour to the CORAS method. BT Technology Journal 25(1), 101–117 (Jan 2007).
9. Bresciani, P., Perini, A., Giorgini, P., Giunchiglia, F., Mylopoulos, J.: Tropos: an agent-oriented software development methodology. Autonomous Agents and Multi-Agent Systems 8(3), 203-236 (May 2004)
10. Chapurlat, V., Daclin, N., Bonydandrieux, A., Tixier, J., Kamissoko, D., Benaben, F., Nastov, B.: Towards a Model-Based Method for Resilient Critical Infrastructure Engineering How to model Critical Infrastructures and evaluate ist Resilience?: How to model Critical Infrastructures and evaluate its Resilience?: 2018 13th Annual Conference on System of Systems Engineering (SoSE). pp. 561–567. IEEE, Paris (2018).
11. Chen, Q., Lambright, J.: Towards Realizing a Self-Protecting Healthcare Information System. In: 2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC). pp. 687–690. IEEE, Atlanta, GA, USA (2016).
12. Chernyshev, M., Zeadally, S., Baig, Z.: Healthcare Data Breaches: Implications for Digital Forensic Readiness. Journal of Medical Systems 43(1), (2019).
13. Cichonski, P., Millar, T., Grance, T., Scarfone, K.: Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology. Tech. Rep. NIST SP 800-61r2, National Institute of Standards and Technology (2012).
14. Cooper, T., Collmann, J., Neidermeier, H.: Organizational Repertoires and Rites in Health Information Security. Cambridge Quarterly of Healthcare Ethics 17(4), 441–452 (2008).
15. Dardenne, A., van Lamsweerde, A., Fickas, S.: Goal-directed requirements acquisition. Science of Computer Programming 20(1-2), 3-50 (1993).
16. DeVoe, C., M. Rahman, S.S.: Incident Response Plan for a Small to Medium Sized Hospital. International Journal of Network Security & Its Applications 5(2), 1–20 (2013).
17. Genes, MD, P.N., Chary, PhD, M., Chason, DO, K.W.: Case study. An academic medical centers response to widespread computer failure. American Journal of Disaster Medicine 8(2), 145–150 (2013).
18. Ghafur, S., Grass, E., Jennings, N.A., Darzi, A.: The challenges of cybersecurity in health care: the UK National Health Service as a case study. The Lancet Digital Health 1(1), e10–e12 (2019).
19. Giorgini, P., Massacci, F., Zannone, N.: Security and Trust Requirements Engineering. In: Hutchison, D., Kanade, T., Kittler, J., Kleinberg, J.M., Mattern, F., Mitchell, J.C., Naor, M., Nierstrasz, O., Pandu Rangan, C., Steffen, B., Sudan, M., Terzopoulos, D., Tygar, D., Vardi, M.Y., Weikum, G., Aldini, A., Gorrieri, R., Martinelli, F. (eds.) Foundations of Security Analysis and Design III, vol. 3655, pp. 237–272. Springer, Berlin, Heidelberg (2005).
20. Giorgini, P., Mylopoulos, J., Sebastiani, R.: Goal-oriented requirements analysis and reasoning in the Tropos methodology. Engineering Applications of Artificial Intelligence 18(2), 159–171 (2005).
21. He, Y., Johnson, C.: Challenges of information security incident learning: An industrial case study in a Chinese healthcare organization. Informatics for Health and Social Care 42(4), 393–408 (2017).
22. Insup Lee, Sokolsky, O., Sanjian Chen, Hatcliff, J., Eunkyoung Jee, BaekGyu Kim, King, A., Mullen-Fortino, M., Soojin Park, Roederer, A., Venkatasubramanian, K.K.: Challenges and Research Directions in Medical CyberPhysical Systems. Proceedings of the IEEE 100(1), 75–90 (2012).

23. Jalali, M.S., Russell, B., Razak, S., Gordon, W.J.: EARS to cyber incidents in health care. Journal of the American Medical Informatics Association 26(1), 81-90 (2019).
24. Jrjens, J.: UMLsec: Extending UML for Secure Systems Development. In: Goos, G., Hartmanis, J., van Leeuwen, J., Jzquel, J.M., Hussmann, H., Cook, S. (eds.) UML 2002 The Unified Modeling Language, vol. 2460, pp. 412–425. Springer, Berlin, Heidelberg (2002).
25. van Lamsweerde, A.: Goal-oriented requirements engineering: a guided tour. In: Proceedings Fifth IEEE International Symposium on the Requirements Engineering, pp. 249-262. IEEE Comput. Soc, Toronto, Ont., Canada (2000).
26. van Lamsweerde, A., Letier, E.: From Object Orientation to Goal Orientation: A Paradigm Shift for Requirements Engineering. In: Wirsing, M., Knapp, A., Balsamo, S. (eds.) Radical Innovations of Software and Systems Engineering in the Future: 9th International Workshop, RISSEF 2002, Venice, Italy, October 7-11, 2002. Revised Papers, pp. 325–340. Springer, Berlin, Heidelberg (2004).
27. Lin, L., Nuseibeh, B., Ince, D., Jackson, M., Moffett, J.: Introducing abuse frames for analyzing security requirements. In: Journaal of Lightwave Technology, pp. 371-372, IEEE Comput. Soc, Monterey Bay, CA, USA (2003).
28. Lodderstedt, T., Basin, D., Doser, J.: SecureUML: A UML-Based Modeling Language for Model-Driven Security. In: Goos, G., Hartmanis, J., van Leeuwen, J., Jzquel, J.M., Hussmann, H., Cook, S. (eds.) UML 2002 The Unified Modeling Language, vol. 2460, pp. 426–441. Springer, Berlin, Heidelberg (2002).
29. McDermott, J., Fox, C.: Using abuse case models for security requirements analysis. In: Proceedings 15th Annual Computer Security Applications Conference (ACSAC'99), pp. 55-64. IEEE Comput. Soc, Phoenix, AZ, USA (1999).
30. McGlade, D., Scott-Hayward, S.: ML-based cyber incident detection for Electronic Medical Record (EMR) systems. Smart Health 12, 3-23 (2019).
31. Mead, N.R., Stehney, T.: Security quality requirements engineering (SQUARE) methodology. ACM SIGSOFT Software Engineering Notes 30(4), 1 (2005).
32. Meland, P.H., Paja, E., Gjre, E.A., Paul, S., Dalpiaz, F., Giorgini, P.: Chapter 85: Threat Analysis in Goal -Oriented Security Requirements Modelling. In: Computer Systems and Software Engineering: Concepts, Methodologies, Tools, and Applications, pp. 2025–2042. IGI Global (2018).
33. Mouratidis, H., Argyropoulos, N., Shei, S.: Security Requirements Engineering for Cloud Computing: The Secure Tropos Approach. In: Karagiannis, D., Mayr, H.C., Mylopoulos, J. (eds.) Domain-Specific Conceptual Modeling, pp. 357–380. Springer International Publishing, Cham (2016).
34. Mouratidis, H., Giorgini, P.: Secure tropos: a security-oriented extension of the tropos methodology. International Journal of Software Engineering and Knowledge Engineering 17(02), 285–309 (2007).
35. Mwiki, H., Dargahi, T., Dehghantanha, A., Choo, K.K.R.: Analysis and Triage of Ad vanced Hacking Groups Targeting Western Countries Critical National Infrastructure: APT28, RED October, and Regin. In: Gritzalis, D., Theocharidou, M., Stergiopoulos, G. (eds.) Critical Infrastructure Security and Resilience: Theories, Methods, Tools and Technologies, pp. 221–244. Advanced Sciences and Technologies for Security Applications, Springer International Publishing, Cham (2019).
36. Pavlidis, M., Islam, S., Mouratidis, H.: A CASE Tool to Support Automated Modelling and Analysis of Security Requirements, Based on Secure Tropos. In: van der Aalst, W., Mylopoulos, J., Rosemann, M., Shaw, M.J., Szyperski, C., Nurcan, S. (eds.) IS Olympics: Information Systems in a Diverse World, vol. 107, pp. 95–109. Springer, Berlin, Heidelberg (2012).

37. Pavlidis, M., Islam, S., Mouratidis, H., Kearney, P.: Modeling Trust Relationships for Developing Trustworthy Information Systems: International Journal of Information System Modeling and Design 5(1), 25–48 (2014).
38. Pavlidis, M., Mouratidis, H., Panaousis, E., Argyropoulos, N.: Selecting Security Mech anisms in Secure Tropos. In: Lopez, J., Fischer-Hbner, S., Lambrinoudakis, C. (eds.) Trust, Privacy and Security in Digital Business, vol. 10442, pp. 99–114. Springer International Publishing, Cham (2017).
39. Ransford, B., Clark, S.S., Kune, D.F., Fu, K., Burleson, W.P.: Design Challenges for Secure Implantable Medical Devices. In: Burleson, W., Carrara, S. (eds.) Security and Privacy for Implantable Medical Devices, pp. 157–173. Springer New York, New York, NY (2014).
40. Ross, R., Graubart, R., Bodeau, D., McQuaid, R.: Systems Security Engineering Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems. Tech. rep., NIST (2018).
41. Schumacher, M.: Toward a Security Core Ontology. In: Security engineering with patterns: origins, theoretical models, and new applications, pp. 87–96. No. 2754 in Lecture notes in computer science, Springer, New York (2003).
42. Sindre, G., Firesmith, D.G., Opdahl, A.L.: A Reuse-Based Approach to Determining Security Requirements. Requirements Engineering 10, 34–44 (2004).
43. Sittig, D., Singh, H.: A Socio-technical Approach to Preventing, Mitigating, and Recovering from Ransomware Attacks. Applied Clinical Informatics 07(02), 624-632 (2016).
44. Wiant, T.L.: Information security policy's impact on reporting security incidents. Computers & Security 24(6), 448-459 (2005).
45. Williams, P.A.H.: Is Cyber Resilience in Medical Practice Security Achievable? In: Proceedings of the 1st International Cyber Resilience Conference. pp. 105 – 111. Edith Cowan University, Perth Western Australia (2010).
46. Yu, E.S.K.: Modeling strategic relationships for process reengineering, PhD Thesis, University of Toronto, Canada (1995).
47. Zhihao Jiang, Pajic, M., Mangharam, R.: CyberPhysical Modeling of Implantable Cardiac Medical Devices. Proceedings of the IEEE 100(1), 122-137 (2012).