Chapter

Ontology-Based Solution for Handling Safety and Cybersecurity Interdependency in Safety-Critical Systems

Dionysia Varvarigou, David Espes and Giacomo Bersano

Abstract

In case, safety-critical systems face an anomaly (either intentional or not), safety and cybersecurity impact humans and environment. Thus, they affect each other and so they are considered as interdependent. An ontology-based solution for safety is needed to handle this interdependency. We propose a new safety ontology for Network Function Virtualization (NFV) framework which is able to cover reliability, availability, maintainability, and integrity-related breakdown types, since they interact and influence safety according to ENISA. Our ontology allows us to have a uniformized representation of the potential anomalies that a system and its elements can face. Based on this representation, a decision-making process takes place to avoid potential conflicts between safety and cybersecurity in order to best handle their interdependency. The results of our implementation show that our ontology handles the safety and cybersecurity interdependency and has little impact on decision-making time, which makes it an effective methodology for NFV framework.

Keywords: safety ontology, NFV safety architecture, safety and cybersecurity interdependency, Network Function Virtualization (NFV)

1. Introduction

In safety-critical systems, safety is the most significant property to be considered. This is because the main focus for these systems is to prevent harm on humans and environment. However, safety is able to interact with other properties as well. According to the ENISA standard [1], safety is a subset of the reliability, maintainability, availability, and integrity properties. In this way, it is understood that safety has the ability to interact with these aforementioned properties while considering their impact to humans and environment. Furthermore nowadays, NFV applications are expanded as they are used to various types of systems. Thus, NFV can be applied in safety-critical systems. In this case, safety is an important property for NFV. In [2], an NFV application is used in a safety-critical use case which proves the importance of safety in these systems. For example, NFV handles services for an autonomous

vehicle. In case, a reliability anomaly happens in one of the NFV services and the vehicle becomes uncontrollable, it can have an impact on the people that it carries, the people in the surrounding, and the surrounding environment itself.

However, as seen in ENISA standard, the properties that interact with safety are shared with some of the properties of cybersecurity. This makes understood that safety is also able to interact with cybersecurity. Thus, the functionalities of safety are able to influence and violate the ones of cybersecurity. Likewise, the functionalities of cybersecurity can affect the ones of safety. As an outcome, it is possible to consider safety and cybersecurity as interdependent. As an example, in order for cybersecurity needs to mitigate an anomaly, it asks for a re-launch of a Virtualized Network Function (VNF). This is issued to the NFV Orchestrator (NFVO) module. This is because this module is the responsible one for implementing all the issued orders. At that moment, safety understands that this action goes against its safety measures and blocks the NFVO from issuing this specific re-launch.

In order to prevent any safety and cybersecurity violations, it is needed to be able to differentiate the safety anomalies from the cybersecurity ones. An ontology-based solution is a good way to automate this process. Thus, it is possible to find ontology-based solutions for each one of the safety-related properties independently. However, in the literature, there are no ontology-based solutions for safety considering all the properties related to it as a whole. Moreover, there are no ontology-based solutions that provide a safety and cybersecurity interdependency. This has the effect of limiting the decision-making process that is used for distinguishing the anomalies created in a system. Furthermore, this prevents from taking into consideration the interdependency of safety and cybersecurity.

Thus, it is understood that in order to ensure safety in a NFV framework, there are specific challenges to be addressed. These challenges deal with: (i) the detection and mitigation of a variety of safety anomalies in a more comprehensive way, and (ii) the management of safety and cybersecurity interdependency. In order to handle safety in a NFV framework, an orchestrator is needed which is able to detect reliability, availability, integrity, and maintainability-related anomalies with respect to safety. Ontology is a good option for addressing this issue, since ontology is an explicit specification of a conceptualization where the knowledge of a domain is represented in a declarative formalism [3]. This makes it possible to represent the different types of anomalies in relation to safety. According to this uniformized representation, the reasoner (piece of software) is able to infer logical consequences. These consequences make it possible to understand whether a safety-related anomaly is also a cybersecurity-related one.

To this end, our solution proposes (i) a new ontology for ensuring safety in NFV framework and (ii) specific rules to be used by the reasoner. Our proposed ontology is used by an orchestrator that handles safety in a NFV framework. This ontology includes (i) the description of safety and the properties related to it (i.e. reliability, availability, maintainability, and integrity) as classes, (ii) the concerned elements for each property as subclasses, and (iii) the breakdown types for the potential adversities as object properties. Our proposed rules allow us to automate the decision-making process. This is because the reasoner needs the rules to make a decision. According to this decision, a NFV safety orchestrator is able to modify the plan of mitigation. With this modification, it is possible to avoid potential safety and cybersecurity conflicts.

The remaining of this paper is organized as follows. Section 2 reviews the relevant works of ontologies. Section 3 introduces our proposed ontology. Section 4 provides the rules for supporting the decision-making process. Section 5 presents the evaluation of

the feasibility of our proposed ontology. Section 6 provides the results and their analysis. Finally, the last section concludes the study, and it discusses possible future work.

2. Related work

In general, ontologies are used for system modeling, since they are capable of describing a whole system with its components and subsystems. This is because an ontology is expressed as the study of what exists in a certain context [3].

2.1 Ontologies for safety-related properties

As follows, it is possible to provide the related work with respect to ontologies for all the safety-related properties but also the integration of safety and cybersecurity. These ontologies are provided in general.

2.1.1 Safety ontologies

In relation to safety, ontologies are commonly used for obtaining safety risk knowledge and handling safety management. For safety risk knowledge, it is possible to develop an ontological method which organizes this knowledge into seven unified classes (i.e. project, construction activity, risk factor, risk, risk grade, risk consequence, and risk prevention measure) [4]. For handling the risk management, an ontology with a case-based reasoning is used as a decision-making approach for safety risk management [5]. Moreover, safety ontologies are able to represent specifically extracted information from databases. In this way, ontologies can assist for identifying additional capabilities of these information [6].

However, ontologies can be integrated with other technologies, algorithms, or methodologies in order to enhance their capabilities. For instance, ontologies can be integrated with computer vision algorithms to develop knowledge graphs that can automatically and accurately recognize hazards even when they are subjected to change [7]. Another example is when ontologies can be combined with wireless networks to identify potential hazards [8].

2.1.2 Reliability ontologies

Reliability with respect to ontologies is expressed as a way to make ontologies reliable, or to use ontologies for increasing reliability in various systems. Agile methodology uses agile principles and practices for ontology development. In this way, it is possible to utilize software engineering to build reliable ontologies [9]. Moreover, ontology alignment is a way to create reliable ontologies. In [10], machine learning techniques are used to automatically align ontologies to make them more reliable.

However, ontologies are able to be used in various methodologies in order to provide a variety of different types of reliability. In general, an ontology-based text mining methodology is able to maximize system reliability, since it is able to extract knowledge from databases [11]. There are many technologies and methods in order to use semantic web and ontologies for providing reliable services. This is because the use of semantic technologies in the modeling of a multi-agent system are very effective in increasing coordination and interoperability, as seen in [12]. Furthermore, ontologies are able to assist into making the numerical simulation techniques more

reliable. This can happen with ontology-based text and data mining techniques, as seen in [13].

2.1.3 Availability ontologies

Ontologies for ensuring availability are not widely researched in the literature, up to our knowledge. However, in [14], ontologies are used to provide and ensure heterogeneous knowledge for a specific concept. By combining these ontologies with optimization algorithms, it is possible to provide high data availability.

To sum up, availability is closely linked to reliability and maintainability. Once a system is reliable and maintainable, then it is possible to satisfy availability [15].

2.1.4 Maintainability ontologies

Maintainability is an attribute that is included in dependability. In order to be able to understand all attributes of dependability but also to compare them, it is possible to use a dependability rating ontology [16]. Thus, it is possible to obtain knowledge about the attribute of maintainability but also in relation to the other attributes. Moreover, ontologies can be created by extracting them from other ontologies or by creating them from scratch. The approach to develop an ontology is able to affect the maintainability. Thus, the evaluation of the ontology development is very important. In [17], the authors propose a methodology for evaluating ontology development from scratch.

Furthermore, it is important to be able to create maintainable ontologies. For achieving this, a methodology is proposed in [18] which is able to construct ontologies using a template-based approach for ontology modeling and instantiation. However, ontologies can be also used to enhance maintainability in a system. In [19], an ontology model is proposed to facilitate maintenance strategies selection and assessment. And in [20], ontologies are used for data accessing in order to enhance system maintainability.

2.1.5 Integrity ontologies

Ontologies can be used for ensuring integrity in a system. This can happen with a framework that is able to leverage an ontology to provide representation of semantically enriched data, as seen in [21]. It is also important to be able to evaluate the ontologies with regard to integrity. In [22], an ontology-based evaluation system is proposed which is a new ontology framework of leverage knowledge modeling. This creates an easy-to-use tool for quantitative identification for integrity by combining ontology and semantic web rule language rules.

However, ontologies need some constraints in their analysis in order to be able to focus on certain attributes. One of the ways that ontology accesses data is by querying via query translation. However, constraints in general in this way of accessing data is not represented. For this reason in [23], a framework for querying data that exploits information with regard to integrity constraints is proposed for ontology-based data access. It is also possible to extend the ontology-based data access into including integrity constraints, as seen in [24].

2.1.6 Confidentiality ontologies

Specifically, ontologies dedicated to confidentiality are not widely researched in the literature, up to our knowledge. However, confidentiality can be found in the

ontologies that cover all attributes of the cybersecurity approach of Confidentiality, Integrity, and Availability (CIA). In [25], an ontology is developed that targets a requirement-based threat analysis. These requirements refer to the attributes of CIA, where confidentiality is included.

2.1.7 Safety and cybersecurity ontologies

Safety and cybersecurity are two different concepts, and so their ontologies are composed of different elements and objects. In [26], it is attempted to link safety and cybersecurity objectives in an ontology in order to gain better theoretical understanding.

In order to build ontologies, it is possible to extract them from already existing ones and then expand them. In this way, safety ontologies can be expanded to include also cybersecurity. In [27], an ontology that already represents safety is expanded to consider also cybersecurity for the early stages of a system life cycle. Like this, it is able to gather and rank operational needs, assess the feasibility of the desired solution, and pinpoint any technological gaps. Moreover, in [28], a functional safety ontology is improved to consider attack scenarios. In this way, an ontology-based model for functional safety and cybersecurity verification and validation is proposed.

Finally, [29] attempts to integrate safety and cybersecurity in an ontology. This is different from the previous because the previous expand an already existing ontology to consider also cybersecurity, and they consider the early stages of a system's life cycle or the verification and validation process. While, this safety and cybersecurity ontology that is based on formal methods is able to represent the reaction of the system in different kind of scenarios.

2.2 Cyber-Physical Systems

With the use of ontologies, it is possible to understand the relationships between components whether they are cyber or physical ones. In [30], an ontology framework is able to capture the relationships between cyber and physical systems. Ontologies have a wide range of usage, since they can be used as analysis tool and a way to build knowledge hubs. For the analysis tool usage, the Technology Function Matrix is developed based on ontologies [31]. In order to build a knowledge hub, the authors in [32] use an ontology-based structure.

2.2.1 Safety properties

In relation to safety and in order to develop an ontology which considers all the properties that it interacts with as a whole, it is needed to understand how each relevant work provides partial coverage of the safety properties. Starting from maintainability, OntoProg is an ontology-based solution which is used for correct decision-making and assisting in the implementation of the Prognostics Health Management, for mechanical machines [33]. Furthermore, adding also the availability property to maintainability, an ontological structure is provided for availability as a criticality analysis which determines the maintenance strategy [34].

In [35], the three properties of reliability, availability, and maintainability, are provided. However, each one of these properties are found in a different super-concept of the solution, which means that they are not associated. Finally, the reliability and availability properties are provided through an ontological solution for

detecting and preventing the failures of the system components of Cyber Physical Systems (CPS) [36]. An ontology is used with all the CPS failures described in order to assist a multi-agent architecture to detect and identify the potential failures. And in [37], an ontology is built by transforming the results of the Failure Modes, Effects, and Criticality Analysis model into a class diagram. This ontology is utilized for detecting and preventing failures. As seen from above, the only paper that is the closest to the global image of safety is the paper that includes availability, maintainability, and reliability [35]. This is because it is the only solution that includes three of the properties that interact with safety.

2.2.2 Confidentiality property

Up to our knowledge, confidentiality ontologies for CPS are not widely researched in the literature. However, since confidentiality is a subproperty of dependability according to ENISA, it is possible to find ontologies that consider confidentiality for CPS in ontologies that concern all attributes of dependability. In [36], an ontology that concerns all attributes of dependability is used to consider various failures.

Additionally, confidentiality is also a subproperty of trustworthiness according to ENISA. Thus, it is possible to find ontologies that consider all attributes of trustworthiness. In [38], SIMON is an ontology framework that is able to ensure trustworthiness and by extension all of its attributes.

2.2.3 Safety and cybersecurity interdependency

In order to build an ontology that handles the safety and cybersecurity interdependency, it is needed to see if there are any research papers in the literature that cover this topic. However, in the literature, there are no papers for safety and cybersecurity interdependency in relation to CPS. In the literature, most of the papers for trustworthiness in CPS use the NIST CPS [39] standard, and none of them is using the ENISA one. In NIST CPS, safety, security, and reliability are subgroups of trustworthiness, while cybersecurity with the CIA approach are subgroups of security. For example, in [40], a framework is provided for reasoning about NIST CPS trustworthiness in CPS, which combines ontology-based reasoning and answer set programming. And in [41], an ontological design and verification framework is presented, which captures the relationships between cyber and physical components in CPS. Once again, NIST CPS trustworthiness is considered.

Furthermore, there is also STRAM, which is one more framework for trustworthiness [42]. According to STRAM, security and trust are its subgroups. Safety and reliability are subgroups of trust, while cybersecurity is a subgroup of security. Both NIST CPS and STRAM consider all of our properties separately and do not associate them. Moreover, in line with NIST and STRAM, safety and cybersecurity share no common properties. This makes us understand that by using NIST CPS or STRAM, there is no way to associate safety and cybersecurity in an interdependent way. However, ENISA gives us an image of the properties that interact with safety, as well as the properties that interact with cybersecurity. Moreover, ENISA also shows the two shared properties between safety and cybersecurity, according to which it is possible to build an architecture that provides safety and cybersecurity as interdependent.

Up to our knowledge, it is possible to distinctively find ontologies for the needed properties in relation to safety in the literature. However, there are no papers for a

safety ontology which includes all the safety properties that are found in ENISA. Furthermore, it is difficult to handle safety and cybersecurity interdependency through the properties of trustworthiness that are found in ENISA. And so, a new ontology for safety is needed to handle this interdependency.

3. NFV safety ontology

This section presents a new safety ontology. This ontology is used by an orchestrator that ensures safety in a NFV framework. Our proposed ontology is able to: (i) describe a variety of different breakdown types related to safety and (ii) help the decision for the best reaction to safety-related anomalies while considering the safety and cybersecurity interdependency. Our ontology-based solution is written in Ontology Web Language (OWL). This is because it provides greater content interpretability, in comparison with eXtensible Markup Language (XML) and Resource Description Framework (RDF). OWL language facilitates the expression of knowledge, and it also provides the means to reason with this knowledge.

As seen in [43], there are many advantages that ontologies bring. These advantages are (i) the modeling clarity which refers to the clear description, (ii) the choice of specificity level which refers to the level of the detailed representation of the content, (iii) the systematicity in information retrieval which makes it possible to access classes and subclasses to get information, (iv) the systematic and coherent definitions where the conceptual information are organized and clarified, and (v) the dynamicity as the ontology is able to represent the concept evolution through time. More specifically, our safety ontology is chosen because of its capabilities to model safety and its properties in a clear way with coherent definitions. Moreover, the possibility to access classes and subclasses in order to retrieve information supports the process of making decisions. These decisions are able to manage the safety and cybersecurity interdependency.

Our safety ontology provides the description of a representation of safety and the properties that it interacts with it according to ENISA. More specifically, all of these properties have the ability to cause anomalies which affect humans and environment. For this reason, the safety principle is decided to be the core of our proposed ontology.

All things considered, a NFV framework consists of a variety of modules. Different orchestrators are able to handle these modules. Thus, for ensuring and handling safety in a NFV framework, an orchestrator is needed. This orchestrator requires a way to identify whether a safety-related anomaly is also affected by cybersecurity. This is where our proposed ontology takes action, since with the help of the reasoner it is able to identify whether an anomaly is both safety and cybersecurity-related. In order to reach to this outcome, the reasoner uses (i) our proposed ontology and (ii) our safety and cybersecurity interdependency rules. NFV safety orchestrator needs this outcome in order to understand whether the mitigation plan creates violations to cybersecurity functionalities during mitigation.

In practice, our ontology consists of three parts: (i) the class of safety, (ii) the concerned elements, and (iii) the object properties (see **Figure 1**).

The first part provides safety as the class of our ontology. The second part describes the elements that are affected by potential safety-related anomalies. These elements are the functionality, structural, operational, and system. Each concerned element is associated with a safety-related anomaly. Thus, these concerned elements are represented as subclasses of safety. Finally, the third part provides the possible

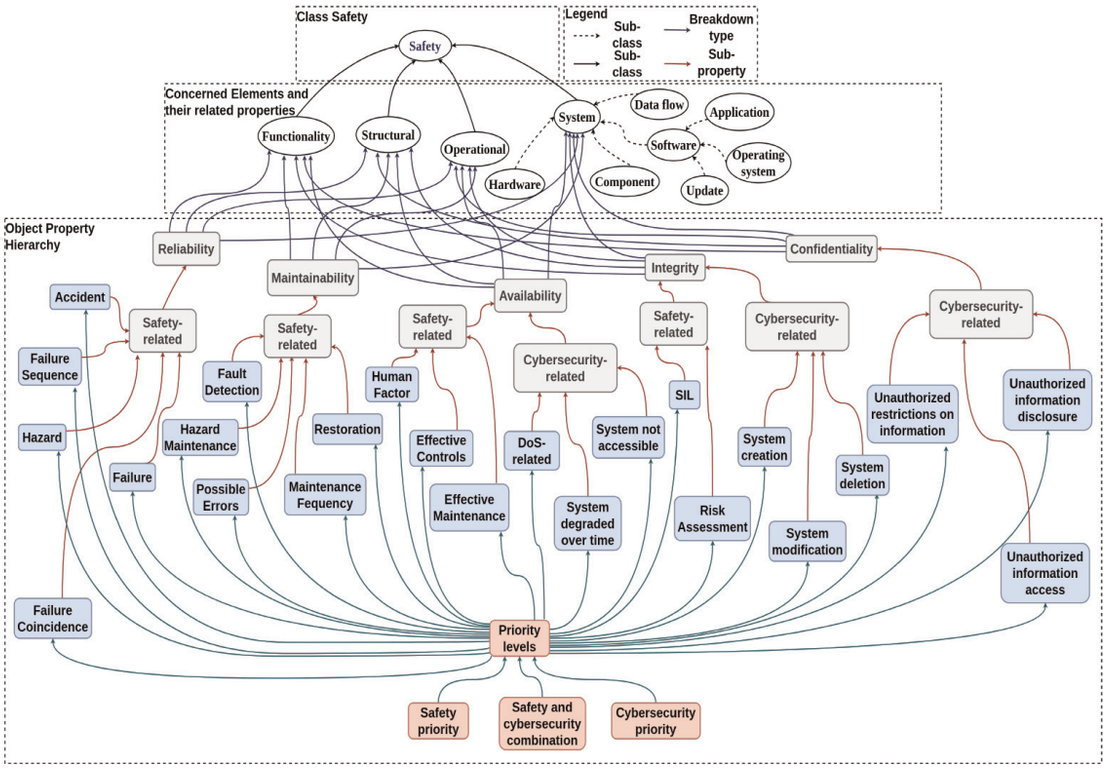

Figure 1.
Safety ontology.

breakdown types related to each one of the safety-related properties as they are found in ENISA. Each one of the safety-related properties and confidentiality is an object property of the concerned elements. And each one of these properties is associated with its relation to safety, cybersecurity, and/or both. By extension, each property is associated with their possible breakdown types. Each breakdown type is then assessed with respect to a priority level which is divided in safety, cybersecurity, and both.

It should be mentioned that our concerned elements and our breakdown types are extracted from the standards: NIST [44], MITER [45], ISO 61508 [46].

In particular, our ontology is able to provide three possible outcomes. The first outcome refers to the anomaly as only safety-related. The second outcome corresponds to an anomaly that is interdependent between safety and cybersecurity. In order to get this specific outcome, it is needed to to describe how the potential anomalies are related to the elements of the ontology. Thus, once a potential anomaly is identified as safety-related, it is then associated with its concerned element. According to the origin property of the anomaly (i.e. reliability, maintainability, availability, integrity, and confidentiality), it is possible to understand if it affects more than one property and if this impact is also creating cybersecurity-related breakdown types. For example, a VNF stops working. This VNF handles the access management of the cybersecurity functions. This event is a reliability problem which affects also availability and integrity. Thus, the reliability-related anomaly is able to affect cybersecurity. In this case, this anomaly is considered as an interdependent one between safety and cybersecurity.

Finally, the third outcome deals with the affected breakdown types, since it is possible to assess the priority level. This priority level indicates that safety, cybersecurity, or both orchestrators can handle the anomaly.

Certain rules are defined in order to handle the safety and cybersecurity interdependency. Based on the rules, the reasoner is able to make decisions for eventually avoiding potential safety and cybersecurity conflicts. There are two types of rules. The first type is composed of three statements concerning: (i) the type of breakdown, (ii) the relation of the anomaly to safety, cybersecurity, or both, (iii) and the affected object property (reliability, availability, maintainability, confidentiality, and integrity-related). According to these rules, it is possible to identify whether cybersecurity is affected through availability and integrity, but also to see how cybersecurity impacts safety through all the safety-related properties. And the second type of rules is composed of two statements considering: (i) the outcome of the first rules and (ii) the breakdown type. Thus, it is both of these types of rules that are used to automate the process of inferring, during decision-making.

4. Interdependency rules

Safety and cybersecurity interdependency rules are the ones that the reasoner uses to understanding whether a safety-related anomaly is also affecting cybersecurity and vice versa. But also, these rules are used to get the indication of which orchestrator between safety and cybersecurity is prioritized for mitigating the anomaly.

4.1 Safety and cybersecurity rules

In general, in order to create these rules, it is taken into account the type of the breakdown and its impact to cybersecurity. More specifically, the type of the breakdown is associated with: (i) the element that is affected by the anomaly and (ii) the specific breakdown type. The impact to cybersecurity refers to the object property that is affected by the specific anomaly. Thus, it is understood that there are three important terms. These terms are (i) the fact that the safety-related anomaly is coming from a cyberattack ($C.A.$ from cyberattack) or has the same effect, (ii) the subproperty of the specific object property ($B.T.$ from breakdown type), and (iii) the object property that is also affected by the anomaly ($O.P.$ from object property). It should be mentioned that our proposed rules are considered only when the event is coming from a cyberattack or has the same effect. Hence, each rule ($I.R.$ from interdependency rule) is a set of three statements referring to these terms, with the following form: $I.R. = C.A. + B.T. + O.P.$

As an example, a VNF at a production unit handles the working time scheduling between humans and robots. This VNF is cyberattacked and stops working. This is a cybersecurity anomaly. However, it also impacts safety since humans may be harmed. Thus, it is a safety-related anomaly which comes from the reliability property. This anomaly affects the functionality concerned element, and it can cause the accident breakdown type. It also impacts the availability, confidentiality, and integrity object properties. Thus, in this case, the corresponding rule is $I.R. = C.A. + Accident + All$, where:$All = Integrity + Availability + Confidentiality$.

All things considered, it is understood that each safety-related property has a total number of safety and cybersecurity interdependency rules. To calculate this total number, it is needed to calculate first the total number of our proposed rules for each one of the safety-related properties. In order to make this calculation, we created the following formula: $I.R._{tot\_x} = C.A. \times \sum_{B.T.} \times \sum_{O.P.}$.

In this formula: (i) the $I.R._{\cdot tot\_x}$ corresponds the total number of the interdependency rules for each one of the safety-related properties, (ii) the x is substituted by the *re* for reliability, *ma* for maintainability, *in* for integrity, *conf* for confidentiality, and *av* for availability, (iii) the $\sum_{B.T.}$ corresponds to the sum of the subproperties for each one of the safety-related properties, (iv) $\sum_{O.P.}$ refers to the sum of the possible object properties affected for the specific anomaly, and (v) the C. A. is equal to one since it is the Boolean true. It should be mentioned that reliability and maintainability are able to impact cybersecurity. However, availability and integrity are able to affect safety.

For each of the reliability and maintainability, the $\sum_{O.P.}$ is equal to four. This is because these properties can have four different possibilities of impacting cybersecurity. These four different possibilities are through availability, integrity, confidentiality, or all. For integrity, it is possible to impact safety through availability, reliability, or maintainability. Thus, the $\sum_{O.P.}$ is also equal to three. For availability, it is possible to impact safety through integrity, reliability, or maintainability. Hence, the $\sum_{O.P.}$ is also equal to three. Finally for confidentiality, it is possible to affect safety through reliability, maintainability, availability, and integrity. Thus, the $\sum_{O.P.}$ is equal to four.

Thus, the calculated total number of interdependency rules for: (i) reliability is: $I.R._{\cdot tot\_re} = 1 \times 5 \times 4 = 20$, (ii) maintainability is: $I.R._{\cdot tot\_ma} = 1 \times 5 \times 4 = 20$, (iii) availability is: $I.R._{\cdot tot\_av} = 1 \times 6 \times 3 = 18$, (iv) integrity is: $I.R._{\cdot tot\_in} = 1 \times 5 \times 3 = 15$, and (v) confidentiality is: $I.R._{\cdot tot\_conf} = 1 \times 3 \times 4 = 12$.

The total number of rules to manage the interdependency between safety and cybersecurity is calculated in the following formula. In this formula, the total number of the interdependency rules is the sum of each one of the interdependency rules of the safety-related properties. Thus, the total number of the interdependency rules is

$$I.R._{\cdot tot} = I.R._{\cdot tot\_re} + I.R._{\cdot tot\_in} + I.R._{\cdot tot\_av} + I.R._{\cdot tot\_ma} + I.R._{\cdot tot\_conf}, I.R._{\cdot tot} = 85$$

4.2 Priority level rules

This type of rules depends on the outcome of the previous reasoning and rules since it is taken into account the type of the anomaly. Thus, there is only one term for this rule which refers to the related types of the anomaly (*R.T.* from related-type). Each rule (*P.L.* from priority level) is equal to this one term: *P.L = R.T.* In case the potential anomaly is safety-related and does not affect cybersecurity, then this rule results that the safety orchestrator has to mitigate this anomaly. In the second case where the safety-related anomaly is impacting cybersecurity, then the outcome of the priority level rule is that both safety and cybersecurity need to handle the anomaly. In the third case where an anomaly is confidentiality and it also affects safety, then the priority level rule decides that only the cybersecurity orchestrator is to handle this anomaly.

The total number of this rule is equal to the sum of the possible related types for an anomaly. The related types for an anomaly are (i) safety-related, (ii) cybersecurity-related, and (iii) safety- and cybersecurity-related. Thus, the total number of the priority level rules is $P.L._{\cdot tot} = \sum_{R.T.} = 3$.

An example is provided for better understanding. A VNF that handles the emergency protection of a system stops working. This is identified as a reliability anomaly which is realted to safety. However, in the specifications of our system, this specific VNF is able to cause our system to degrade over time, in case it stops working. The breakdown type of system degraded over time is a cybersecurity-related bone. According to our ontology, this is a breakdown type that is subproperty of availability.

DOI: http://dx.doi.org/10.5772/intechopen.110333

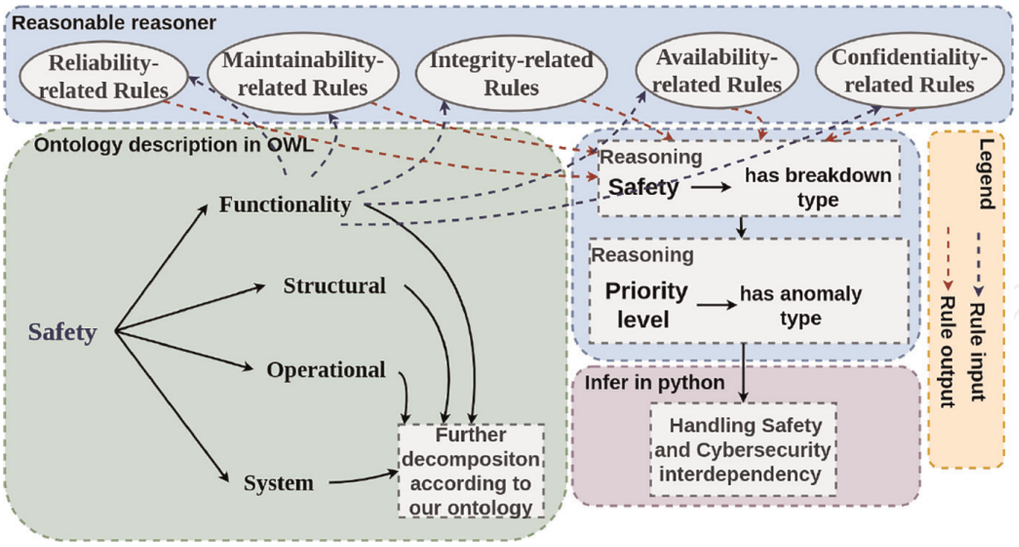

Figure 2.
Handling safety and cybersecurity interdependency, with the combination of our ontology and a rule-based reasoner.

Thus, it is understood that a safety anomaly has the same effect as a cyberattack to our system, and that both safety and cybersecurity are affected. Moreover, a reliability anomaly has impacted an availability one. Thus, based on the priority level rules, our reasoner decides that the priority-level outcome is for both safety and cybersecurity orchestrators to act upon the anomaly. More specifically, it is suggested that the safety orchestrator can handle the safety-related anomaly, while the cybersecurity orchestrator can handle the cybersecurity-related anomaly.

Considering everything, in **Figure 2**, it is possible to see the functioning model of our solution. Our model consists of three parts which are the ontology, the reasoner, and the outcome. Our ontology is represented in OWL in order to fully described the whole knowledge of safety in one common language. Each property of safety and confidentiality corresponds to a specific set of rules. The reasoner is able to make decisions based on these sets of rules and to provide an outcome that best handles the interdependency between safety and cybersecurity.

5. Evaluation and results

For the implementation and evaluation phase, a testbed is constructed with the intention to test our proposed safety orchestrator. Our testbed is composed of six Virtual Machines (VMs). These VMs are executed in a computer with an Intel core i7 processor which is running at 4.6 GHz. More specifically, the number of threads that are able to execute instructions at once is 16. Our machine uses 15.744 GB of RAM, with an additional Swap memory of 15.6 GB. The OS running is Linux, and more especially Pop OS 20.04 focal which is based on Ubuntu 20.04. Each VM uses 6 GB of RAM and 3 vCPU. Open Source MANO (OSM) handles all the VNF by using the VNF and NS descriptors for instantiation. And Openstack handles the whole architecture of the servers. Furthermore, each orchestrator of our proposed safety architecture corresponds to one VNF and one instantiated VM. It is possible to access these VM via openstack.

Our use case is provided in **Figure 3**. Free5GC includes the functions: (i) Network Repository Function (NRF): serves as a central repository for virtualized functions, (ii) Authentication Server Function (AUSF): supports the authentication of an entity that attempts to access a network, (iii) Access and mobility Management Function (AMF): manages the reachability, registration, mobility, and connection, (iv) Session Management Function (SMF): controls the session, and (v) User Plane Function (UPF): serves for the part of the network that carries the data traffic. In our testbed, the Free5GC core corresponds to the first server and represents the various VNF of a NFV framework. Each one of these functions corresponds to a VNF. Each one of these VNF is able to generate anomalies which are related to virtualized function and service issues with respect to NFV framework. For example, the VNF which corresponds to UPF function is not able to migrate. In this way, it is possible to simulate the issues of a NFV with respect to VNF. This is structured in a docker environment with each VNF occupying a container which uses Ubuntu 20.04.

Furthermore, the safety orchestrator needs to be able to receive the anomaly messages from the rest of the orchestrators. For this to happen, a client–server

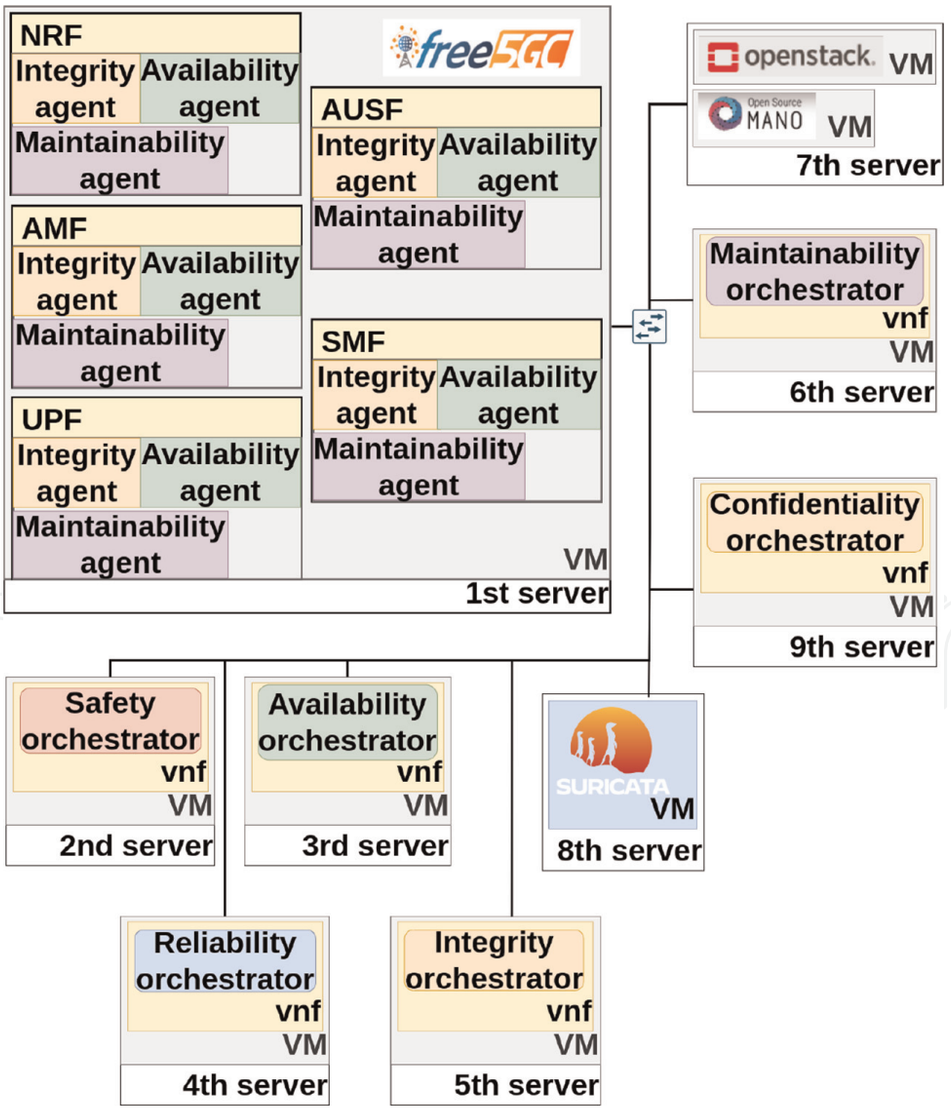

Figure 3.
NFV safety architecture use case.

architecture is implemented. This architecture uses the WSGIserver technology. According to this architecture, (i) safety orchestrator is the server which receives the anomaly message, treats it, and sends back the best response, (ii) and each one of the rest of the orchestrators is the client which sends the anomaly message and then receives the reply. Furthermore, the server sends two types of messages to the client: (i) one message is for sending the course of action to the act module of the client in order to implement them in case that the anomaly type is safety-related, (ii) and the second message is for sending back the anomaly information in case that the anomaly type is not safety-related. In case of a safety-related anomaly, it is possible to handle the interdependency between safety and cybersecurity. This is because the decided course of action is already verified from the reasoner feature in the conflict management module of the safety orchestrator.

The anomaly messages are pulled by a REST API, as it retrieves the message with a GET request. Each anomaly is therefore addressed in the URL, which makes the safety orchestrator able to access and process the message. In this way, the objects are retrieved by this specific URL. At first, they are treated to find the appropriate course of action. And then, they are sent to the Reasonable reasoner in the conflict management module for handling the safety and cybersecurity interdependency. In our case, our implementation handles the anomalies in parallel and more specifically between five processes.

In order for safety to be achieved, it is needed to analyze the results obtained from our implementation. These results are the type of the anomaly and the decided course of action that ensure safety and cybersecurity interdependency. Thus, safety is achieved once the anomaly message is treated and the course of action is decided and sent back to one of the rest of the orchestrators. Moreover, the total number of messages treated shows how effective and stable our proposal is. For this reason, it is important to acquire the time that each message takes to be treated. The shorter the time that an anomaly takes to be treated, the greater the number of the messages are treated. Consequently, the outcomes of our implementation are provided in terms of time which are as follows: (i) the reasoner processing time: the time that the conflict management module takes to decide how to best handle the safety and cybersecurity interdependency, and (ii) the total response time: the amount of time that it takes for one of the orchestrators to receive the response from the safety orchestrator.

For realizing **Figure 4a**, the number of the repeated tests is greater than 30 with 1 minute as a running time per each test. The number of anomalies treated is affected by the time that the reasoner needs to execute the rules in the safety architecture

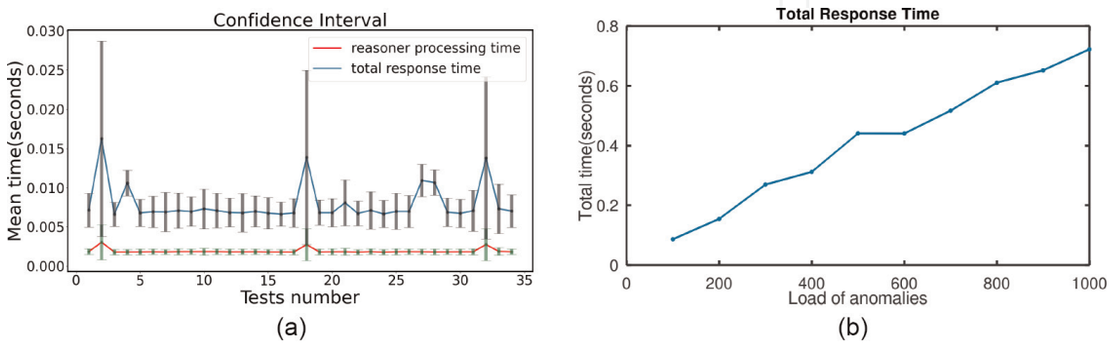

Figure 4.
(a) Reasoner processing time and total response time; (b) total response time's mean value in relation to different load of anomalies per second.

ontology, since it needs to be able to make decisions about the safety and cybersecurity interdependency. **Figure 4a** provides our two metrics. The total response time is in blue, and the reasoner processing time is in red. Each point of the lines corresponds to the mean value of one test. For each mean value point, the above and below standard deviation bars are provided. Some points have greater standard deviation values than others, since standard deviation is affected by the number of the samples and the mean value which both change from test to test. Thus, the points with the higher mean values are the ones with the greatest standard deviation. Finally, our study provides 95% of assurance that an anomaly is treated with confidence interval bounds of 0.0072 s to 0.0088 s for the total response time, and 0.0018 s to 0.0020 s for the reasoner processing time. Consequently, the mean time values for both of our metrics are quite low, and our solution is considered stable. This makes it seem possible to use our solution for real-time systems.

Figure 4b illustrates the total response time. In this test, the number of anomalies that are generated per second are iterated by 100 each time. It is understood that as the load of anomalies increases, the latency of the response time gradually rises. And it is almost linear. This is possible because the anomalies may be generated in 1 second, but the conflict management needs time to treat them all. Moreover, the anomalies are handled in parallel between five processes. However, the latency grows gently which seems to suggest that it is possible to meet the real-time constraints of many applications. Overall, this graph shows that our solution is scalable, and that it can be used for larger architectures.

6. Conclusion

Safety and cybersecurity are able to impact each other in a NFV framework, and so both of them need to be taken into consideration. Thus, it is important to be able to manage safety in a more comprehensive way. But, it is also important to handle the safety and cybersecurity interdependency. In this paper, an ontological-based solution for handling safety is proposed. Moreover, the safety and cybersecurity interdependency rules are proposed. More specifically, our proposed ontology is able to describe safety through the safety-related properties found in ENISA (i.e. reliability, availability, maintainability, and integrity). Together, the ontology and the rules are used by an orchestrator that manages the safety of a NFV framework. This is because the safety orchestrator needs to understand whether a safety-related anomaly is also affecting cybersecurity. This specific information is able to help the safety orchestrator to modify the plan of mitigation in order to avoid and functionality violations between safety and cybersecurity. In order to evaluate and test our solution, a testbed is created. This testbed is a safety and security management in 5G core network. According to the obtained results, our solution is able to ensure safety. Moreover, our solution is scalable, and it can be used in other applications.

DOI: http://dx.doi.org/10.5772/intechopen.110333

Author details

Dionysia Varvarigou[1,2]*, David Espes[1] and Giacomo Bersano[2]

1 Université de Bretagne Occidentale, Paris, France

2 Ikos Consulting, Paris, France

*Address all correspondence to: dionysia.varvarigou@etudiant.univ-brest.fr

References

[1] European Network and Information Security Agency. Measurement Frameworks and Metrics for Resilient Networks and Services: Technical report, Discussion draft. 2011

[2] Nogales B, Silva M, Vidal I, Luís M, Valera F, Sargento S, et al. Using aerial and vehicular NFV infrastructures to agilely create vertical services. Sensors. 2021;**21**:1342

[3] Gruber T. Ontology. 2018

[4] Xing X, Zhong B, Luo H, Li H, Wu H. Ontology for safety risk identification in metro construction. Computers in Industry. 2019;**109**:14-30

[5] Jiang X, Wang S, Wang J, Lyu S, Skitmore M. A decision method for construction safety risk management based on ontology and improved CBR: Example of a subway project. International Journal of Environmental Research and Public Health. 2020;**17**:3928

[6] Single J, Schmidt J, Denecke J. Knowledge acquisition from chemical accident databases using an ontology-based method and natural language processing. Safety Science. 2020;**129**:104747

[7] Fang W, Ma L, Love P, Luo H, Ding L, Zhou A. Knowledge graph for identifying hazards on construction sites: Integrating computer vision with ontology. Automation in Construction. 2020;**119**:103310

[8] Zhong B, Li H, Luo H, Zhou J, Fang W, Xing X. Ontology-based semantic modeling of knowledge in construction: classification and identification of hazards implied in images. Journal of Construction Engineering and Management. 2020; **146**:04020013

[9] Abdelghany AS, Darwish NR, Hefni HA. An agile methodology for ontology development. International Journal of Intelligent Engineering and Systems. 2019;**12**:170-181

[10] Bento A, Zouaq A, Gagnon M. Ontology matching using convolutional neural networks. In: Proceedings of the 12th Language Resources and Evaluation Conference. 2020

[11] Alkahtani M, Choudhary A, De A, Harding J. A decision support system based on ontology and data mining to improve design using warranty data. Computers & Industrial Engineering. 2019;**128**:1027-1039

[12] Ageed ZS, Ibrahim RK, Sadeeq M. Unified ontology implementation of cloud computing for distributed systems. Current Journal of Applied Science and Technology. 2020;**39**:82-97

[13] Kestel P, Kügler P, Zirngibl C, Schleich B, Wartzack S. Ontology-based approach for the provision of simulation knowledge acquired by Data and Text Mining processes. Advanced Engineering Informatics. 2019;**39**:292-305

[14] Banane M, Belangour A. Towards a new scalable big data system semantic web applied on Mobile learning. International Journal of Interactive Mobile Technologies. 2020;**14**

[15] Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS). BS EN 50126. 2017

[16] Frühwirth T, Preindl T, Kastner W. Ontology for rating dependability attributes. In: IECON2022–48th Annual Conference of the IEEE Industrial Electronics Society. IEEE; 2022

[17] Gobin-Rahimbux B. Evaluation metrics for ontology modules. In: 2022 IEEE International Conference on Data Science and Information System (ICDSIS). IEEE; 2022

[18] Lupp D, Hodkiewicz M, Skjæveland MG. Template libraries for industrial asset maintenance: A methodology for scalable and maintainable ontologies. In: Proceedings CEUR Workshop. 2020

[19] Montero JJ, Vingerhoeds R, Grabot B, Schwartz S. An ontology model for maintenance strategy selection and assessment. Journal of Intelligent Manufacturing. 2021:1-19

[20] Iglesias-Molina A., Chaves-Fraga D., Priyatna F., and Corcho O. Enhancing the Maintainability of the Bio2RDF Project Using Declarative Mappings. 2019.

[21] Kilintzis V, Chouvarda I, Beredimas N, Natsiavas P, Maglaveras N. Supporting integrated care with a flexible data management framework built upon Linked Data, HL7 FHIR and ontologies. Journal of Biomedical Informatics. 2019;**94**:103179

[22] Meng K, Cui C, Li H. An ontology framework for pile integrity evaluation based on analytical methodology. IEEE Access. 2020;**8**:72158-72168

[23] Chaves-Fraga D, Ruckhaus E, Priyatna F, Vidal ME, Corcho O. Enhancing virtual ontology based access over tabular data with Morph-CSV. In: Semantic Web. IOS Press; 2021

[24] Nikolaou C, Cuenca GB, Kostylev EV, Kaminski M, Horrocks I. Satisfaction and implication of integrity constraints in ontology-based data access. In: International Joint Conferences on Artificial Intelligence. 2019

[25] Manzoor S, Vateva-Gurova T, Trapero R, Suri N. Threat modeling the cloud: an ontology based approach. In: International Workshop on Information and Operational Technology Security Systems. Springer; 2019;**12**:170-181

[26] Blokland P, Reniers G. An ontological and semantic foundation for safety and security science. Sustainability. 2019;**11**:6024

[27] Pereira DP, Hirata C, Nadjm-Tehrani S. A STAMP-based ontology approach to support safety and security analyses. Journal of Information Security and Applications. 2019;**47**:302-319

[28] Shaaban AM, Schmittner C, Gruber T, Mohamed AB, Quirchmayr G, Schikuta E. Ontology-based model for automotive security verification and validation. In: Proceedings of the 21st International Conference on Information Integration and Web-based Applications & Services. 2019

[29] Alkhammash E. Formal modelling of OWL ontologies-based requirements for the development of safe and secure smart city systems. Soft Computing. 2020;**24**:11095-11108

[30] Venkata RY, Kamongi P, Kavi K. An Ontology-Driven Framework for Security and Resiliency in Cyber Physical Systems. ICSEA; 2018

[31] Trappey AJC, Trappey CV, Govindarajan UH, Jhuang ACC. Construction and validation of an ontology-based technology function matrix: technology mining of cyber physical system patent portfolios. In: World Patent Information. Elsevier; 2018

[32] Fang Y, Nazila RE, Chimay A. A Knowledge-Based Cyber-Physical System (CPS) Architecture for Informed Decision Making in Construction. In:

Construction Research Congress. American Society of Civil Engineers; 2018

[33] Nuñez DL, Borsato M. OntoProg: An ontology-based model for implementing Prognostics Health Management in mechanical machines. In: Advanced Engineering Informatics. Elsevier; 2018

[34] Polenghi A, Roda I, Macchi M, Pozzetti A. Multi-attribute Ontology-based Criticality Analysis of manufacturing assets for maintenance strategies planning. In: IFAC-PapersOnLine. Elsevier; 2021

[35] Ansari F, Khobreh M, Seidenberg U, Sihn W. A problem-solving ontology for human-centered cyber physical production systems. CIRP Journal of Manufacturing Science and Technology. 2018;**22**:91-106

[36] Sanislav T, Zeadally S, Mois GD, Fouchal H. Reliability, failure detection and prevention in cyber-physical systems (CPSs) with agents. In: Concurrency and Computation: Practice and Experience. Wiley Online Library; 2019

[37] Ali N, Hong JE. Failure detection and prevention for cyber-physical systems using ontology-based knowledge base. In: Computers. Multidisciplinary Digital Publishing Institute; 2018

[38] Venkata RY, Maheshwari R, Kavi K. Simon: Semantic inference model for security in cyber physical systems using ontologies. ICSEA; 2019

[39] Griffor E, Greer C, Wollman D, Burns M. Framework for Cyber-Physical Systems: Volume 1, Overview. Gaithersburg, MD: National Institute of Standards and Technology; 2017

[40] Nguyen TH, Son TC, Bundas M, Balduccini M, Garwood KC, Griffor ER. Reasoning about trustworthiness in Cyber-Physical Systems using ontology-based representation and ASP. In: International Conference on Principles and Practice of Multi-Agent Systems. Springer; 2020

[41] Venkata RY, Brown N, Maheshwari R, Kavi K. A domain-agnostic framework for secure design and validation of CPS systems. International Journal on Advances in Security. 2020

[42] Cho JH, Xu S, Hurley PM, Mackay M, Benjamin T, Beaumont M. Stram: Measuring the Trustworthiness of Computer-based Systems. NY: ACM; 2019

[43] Durán-Muñoz I, Bautista-Zambrana MR. Applying ontologies to terminology: Advantages and disadvantages. Hermes-Journal of Language and Communication in Business. 2013

[44] Ross R, Pillitteri V, Graubart R, Bodeau D, McQuaid R. Developing Cyber Resilient Systems: A Systems Security Engineering Approach. National Institute of Standards and Technology; 2019

[45] Bodeau G. MITRE, Cyber Resiliency Design Principles, Selective Use throughout the Lifecycle and in Conjunction with Related Disciplines. 2017.

[46] International Organization for Standardization. Functional safety of electrical/electronic/programmable electronic safety-related systems. ISO/IEC 61508-7:2010. International Organization for Standardization. 2010