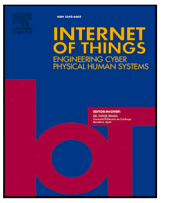
Internet of Things 27 (2024) 101267

Contents lists available at ScienceDirect

Internet of Things

journal homepage: www.elsevier.com/locate/iot



Research article

A methodology for ontology-based interoperability of dynamic risk assessment frameworks in IoT environments

Carmen Sánchez-Zas *, Xavier Larriva-Novo, Víctor A. Villagrá, Diego Rivera, Andrés Marín-Lopez

ETSI Telecomunicación, Universidad Politécnica de Madrid (UPM), Av. Complutense, 30, 28040, Madrid, Spain

ARTICLE INFO

Keywords:
Methodology
Risk assessment
Ontology
Internet of Things
Cybersecurity
Support to decision making

ABSTRACT

Proper cyber risk management is essential for organizations to make informed decisions and avoid potential financial losses, reputational damage, operational disruptions and other negative impacts. To this end, different institutions have defined risk analysis and risk management methodologies to address the problem and monitor cyber security in organizations. In this aspect, ontologies provide a very powerful tool for interoperability in risk management, given the heterogeneity of input information considered in the different steps of each framework and the ability they provide to perform logical reasoning in order to infer new knowledge. Throughout this study we analyze the different properties of some of the methodologies with the highest adoption rate, proposing an interoperable framework based on an ontology that allows compatibility between different systems, with a dynamic, flexible and efficient operation.

1. Introduction

In today's age of Internet of Things and its role in communications, any organization is exposed to a large number of cyber security attacks. Successful attacks can result in large financial losses, reputational damage or even indefinite business interruption. It is therefore essential to be continuously aware of the level of risk to which systems are exposed, to react and protect sensitive information dynamically in the event of an attack [1].

With this objective in mind, the agencies responsible for cybersecurity in different nations, together with groups of experts in the field, have defined frameworks to be followed when analyzing and managing security risks, especially information security. These frameworks are currently applied in most institutions worldwide and establish a set of steps or processes to estimate the level of risk that threatens the system and, in some of them, provide countermeasures to deal with attacks and estimate a residual risk level.

However, although these methodologies share the same objectives and nomenclature, some concepts or procedures differ, as shown below, so sharing information between them or comparing results becomes a difficult task, especially in the calculation of risk level.

The need for unification and interoperability in the cybersecurity domain strongly motivates this research. One of the key previous works in this context is an ontology to unify cybersecurity terms and concepts to support cybersituational awareness with rules for inferring new information [2]. In that research, the validation of the ontology is through a prototype following an Internet of Things use case and the comparison of the execution of certain queries and the expected result. This type of environment is chosen because it contains a high volume of assets, and because it is one of the most incident-prone environments in the world today. This proposal demonstrates that ontologies can manage very heterogeneous information, offering the possibility of giving them meaning

* Corresponding author.
E-mail address: carmen.szas@upm.es (C. Sánchez-Zas).

https://doi.org/10.1016/j.iot.2024.101267
Received 29 January 2024; Received in revised form 3 June 2024; Accepted 23 June 2024
Available online 2 July 2024

and establishing the series of reasoning rules required to follow one of these methodologies when combined with inference rules such as SPARQL Inference Notation (SPIN) [3] or Semantic Web Rule Language (SWRL) [4].

The main objective of this proposal, therefore, is to provide a single framework for risk management where different methodologies can be entered as input, and assessment is carried out based on an interoperable ontology, following the guidelines of the selected methodology and a standard risk management procedure, ITSRM. Today, with the popularization of the Internet of Things and the emergence of all kinds of sensors, it is essential to anticipate the various adverse situations that may arise, as well as to identify and assess the risks to which organizations are exposed and take measures to reduce their impact, identifying threats and knowing the level of risk is vital to respond to possible contingencies and establish appropriate preventive measures. In this proposal, the system is gathering information to perform a risk analysis and management, and map concepts from the input methodology into an interoperable risk assessment ontology.

Therefore, the novelty and contribution of this proposal to the interoperability concept lies in the implementation of a risk management and assessment methodology through an ontology capable of integrating information extracted from other frameworks, to transfer the processes of these methodologies to a common scale and thus being able to compare the effects of incidents or mitigations in different systems and to exchange vital information on threat responses between organizations. At the same time, the proposed system can carry out real-time risk management.

For this purpose, and after analyzing the methodologies in the field of risk management with the highest adoption rate at present, we decided to focus on the European frameworks, such as *Expression des Besoins et Identification des Objectifs de Sécurité* (EBIOS) [5–8], *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información* (MAGERIT) [8,9], Method for an Optimized aNAlysis of Risks by Cases (MONARC) [8,10], IT Security Risk Management Methodology (ITSRM) [8,11] and CCTA Risk Analysis and Management Method (CRAMM) [12]. This research aims to define an ontology that can be interoperable to apply any of these methodologies, thus obtaining a dynamic model compatible with the most widely used risk management standards. We have identified an IoT use case to validate the ontology. This validation is performed with a prototype which allows the execution of the risk management and assessment procedure using a developed ontology and a manager.

In Section 2, we present the key concepts of this subject: ontologies, risk management and a detailed analysis of the selected methodologies. In Section 3, we discuss existing works related to ontology applications in cybersecurity and risk management. To continue, in Section 4 the main proposal is defined, including a comparison among the frameworks introduced. We define the system developed in Section 5, including a formal definition of the ontology. Finally, a validation of the proposal is presented in Section 6, to end the document with the conclusions drawn and future directions in Section 7.

2. Background

2.1. Ontology

Ontologies [13] is one of the most popular tools for handling heterogeneous amounts of data when related entities stand out in the environments to be analyzed, as in the case of risk management.

They are considered formal specifications of the terms of a domain, and the relationships between them. They allow the exchange of information employing definitions of basic concepts that can be interpreted by machines and, therefore, can be automated [14].

This tool for data modeling serves as a knowledge base for other systems, and using reasoning rules allows the inference of new data, following a given behavior. The most commonly used languages to build the rules are SWRL [4], in which the rules consist of an antecedent which, when fulfilled, infers the second or consequent part, and SPIN [3], a W3C recommendation.

2.2. Risk management

Risk management consists of identifying and assessing the risks that could affect the organization, together with the creation of a plan to reduce or control those risks and their effect on their assets. These risks are related to losses and damages if an attacker manages to use one of the vulnerabilities in any of the systems to carry out an intrusion, so security must be a basic pillar, in order to be able not only to respond to threats but also to prevent them [15].

Among the processes included in risk management, we must differentiate between risk analysis and assessment. The objective of the first is to measure the risk and its associated impacts, obtaining an estimate of the impact associated with a possible incident, to prioritize and establish a risk mitigation strategy. On the other hand, the risk assessment process allows us to classify threats according to their category and the impact they may cause.

The main concepts common to any risk analysis or risk management process are [16]: assets, threats, vulnerabilities, impact, probability and risk.

- **Asset**: Any resource that an organization possesses in order to carry out its core business and whose deterioration implies damage to the institution.
- **Threat**: An unfavorable circumstance that may occur and harm assets, leading to a loss in value.
- **Vulnerability**: Weaknesses in assets that facilitate the materialization of threats.
- **Impact**: Materialization of the threat to the asset, taking advantage of a vulnerability. As a general rule, it estimates the percentage of degradation in the value of the asset.
- **Probability**: Frequency of occurrence of a threat, based on objective data or expert opinion.

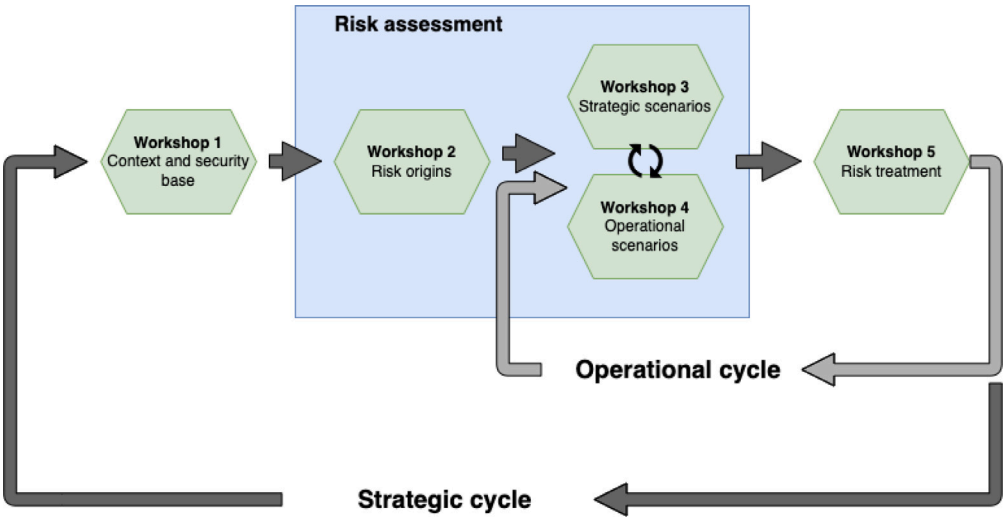


Fig. 1. EBIOS risk analysis and management process outline.

- **Risk**: It determines the likelihood that the threat to an asset will materialize, causing damage. Depending on this damage, there are four options to manage it: transfer it to another company or institution, avoid it, accept it or mitigate it.

Based on these concepts, and in order to establish a unified risk management framework, different organizations or institutions have defined methodologies adapted to their needs, which is detailed in Section 2.3.

2.3. Risk management methodologies

The main features of the most commonly used existing methodologies are presented below.

2.3.1. EBIOS

Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS) [5–8] is a French methodology created in 1995 to assess and address information security risks. It provides a risk management environment comprising the installation of a management system accompanied by a security strategy and its integration into different projects. In Fig. 1 the five workshops that compose this methodology are represented. The objective is first to characterize the system under study and then to define risks as twofold (origin of the risk, origin of the target). Next is analyzed at the primary and supporting asset level. Finally, the last workshop allows the assessment of risks previously identified and analyzed and provides means to address them and decide whether to accept the residual risk or not.

It stands out for its flexibility and its ability to identify the blocks that make up the risk, unlike other methodologies that only determine the elements of predefined scenarios. However, it is a self-assessment and subjective methodology.

2.3.2. MAGERIT

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT) [8,9] is a risk analysis and management framework developed by the Spanish Government's High Council for e-Government to reduce the risks of the implementation and use of Information Technologies in the public sector. The main objective is to make organizations and administrations aware of the existence of these risks by providing a systematic method of analysis including risk treatment planning.

It is composed by three books, "The method", "The Elements Catalog" and "The Technical Guide". The first covers risk analysis procedures and risk management, the second contains catalogues of assets, threats or safeguards, and finally, the last is a technical guide on the legal basis, conceptualization and purpose of the analysis.

This framework is a qualitative, asset-based methodology that provides a tool for analyzing information systems risks named PILAR (*Procedimiento Informático-Lógico para el Análisis de Riesgos*), a Computerized-Logical Procedure for Risk Analysis developed by the Intelligence National Center.

The processes that this methodology carries out to perform risk management are represented in Fig. 2. It starts characterizing assets, finding their dependencies and valuation; threats, occurrence and damage caused; and safeguards, identification and assessment (how to protect it and monitor the risk). Then, the system estimates what is expected to occur and, depending on the residual risk assessment, treatment is initiated. Finally, a security plan is defined, where the treatment of risks are materialized. It comprises three tasks: identification of the security process, implementation plan and execution, which will serve as an aid to subsequent treatments or as a source for standards.

It offers a systematic approach for evaluation, audit, certification or accreditation processes, but it evaluates everything in economic aspects, so it has to be translated from other types of valuations.

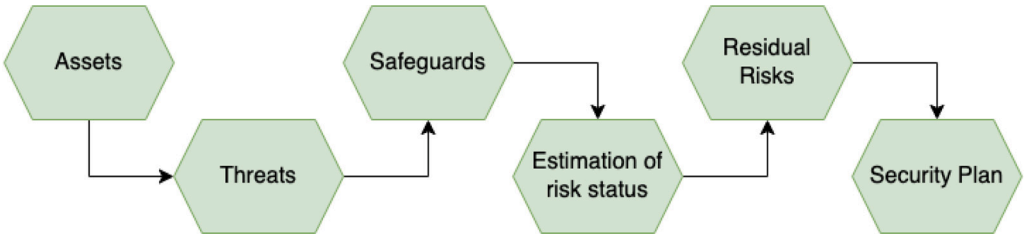


Fig. 2. Outline of the MAGERIT risk analysis and management process.

Fig. 3. Outline of the MONARC risk analysis and management process.

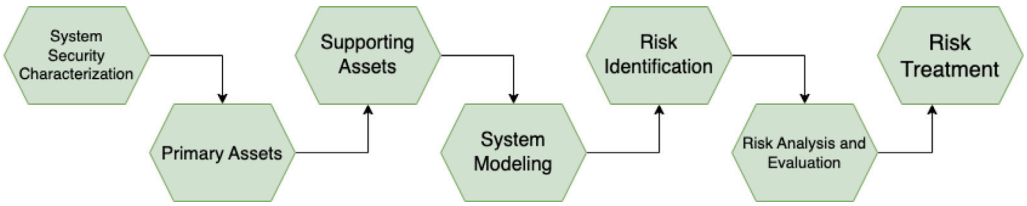


Fig. 4. Outline of the ITSRM risk analysis and management process.

2.3.3. MONARC

Method for an Optimized aNAlysis of Risks by Cases (MONARC) [8,10] is a risk management tool that capitalizes risk based on previous analysis. It is based on a library of risk models that offer different scenarios depending on the assets. It is divided into four phases represented in Fig. 3. First, the identification of key activities, critical business processes, as well as their potential threats and vulnerabilities following a qualitative assessment method. Then, the identified assets will be represented in a diagram showing their dependencies and the threats or vulnerabilities that affect them. To continue, a quantification method is used to estimate the risk of the system, based on which the necessary measures and a plan to reduce the risk are deployed. The different risks are ranked according to different criteria, which allows them to be compared according to a defined acceptance threshold. Finally, the aim is to optimize security and extend the scope of the risk analysis by performing a recurring system security check.

MONARC leverages previous analyses on other systems in the same business environment, which will suffer similar attacks on similar asset structures, resulting in generalized risk scenarios for each type of business.

2.3.4. ITSRM

IT Security Risk Management Methodology (ITSRM) [8,11] is a methodology that is part of a set of standards for information security by the European Commission Directorate-General for Informatics.

This framework consists of seven processes, as shown in Fig. 4. The first step is gathering information about the system. Then, the identification of primary assets (mainly data and functions), crucial for the organization in achieving its business objectives and the identification of those assets used in the management of the primary assets. Also, an association model between primary and supporting assets is developed, following the data flow and system architecture. In the risk identification step, the scenarios to be analyzed are constructed, representing the risks of the primary assets and their consequences on themselves and the supporting assets. The objective is to determine the risks that will be later analyzed, assessed and addressed. In the next process, the system will calculate the residual risk level in the defined scenarios, according to a list of security measures defined to mitigate those threats. Finally, the most appropriate measures will be selected to respond to the identified risks, taking into account the organization's limitations.

This methodology uses highly adaptable ISO standards and provides a common framework for risk management. It also provides catalogues of threats, security measures, constraints, potential adversaries and supporting assets. However, it is not yet a complete solution, and its implementation is complex.

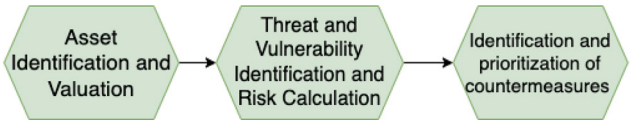


Fig. 5. Outline of the CRAMM risk analysis and management process.

2.3.5. CRAMM

CCTA Risk Analysis and Management Method (CRAMM) [12] performs a qualitative risk analysis proposed by the UK government and has a tool to carry out the process. The main objective here is to justify the investments made in security by quantitatively demonstrating the need for action.

CRAMM phases are represented in Fig. 5. First, asset identification and valuation are performed (the three types of assets that are assessed in this methodology are data, application software and physical assets). Then, threats and vulnerabilities are studied according to the selected asset groups. In addition, the risk of each group of assets is estimated against their threats and vulnerabilities. Finally, a series of countermeasures applicable to the system are selected, evaluating positively if it protects against more than one threat, if there are no other alternatives, if the cost is lower, if it is more effective or if it prevents incidents.

This framework takes into account all stages of a system's life-cycle, has an extensive database of countermeasures that is frequently updated, allows for reviews and raises awareness of the need for cyber security, but requires a qualified professional to implement.

3. Related works

In the literature review, we have found a number of previous research works focused on the use and creation of ontological models for cybersecurity, such as attacks or vulnerabilities. However, few works are focusing on threat modeling and operational security, including Cyber Threat Intelligence, proving the challenge of using and integrating them.

In the search for ontology models, first, those related to Threat Intelligence were analyzed. In this way, [17] introduces an ontological approach to analyze a system design and the creation of security patterns using sources of threats and countermeasures for automatic threat modeling in cloud-based systems. Authors in [18] describe a CTI model to analyze and share threat information in an effective way using ontologies. There was also found a vulnerability ontology in [19] designed for an alert system for vulnerabilities and countermeasures using SWRL rules.

In recent years, an increasing amount of research based on risk management was developed, especially using ontologies [20–24]. The strength of the tool in this type of work, allowing interoperability between different domains, is highlighted in [25,26], where authors apply ontologies to identify threats and risks using a reasoner and information from external sources, as vulnerabilities databases, validating the results with a use case. However, they emphasize the impossibility of creating new instances by inference. This limitation, in certain contexts, such as ours, is a weakness of the SWRL rules, as risk management is not only intended to modify attributes or create relationships, but the incidents received should trigger the automatic creation of threats and the calculation of risks.

Nevertheless, we could also find previous examples where ontologies are not the core technology of the proposal such as in [27], where authors introduce a risk assessment and response management method validated through a use case, emphasizing the use of attack graph generators to define possible risk scenarios. A similar methodology is used in [28] to assess risks using attack vector modeling. Authors in [29] apply Machine Learning (Bayesian Neural Networks) to predict the severity of future risks based on previous assessments.

Moreover, the large number of proposals based on ontological models allows us to consider them as one of the preferred technologies for the undertaken task, thanks to their reasoning capacity. They are used to exchange information, as observed in [30], centered on operational risk management using ontologies. They facilitate information sharing across an organization and heterogeneous business areas, supporting decision-making helped by reasoning rules. In [31], authors define an ontology in cybersecurity to help in info-gathering and risk assessment procedures in complex systems.

Thus, authors in [32] present a technique based on an ontology for risk propagation calculation, used to measure the impact on different assets. The risk is expressed according to the impact of the CIA-triad (confidentiality, integrity, availability). Also, in [33] a framework to assess security risks in cloud computing platforms is presented, where risk is defined as a combination of the probability and impact of an event. Risks and impacts are categorized following different defined security objectives, whereas impact scales follow FIPS model. An ontology specialized in risk assessment is presented in [34], using a threat-driven method to evaluate how dangerous APT attacks are from different perspectives (tactical risks, assets risks and responses to APT attacks), and authors in [35] propose a methodology for assessing risk in information systems, including as a novelty known and unknown vulnerabilities, which are not usually considered.

The need for concept unification and interoperability presented in [2] is also the motivation in more recent works as [36], highlighting the urge for using standardized terminology in cybersecurity, specially in risk management.

However, the only proposals found that are specifically based on ontologies applied to risk management frameworks, as is the case of our proposal, are the following: Authors in [37] show an example of an ontology to model Cyber Threat Intelligence data and reasoning rules for real-time risk monitoring, based on risk definitions in ISO 27005 and dependencies between risks,

Table 1
Comparison of methodologies in relation to general aspects.

Analyzed methodology	Qualitative analysis vs. Quantitative analysis	Asset-based vs. Process-based
EBIOS	Both	Both
MAGERIT	Both	Assets
MONARC	Qualitative	Assets
ITSRM	Both	Assets
CRAMM	Both	Assets

threats, vulnerabilities and assets. They highlight the importance of using semantic reasoning in a cybersecurity decision-making system. Moreover, graphical risk models to develop risk assessment algorithms based on ISO 31000 are presented in [38]. Also, in [39] authors present a solution to manage ISO 27005:2011 standard to help understand concepts using an ontology and a case scenario as an example. The model captures the core concepts and relations from the risk management methodology. On a different approach, authors in [40] develop an ontology to select the most appropriate methodology for risk management according to the characteristics of the organization. It is based on ISO 31000, ISO 31010 and ISO 73 to support those standards on identification, analysis and risk assessment, and to help in the choice of risk management techniques. Also, in [41] an extension of MAGERIT to include fuzzy concepts is developed. Finally, as a preliminary work, it is necessary to mention [42], where authors presented a formalized definition of cybersecurity risks, related to ENISA risk management methodologies comparison document [8], and where they propose as future work a framework to manage the implementation of risk analysis according to standards.

As a first solution to the problem posed in some of the previous research works on instance creation and real-time processing, we validated the use of SPIN rules in a dynamic system in the research presented in [43]. The conclusion drawn from the analysis of these research works is therefore that the existing need for interoperability is not fully met and is a focus of ongoing work. Most cybersecurity ontologies analyzed are domain-specific and therefore reusing them implies significant modifications to obtain the generalization necessary for interoperability. Furthermore, as we have presented, some initiatives are trying to unify the cybersecurity domain in its various aspects, but in terms of risk analysis and management, we find theoretical work such as the mentioned above, but any systems that enable this interoperability.

4. Proposal

This methodology arises from the comparison of a set of risk management methodologies. These have been chosen from among those that appear in the comparison carried out by ENISA [8,11] according to the following criteria: must be European frameworks; must have accessible and detailed documentation on their processes, as the objective is to extract information to be able to establish interoperability; and must carry out asset-focused risk management.

After analyzing the information of each framework and following ENISA guidelines, we designed an ontology using ITSRM concepts to perform risk management.

Finally, a management system is developed. It is in charge of performing translations among the selected methodologies and ITSRM concepts and runs through the various processes until a potential risk calculation is obtained according to ITSRM, to the original methodology and, after automatic recommendation of countermeasures, the residual risk level.

In the following sub-section, the comparison of countermeasures is detailed and, subsequently, the description of the ontology and the system as a whole is further elaborated.

4.1. Comparison of methodologies

In this section, and intending to find common points between the different methodologies analyzed that can be used in the development of the ontology for an interoperable methodology, we present an analysis of the conclusions of the study carried out in the document produced by ENISA [8,11].

Firstly, the general aspects of the frameworks considered are:

- Quantitative or qualitative analysis, depending on whether the assessment is based on perception or available and verifiable data.
- Asset-based or process-based risk management, whether the focus is on assessing assets and the threats and vulnerabilities are exposed to in order to estimate risk, or whether the focus is on situations or processes within the system that can be exploited by attackers.

This comparison of the methodologies introduced is presented in Table 1. In it, we can see that most methodologies are based on assets rather than processes, and almost all of them perform both types of analysis, qualitative and quantitative. Therefore, the methodology developed in this proposal is asset-based and performs both analyses.

To continue, the functional aspects analyzed are as follows:

- Asset taxonomy: systematic classification of assets, analyzing the category to which they belong, whether they can be modified or new assets can be introduced.

- Asset evaluation: whether the methodology contains guidelines for evaluating assets using a scale or criteria, and whether this scale can be modified or new criteria added.
- Threat Catalogue: whether the methodology has an internal catalogue of threats and whether this catalogue is modifiable.
- Vulnerability catalogue: whether the methodology has an internal catalogue of vulnerabilities and whether it is adaptable.
- Calculation of risk: establishment of a method for calculating the level of risk.
- Catalogue of countermeasures and calculation of residual risk: the existence of a manual of countermeasures to deal with the risk and whether exists a method to calculate the residual risk after applying one of the defined measures.

The characteristics of the methodologies chosen in this respect are:

- Asset Taxonomy:
  - **EBIOS**: Classification in Primary Assets and Supporting Asset.
  - **MAGERIT**: Provides a catalogue of assets in Book II of the methodology. Allows the import of new assets, not new types.
  - **MONARC**: Classification in Principal Assets and Secondary Assets.
  - **ITSRM**: Classification in Primary Assets and Supporting Assets.
  - **CRAMM**: Classification in three types of assets (Data, Application Software and Physical Assets).
- Asset Valuation:
  - **EBIOS**: Provides severity thresholds. Modifiable.
  - **MAGERIT**: A scale of assessment criteria between 0 and 10 is presented in Book II of the methodology.
  - **MONARC**: Assessment on the basis of implementation. Not modifiable.
  - **ITSRM**: Offers different options (reuse assessments, by impact scale or by formal impact assessment). Modifiable.
  - **CRAMM**: Scale defining the impact on asset dimensions from 1 to 10 on a subjective basis.
- Threats Catalogue:
  - **EBIOS**: Provides examples. Modifiable.
  - **MAGERIT**: A default list is presented in Book II of the methodology. New catalogues can be added, but the existing one cannot be modified.
  - **MONARC**: Exists a predefined list. Modifiable.
  - **ITSRM**: Contains threat catalogue. Allows new catalogues to be added.
  - **CRAMM**: Predefined Threat tables according to asset group.
- Vulnerabilities Catalogue:
  - **EBIOS**: Not specified. New catalogues cannot be imported.
  - **MAGERIT**: Not specified.
  - **MONARC**: Predefined list. Modifiable.
  - **ITSRM**: There are no catalogues. Vulnerabilities are an independent functional component.
  - **CRAMM**: Added through interviews.
- Risk Calculation:
  - **EBIOS**: Risk calculation is not specified. Based on probability and impact.
  - **MAGERIT**: Book III provides techniques for qualitative and quantitative calculations. They are not modifiable.
  - **MONARC**: The standard formula is Risk = Threat × Vulnerability × Impact. This formula is modifiable.
  - **ITSRM**: The formula for this methodology is Risk = Probability × Consequence. The matrices are modifiable, the formula remains the same.
  - **CRAMM**: The tool is used to calculate risks, which are ranked on a scale of 1 to 7.

As seen, when comparing different frameworks, each one carries out risk assessment focused on a specific area, so that interoperability, understood as the capacity to reuse the information provided by components of other methodologies, could be considered a point for improvement in terms of current methodologies. Our design is a first step towards achieving this interoperability, as it allows data from different methodologies to be transformed into a common calculation, thus allowing comparisons or exchange of information.

5. System design

The proposed system receives as inputs the outputs of the experts' activities in each methodology: the organization's assets, the vulnerabilities associated with those assets, the system's information, the countermeasures available for that system or organization, and the identified risk scenarios for the organization. Incidents occurring in the system in real time, previously identified by a detection system, and characterized, shall also be recorded.

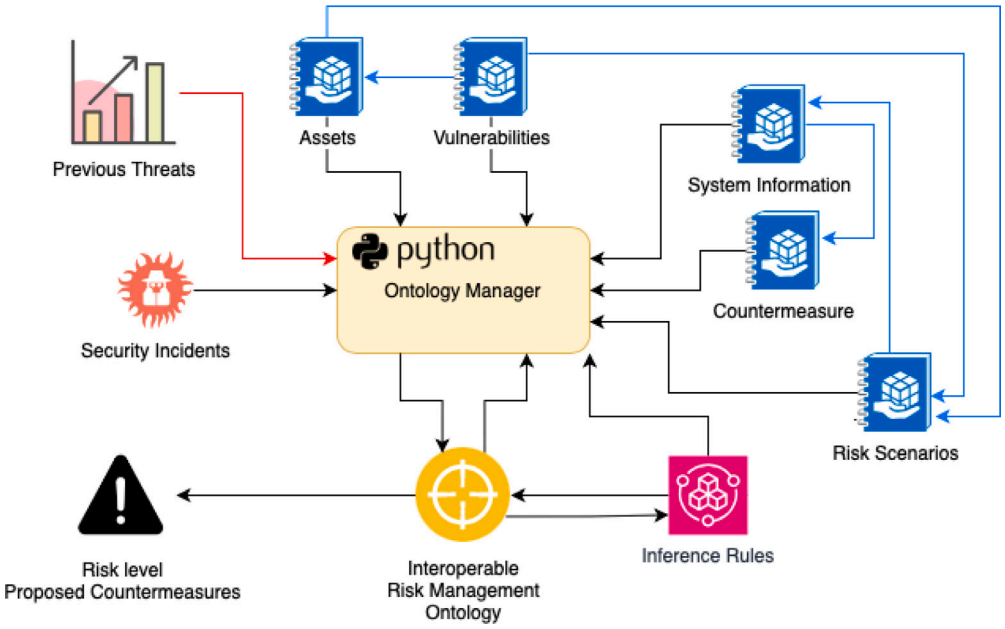


Fig. 6. Scenario of the proposal.

All this data is collected by the management module, which is in charge of loading the catalogues coming from one of the interoperable methodologies, into the concepts defined in the ontology. This subsystem also manages the ontology and inference rules, which allows estimating probability and impact values for each threat. Also, according to defined risk scenarios, the manager performs the calculation of the risk level and the propagation of the effect of these incidents on the system assets, as well as selecting the most appropriate countermeasures to protect them, calculating the residual risk for each identified threat.

ENISA has carried out work before this development, proposing a toolbox [44] for translating between other risk management methodologies and the one proposed by them as a standard methodology, to share information and compare them. Following the guidelines set out in that document, the designed joint system presented here aims at collecting information to perform risk analysis and management automatically, performing calculations on a standardized scale, but it also can normalize values from other risk management reports performed by other methodologies, to compare results. In addition, logic is included in the system to provide decision support for the choice of the optimal countermeasures.

Starting from the theoretical basis provided by ENISA, we obtain a functional and interoperable system that allows the management and assessment of risks in real-time.

The ontology classes and the different rules and processes are described in the next section. An overview of the procedures and the architecture is shown in Fig. 6, where red arrows represent optional inputs, the black ones relationships between inputs, outputs and processes of the proposed methodology and the blue ones represent relationships between the different catalogues.

The system that manages the ontology is also in charge of populating it using JSON format catalogues, considering the main characteristics of each input in the analyzed methodologies:

- **System Information**: This file contains general information about the system analyzed: identifier, risk acceptance level and the original methodology (MAGERIT, EBIOS, MONARC, CRAMM).
- **Assets**: This file contains a list of the organization's primary assets, and its related supporting assets: type and values for the security dimensions.
- **Vulnerability**: This file contains a list of vulnerabilities affecting assets that exist on the system: CVE, description, type, CWEs, CPEs, CVSS and the ID of the asset.
- **Previous Threats**: This file contains previous existing threats on the system, generated in other management processes, if they want to be imported into the system. This catalogue accepts threat definitions from other methodologies (words in Spanish or different denominations for mapped threats). The information included refers to its classification, consequence on security dimensions, origin and a list of involved assets.
- **Risk Scenarios**: This file contains the result of expert analysis regarding risk scenarios, identifying possible targeted assets (primary assets and supporting assets), the vulnerabilities that expose them and the type and properties of the threats that will be generated in case an incident matches those fields.
- **Security Incidents**: This information is generated in an IDS and is processed and enriched previously to this system, and contains information related to the Tactics, Techniques and Procedures (TTPs) of the incident, and the exploited vulnerabilities and affected assets.

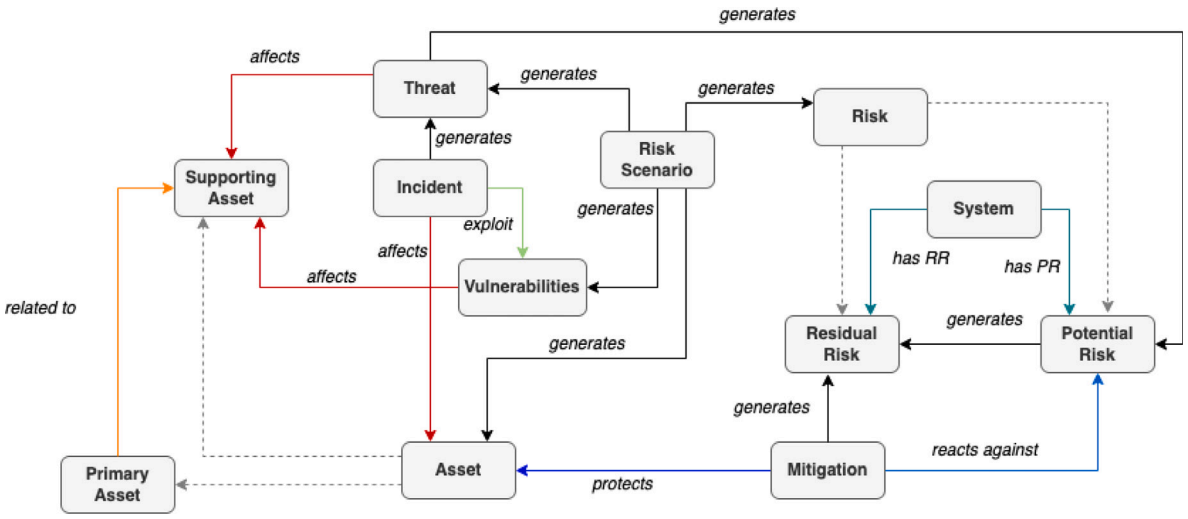


Fig. 7. Ontology Schema. Dashed lines reflect classes that are sub-classes of others, while solid lines represent relationships between classes.

- **Countermeasures**: This catalogue contains the existing countermeasures in the environment and information to select the optimal and estimate the residual risk and its mitigation effect. The information given about the responses is related to their type, keywords to define it, deployment cost and effort, impact, installation and operation complexity, time to be up and running, effectiveness, mitigation factor and the type of asset they protect.

5.1. Ontology design

Based on the conclusions obtained in the previous analysis, the design of an ontology that can follow the processes defined in the risk management methodologies presented in Section 2.3 is proposed. It is adaptable, trying to model a generic dynamic methodology that is interoperable with them. Despite all the ontologies identified in Section 3, due to the need to use terms from the ENISA toolbox and ITSRM methodology, which are interoperable, it has been decided to build the ontology from scratch instead of reusing an existing one, as they are usually very specific and include concepts and relationships specific to the scenario for which they were designed.

By being defined in a recommendation from an entity such as ENISA, the organization in charge of ITSRM, the classes fit with the core concepts of any risk management methodology. These entities and the attributes and relationships created are common to most of the related work identified in charge of risk analysis.

OWL is used as the ontology definition language, chosen as one of the most modern, flexible and up-to-date W3C recommendations [45]. Besides, its main strength is being compatible with rule-definition languages such as SPARQL [46] to define the behavior of the environment. For this reason, the combination of OWL + SPIN rules is applied to this proposal.

Fig. 7 represents the classes identified to depict the risk management methodology. These classes have a number of properties, as described below, that allow the creation of individuals from the catalogues proposed in the methodologies presented throughout this document.

The properties and relationships that make up each of the classes would be as follows, based on previous work and own contributions:

- System: In this class, properties from the global system are stored, such as the original methodology, if it exists, or the risk acceptance level. Regarding risk calculation, we can find the overall system risk level calculated with the interoperable method and with the original methodology, and finally, the residual risk level, once the countermeasures have been applied.
- Asset: This class shall present the properties common to all sub-classes: Asset Type, Security Dimensions (Confidentiality, Integrity, Availability) and Description.
  - Primary Asset: This subclass defines the assets that are crucial for the activity of the organizations. It contains as asset types Information and Data, and Processes, Functions and Services. They are "*related to*", at least, a Supporting Asset.
  - Supporting Asset: Subclass that represents the assets that are used in the management of the primary assets. They are also "*affected by*" vulnerabilities. The types of assets inside this subclass are Hardware, Devices and Equipment, Infrastructure, Location and Utilities, Personnel and Software and Applications.

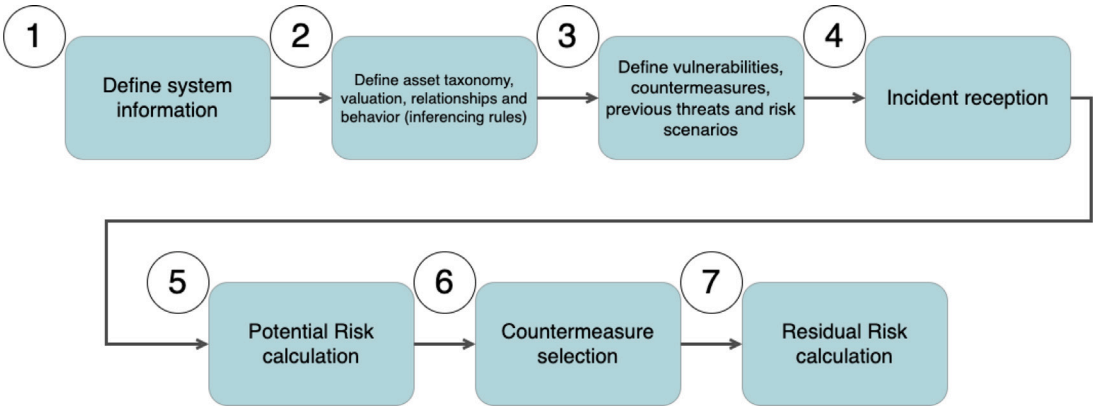


Fig. 8. Sequence of processes defined for the proposed methodology.

- Vulnerabilities: Shall be defined by an Identifier (CVE), Type, Description, Common Weakness Enumeration (CWE), Common Platform Enumeration (CPE) and Common Vulnerability Score System (CVSS). As the inverse property from Supporting Assets, Vulnerabilities "*affect*" this subclass.
- Incident: This class represents the security incidents detected in the system. Its properties shall be, as a minimum: ID, Description, Date and TTPs. In order to link it with other classes, the properties "*affect*" Assets, "*exploit*" Vulnerabilities and "*generate*" Threats.
- Threats: They are defined by Description, Origin and two sets of properties to define which security dimension it affects and its consequence. In addition, they are related to Potential Risks by the property "*generate*" and with Supporting Assets by "*affects*". As sub-classes, we included Errors and unintentional failure, Industrial, Natural, Willful attacks and Service-related threats. Each one has the sub-classes identified in the ENISA document [44].
- Risk item: The main property for this class is risk level. It is mainly used to store the risk calculation using the original methodologies. Its sub-classes are Potential Risk and Residual Risk. Potential Risks "*generate*" Residual Risks, and they are "*affected by*" Mitigations. Residual Risk has the inverse properties "*related to*" with Mitigations and Potential Risks, and as a property, the calculation of residual risk level.
- Countermeasures: This class is defined by Identifier, Description, Type, Keywords, Deployment Cost, Deployment Effort, Installation Complexity, Operation Complexity, Time to be Up and Running, Impact, Effectiveness and Mitigation Factor. It has also defined the properties disabled if, for any reason, this countermeasure is not available, and enabled, if it has been selected and proposed. Regarding other classes Mitigations "*generate*" Residual Risks, "*protects*" Assets and "*reacts against*" Potential Risks.
- Risk Scenario: This class is characterized by properties Identifier, Impact and Probability. It is related to other classes: It "*generates*" Risks and Threats, and "*involves*" Assets and Vulnerabilities.

5.2. Ontology manager design

The objective of the module is to automate the risk calculation and assessment using the original methodology and an interoperable method so that when an incident is detected affecting an asset of the organization, threats, new relationships and changes in the corresponding risk values or asset valuation are generated. Countermeasures should also be recommended from the catalogue based on the calculated risk level, and the risk acceptance criteria.

The main contribution of this work is to achieve an ontology applicable to practical use cases where risk management is based on any of the analyzed frameworks. To this end, we developed a system manager and defined the behavior of the model, building a series of restrictions and rules of reasoning. Before the operation of the system, a group of experts must analyze the environment and carry out a study to define the assets, the available vulnerabilities and countermeasures, and compose risk scenarios, generating the catalogues defined above.

Fig. 8 shows the different steps to be followed in the methodology presented.

The first step in the ontology manager is to load the ontology and include context information (identifier of the system, original methodology if existed, and the risk acceptance level, below which risks will not be treated). To continue, the asset catalogue is loaded, creating individuals and relations for each Primary and Supporting Asset listed in the catalogue. Then, an inference rule is executed to update the primary asset valuations in terms of security dimensions, considering the supporting assets related to it.

```
DELETE {
?pa uri:confidentiality ?c.
?pa uri:integrity ?i.
?pa uri:availability ?a.
} INSERT {
?pa uri:confidentiality ?nc.
?pa uri:integrity ?ni.
?pa uri:availability ?na.
} WHERE {
?asset a uri:Supporting_Asset.
?asset uri:confidentiality ?c.
?asset uri:integrity ?i.
?asset uri:availability ?a.
?pa a uri:Primary_Asset.
?pa o:related_to ?asset.
BIND(AVG(?c) as ?nc)
BIND(AVG(?i) as ?ni)
BIND(AVG(?a) as ?na)
} group by ?pa
```

SPARQL Inferencing rule: Update of primary asset valuation

The next step is to load the vulnerability catalogue, creating instances of the identified vulnerabilities that expose an asset, and, the mitigations catalogue, relating those new instances to the assets affected and protected. If there are relevant threats previous to the importation and use of the system, they are loaded and mapped into the sub-types defined in the ontology, creating the corresponding individuals. For instance, if the original methodology is MAGERIT, threats are introduced in Spanish, and converted to the toolbox corresponding threat, in English. Also, those threats affect Supporting Assets and have an impact on their security measures, by reducing their values. This effect should be extended to the related Primary Assets.

Then, risk scenarios are created as instances, with the required information to generate threats if an incident is registered and matches the fields of one of those instances. At this point, all previously existing data has been uploaded to the system, and it is awaiting the registration of incidents. The first risk calculation is performed, firstly, following the original methodology. The system generates Risk Instances related to the previous threats, estimating their impact and probability, and obtaining a risk level value according to its definition: EBIOS (Low, Medium, High), MAGERIT (*Muy Bajo* (Very Low), *Bajo* (Low), *Medio* (Medium), *Alto* (High), *Muy Alto* (Very High)), MONARC (Low, Medium, High) and ITSRM (Very Low, Low, Medium, High, Very High). CRAMM methodology is centered on assets valuation, vulnerabilities' CVSS and threat consequences, instead of threats impact and probability or likelihood and consequence, and the obtained risk scale are integer numbers between 1 and 7. Then, the calculation following the toolbox methodology is performed, generating Potential Risks. In both methods, a general system risk level is calculated, and the results can be compared.

When an incident is registered, the system generates an instance for it, and the vulnerabilities and assets involved are compared to the existing risk scenarios. If there is a match, then the threat defined in the risk scenario is created. Then, risk levels are updated, taking into account that the risk scenarios may be defined according to the scales of each methodology, and must be translated to perform the calculation according to the toolbox method.

As part of the decision support system, the module should analyze the available countermeasures and mitigations, rank them according to their properties, and select the optimal, which is used to calculate the residual risk. The pre-selection of mitigations related to each potential risk is obtained using inference rules. As an example, if the type of threat is registered as a keyword of a mitigation it is selected as a possible countermeasure for that specific case:

```
CONSTRUCT {
?m uri:reacts_against ?risk.
?risk uri:is_affected_by ?m.
} WHERE {
?risk a uri:Potential_Risk.
?threat a uri:Threat.
?threat rdf:type ?x.
?threat uri:generates ?risk.
?asset a uri:Assets.
?threat uri:affects ?asset.
?m a uri:Mitigations.
?m uri:protects ?asset.
?m uri:keywords ?k.
FILTER CONTAINS(str(?x), str(?k))
}
```

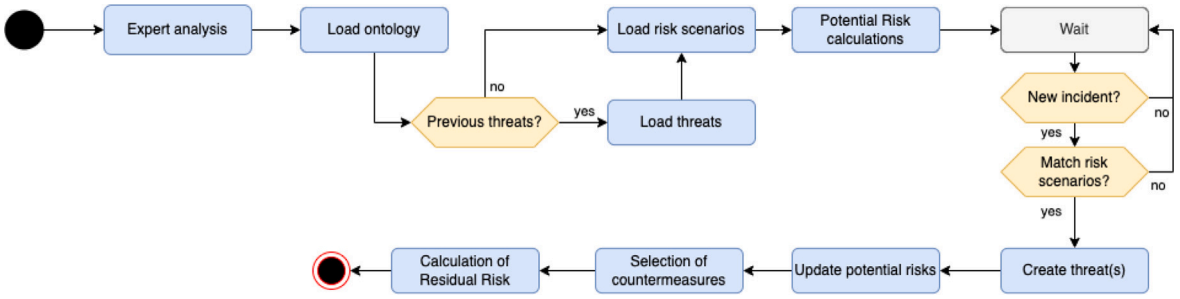


Fig. 9. Ontology manager workflow.

SPARQL Inferencing rule: Pre-selection of countermeasures

Then, with the pre-selected mitigations, the system discards for the calculation of the optimal countermeasure for those which are disabled, and those with a higher impact than the risk addressed. The remaining are sorted considering its deployment cost on one side, the required time to be up and running on the other, and finally, the rest of the parameters scaled from 0–10, obtaining a score. The optimal countermeasure would be the one with the maximum score, minimum cost and required time, and is updated as enabled.

The residual risk is calculated assuming this mitigation has been deployed, for those potential risks with levels higher than the risk acceptance level defined for the system. The global risk calculation is also updated, in this case only following the toolbox methodology.

As a summary, Fig. 9 presents the workflow in the Ontology Manager.

6. Validation

As it is an ontology-based development, as seen in the related literature, the results are evaluated by verifying the system's behavior in defined use cases. This proposal belongs to a project under development, so for validation, a prototype is developed and information on the inputs and results obtained is presented here.

6.1. Validation methodology

In order to carry out the validation of the proposal, different approaches are used. Regarding the interoperability of the designed ontology and methodology, the functional aspects described in Section 4.1 are checked.

To verify the interoperability of the system, the objective proposal, and a validation following the use cases defined in [44] are described, to check if the expected results are obtained, and after that, a use case to verify the functioning of the complete system. For this, a prototype is developed in Python, using the Protégé tool to visualize the ontology. The first use case focuses on introducing into the system certain data in the format of a specific framework and performing the risk calculation according to that methodology and the standardized calculation. For the MONARC Use Case and MAGERIT Use Case, we created the same simulated scenario. The asset catalogue is filled with eight assets (three primary assets and five secondary assets), with its relations and values in the different security dimensions. The threat to be used to assess the translation of the risk level is Denial of Service.

In the last use case presented, all the system processes presented in Fig. 9 will be tested in an IoT environment.

6.2. Functional aspects validation

The objective here is to verify whether the proposed methodology and system are capable of adapting to the requirements in these functional aspects of the risk management methodologies: Taxonomy and Valuation of assets, Threat and Vulnerabilities catalogues and Risk Calculation.

- Asset taxonomy: This aspect assesses the asset classification in the methodology. In the proposal, two main sub-classes were created, Primary Asset, containing Information/Data and Processes/Functions/ Services, and Supporting Asset, which contains Hardware, Infrastructure, Locations, Personnel and Software. With this structure, and the code developed in the manager to map the entries of each framework, all the classes of the considered methodologies can be translated to one of the sub-classes defined in the ontology:
  - EBIOS defines a classification between primary assets and supporting assets which coincides with those defined in the ITSRM-based ontology. Similarly, MONARC uses the terms 'principal asset' and 'secondary asset', but they can be associated with the terms of the ontology 'primary asset' and 'supporting asset', which represent the same concepts.

Table 2
Asset catalogue in MONARC use case (PA: Principal Asset, SA: Secondary Asset).

Asset	PA/SA	Type	C	I	A
Asset_Monarc_1	PA(1)	Information	–	–	–
Asset_Monarc_4	SA(1)	HW	5	3	2
Asset_Monarc_5	SA(2)	SW	10	6	3
Asset_Monarc_2	PA(2)	Functions	–	–	–
Asset_Monarc_6	SA(3)	Personnel	7	9	3
Asset_Monarc_7	SA(4)	SW	9	8	7
Asset_Monarc_3	PA(3)	Information	–	–	–
Asset_Monarc_8	SA(5)	SW	1	2	3

Table 3
Threat in MONARC use case.

DoS threat features	Value
Primary assets	Asset_Monarc_2
Supporting assets	Asset_Monarc_6
General category	Willful
Specific category	Denial of Service (DoS)
Security dimensions affected	C,I,A
Security dimensions value	0.7,0.6,0.4
Origin	Deliberated
Impact	4
Probability	4

  - MAGERIT does not separate into primary and supporting assets. The categorization defined in Book II (Data, Services, Software, hardware, networks, personnel, etc.) is mapped into a type of asset from the ITSRM catalogue listed above. The same applies to CRAMM, which considers three types of assets (data, application software and physical assets).

- Asset valuation: This feature considers the possibility of valuating assets according to some criteria. For the presented system, assets are evaluated in three of the dimensions of security (Confidentiality, Integrity and Availability) on a scale of 1 to 10, which varies dynamically according to the threats to which they are exposed and the countermeasures that protect them. In this way, the asset valuation of this proposal is compatible with the methodologies studied previously.
- Threat Catalog: The type of threats accepted by the system is the predefined list in ITSRM methodology, considered the basis of the interoperable system. In addition, in the code developed for the prototype manager, translations are made between the defined threats in other methodologies, even if they are in their original languages, such as Spanish in the case of MAGERIT, and they are mapped to the equivalent within the ITSRM framework. For example, the system accepts as input a list of threats exported from the original methodology, and handles the translation according to this interoperable methodology.
- Vulnerability Catalog: This aspect, in most of the methodologies studied, is considered an optional input. For the system presented, the vulnerability catalogue is an input that uses values specific to the CVE vulnerabilities.
- Risk Calculation: Each methodology studied has its formula or heat map for calculating the level of risk. In this proposal, this calculation is maintained, in addition to the standardized procedure, using the ITSRM method, to make comparisons.

The steps or processes that make up each of the methodologies define the steps to follow when filling the catalogues or executing certain conditions in the code, especially in the case of assets and threats or risk calculation.

6.3. Use case 1: MONARC and MAGERIT

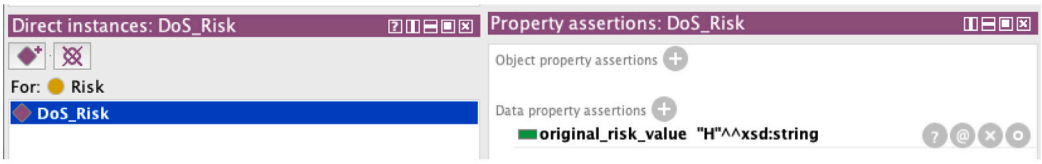
In the first use case presented, the interoperability of the system is tested with the MONARC and MAGERIT frameworks as the original methodology. For this purpose, two reduced use cases will be created in the same environment and their result will be compared.

To begin, the system has as input data from the MONARC framework, whose risk calculation method and the standard (ITSRM) differ in the number of levels (3 in MONARC and 5 in ITSRM), so that initially a risk classified as high or low in MONARC is not comparable with one classified the same in ITSRM, the former referring to the limits of the scale while the latter are intermediate levels. The input asset values for the simulated scenario in this use case are detailed in Table 2.

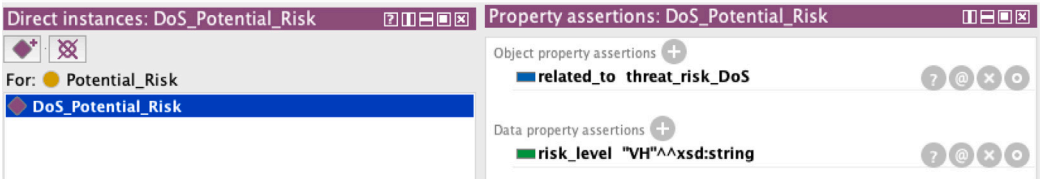
We want to verify the calculation of this tool for a Denial of Service threat with the highest probability and impact in MONARC methodology (4 out of 4). To do this, we created a threat that meets these requirements (Table 3).

Once the tool is executed, as expected, the expected result following MONARC Methodology is that the DoS Risk level is High(H), the maximum value within this scale, while using the presented system based on ITSRM, it is Very High (VH), maximum value in this procedure. In Fig. 10 the results obtained are presented, in line with the expectations. Inputs from MONARC terms have also been found to be compatible with the proposed system.

Secondly, a similar case is generated, but with the input methodology data coming from the MAGERIT framework and, therefore, in Spanish. Its risk scale is similar to ITSRM, both have five levels, although the conditions and calculations for belonging to each



(a) Results for MONARC Methodology - Use Case 1.1



(b) Results for ITSRM Methodology - Use Case 1.1

Fig. 10. Results for DoS risk calculation — Use case 1.1.

Table 4
Asset catalogue in MAGERIT use case.

Asset	Type	C	I	A
Asset_Magerit_1	*Datos*	–	–	–
Asset_Magerit_4	HW	5	3	2
Asset_Magerit_5	SW	10	6	3
Asset_Magerit_2	*Servicios*	–	–	–
Asset_Magerit_6	*Personal*	7	9	3
Asset_Magerit_7	SW	9	8	7
Asset_Magerit_3	*Datos*	–	–	–
Asset_Magerit_8	SW	1	2	3

Table 5
Threat in MAGERIT use case.

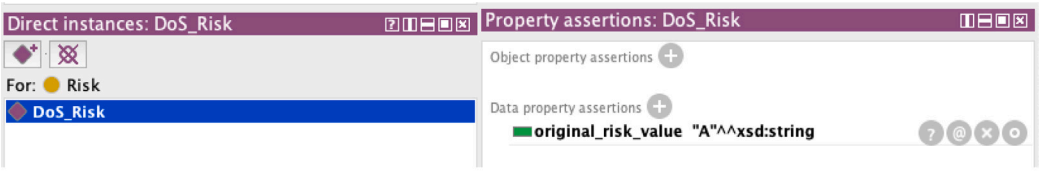
DoS threat features	Value
Primary assets	Asset_Magerit_1
Supporting assets	Asset_Magerit_4
General category	*Deliberada*
Specific category	*Denegación de Servicio*
Security dimensions affected	C,I,A
Security dimensions Value	0.7,0.6,0.4
Origin	Deliberated
Impact	A
Probability	M

of them differ. The previous simulated scenario is adapted to the new methodology (Table 4). The asset type here is in Spanish and not explicitly divided into Primary and Supporting Assets.

Again, we want to verify the calculation of this tool for a Denial of Service threat with a probability of 3 out of 5 (“M”, Medium) and an impact of 4 out of 5 (“A”, High), using the MAGERIT methodology. For that, we created a threat that meets these requirements (Table 5).

The obtained results with the system are, again, as expected: the result with MAGERIT Methodology is that DoS Risk level is “*Alto*” (A, High value, 4 out of 5) the same as using the toolbox, High (H, value 4 out of 5), as shown in Fig. 11. Here, also the terms from the MAGERIT methodology are compatible with the interoperable system.

In this use case as a whole, it has been possible to validate the processes of translating terms and calculating risks using MONARC, MAGERIT and ITSRM. In addition, the main objective, which was to be able to compare risks, is also verified: in the MONARC scenario, the risk according to the methodology was high (H), as in the MAGERIT scenario (A), having two threats with different properties. At first sight, these two threats might seem equally important, but when compared on a standard scale, ITSRM, it is observed that the risk in the MONARC scenario is very high (VH), while the MAGERIT scenario is still high (H), one level below, so that the first threat should be prioritized. Moreover, this system would allow the sharing of information from other methodologies to address risks, such as catalogues of countermeasures that have been previously effective.



(a) Results for MAGERIT Methodology - Use Case 1.2

(b) Results for ITSRM Methodology - Use Case 1.2

Fig. 11. Results for DoS risk calculation — Use case 1.2.

Table 6
Asset catalog.

Asset	Confidentiality	Integrity	Availability
Primary Asset 1	7.5	4.5	2.5
Supporting Asset 1	5	3	2
Supporting Asset 2	10	6	3
Primary Asset 2	5	5	5
Supporting Asset 3	1	2	3
Supporting Asset 4	9	8	7

Table 7
Vulnerability catalog.

CVE	CWE	CPE	CVSS	Asset
CVE-2023–0001	CWE-{001,002}	CPE-1	High	S.A. 3
CVE-2023–0002	CWE-003	CPE-{2,3}	Medium	S.A. 2
CVE-2023–0003	CWE-{004,005}	CPE-1	Critical	S.A. 1,2

6.4. Use case 2 — IoT environment

For this validation case, we are using EBIOS methodology as original input, to check that it is also compatible with the system, leaving only CRAMM methodology unchecked in this document, due to extension purposes. We also verify the functioning of every process described in previous sections, to validate the full operation of the tool in a Internet of Things environment.

Input catalogues: For this case, we have created the following information within the catalogues:

- Assets: In this case, we are working with an environment in which we are going to monitor light sensors (hardware) as assets, which are controlled by software and generate information. Primary Asset 1 (information) is related to Supporting Assets 1 (Hardware) and 2 (Software). On the other side, Primary Asset 2 (Service), is related to Supporting Asset 3 (Hardware) and 4 (Software). The security dimensions from the primary assets are calculated from their related supporting assets when the inferencing rule described above is executed. The results are shown in Table 6:
- Vulnerabilities, presented in Table 7, represent typical vulnerabilities of this type of sensors. Their identifiers represent formats to identify these vulnerabilities but do not refer to concrete examples, as we are not displaying specific information on the assets to identify their related vulnerabilities.
- Previous threats to the beginning of the use case are introduced in Table 8. These threats have an impact on the security dimensions of the affected assets.
  The changes produced by the creation of these threats are presented in Table 9, representing how vulnerable are those assets to threats in this environment. The values assigned to the security dimensions of supporting assets in the ontology are updated and through the execution of the inferencing rule, the primary assets are updated to show the consequence of threats.
- Mitigations, introduced in Table 10. Any of the mitigations is initially deployed or disabled for any reason. With the countermeasure selection, this situation might change. The range of values is defined manually to prove this process, specially the impact, which is one of the major filters.

Table 8
Threat catalog.

ID	Type	Subtype	Consequence on C,I,A	Asset
Threat1	Natural	Flood	(0, 0, 0.2)	S.A. 1
Threat2	Industrial	Fire	(0, 0, 0.8)	S.A. 1
Threat3	Unintentional failure	User Error	(0.1, 0.4, 0.6)	S.A. 1
Threat4	Willful attack	DoS	(0, 0, 0.7)	S.A. 1
Threat5	Service related	Lock-In	(0, 0, 0.9)	S.A. 4
Threat6	Service related	Lock-In	(0.7, 0.2, 0.9)	S.A. 2

Table 9
Asset catalogue affected by threats.

Asset	Confidentiality	Integrity	Availability
Primary Asset 1	7.5 ⇒ 3.75	4.5 ⇒ 3.3	2.5 ⇒ 0.169
Supporting Asset 1	5 ⇒ 4.5	3 ⇒ 1.8	2 ⇒ 0.0384
Supporting Asset 2	10 ⇒ 3	6 ⇒ 4.8	3 ⇒ 0.3
Primary Asset 2	5	5	5 ⇒ 1.85
Supporting Asset 3	1	2	3
Supporting Asset 4	9	8	7 ⇒ 0.7

Table 10
Countermeasure catalog.

ID	Mitigation 1	Mitigation 2	Mitigation 3	Mitigation 4	Mitigation 5
Keywords	SW Tampering Destructive Attack User Error CVE-2023-0001	Destructive Attack	User Error	User Error	User Error
Complexity (op./inst.)	1/4	2/8	7/8	2/8	5/7
Deployment cost/effort	2000/5	10000/9	10/9	100/9	120/9
Time to be up and running	1	365	365	36	120
Impact	VH	VL	VH	VL	VL
Mitigation factor	0.6	0.9	0.6	0.6	0.9
Disabled	False	False	False	False	False
Enabled	False	False	False	False	False
Asset protected	S.A. 2	S.A. 3	S.A. 1	S.A. 1	S.A. 1

Table 11
Risk scenarios.

ID	Assets	Vulnerability	Threat	Probability	Impact
Risk Scenario 1	S.A. 1, P.A. 1	CVE-2023-0001	Deliberated malware diffusion	1	3
Risk Scenario 2	S.A. 3, P.A. 2	CVE-2023-0001	Destruction of media	2	4

Table 12
Incidents registered.

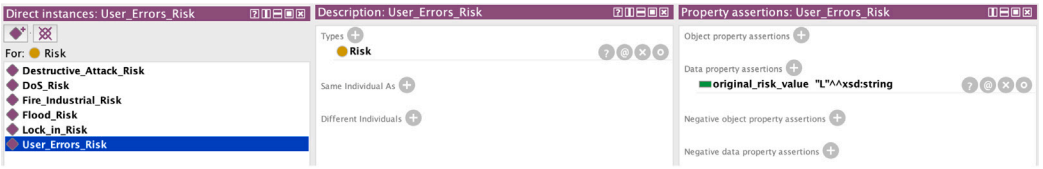
ID	TTPs	Assets	Vulnerability	Risk scenario matched
Incident 1	TTP1, TTP3, TTP5, TTP7	S.A. 1, S.A. 4	CVE-2023-0002	None
Incident 2	TTP2, TTP4, TTP6, TTP8	S.A. 3, S.A 4	CVE-2023-0001 CVE-2023-0003	Risk Scenario 2

Risk Scenarios and Incidents: Based on the experts' analysis, we identify a set of risk scenarios, defined by the incidents received in the system, and the vulnerabilities and assets involved. Those situations generate the defined threats with a given impact and probability (Table 11).

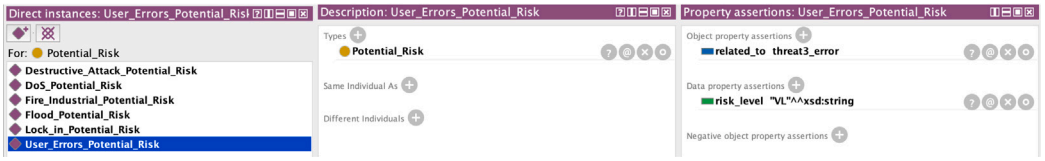
When any incident is registered (Table 12) and it affects an asset exploiting a certain vulnerability, matching with one or more risk scenarios, the threat related to those cases is generated. In this case, the first incident does not generate a threat, meanwhile, the second incident generates the threat related to the second risk scenario in Table 11. This incident affects Supporting Asset 3, using Vulnerability CVE-2023-0001 and generates a Destructive Attack (Type: Willful) with a consequence equal to 0.4 on the availability dimension of Supporting Asset 3.

Table 13
Asset catalogue affected by risk scenario threat.

Asset	Confidentiality	Integrity	Availability
Primary Asset 1	3.75	3.3	0.169
Supporting Asset 1	4.5	1.8	0.0384
Supporting Asset 2	3	4.8	0.3
Primary Asset 2	5	5	1.85 ⇒ 1.25
Supporting Asset 3	1	2	3 ⇒ 1.8
Supporting Asset 4	9	8	0.7



(a) Results for EBIOS Methodology: User Error Threat Risk - Use Case 2



(b) Results for ITSRM Methodology: User Error Threat Risk - Use Case 2

Fig. 12. User error threat potential risk — Use case 2.

Fig. 13. Global potential risk — Use case 2.

In Table 13 the final asset valuation is displayed, as an evolution from Tables 6 and 9.

Potential Risk Calculation: The next step is to estimate the risk level regarding all the threats included in the system. This calculation is performed following both the original methodology and the interoperable procedure. As an example, the risk calculation for User Error Threat is presented: The only threat of this type is the previous threat with identifier Threat 3. Following EBIOS Methodology, this threat has impact 2 and probability 1, meaning a LOW (L) risk level, while in the interoperable framework, it has a LOW impact and VERY LOW probability, resulting in a VERY LOW (VL) risk level. In this case, the two calculations do not match, and therefore the threat would not be treated the same in each methodology (Fig. 12).

In the system instance, the global potential calculations considering all threats instantiated for both methodologies are registered: MEDIUM (M) risk for EBIOS methodology and LOW (L) risk in the interoperable calculation. Both in the case of a specific threat and for the overall potential risk, lower levels are obtained using the interoperable framework (Fig. 13). In both the User Error Threat risk and here, the interoperable calculation obtains one level down in the scale than the original. This is because EBIOS only has three levels, while ITSRM has five.

Countermeasure selection and Residual Risk Calculation: In this step, several checks are made. In Table 10 we could see that any mitigation was selected since any of the assets protected by it was not attacked. After registering incidents, Mitigations 3, 4 and 5 react against the same type of risk (keyword User Error), and therefore they are proposed for optimization. Mitigation 3 is discarded because its impact (VH) is higher than the risk level (VL) of the threat. According to the parameters introduced and the algorithm created, Mitigation 4 was selected (enabled attribute changed from False to True), hence, it generates a residual risk. Mitigation 2 is also selected to protect against Destructive Attacks directly because there are no other options. In this procedure, only the risks generated with the toolbox, not the original methodology, are considered: User Error potential risk level was VERY LOW and the countermeasure action could not further decrease its value (residual risk level is also VERY LOW) and, on the other hand, Destructive Attack level was HIGH and, when applying a countermeasure with mitigation factor equals to 0.9, the residual risk is reduced to LOW. Also, the global residual risk is calculated for the whole system. In this case, since the reduction of risks is

Table 14
Risk calculation for user error threat.

Threat	EBIOS risk level	Interoperable potential risk level	Interoperable residual risk level
User Error	L	VL	VL
Destructive Attack	M	H	L

Table 15
Global risk calculation.

EBIOS risk level	Interoperable potential risk level	Interoperable residual risk level
Medium	Low	Low

not significant, compared to the rest of the risks that are not mitigated, the potential global risk and the residual global risk coincide. The risk level evolution is summarized in Tables 14 and 15.

7. Conclusions and future lines

Considering the importance of Risk Analysis and Management as procedures in cybersecurity, and the amount of threats that IoT devices receive, the study and comparison of methodologies is nowadays a highly relevant topic. Being able to compare them and, in some cases, work with several at the same time, is a source of great development at the moment. This, together with the advantage that ontologies pose in this field, as stated in the Related Works analyzed, was at the origin of this development.

The most widely accepted risk management methodologies today cover all the main aspects, however, some differences can be seen in the way risk is treated, or in the way catalogues are provided to complete the analysis. It is therefore difficult to compare the results of applying two standards and thus to assess which one would be better suited to the needs of a given situation. The aim of this development is therefore to obtain an interoperable methodology, which must also be dynamic and provide real-time analysis.

The solutions found in the literature review were focused on the analysis of a specific environment and therefore lacked the interoperability that we consider relevant in risk management, as ENISA's developments show in this aspect. The proposal is a possible continuation of the toolbox for interoperability published by ENISA, which defines at a theoretical level the processes for translation between methodologies that are implemented in this system.

Using ontologies, as a tool with great potential in this type of system, it is possible not only to model the processes of a methodology but also to add the necessary behavior to calculate the level of risk or provide countermeasures to respond to attacks dynamically.

One of the advantages of this type of risk scenario-based approach is that, although the system is focused on cybersecurity risks, the methodology contemplates other types of unintended threats, such as natural incidents, industrial incidents or errors. This includes loss of devices, damage, or problems such as fire, floods, power failures, electromagnetic emissions, etc.

Furthermore, the methodology is designed to co-exist with current systems using different frameworks. The intention is to be able to extract information from any of these systems and to share it between organizations.

Two types of use cases have been proposed to validate the ontology and the management system. The first consisted of testing the input of previous threats for two different methodologies (MONARC and MAGERIT), comparing the risk levels obtained according to the original calculation and according to the proposed interoperable system. Finally, a use case is proposed in an IoT environment in which the entire system is tested. The results in all cases have been positive. As expected, the risk levels obtained in the calculations of the original methodology and through the system do not always coincide. However, by transferring them to a common scale, our proposal allows us to compare the cybersecurity risk status of each use case although they originally used different, and therefore not comparable, methodologies.

Although scalability could be an issue, with slight upgrades and a powerful engine, as shown in previous developments as [47], in the future this system can adapt to any IoT configuration, having the flexibility to define any number and type of devices (assets) and relations between them. All the environments of the examples analyzed in the related works could be adapted to perform risk management and the countermeasures recommendation to mitigate it on the ontology described in this proposal, as it is prepared to deal with different kinds of situations. In the specific case of smart cities, the different sensors and devices that monitor the city can be included in the analysis, establishing the possible risk scenarios that these new infrastructures must face. It allows the optimization of risk management processes and automation of the recommendation of protections in real time for these types of new developments.

This proposal opens the path to future works including the automation of the vulnerabilities catalogue, and the consideration of its effect, not only over threats but over assets, the development of TTPs analysis to propose more adequate countermeasures, and the definition of conditions for the execution of those countermeasures. To improve the asset catalogue, introducing different weights to measure the importance of each security dimension for the organization could be considered. Focused on interoperability, other risk methodologies might be introduced, reasoning rules upgraded or unknown threats considered. If the prototype is developed for deployment in real environments, it will be necessary to take into consideration aspects to protect the security and privacy of the data being processed in risk management.

CRediT authorship contribution statement

Carmen Sánchez-Zas: Writing – original draft, Validation, Software, Resources, Methodology, Investigation, Formal analysis, Data curation, Conceptualization. **Xavier Larriva-Novo:** Writing – review & editing, Supervision, Resources, Methodology, Investigation, Conceptualization. **Víctor A. Villagrá:** Writing – review & editing, Supervision, Project administration, Methodology, Funding acquisition, Conceptualization. **Diego Rivera:** Writing – review & editing, Investigation, Conceptualization. **Andrés Marín-Lopez:** Writing – review & editing, Investigation, Conceptualization.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

Acknowledgment

This research has received funding from the European Defence Industrial Development Programme (EDIDP) under the grant agreement Number EDIDP-CSAMN-SSC-2019-022-ECYSAP (European Cyber Situational Awareness Platform).

References

[1] W. Widel, P. Mukherjee, M. Ekstedt, Security countermeasures selection using the meta attack language and probabilistic attack graphs, IEEE Access 10 (2022) 89645–89662, http://dx.doi.org/10.1109/ACCESS.2022.3200601, URL https://ieeexplore.ieee.org/document/9864201/.
[2] Z. Syed, A. Padia, T. Finin, L. Mathews, A. Joshi, UCO: A unified cybersecurity ontology, 2016, http://dx.doi.org/10.13016/M2862BG1V, 8 pages. Artwork Size: 8 pages Publisher: AAAI Press. URL http://mdsoar.org/handle/11603/11804.
[3] SPIN - overview and motivation, 2023, URL https://www.w3.org/Submission/spin-overview/. (Visited 10 October 2023).
[4] SWRL: A semantic web rule language combining OWL and ruleml, 2023, https://www.w3.org/Submission/SWRL/. (Visited 10 October 2023).
[5] EBIOS-enisa, 2023, https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_ebios.html. (Visited 10 October 2023).
[6] EBIOS-generic approach, 2023, https://club-ebios.org/site/wp-content/uploads/productions/EBIOS-GenericApproach-2018-09-05-Approved.pdf. (Visited 10 October 2023).
[7] EBIOS-risk manager, 2023, https://www.ssi.gouv.fr/uploads/2019/11/anssi-guide-ebios_risk_manager-en-v1.0.pdf. (Visited 10 October 2023).
[8] Compendium of risk management frameworks with potential interoperability — ENISA, 2023, URL https://www.enisa.europa.eu/publications/compendium-of-risk-management-frameworks. (Visited 10 October 2023).
[9] PAe - MAGERIT v.3 : Metodología de análisis y gestión de riesgos de los sistemas de información, 2023, https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html. (Visited 10 October 2023).
[10] What is monarc? - MONARC, 2023, https://www.monarc.lu/. (Visited 10 October 2023).
[11] Interoperable EU risk management framework — ENISA, 2023, https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-framework. (Visited 10 October 2023).
[12] Cramm — ENISA, 2023, https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_cramm.html.
[13] C. Mercier, L. Roux, M. Romero, F. Alexandre, T. Vieville, Formalizing problem solving in computational thinking : an ontology approach, in: 2021 IEEE International Conference on Development and Learning, ICDL, 2021, pp. 1–8.
[14] What is an ontology and why we need it, 2023, https://protege.stanford.edu/publications/ontology_development/ontology101-noy-mcguinness.html. (Visited 10 October 2023).
[15] What is risk management?, 2023, https://www.redhat.com/en/topics/management/what-is-risk-management. (Visited 10 October 2023).
[16] Gestión de riesgos - una guía de aproximación para el empresario, 2023, https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_gestion_riesgos_metad.pdf. (Visited 10 October 2023).
[17] A. Brazhuk, Threat modeling of cloud systems with ontological security pattern catalog, Int. J. Open Inf. Technol. 9 (5) (2021) 36–41.
[18] V. Mavroeidis, S. Bromander, Cyber threat intelligence model: An evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence, in: 2017 European Intelligence and Security Informatics Conference, EISIC, IEEE, Athens, 2017, pp. 91–98, http://dx.doi.org/10.1109/EISIC.2017.20, URL http://ieeexplore.ieee.org/document/8240774/.
[19] R. Syed, Cybersecurity vulnerability management: A conceptual ontology and cyber intelligence alert system, Inf. Manage. 57 (6) (2020) 103334, http://dx.doi.org/10.1016/j.im.2020.103334, URL https://linkinghub.elsevier.com/retrieve/pii/S0378720620302718.
[20] R. Bitton, N. Maman, I. Singh, S. Momiyama, Y. Elovici, A. Shabtai, Evaluating the cybersecurity risk of real-world, machine learning production systems, ACM Comput. Surv. 55 (9) (2023) 1–36, http://dx.doi.org/10.1145/3559104, URL https://dl.acm.org/doi/10.1145/3559104.
[21] B. Bokan, J. Santos, Managing cybersecurity risk using threat based methodology for evaluation of cybersecurity architectures, in: 2021 Systems and Information Engineering Design Symposium, SIEDS, IEEE, Charlottesville, VA, USA, 2021, pp. 1–6, http://dx.doi.org/10.1109/SIEDS52267.2021.9483736, URL https://ieeexplore.ieee.org/document/9483736/.
[22] T.E. Abioye, O.T. Arogundade, S. Misra, A.T. Akinwale, O.J. Adeniran, Toward ontology-based risk management framework for software projects: An empirical study, J. Softw.: Evol. Process 32 (12) (2020) e2269, http://dx.doi.org/10.1002/smr.2269, URL https://onlinelibrary.wiley.com/doi/10.1002/smr.2269.
[23] O.T. Arogundade, A. Abayomi-Alli, S. Misra, An ontology-based security risk management model for information systems, Arab. J. Sci. Eng. 45 (8) (2020) 6183–6198, http://dx.doi.org/10.1007/s13369-020-04524-4, URL https://link.springer.com/10.1007/s13369-020-04524-4.
[24] I.A. Wulandari, D.I. Sensuse, A.A. Krisnadhi, I.F. Akmaliah, P. Rahayu, Ontologies for decision support system: The study of focus and techniques, in: 2018 10th International Conference on Information Technology and Electrical Engineering, ICITEE, IEEE, Kuta, 2018, pp. 609–614, http://dx.doi.org/10.1109/ICITEED.2018.8534947, URL https://ieeexplore.ieee.org/document/8534947/.

[25] A. Shaked, O. Margalit, OnToRisk – a formal ontology approach to automate cyber security risk identification, in: 2022 17th Annual System of Systems Engineering Conference, SOSE, IEEE, Rochester, NY, USA, 2022, pp. 74–79, http://dx.doi.org/10.1109/SOSE55472.2022.9812653, URL https://ieeexplore.ieee.org/document/9812653/.
[26] A. Shaked, O. Margalit, Sustainable risk identification using formal ontologies, Algorithms 15 (9) (2022) 316, http://dx.doi.org/10.3390/a15090316, URL https://www.mdpi.com/1999-4893/15/9/316.
[27] G. Gonzalez-Granadillo, S. Dubus, A. Motzek, J. Garcia-Alfaro, E. Alvarez, M. Merialdo, S. Papillon, H. Debar, Dynamic risk management response system to handle cyber threats, Future Gener. Comput. Syst. 83 (2018) 535–552, http://dx.doi.org/10.1016/j.future.2017.05.043, URL https://linkinghub.elsevier.com/retrieve/pii/S0167739X17311433.
[28] V. Vasilyev, A. Kirillova, A. Vulfin, A. Nikonov, Cybersecurity risk assessment based on cognitive attack vector modeling with CVSS score, in: 2021 International Conference on Information Technology and Nanotechnology, ITNT, IEEE, Samara, Russian Federation, 2021, pp. 1–6, http://dx.doi.org/10.1109/ITNT52450.2021.9649191, URL https://ieeexplore.ieee.org/document/9649191/.
[29] F.H. Alshammari, Design of capability maturity model integration with cybersecurity risk severity complex prediction using bayesian-based machine learning models, Serv. Orient. Comput. Appl. 17 (1) (2023) 59–72, http://dx.doi.org/10.1007/s11761-022-00354-4, URL https://link.springer.com/10.1007/s11761-022-00354-4.
[30] I. Lykourentzou, K. Papadaki, A. Kalliakmanis, Y. Djaghloul, T. Latour, I. Charalabis, E. Kapetanios, Ontology-based operational risk management, in: 2011 IEEE 13th Conference on Commerce and Enterprise Computing, IEEE, Luxembourg-Kirchberg, Luxembourg, 2011, pp. 153–160, http://dx.doi.org/10.1109/CEC.2011.18, URL http://ieeexplore.ieee.org/document/6046967/.
[31] C. Grigoriadis, A.M. Berzovitis, I. Stellios, P. Kotzanikolaou, A cybersecurity ontology to support risk information gathering in cyber-physical systems, in: S. Katsikas, C. Lambrinoudakis, N. Cuppens, J. Mylopoulos, C. Kalloniatis, W. Meng, S. Furnell, F. Pallas, J. Pohle, M.A. Sasse, H. Abie, S. Ranise, L. Verderame, E. Cambiaso, J. Maestre Vidal, M.A. Sotelo Monge (Eds.), Computer Security. ESORICS 2021 International Workshops, in: Lecture Notes in Computer Science, vol. 13106, Springer International Publishing, Cham, 2022, pp. 23–39, http://dx.doi.org/10.1007/978-3-030-95484-0_2, URL https://link.springer.com/10.1007/978-3-030-95484-0_2.
[32] G. Engelberg, M. Fumagalli, A. Kuboszek, D. Klein, P. Soffer, G. Guizzardi, An ontology-driven approach for process-aware risk propagation, in: Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing, ACM, Tallinn Estonia, 2023, pp. 1742–1745, http://dx.doi.org/10.1145/3555776.3577795, URL https://dl.acm.org/doi/10.1145/3555776.3577795.
[33] P. Saripalli, B. Walters, QUIRC: A quantitative impact and risk assessment framework for cloud security, in: 2010 IEEE 3rd International Conference on Cloud Computing, IEEE, Miami, FL, USA, 2010, pp. 280–288, http://dx.doi.org/10.1109/CLOUD.2010.22, URL http://ieeexplore.ieee.org/document/5557981/.
[34] S.-H. Park, S.-W. Lee, Threat-driven risk assessment for APT attacks using risk-aware problem domain ontology, in: 2022 IEEE 30th International Requirements Engineering Conference Workshops, REW, IEEE, Melbourne, Australia, 2022, pp. 226–231, http://dx.doi.org/10.1109/REW56159.2022.00050, URL https://ieeexplore.ieee.org/document/9920123/.
[35] L. Meshkat, R.L. Miller, A systems approach for cybersecurity risk assessment, in: 2022 Annual Reliability and Maintainability Symposium, RAMS, IEEE, Tucson, AZ, USA, 2022, pp. 1–9, http://dx.doi.org/10.1109/RAMS51457.2022.9893966, URL https://ieeexplore.ieee.org/document/9893966/.
[36] M.G. Cains, L. Flora, D. Taber, Z. King, D.S. Henshel, Defining cyber security and cyber security risk within a multidisciplinary context using expert elicitation, Risk Anal. 42 (8) (2022) 1643–1669, http://dx.doi.org/10.1111/risa.13687, URL https://onlinelibrary.wiley.com/doi/10.1111/risa.13687.
[37] Y. Merah, T. Kenaza, Ontology-based cyber risk monitoring using cyber threat intelligence, in: Proceedings of the 16th International Conference on Availability, Reliability and Security, ACM, Vienna Austria, 2021, pp. 1–8, http://dx.doi.org/10.1145/3465481.3470024, URL https://dl.acm.org/doi/10.1145/3465481.3470024.
[38] A. Černivec, G. Erdogan, A. Gonzalez, A. Refsdal, A.A. Romero, Employing graphical risk models to facilitate cyber-risk monitoring - the WISER approach, in: P. Liu, S. Mauw, K. Stolen (Eds.), Graphical Models for Security, in: Lecture Notes in Computer Science, vol. 10744, Springer International Publishing, Cham, 2018, pp. 127–146, http://dx.doi.org/10.1007/978-3-319-74860-3_10, URL http://link.springer.com/10.1007/978-3-319-74860-3_10.
[39] V. Agrawal, Towards the ontology of ISO/IEC 27005:2011 risk management standard, in: Tenth International Symposium on Human Aspects of Information Security & Assurance, HAISA 2016, Frankfurt, Germany, 2016, pp. 101–111.
[40] S. Ansaldi, M. Monti, P. Agnello, F. Giannini, An ontology for the identification of the most appropriate risk management methodology, in: D. Hutchison, T. Kanade, J. Kittler, J.M. Kleinberg, F. Mattern, J.C. Mitchell, M. Naor, O. Nierstrasz, C. Pandu Rangan, B. Steffen, M. Sudan, D. Terzopoulos, D. Tygar, M.Y. Vardi, G. Weikum, P. Herrero, H. Panetto, R. Meersman, T. Dillon (Eds.), On the Move To Meaningful Internet Systems: OTM 2012 Workshops, in: Lecture Notes in Computer Science, vol. 7567, Springer Berlin Heidelberg, Berlin, Heidelberg, 2012, pp. 444–453, http://dx.doi.org/10.1007/978-3-642-33618-8_60, URL http://link.springer.com/10.1007/978-3-642-33618-8_60.
[41] E. Vicente, A. Mateos, A. Jiménez-Martín, Risk analysis in information systems: A fuzzification of the MAGERIT methodology, Knowl.-Based Syst. 66 (2014) 1–12, http://dx.doi.org/10.1016/j.knosys.2014.02.018, URL https://linkinghub.elsevier.com/retrieve/pii/S0950705114000732.
[42] D.J. Ferreira, H. São Mamede, Predicting cybersecurity risk - a methodology for assessments, ARIS2 - Adv. Res. Inf. Syst. Secur. 2 (2) (2022) 50–63, http://dx.doi.org/10.56394/aris2.v2i2.23, URL https://aris-journal.com/aris/index.php/journal/article/view/23.
[43] C. Sánchez-Zas, V.A. Villagrá, M. Vega-Barbas, X. Larriva-Novo, J.I. Moreno, J. Berrocal, Ontology-based approach to real-time risk management and cyber-situational awareness, Future Gener. Comput. Syst. 141 (2023) 462–472, http://dx.doi.org/10.1016/j.future.2022.12.006, URL https://linkinghub.elsevier.com/retrieve/pii/S0167739X22004058.
[44] Interoperable EU risk management toolbox - ENISA, 2023, URL https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-toolbox. (Visited 11 October 2023).
[45] OWL web ontology language - overview, 2024, URL https://www.w3.org/TR/owl-features/. (Visited 27 April 2024).
[46] SPIN - SPARQL syntax, 2024, URL https://www.w3.org/submissions/spin-sparql/. (Visited 27 April 2024).
[47] C. Sánchez-Zas, V.A. Villagrá, M. Vega-Barbas, X. Larriva-Novo, J.I. Moreno, J. Berrocal, Ontology-based approach to real-time risk management and cyber-situational awareness, Future Gener. Comput. Syst. 141 (2023) 462–472, http://dx.doi.org/10.1016/j.future.2022.12.006, URL https://www.sciencedirect.com/science/article/pii/S0167739X22004058.