A Hybrid Dynamic Risk Analysis Methodology for Cyber-Physical Systems

Christos Lyvas[1 [0000−0003−4481−1000]], Konstantinos Maliatsos[2 [0000−0002−8823−018X]], Andreas Menegatos[1 [0000−0002−2469−5535]], Thrasyvoulos Giannakopoulos[1 [0000−0002−3453−1892]], Costas Lambrinoudakis[1 [0000−0003−3101−5347]], Christos Kalloniatis[3 [0000−0002−8844−2596]], and Athanasios Kanatas[1 [0000−0002−1966−4937]]

[1] Department of Digital Systems, University of Piraeus, Greece
{clyvas, amenegatos, tgian, clam, kanatas}@unipi.gr
[2] Department of Information and Communication Systems Engineering, University of the Aegean, Greece
kmaliat@aegean.gr
[3] Department of Cultural Technology and Communication, University of the Aegean, Greece
chkallon@aegean.gr

Abstract. Recent technological advances allow us to design and implement sophisticated infrastructures to assist users' everyday life; technological paradigms such as Intelligent Transportation Systems (ITS) and Multi-modal Transport are excellent instances of those cases. Therefore, a systematic risk evaluation process in conjunction with proper threat identification are essential for environments like those mentioned above as they involve human safety. Threat modelling is the process of identifying and understanding threats while risk analysis is the process of identifying and analyzing potential risks. This research initially focuses on the most widely-used threat modelling and risk analysis approaches and reviewing their characteristics. Then, it presents a service-oriented dynamic risk analysis approach that focuses on Cyber-Physical Systems (CPS) by adopting threat modelling characteristics and by blending other methods and well-established sources to achieve automation in several stages. Finally, it provides the qualitative features of the proposed method and other related threat modelling and risk analysis approaches with a discussion regarding their similarities, differences, advantages and drawbacks.

Keywords: Dynamic Risk Analysis · Threat Analysis · Threat Modelling · Security and Asset Management · Intelligent Transportation Systems Security · Multimodal Transport Security · Cyber-Physical Systems Security.

1 Introduction

Over the past years, advances in information and communications technology (ICT) enabled the implementation of numerous technological paradigms where a global network of machines and devices can interact with each other for medical, industrial, transportation, decision-making or other purposes. In this context, both security and privacy aspects are considered crucial for those types of infrastructures. That is because, in many

cases, the effect of new emerging threats targeting those schemes ranges from cyber to physical impacts, resulting frequently in severe safety implications for their users.

There are several systematic approaches and methodologies in cybersecurity regarding the identification, mitigation, assessment and quantification of vulnerabilities, threats, risks and countermeasures. Generally, Risk Management (RM) [21] is the procedure of managing risk to an acceptable level mainly consisting of two main stages; the risk assessment and the risk treatment. Risk Assessment [25] allows analysts to identify vulnerabilities and threats on specific elements. In the risk analysis (RA) a score is assigned to each identified risk using one of two types of scoring system: quantitative or qualitative. These scores enable analysts to prioritize risks in order to determine the best ways to address them with controls and countermeasures known as Risk Treatment (RT). Moreover, Threat Modelling (TM) is an essential part of the risk analysis with its definition varying from a process that can be used to analyze potential attacks and threats to the thorough analysis of architectures for potential security threats identification and the appropriate selection of countermeasures and controls for their mitigation [52].

Many risk analysis and threat modelling methodologies exist from academic [17,22, 37,39,42,44,46,50,53], corporate [7,38,49] and national organizations [3,15,19,24,34] perspectives. Regarding the limitations of existing risk analysis and threat modelling approaches, several of them are too technical [49, 53] and thus require deep knowledge in order to be applied, while others are too generic [7, 34] and provide non-insightful but high-level results. Also, some of them are very well-documented [19, 24, 49], while others are mainly targeted to non-English speaking users [3, 15]. Furthermore, some require manual intervention [49, 50] by the analysts, while others are tool-assisted [15, 19, 24] and provide automation to some extent. The majority of them are generic approaches that support exclusively conventional information technology (IT) infrastructures [15, 19, 22, 24, 34, 46] based upon the size [17] and scope of the system under review. In contrast, others require modifications and extensions [24, 49] in order to support analysis in Cyber-Physical Systems and Industrial Internet of Things (IIoT) architectures. In addition, several approaches borrow characteristics [24] or require input [34, 46] from other methodologies in order to provide a holistic analysis. Finally, some are privacy-oriented [50] whereas others are mostly security-oriented [24, 34, 46] and others supporting both security and privacy [15, 19, 24].

This research describes a dynamic Risk Analysis (RA) methodology with Threat Modeling (TM) characteristics dedicated to Cyber-Physical Systems, especially for Intelligent Transportation Systems and Multimodal transport. Its novelty relies on the detailed description of complicated assets constructed by elementary assets which allow the method to be applied to any non-conventional Information Technology (IT) infrastructure such as Industrial Internet of Things (IIoT) Multi-Modal Transportation, Intelligent Transportation etc. Moreover, it leverages well-established sources to perform automated threat valuations and risk assessments.

Summarizing, the contributions of this work are:

- The design of a prototype hybrid dynamic risk analysis framework with embedded automatic threat modeling capabilities.

- A thorough comparative analysis among the proposed framework and other related risk analysis and threat modeling approaches from literature.
- Access to the current proof-of-concept implementation[4] of the proposed framework.

The rest of this paper is structured as follows. Section 2 provides an overview of the related work. Section 3 presents the dynamic risk analysis framework design along with it's applicability in 4. Further discussion is elaborated in Section 5 by introducing a comparative analysis with other related works. Finally, Section 6 provides both the conclusions and pointers for future improvements.

2 Related Work

Risk analysis and threat modelling methodologies are undoubtedly vital procedures for Cyber-Physical Systems, from security and privacy by design to quantitative or qualitative assessment of the security level of such systems. The approaches mentioned above are further discussed in the following subsections, while a comparative analysis between these methods and the proposed one in this research is provided in Section 5.

2.1 Threat Modelling Methodologies

UcedaVélez and Morana [47] developed a risk-centric threat modeling framework named PASTA (Process for Attack Simulation and Threat Analysis) to process attack scenarios and vulnerabilities within either a proposed or existing information technology (IT) infrastructure in order to identify risks and impact levels. PASTA is composed of seven stages. At the initial stage, the objectives are defined, including business objectives, security and compliance requirements, along with business impact analysis. In the second stage, the technical scope is defined, and then the decomposition of the infrastructure takes place. The fourth stage appertains to the threat analysis with probabilistic attack scenarios and threat intelligence correlation. The fifth stage regards the vulnerability and weaknesses analysis, followed by the attack modelling. Finally, in the latter stage, the risk and impact analysis are conducted.

LINDDUN (Linkability, Identifiability, Non-Repudiation, Detectability, Disclosure of Information, Unawareness, Non-Compliance) [50, 51] is another threat modelling methodology, which is dedicated to privacy and data protection for privacy impact assessment. It consists of six stages. In the first stage LINDDUN, with the aid of Data Flow Diagrams (DFDs), define the system's boundaries with data flows, data storages, processes, and external entities. Stage two refers to the mapping of privacy threats to the system model. Stage three entails scenarios in which these threats could apply. Stage four concerns the selection and prioritization of identified threats followed by the next stage in which the elicit mitigation strategies are defined. Finally, stage six concerns the selection of appropriate privacy-enhancing technologies.

STRIDE [38] is one of the most known threat modelling methods initially maintained by Microsoft. STRIDE consists of three phases. In the first phase, data flow

[4] `https://rmt.ds.unipi.gr`

diagrams (DFDs) model the scope and the under examination system. In the second phase, STRIDE proceeds with the threat identification based on a predefined set of known threats. In the final phase, the identified threats and mitigation strategies are documented and prioritized.

Hamad *et al*. [37] proposed a threat modelling approach for classifying attacks in vehicular environments. It consists of three (3) layers: (i) target domains, in which all the vulnerabilities within an asset are considered to identify potential threats affecting it, (ii) requirements violation, in which any of the security requirements that have been violated by exploiting a specific vulnerability within an asset is defined, (iii) accessibility, referring to how the vehicle is accessed (remotely, directly) to take advantage of a specific vulnerability. Based upon the collected information, attack trees are then formed to compute the probability of a successful attack within each asset. The root of each tree represents the threat to be accomplished and the overall tree indicates the attack path to exploit an asset's certain vulnerability.

Petit *et al*. [42] created a threat modelling tool based on attack trees to represent the distinct attack steps of individual attack scenarios targeting the vehicular domain. During the attack tree construction phase, for high-level attacks, authors considered necessary to create reusable "general" attack trees to evade redundancy. However, as the attack trees become more detailed, these general attack sub-trees may become more specific as different applications are subject to different kinds of vulnerabilities.

Jbair *et al*. [39] proposed a threat modeling approach for Industrial Cyber-Physical Systems (ICPS) making use of a digital twin that was built with the VueOne tool. Their threat modelling process consists of five steps. In the first step, ICPS target assets are identified while in the second step feasible attack scenarios are built based on Tactics, Techniques, and Procedures (TTPs) from MITREs ATT&CK [18] for Industrial Control Systems (ICS). In the next step, both the Attack Vector (AV) and the Attack Likelihood (AL) are measured for each attack, with step four producing a risk matrix based on the measured values of the previous step by using both a quantitative and a qualitative method to measure the risks. Finally, countermeasures are proposed to reduce the calculated risk.

2.2 Risk Analysis Methodologies

IT-Grundschutz [2] is a risk management rather than a risk analysis method developed by the German Federal Office for Information Security (BSI). Part of the BSI Standards of Information Security, IT-Grundschutz provides a methodology for establishing and operating an Information Security Management System (ISMS), and a risk analysis methodology. BSI also publishes the IT-Grundschutz Compendium [8] that analyzes the most common threats and vulnerabilities and determines the risks involved. The risk analysis methodology based on IT-Grundschutz [4] consists of four steps regarding risk determination and risk treatment. In step one a threat overview is created from threats that may arise from different situations. Step two is the risk classification where the frequency of occurrence and the impact is estimated. Step three consists of various risk treatment techniques. Finally in step four the security concept is consolidated, with the integration of any additional safeguards.

OCTAVE Allegro (Operationally Critical Threat, Asset, and Vulnerability Evaluation) [22] is a variation of the apparently discontinued, OCTAVE [16] risk management methodology. OCTAVE Allegro is an asset-based methodology, focusing on how the assets are used and exposed to threats and vulnerabilities that can cause disruptions. It is composed of eight steps across four phases. Phase one focuses on risk measurement criteria. In phase two critical assets are identified and profiled, identifying boundaries and security requirements. Phase three identifies the threats, with the last phase focusing on risk identification, risk analysis and risk mitigation. OCTAVE-S [17] was developed to support small-sized organizations (with less than 100 employees). The difference with the other variants is that the assessment team has an extensive knowledge of the organisation, thus reducing the need for workshops to gather information. It is also more structured and contains security concepts in the provided worksheets and guidance. Finally, OCTAVE-S includes a limited selection of infrastructure risks in order to assist with adoption. OCTAVE FORTE (FOR The Enterprise) [46] method aims to help organizations evaluate their security risks and use Enterprise Risk Management (ERM) to bridge the gap between managerial and technical personnel. It consists of 10 iterative steps that, among other things, establish risk requirements, identify critical assets and estimate their resiliency, identify risks, threats and vulnerabilities for those assets and finally implement controls, before the process starts again.

Perhaps the most well known information security risk management framework is the ISO/IEC 27005 [7] which is part of the ISO/IEC 27000 [6] series. The methodology consists of several steps. The initial step is the context establishment step. The second step is the risk assessment which is comprised by the risk analysis that contains the risk identification and the risk estimation steps, followed by risk evaluation. The third step is the risk treatment, which may result in the entire process starting again if the remaining risk level is considered as not acceptable. Throughout the whole process the risk communication and the risk monitoring and review steps take place. ISO also publishes ISO/IEC 31000 [5], that follows a similar approach to ISO/IEC 27005 [7], with a more generic risk management methodology that isn't specific to information security.

EBIOS Risk Manager [19] is a risk management method developed by ANSSI. It adopts an iterative approach that can be used by any kind of organization and consists of five (5) phases defined as workshops: (i) scope and security baseline, in which both organizational and risk analysis aspects are considered (ii) risk origins along with their targets, which are identified and organized in pairs with the most relevant of them being chosen at the end of this phase (iii) strategic scenarios, which are high-level attack scenarios against the business assets that are followed by an assessment process to define the security measures for the studied ecosystem (iv) operational scenarios, which are technical scenarios with an approach similar to that of the previous workshop dedicated to support assets, and (v) risk treatment, during which security measures are applied to calculate the residual risks and set up the risk-monitoring framework.

The Methodology of Analysis and Management of Risks of Information Systems (MAGERIT) [15] is a qualitative risk management framework for public administration. Over the years, MAGERIT established itself as an asset-based method consisting of three books [13–15]. The main phases of MAGERIT are the following: (i) asset iden-

tification and evaluation, based on security requirements as well as on a scale ranging from 0 (negligible) to 10 (very high) to calculate both the impact on an asset and the likelihood of threat occurrence on a yearly basis. Also, the bidirectional relationships between the assets are represented in either tree or graph structures, indicating that the top-layer assets rely on on the lower-layer assets and vice versa. (ii) In the second phase, certain safeguards are determined to mitigate the impact of the assets to the identified threats. In this context, potential safeguards per asset type are enlisted in [13]. Finally, (iii) a security plan for risk monitoring is formed where security projects are defined and the specification of the appropriate continuously-monitored risk treatment actions is finalized. MAGERIT provides a complete commercial [26] software solution named as EAR-PILAR[5]. The latter incorporates a standard library that contains a predefined list of assets, threats and safeguards [48].

MONARC (Optimised Risk Analysis Method) is a tool-assisted methodology [24] that was developed to provide a framework for organizations to conduct repeatable risk assessments regardless of their size. MONARC abides to several standards [36, 40]. Furthermore, it makes use of a qualitative evaluation method, while for vulnerabilities, threats and impacts it uses quantitative criteria. MONARC consists of four (4) phases. (i) In the Context Establishment phase, all the information regarding the scope of the risk analysis is collected as well as the valuation, the acceptance and impact criteria. (ii) In the Risk Modelling phase, the threats, vulnerabilities, and the impacts are explicitly defined. (iii) In the Risk Assessment and Treatment phase, risk calculation is performed along with the development of a risk treatment plan to reduce the risk to acceptable levels in quantifying manner. (iv) In the Implementation and Monitoring phase, a management phase with continuous security monitoring and control of security measures is carried out.

ITSRM[2] [34] is a process-based risk framework developed by the European Commission that consists of seven (7) phases: (i) system security characterization, which entails a high-level representation of the system, roles and security requirements, (ii) primary assets' identification, where data, functions, and other assets are recognized with both their value and impact being quantified based on predetermined catalogues, (iii) supporting assets definition, that are being used/managed by the primary assets, (iv) system modelling, where the dependencies between the assets, the data paths and the system architecture is provided, (v) risk identification, where the system model of the previous phase is used to develop the risk scenarios against the primary assets, (vi) risk analysis and evaluation which, after enforcing security measures to mitigate each risk identified in the previous step, calculates the residual risk for each one, (vii) risk treatment, where the best applicable risk treatment option for each identified risk is specified.

Zeddini *et al*. [53] proposed a qualitative risk analysis of Intelligent Transport Systems based on the ETSI-TVRA [35] methodology. According to the ETSI Intelligent Transport Systems-Station (ITS-S) Communication Architecture, first the system is modelled focusing on its assets and then weaknesses are identified for each one. Afterwards, a table of attacks is produced which indicates the impact to authentication and availability, based on both the asset and its vulnerabilities. Then, considering the

[5] https://www.pilar-tools.com/en/tools/buy.html

difficulty of carrying out an attack and the potential gain, the attack likelihood is calculated, with the impact taken into account on a scale of low to high. The result of their analysis is a comprehensive list of Intelligent Transport Systems vulnerabilities, with their respective severities followed by countermeasures for those identified attacks.

Semertzis *et al*. [44] proposed a quantitative risk assessment method for Cyber-Physical Power Systems (CPPS) which uses attack graphs by leveraging a combination of probabilistic and deterministic techniques. Their proposed methodology relies on attack graphs to calculate the probability of attack through Time-to-Compromise (TTC) and Mean-Time to Detect (MTTD) metrics and the impact calculation based on power system stability using metrics such as the loss of load and voltage deviation. In order to accomplish that, a digital twin on the cyber-physical system is proposed to run simulations and calculate cascading failures of the power system as a result of the cyber attacks. To calculate the TTC metric the attack steps are initially defined, based on MITRE ATT&CK [18] for Industrial Control Systems (ICS), for each asset in the attack graph and then use CVE [10] to identify the known vulnerabilities of each asset and categorise them based on the type of compromise. Then, to calculate the TTC, they use Monte-Carlo simulations taking as inputs the number of vulnerabilities, the attacker skill level and the number of simulation samples. Finally, to capture a wide gamut of attacker skill levels, probabilistic distributions are fed into the Monte-Carlo simulations.

3 System Model

An adaptable, dynamic, quantifying risk analysis method is presented in this section to overcome both the limitations and the adaptation overhead introduced by the already existing risk analysis methodologies to specific architectures (such as Industrial IoT and Cyber-Physical Systems). The main characteristics of the proposed dynamic risk analysis methodology revolve around the ability to automatically assign new vulnerabilities to the architecture's assets and automatically evaluate the impact of a successful exploitation of a vulnerability. As Figure 1 depicts, it consists of several phases: the service-oriented scope establishment and valuation, the composition of basic assets or decomposition of composite assets, the correlation of threats and vulnerabilities and, finally, the risk estimation.

3.1 Service-Oriented Scope Establishment and Valuation

In the initial phase, the analyst is responsible for defining the boundaries of the under examination infrastructure. This process involves the identification of the architecture's purpose and services. Figure 2 illustrates such an example (derived from the use cases of CitySCAPE [1] project) where several devices interact with each other in order to provide Multi-Modal Transport services.

The design of the proposed methodology is fully aligned with the fact that most of Cyber-Physical Systems tend to become Service-Oriented Architectures (SOAs) [45]; for this purpose, the analysts, after the definition of the scope and the involved services, valuate their impact based on several factors, such as integrity, confidentiality, availability, reputation, financial consequences and safety. The impact scales range from zero (0)

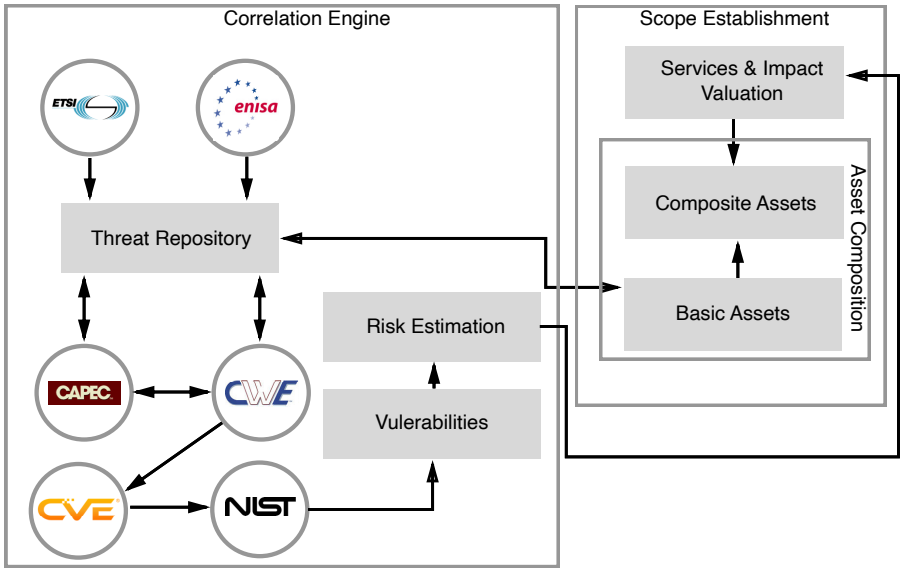

Fig. 1: Dynamic Risk Analysis High-Level Overview

to five (5). For instance, concerning confidentiality, the zero impact implies that no confidentiality requirements are needed for the reviewed service, whereas five indicates very strong confidentiality requirements for the service.

3.2 Manual Composition or Automatic Decomposition of Assets

The asset identification phase is one of the most critical and the last user-driven part of the proposed methodology. It consists of either the manual composition of assets by risk analysts for outlined architectures or the automatic decomposition of assets for already existing infrastructures. For the first case, a set of generic basic assets exists in a predefined list in the methodology's rule engine named as correlation engine. The main concept behind the definition of the basic asset is re-usability and the fact that all assets involved in a Cyber-Physical System can be decomposed into basic assets – thus, sharing a large number of standard features, threats and vulnerabilities.

More precisely, as Figure 3 depicts, several basic assets such as an Operating System, a Mobile Application, a Central Process Unit *etc*. originating from different asset categories Application Software (blue), Storage (purple), System Software and Middleware (red), Hardware (green), Network (green) can be combined to formulate a composite asset such as a mobile device. For existing infrastructures, various network scanners, asset inventory, and vulnerability assessment tools are combined in order to decompose composite assets to basic assets and identify those that interact inside a service. In both cases, the methodology follows a top-down approach for the impact valuation of the basic assets in respect with the composite asset and the service they belong to. Thus,

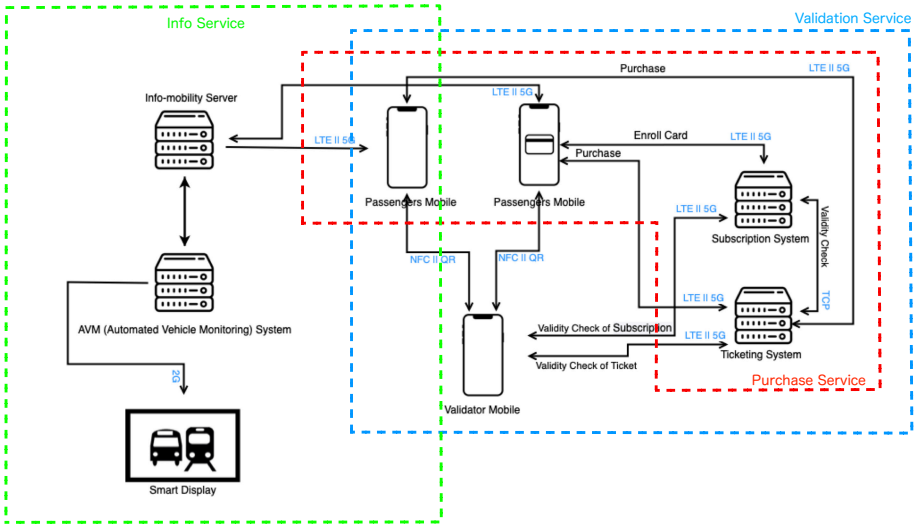

Fig. 2: High-Level Overview of the First Indicative CitySCAPE [1] Project Use-Case Divided in Services

a composite asset inherits the impact valuations based on the service it belongs to, as well as the basic assets that comprise it. Therefore,

- The composite asset retrieves the vulnerabilities and threats of the basic assets that compose it, enabling an automatic threat-vulnerability assignment process.
- The impact on a composite asset is defined by the service requirements.

3.3 Correlation of Threats and Vulnerabilities

The correlation of threats and vulnerabilities phase entails the proposed method's correlation engine. It provides all the automation from vulnerability identification to the estimation of the identified threats' probability on basic assets into a service.

Initially, the method contains a set of threats extracted from several ENISA reports referring to various fields including critical infrastructures. Also, threats correlated to new technologies (e.g. 5G) were appended and Cyber-Physical Systems with threats from ETSI-TVRA were reviewed. The following reports were included in the generation of the correlation engine's threat list: a) Baseline Security Recommendations for IoT [30], that focuses mainly on IoT on critical infrastructure, b) the ENISA Smartphones: Information security risks, opportunities and recommendations for users report [28], c) the Cloud Computing Security Risk Assessment [27] d) the ENISA Threat Landscape For 5G Networks [33], e) the Smart Grid Threat Landscape and Good Practice Guide [29], f) Port Cybersecurity - Good practices for cybersecurity in the maritime

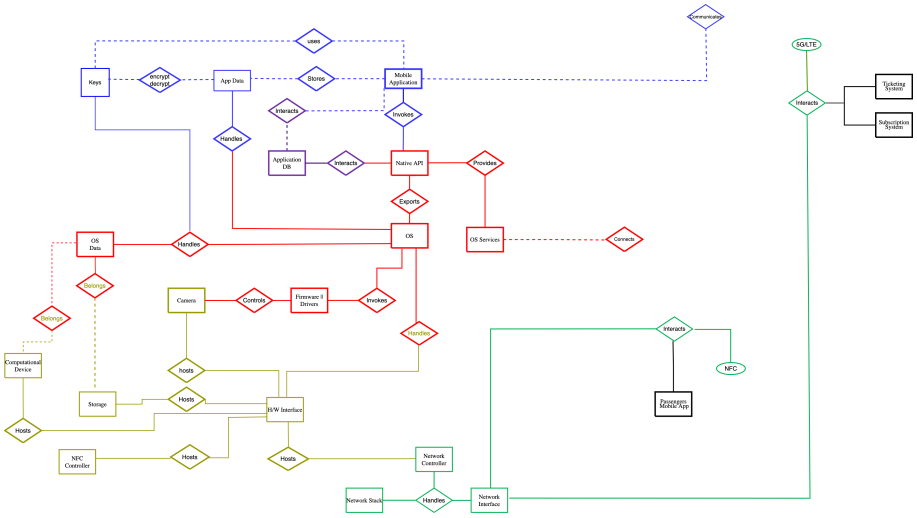

Fig. 3: Synthesis of Basic Assets that Form the Composite Asset Mobile Device

sector [32] g) the ENISA good practices for security of Smart Cars [31] and finally, technical specifications by ETSI-TVRA standard [35].

Once the threats were identified, and after some merging towards a common threat taxonomy, correlations between Threats, Common Weakness Enumerations (CWEs) [11] and Common Attack Pattern Enumeration and Classifications (CAPECs) were created [9]. Because of the fact that Common Vulnerability Enumerations (CVEs) do not have a direct mapping to CAPECs, threats that are mapped to CAPECs are linked using the CWE-CAPEC relations. By using this approach the method is able to map threats to new vulnerabilities, as soon as they are analyzed by NIST's National Vulnerability Database (NVD), and assigned related weaknesses (CWE) as well as a Common Vulnerability Scoring System (CVSS) score [43]. Also, by using CVSS metrics the methodology is able to distinguish the impact that each new vulnerability will pose to the service in terms of confidentiality, integrity and availability independently, in order to provide a more accurate estimation of the impact across these requirements.

The aforementioned approach regarding the correlation among threats and CWEs allows the automatic estimation of the occurrence probability for the identified threats, which contrasts with other risk analysis methodologies where those values are user-driven estimations based on the experience of the analyst. More precisely, whenever an instance of a particular basic asset is generated with vendor-specific characteristics (type, vendor and version) during the process of risk assessment, the correlation engine calculates the probability of occurrence as the threat occurrence rate. This is calculated as the amount of CVEs concerning the specific threat and the instance of the basic asset (type, vendor and version), divided by the total amount of the CVEs regarding the threat and the product family.

3.4 Risk Estimation

This phase is the final step of the presented service-oriented risk analysis methodology focusing on the calculation of risks. First, for each instance of a basic asset (BA) during an assessment, the risk is calculated as the multiplication of its impact valuation (I) based on the three security requirements of confidentiality, integrity, and availability (C,I,A) with the probability of occurrence of a threat (T) for any identified vulnerability and the CVSS Vulnerability Scale (V) for the three security requirements (C,I,A) and any identified vulnerability.

$$R_{BA}[C,I,A] = I[C,I,A] \times T \times V[C,I,A] \tag{1}$$

The CVSS Vulnerability Scale is a numerical representation of the severity of each vulnerability to the CIA requirements with the possible values being None (0), Low (1) and High (2). Then, after calculating the risk value of each basic asset (BA), the risk estimation for the composite asset (CA) comprised by N basic assets is calculated as the maximum for each security requirement of the identified risks of basic assets. Likewise, the overall risk score for services (S) equals the maximum risk scores of the involved composite assets. Therefore:

$$\begin{aligned} R_{CA}[C,I,A] &= \{R_{BA}[C,I,A]_1^N\}_{\max} \\ R_S[C,I,A] &= \{R_{CA}[C,I,A]_1^N\}_{\max} \end{aligned} \tag{2}$$

4 Dynamic Risk Analysis and Threat Modelling

This section provides example of the risk assessment conducted with the proposed methodology in the first multi-modal transport use case of CitySCAPE's project (in Genoa city), as Figure 2 depicts. For simplification and presentation purposes, only a small number of basic assets per composite asset are considered as parts of a service.

Initially, the risk analyst is responsible for defining the scope and the infrastructural functional services. In the current example, as Table 1 shows, the *SERV-GEN-02 - Ticket Validation* service is chosen. It is noted that in the context of the project, the following naming notation is used: Level of Abstraction (e.g. service, CA, BA, etc.), - use case (GEN refers to the city of Genoa), - the type of asset (applicable to CAs and BAs only),and - an index used to enumerate the different services, or assets in the use case. The valuation of the service impact entails several factors as explained in Section 3, resulting in high (4) confidentiality and very high (5) integrity and availability requirements due the financial and operational needs.

Then, the analysts define the high-level components known as composite assets (CA) along with their interactions; in this case these are the *COM-GEN-AS-01 - Validator's Mobile Device* which is used to validate passengers' digital tickets via either Near Field Communication (NFC) or Quick Response Codes (QR) and the *COM-GEN-AS-03 - Ticketing System* which is the server for issuing and validating the tickets. In the final stage, the analyst synthesizes basic assets (BA) and their interconnection to construct the service's composite assets. In this case, the analyst should synthesize *AS-OS-04 - Android 11* Operating System for the composite asset *COM-GEN-AS-01 - Validator's Mobile Device* and the *AS-OS-04 - Debian Linux 10* along with the *AS-SO-01*

Apache HTTP Server 2.4.18 for the composite asset *COM-GEN-AS-03 - Ticketing System*). In the specific example, the network is considered trusted and it is excluded by the analysis. Table 1 depicts the decomposition of the service to composite assets and subsequently to basic assets.

The user-defined catalogue of services, their impact valuation, the composite assets with their network connection, and the basic assets along with their interconnections are all provided to the correlation engine where the risk analysis is performed. The correlation engine first assigns impact valuations to composite and basic assets hierarchically and then searches and identifies threats for the given basic asset types (*AS-OS-04 - Operating System* and *AS-SO-01 - Web-Based Services*). Afterwards, upon identifying threats on basic assets and their instances (type, vendor, product, version *etc*.) the correlation engine identifies the applicable to them CVEs. For example, in the asset *COM-GEN-AS-01 - Validator's Mobile Device* for *TH-25 - Abuse of Authorisation / Privilege Escalation* among others, the CVEs that were identified were CVE-2021-39627[6] and CVE-2022-20114[7] with their CIA impact being (High, High, High) in both cases. For *AS-OS-04 - Debian Linux 10* and *TH-02 - Denial of Service* a couple of CVEs that were identified are CVE-2022-0908[8] and CVE-2019-9516[9] with both their CIA impacts being (None, None, High). For the asset *AS-SO-01 Apache HTTP Server 2.4.18* and *TH-11 - Software Exploitation / Malicious Code Injection* CVE-2016-8740[10] and CVE-2017-3169[11] were identified, among others, with their CIA impacts being (None, None, High) and (High, High, High) respectively. It should be emphasised that due to the basic asset decomposition, this process can be done automatically.

Finally, risk estimations take place using (2) as demonstrated in Table 1. The overall risk of the under examination service is calculated following the risk estimation of the involved composite assets and their basic assets. More precisely, for the composite asset *COM-GEN-AS-01 - Validator's Mobile Device*, the risk is estimated as the maximum risk of it's basic asset $\max([3.44,\ 4.3,\ 4.3]) = [3.44,\ 4.3,\ 4.3]$. Similarly, for the composite asset *COM-GEN-AS-03 - Ticketing System* the risk score is calculated as the maximum among its basic assets, *i.e*. $\max(([0,\ 0,\ 2.4], [0,\ 0,\ 2.4]), ([0,\ 0,\ 5.4], [4.32,\ 5.4,\ 5.4])) = [4.32,\ 5.4,\ 5.4]$. Finally, the overall risk for the service (*SERV-GEN-02 - Ticket Validation*) is calculated as the maximum risk of the composite assets that comprises it, *i.e*. $\max([3.44,\ 4.3,\ 4.3], [4.32,\ 5.4,\ 5.4]) = [4.32,\ 5.4,\ 5.4]$.

5 Comparative Analysis

As discussed in Section 2, several risk analysis, privacy impact assessment, and threat modelling methodologies have been proposed from corporate and academic perspectives in order to provide an insightful analysis regarding the nature and purpose of each

[6] https://nvd.nist.gov/vuln/detail/CVE-2021-39627
[7] https://nvd.nist.gov/vuln/detail/CVE-2022-20114
[8] https://nvd.nist.gov/vuln/detail/CVE-2022-0908
[9] https://nvd.nist.gov/vuln/detail/CVE-2019-9516
[10] https://nvd.nist.gov/vuln/detail/CVE-2016-8740
[11] https://nvd.nist.gov/vuln/detail/CVE-2017-3169

Service	Impact			Composite Asset	Basic Asset		Threat	Threat Probability	Vulnerability	Vulnerability Scale			Risk		
	C	I	A		Type	Instance				C	I	A	C	I	A
SERV-GEN-02	4	5	5	COM-GEN-AS-01	AS-OS-04	Android 11	TH-25	0,43	CVE-2021-39627	High (2)	High (2)	High (2)	3,44	4,3	4,3
									CVE-2022-20114	High (2)	High (2)	High (2)	3,44	4,3	4,3
				COM-GEN-AS-03	AS-OS-04	Debian Linux 10	TH-02	0,24	CVE-2022-0908	None (0)	None (0)	High (2)	0	0	2,4
									CVE-2019-9516	None (0)	None (0)	High (2)	0	0	2,4
					AS-SO-01	Apache Tomcat 10.0	TH-11	0,54	CVE-2016-8740	None (0)	None (0)	High (2)	0	0	5,4
									CVE-2017-3169	High (2)	High (2)	High (2)	4,32	5,4	5,4

Table 1: Snapshot of CitySCAPE Genoa Use Case Risk Assessment

method. Table 2 provides a list of *qualitative* properties with the main characteristics and the major limitations of each related to our proposed framework methodologies.

More precisely, regarding threat modelling methodologies, IT-Grundschutz [4] despite its wide applicability, frequently requires manual intervention by the analysts in order to perform a risk analysis. Additionally, in several cases, target objects may not be depicted correctly with the existing modules of IT-Grundschutz. Finally, even BSI acknowledges on their website [2] that the English version of the IT-Grundschutz Compendium may contain errors and omissions. OCTAVE [16, 17, 22, 46] has plenty of variations that differ significantly. For example, OCTAVE-S and OCTAVE Allegro provide threat and vulnerability catalogues, while OCTAVE FORTE does not and recommends other sources for threats such as PASTA or STRIDE [34]. EBIOS Risk Manager's [19] most valuable solution is its large toolbox[12]. Many of those tools are provided as freemium [20]. Nonetheless, the fact that new threats can only be added manually to the provided threat repository along with the case that no vulnerability catalogues are provided as well as new vulnerabilities cannot be imported should be considered [34]. MAGERIT [13–15] contemplates all aspects of a risk management procedure providing either a qualitative or a quantitative approach. There is no clear distinction between threats and vulnerabilities in the respective catalogues. In addition, a large part of MAGERIT [13,14] is written solely in Spanish which hinders the study process for non-Spanish speakers. Finally, another limitation is that a commercial license is required to conduct risk analysis projects [48]. MONARC [23] simplifies risk management procedure by supplying a risk management solution that permits importing data from existing and customizable models during the risk analysis phase but it does not provide measures catalogues [34]. MOSP[13] platform provides new objects to the MONARC's knowledge base. Also, to conduct a risk analysis for cyber-physical systems or ITSs, the knowledge base of MONARC should be extended manually. ITSRM^2 [34] offers both a qualitative and a quantitative process-based approach. It borrows threats from MAGERIT/PILAR [34] and measures from NIST SP800-53r5 [41]. Finally, ITSRM^2 is too strict in the process of computing the residual risk, narrowing down its flexibility. The work proposed by Zeddini *et al*. [53] is noteworthy, producing an extensive list of attacks, the vulnerabilities that cause them, the threats they pose on each asset and proposed countermeasures, all within the scope of ITSs, based on the ETSI-TVRA methodology. However it appears to be a mostly manual process and a theoretical approach. The risk

[12] https://www.ssi.gouv.fr/entreprise/management-du-risque/la-methode-ebios-risk-manager/label-ebios-risk-manager-des-outils-pour-faciliter-le-management-du-risque-numerique

[13] https://objects.monarc.lu

assessment methodology of Semertzis *et al*. [44] offers a major advantage over other methodologies, given that it uses a digital twin of Cyber-Physical Systems, it is able to calculate the cascading effects on attacks to various components of the system. However, it appears that the CVE categorisation of the different types of compromise is manual and since the vulnerabilities affecting assets can be vast, that categorisation will require a lot of user intervention to get results.

Additionally, regarding threat modelling approaches, though the effectiveness and novelty of PASTA [47] methodology is beyond doubt, it seems that it requires manual intervention and technical skills in several stages by the analysts in order to perform a reliable audit. Due to its very technical nature, threat modelling can be a very time-consuming and complex process as it provides neither automation nor any supportive tool. Using the PASTA methodology in non-trivial environments such as IoT (Internet of Things) infrastructures requires several modifications and extensions in the method's core, especially for adding hardware support and extending threat categories [49]. STRIDE [38] is a well-documented method that can be applied. Still, it can be a time-consuming process with increasing complexity equivalent to the size and scope of the analysis, meaning that the number of threats can overgrow when it is applied to complicated systems. Additionally, even though Microsoft does not support STRIDE anymore, there is an open-source tool [12] which supports the methodology. LINDDUN [50] is a privacy-oriented threat modelling approach. Despite the fact that it contains an extensive privacy knowledge base including threats, thorough documentation and prioritization of mitigation mechanisms, the analysis is a very time-consuming process requiring deep knowledge in order to be applied with increasing complexity equivalent to the size and scope of the analysis. Additionally, it has been reported that LINDDUN can provide sets of not relevant, impossible, or insignificant threats during an analysis [51]. The three-layer threat modelling approach presented by Hamad *et al*. [37] is a comprehensive model that makes use of attack trees to assess the security risks of the system as well as calculate the probability of a potential attack. However, in the vehicular domain, the computation of the probability by assigning numeric values to each level of the factors that pertain to the specific possibility (e.g. time needed to conduct an attack, required attack tools) is no-longer sufficient. Also, no mitigation mechanisms for the identified risks are provided. In the threat modelling approach proposed by Petit *et al*. [42], general attack trees for the high-level attacks are used by the authors to evade redundancy, during the attack tree construction phase. Nevertheless, as the attack trees become more detailed, those general attack sub-trees tend to become specific leading to scalability and extendability issues. The threat modelling approach of Jbair *et al*. [39] provides threat modeling for the lifetime of the ICPS using threats derived from MITRE ATT&CK for ICS. However asset categorisation is based on the Purdue model and as such does not appear to provide a method for user based asset criticality.

The proposed methodology shares similarities with several approaches. It uses well-established sources [9, 11, 27–33, 35] for threats and vulnerability identification in the correlation engine similarly to what MONARC [24] and ITSRM^2 [34] do. Additionally, PASTA [47] and the proposed risk analysis approach use CWEs but for different means. PASTA primarily uses CWEs as vulnerabilities while our presented method

correlates CWEs with all the identified threats and assets to measure the threat probability of occurrences, assign actual vulnerabilities to them, and measure their risk at the service level automatically. In contrast with the existing approaches, it is designed to support and perform risk analysis on any information technology asset with the concept of composition of basic assets to larger entities, the composite assets, in order to support non-conventional architectures such as IIoT, CPS, ITS and Multi-Modal Transport environments.

Method	**Type**			**Characteristics**	**Limitations**
	RA	**TM**	**PIA**		
PASTA [47]	✓	✓	×	A technical and holistic approach with thorough documentation that leverages well-established sources [9–11] to provide reliable threat models.	It requires manual intervention and profound technical knowledge in order to be applied. For environments such as IIoT and CPS infrastructures it would require several modifications and extensions [49].
LINDDUN [50, 51]	×	✓	✓	Extensive privacy knowledge base, thorough documentation and prioritization of mitigation mechanisms.	It requires manual evaluation of identified threats due to the reporting of not relevant, impossible, or insignificant threats.
STRIDE [38]	×	✓	×	An easy to apply and well documented tool-assisted methodology.	A time-consuming process with overgrown risks that requires manual evaluation whenever it is applied in complex architectures.
IT-Grundschutz [3]	✓	✓	×	It provides an extensive list of security recommendations for a variety of topics, including safeguards. It does not require risk analysis for some cases.	It is mostly targeted to German speaking organisations and requires a manual risk analysis for several cases.
OCTAVE Allegro [22]	✓	✓	×	It can be tailored for most organisations and provides guidance and worksheets.	It does not provide extensive threat and vulnerability catalogues.
OCTAVE-S [17]	✓	✓	×	It is tailored for small organisations and and can be led by a small team.	The team conducting the method requires knowledge of both business and security processes of the organization.
OCTAVE FORTE [46]	✓	×	×	Compared to OCTAVE Allegro, OCTAVE FORTE analyzes all types of risks, with cyber risks being part of the risk portfolio.	It does not provide any threat and vulnerability catalogues and makes recommendations using other methodologies for threat modeling such as PASTA or STRIDE.

Method	Type			Characteristics	Limitations
	RA	TM	PIA		
ISO/IEC 27005 [7]	✓	×	×	It is the de-facto risk management method and compatible with most other methods.	Because of its general nature, it requires a lot of effort in context establishment, risk identification etc. As such the implementation cost will be substantial.
EBIOS Risk Manager [19]	✓	×	✓	A configurable and agile approach providing quick results to the decision makers. Large set of tools available for free.	New threats can be added only manually to the provided threat repository [34]. Also, no vulnerability catalogues are provided, and new vulnerabilities cannot be imported [34].
MAGERIT [15]	✓	✓	✓	Contemplates all aspects of a risk management procedure providing either a qualitative or a quantitative approach.	Threat and vulnerabilites catalogues are not clearly distinguished. [34]. Requires a commercial license to conduct risk analysis projects [48]. Books 2 and 3 [13, 14] are written solely in Spanish.
MONARC [24]	✓	✓	✓	It takes advantage of risk analyses already carried out. The provided tool promotes flexibility and expandability by permitting new elements to be added to its knowledge base.	It does not provide a countermeasures catalogue and requires manual extensions to conduct risk analysis in CPS or ITS.
ITSRM^2 [34]	✓	×	×	It offers both a qualitative and a quantitative process-based approach.	It does not permit new asset categories to be appended and retrieves threats and countermeasures from other methodologies [34, 41]. Vulnerabilities are not used in the overall risk analysis process. It is strict in the process of computing the residual risks.
Semertzis *et al*. [44]	✓	×	×	An approach that is able to calculate the cascading effects on attack of Cyber-Physical Systems, using digital twins.	The CVE categorisation of the different types of compromises appears to be manual. Difficult to deploy
Zeddini *et al*. [53]	✓	✓	×	It offers an extensive list of attacks, assets, vulnerabilities, and countermeasures.	The approach appears to be theoretical and the list generation a manual process.

Method	Type			Characteristics	Limitations
	RA	TM	PIA		
Hamad *et al*. [37]	✓	✓	×	A threat modelling approach for vehicular environments that uses attack trees to represent attack paths to exploit an asset's certain vulnerability.	It does not appear to be a scalable solution. It does not provide mitigation mechanisms for the identified risks.
Petit *et al*. [42]	✓	✓	×	It provides a threat modelling tool based on attack trees that illustrate individual attack scenarios for the vehicular domain.	As the attack trees become more detailed, the general attack sub-trees may become more specific which could lead to scalability issues.
Jbair *et al*. [39]	✓	✓	×	It uses digital twins to perform threat modeling for the lifetime of the ICPS, based on MITREs ATT&CK for ICS.	It does not appear to provide a method for user control over asset criticality.
Proposed Framework	✓	✓	×	Dynamic Service-Oriented Risk Analysis Method focusing on Cyber-Physical Systems. Automated, hierarchical process covering a multitude of CPS domains.	The current version does not provide measures nor controls regarding the identified vulnerabilities. This is currently under development. Future work includes integration of PIA.

Table 2: Comparative Analysis Among Threat Modelling (TM), Risk Analysis (RA) and Privacy Impact Assessment (PIA) Methodologies.

6 Conclusions

The current research introduces a hybrid dynamic risk analysis with threat modelling capabilities and characteristics of a proof-of-concept implementation. Our procedure allows automatic valuation of risks and impacts through a hierarchical model that decomposes services to composite assets and then to basic assets, as well as through the integration of new vulnerabilities automatically using well-established public sources (CVEs, CWEs, CAPECs). Since it currently does not support risk mitigation for suggesting measures or controls for the identified vulnerabilities, the development of a security control and countermeasure suggestion mechanism to the identified vulnerabilities is in progress. To do so, the use of a machine-learning based approach to automatically assign CVEs to high-level vulnerabilities, as well as assign threats to unlabeled CVEs with CWEs will be developed, using our existing mapping of CWEs - Threats. Finally, through the use of probabilistic models, we aim to be able to evaluate the impact of a threat on an asset as well as how it cascades into other threats for connected assets in order to enhance the threat modelling capabilities of the proposed risk analysis methodology.

Acknowledgment

This work is a part of the CitySCAPE project. CitySCAPE has received funding from the European Union's Horizon 2020 research & innovation programme under grant agreement no 883321. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

References

1. The H2020 CitySCAPE project website, https://www.cityscape-project.eu
2. BSI-Standard 200-1: Information Security Management Systems (ISMS) (2018), https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.htm
3. BSI-Standard 200-2: IT-Grundschutz-Methodology (2018), https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.htm
4. BSI-Standard 200-3: Risk Analysis based on IT-Grundschutz (2018), https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.htm
5. ISO 31000:2018 Risk Management — Guidelines (2018), https://www.iso.org/standard/65694.html
6. ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary (2018), https://www.iso.org/standard/73906.html
7. ISO/IEC 27005:2018 Information Technology — Security Techniques — Information Security Risk Management (2018), https://www.iso.org/standard/75281.html
8. IT-Grundschutz-Compendium (2021), https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.htm
9. Common Attack Pattern Enumeration and Classification (2022), https://capec.mitre.org
10. Common Vulnerabilities and Exposures (2022), https://cve.mitre.org
11. Common Weakness Enumeration (2022), https://cwe.mitre.org
12. Threat Modeling (2022), https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling
13. Spanish Ministry of Finance & Public Administration: MAGERIT – versión 3.0.Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos (2012)
14. Spanish Ministry of Finance & Public Administration: MAGERIT – versión 3.0.Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro III - Guía de Técnicas (2012)
15. Spanish Ministry of Finance & Public Administration: MAGERIT–version 3.0.Methodology for Information Systems Risk Analysis and Management. Book I - The Method (2014)
16. Alberts, C., Behrens, S., Pethia, R., Wilson, W.: Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Framework, Version 1.0. Tech. Rep. CMU/SEI-99-TR-017, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA (1999)
17. Alberts, C., Dorofee, A., Stevens, J., Woody, C.: Introduction to the OCTAVE Approach (2003)
18. Alexander, O., Belisle, M., Steele, J.: MITRE ATT&CK® for Industrial Control Systems: Design and Philosophy (2020)
19. ANNSI: EBIOS Risk Manager (2019), https://www.ssi.gouv.fr/uploads/2019/11/anssi-guide-ebios_risk_manager-en-v1.0.pdf

20. ANSSI: Label EBIOS Risk Manager: Solutions Logicielles Conformes Ebios Risk Manager (2018), https://www.ssi.gouv.fr/entreprise/management-du-risque/la-methode-ebios-risk-manager/label-ebios-risk-manager-des-outils-pour-faciliter-le-management-du-risque-numerique
21. Bojanc, R., Jerman-Blažič, B.: A quantitative model for information-security risk management. Engineering Management Journal **25**(2), 25–37 (2013)
22. Caralli, R., Stevens, J., Young, L., Wilson, W.: Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. Tech. Rep. CMU/SEI-2007-TR-012, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA (2007), http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=8419
23. CASES: Optimised risk analysis method (2016), https://www.cases.lu/assets/docs/CASES_Monarc2016EN-web.pdf
24. CASES MONARC: Technical Guide (2021), https://www.monarc.lu/documentation/technical-guide/
25. Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., Stoddart, K.: A review of cyber security risk assessment methods for scada systems. Computers & Security **56**, 1–27 (2016)
26. ENISA: Magerit, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_magerit.html
27. ENISA: Cloud Computing Risk Assessment (2009), https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment
28. ENISA: Smartphones: Information security risks, opportunities and recommendations for users (2010), https://www.enisa.europa.eu/publications/smartphones-information-security-risks-opportunities-and-recommendations-for-users
29. ENISA: Smart Grid Threat Landscape and Good Practice Guide (2013), https://www.enisa.europa.eu/publications/smart-grid-threat-landscape-and-good-practice-guide
30. ENISA: Baseline Security Recommendations for IoT (2017), https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot
31. ENISA: ENISA good practices for security of Smart Cars (2019), https://www.enisa.europa.eu/publications/smart-cars
32. ENISA: Port Cybersecurity - Good practices for cybersecurity in the maritime sector (2019), https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector
33. ENISA: ENISA Threat Landscape for 5G Networks Report (2020), https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks
34. ENISA: Interoperable EU Risk Management Framework (2022), https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-framework
35. ETSI: Telecommunications and internet converged services and protocols for advanced networking (tispan); methods and protocols; part 1: Method and proforma for threat, risk, vulnerability analysis (2011)
36. EUR-LEX: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data

and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1532348683434,
37. Hamad, M., Nolte, M., Prevelakis, V.: Towards comprehensive threat modeling for vehicles. In: the 1st Workshop on Security and Dependability of Critical Embedded Real-Time Systems. p. 31 (2016)
38. Hernan, S., Lambert, S., Ostwald, T., Shostack, A.: Uncover security design flaws using the STRIDE approach (2006), https://docs.microsoft.com/en-us/archive/msdn-magazine/2006/november/uncover-security-design-flaws-using-the-stride-approach
39. Jbair, M., Ahmad, B., Maple, C., Harrison, R.: Threat modelling for industrial cyber physical systems in the era of smart manufacturing. Computers in Industry **137**, 103611 (2022)
40. Mataracioglu, T.: Comparison of PCI DSS and ISO/IEC 27001 Standards. ISACA **1** (2016), https://www.isaca.org/resources/isaca-journal/issues/2016/volume-1/comparison-of-pci-dss-and-isoiec-27001-standards#f1
41. NIST: Security and Privacy Controls for Information Systems and Organizations. Tech. rep. (2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
42. Petit, J., Shladover, S.E.: Potential cyberattacks on automated vehicles. IEEE Transactions on Intelligent Transportation Systems **16**(2), 546–556 (2015)
43. Scarfone, K., Mell, P.: An analysis of cvss version 2 vulnerability scoring. In: 2009 3rd International Symposium on Empirical Software Engineering and Measurement. pp. 516–525. IEEE (2009)
44. Semertzis, I., Rajkumar, V.S., Ştefanov, A., Fransen, F., Palensky, P.: Quantitative risk assessment of cyber attacks on cyber-physical systems using attack graphs. pp. 1–6 (2022)
45. Stefan Sacala, I., Pop, E., Alexandru Moisescu, M., Dumitrache, I., Iuliana Caramihai, S., Culita, J.: Enhancing cps architectures with soa for industry 4.0 enterprise systems. In: 2021 29th Mediterranean Conference on Control and Automation (MED). pp. 71–76 (2021)
46. Tucker, B.: Advancing Risk Management Capability Using the OCTAVE FORTE Process. Tech. rep., Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA (2020), http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=644636
47. UcedaVélez, T., Morana, M.M.: Risk Centric Threat Modeling: process for attack simulation and threat analysis. John Wiley & Sons (2015), https://www.wiley.com/en-us/Risk+Centric+Threat+Modeling%3A+Process+for+Attack+Simulation+and+Threat+Analysis-p-9780470500965
48. Vega, R., Arroyo, R., Yoo, S.G.: Experience in applying the analysis and risk management methodology called magerit to identify threats and vulnerabilities in an agro-industrial company. International Journal of Applied Engineering Research **12**, 6741–6750 (09 2017)
49. Wolf, A., Simopoulos, D., D'Avino, L., Schwaiger, P.: The PASTA threat model implementation in the IoT development life cycle. INFORMATIK 2020 pp. 1195–1204 (2021)
50. Wuyts, K., Joosen, W.: Linddun privacy threat modeling: a tutorial (2015), https://lirias.kuleuven.be/retrieve/331950
51. Wuyts, K., Van Landuyt, D., Hovsepyan, A., Joosen, W.: Effective and efficient privacy threat modeling through domain refinements. In: Proceedings of the 33rd Annual ACM Symposium on Applied Computing. p. 1175–1178. SAC '18, Association for Computing Machinery, New York, NY, USA (2018)
52. Xiong, W., Lagerström, R.: Threat modeling – a systematic literature review. Computers & Security **84**, 53–69 (2019)
53. Zeddini, B., Maachaoui, M., Inedjaren, Y.: Security threats in intelligent transportation systems and their risk levels. Risks **10**(5) (2022)