Journal of Data Intelligence, Vol. 1, No. 4 (2020) 401–418
© Rinton Press

AUTOMATED ONTOLOGY-BASED SECURITY REQUIREMENTS IDENTIFICATION FOR THE VEHICULAR DOMAIN [a]

ABDELKADER MAGDY SHAABAN
Center for Digital Safety & Security
Austrian Institute of Technology, Vienna, Austria
abdelkader.shaaban@ait.ac.at

CHRISTOPH SCHMITTNER
Center for Digital Safety & Security
Austrian Institute of Technology, Vienna, Austria
christoph.schmittner@ait.ac.at

THOMAS GRUBER
Center for Digital Safety & Security
Austrian Institute of Technology, Vienna, Austria
thomas.gruber@ait.ac.at

A. BAITH MOHAMED
Faculty of Computer Science
University of Vienna, Vienna, Austria
abdel.baes.mohamed@univie.ac.at

GERALD QUIRCHMAYR
Faculty of Computer Science
University of Vienna, Vienna, Austria
gerald.quirchmayr@univie.ac.at

ERICH SCHIKUTA
Faculty of Computer Science
University of Vienna, Vienna, Austria
erich.schikuta@univie.ac.at

Many electronic and electrical systems are now incorporated with modern vehicles to control functional safety. Lack of security protection mechanisms in vehicular design may lead to different ways of executing malicious attacks against the vehicular network. These attacks may have various types of negative consequences, such as safe vehicle operation. This work presents an ontology-based framework as a new automated approach to verify and validate security requirements against security issues in the vehicular domain. The system also applies a set of logical rules to identify a set of security requirements as a category of necessary security requirements that could be proposed to be integrated within the vehicle design to address a specific security issue.

Keywords: Ontology, Automotive, Security Requirements, Threats, Protection Profile, Verification and Validation.

1. Introduction

The vehicular industry is rapidly evolved from mechanical units working on gears and shafts to electronic components interacting using different communication protocols. The

[a] This paper is an extended version of the work published in the 21st International Conference on Information Integration and Web-based Applications & Services (iiWAS2019) [28]

modern vehicles combine a considerable number of interconnected units as Sensors, Electronic Control Units (ECUs), Buses, Actuators, and other electronic elements for monitoring and controlling the state of the vehicle [16]. Next-generation vehicles will include 20+ computers with storage sizes range from 8GB to 256GB [18]; wherever Voyager 1 and Voyager 2 have 69.63 kilobytes of memory for each [19]. Furthermore, modern vehicles have more powerful processing capabilities than the former space probs. The high-end car has over 100 million lines of code, and it is expected that the number would continue to grow shortly. Such codes are implemented for various control applications over numerous functionalities like safety-critical functions, driver-assistance, and others. The software operates on hundreds of programmable ECUs that interact via several types of communication protocols and buses (i.e., Controller Area Network (CAN bus), FlexRay, and Ethernet) [7]. In addition modern vehicles contain a large range of assets, from personal information like localization data and financial relevant information to safety-critical configuration and communication.

A research group from the University of Washington and the University of California San Diego has proved that it is possible for a code stored in any electronic unit to control critical components in a vehicle such as the brakes system. They have demonstrated that attackers can inject malicious code with physical access to the vehicle or even remotely using different wireless communication methods. This illustrates the real threat is not the accidental failure of any components in the vehicle, but the consequence of malicious code on the vehicular safety [16]. Accordingly, cybersecurity needs to be a part of the designing phases of the vehicular industry. Cybersecurity in the vehicular domain plays an integral role because it is responsible for protecting components and software that are managing the safety in a vehicle from different attack scenarios (i.e., unauthorized access, information infiltration, man-in-the-middle, or others) [20]. Besides safety there are also other assets in a vehicle, important for different types of stakeholders. Moreover, to improve the safety in the current and future vehicular industry, it is essential to develop requirements for vehicular components to assure their reliability and security [26]. However, the diversity in communication protocols and heterogeneity of electronic parts in the vehicle lead to an increase in the abundance of security vulnerabilities. Further, the process of security verification and validation (V&V) will be more complicated because this process must be aware of all vehicular components, potential threats, and related security requirements, which is considered a challenging process.

This research proposes an ontology-based model for vehicular security requirements. The model uses the ontology approach to represent the vehicular components, threats, vulnerabilities, and security requirements. We extend this to also include the assets and extend the assets from safety-related to a more holistic view. The security requirements are defined in terms of a group of documents that are called protection profiles (PP) [2]. The PP describes the security considerations for a Target of Evaluation (ToE) according to Common Criteria (CC). The ToE is a conceptual explanation of a system or system unit for a particular usage that is subjected to the evaluation. The ontology helps to create a complete overview of vehicle ToEs, related threats, and selected security requirements that are to be used in the validation and verification process. The model supports logical queries and inference rules to determine whether the selected security requirements are completely fulfilled. Additionally, the model improves the current security level of a vehicle system by identifying additional security requirements from several PPs. This leads to handle some existing security gaps and reach to the actual security goal that is needed to be achieved. Here a vehicle can utilize multiple PP for different security-related elements, and this can be combined to form a holistic approach. While a singular PP can not cover a whole vehicle, this approach is able to support security in the vehicular domain.

This paper is organized as follows; a short discussion about the existing research contributions in automotive security is presented in the ”Related Work” section. Section ”The Building blocks of the ontology framework” introduces the main concept of this work to describe the main building blocks of the proposed ontology-based security framework. The framework is applied to a vehicular assets case-study to investigate the potential threats and related security requirements. Then the model verifies and validates the selected security requirements as described in the ”case study” section. Also, this section demonstrates the influence of ontologies in managing a considerable number of security requirements. Finally, the paper ends with a summary, conclusion, and presents future work. While this paper was originally published in **the 21st International Conference on Information Integration and Web-based Applications & Services (iiWAS2019)** [28], we extended the scope of concerns and integrated this concerns as assets in the ontology.

2. Related Work

Any such device connects to the internet is exposed to be attacked by different ways of malicious activities, as the same as modern vehicles, which are considered as a complex system contains a vast amount of interconnecting objects [14]. Furthermore, vehicular cybersecurity is becoming one of the primary research topics in the automotive industry. The security engineering process in the vehicular domain contains sequence stages of activities that need to be conducted with the automotive development lifecycle. Figure 1 depicts the main activities of the security development phases in the automotive domain.

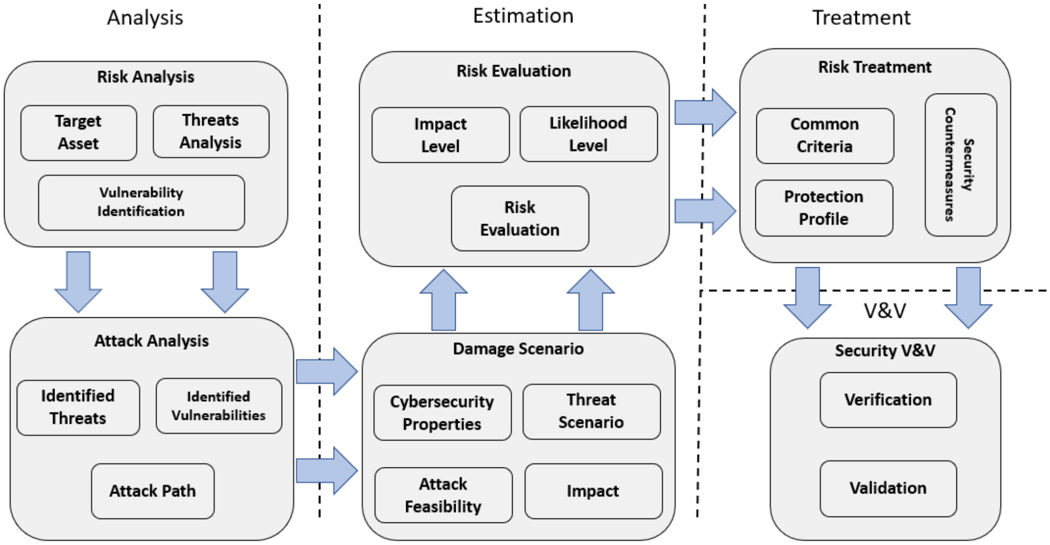

Fig. 1: Security development activities in the vehicular industry

2.1. *Risk Analysis*

One single vulnerable unit in a vehicle could expose all components and vehicles to additional attacks. Furthermore, it is essential to understand the exact security weaknesses in a vehicle at the early stages of the security engineering process because once the vehicle is built is becomes more difficult to add security. Here we add also the consideration of assets where a asset can range from something like a brake signal/configuration as a safety-critical asset to credit card information stored in the infotainment system to the communication link to the back end system of the vehicle manufacturer. Information about the assets and the potential threats allows the identification of security focus points. Efforts should be aimed at the intersection of critical assets and relevant threats. For this there are two main activities, the one is aimed at identifying potential attacks, the other one is aimed at identifying potential damage scenarios. If a combination of damage scenario (e.g. an asset which could be misused) and a potential attack (e.g. a set of threats/vulnerabilities) are identified there is a risk which might require further action, depending on the risk level.

2.1.1. *Target Asset*

It is essential to identify assets in a vehicle, to be used further in the other phases of the cybersecurity management process. This phase determines the security properties of the defined components (such as Secure Boot, Authentication, Encryption, others). These properties are essential in the threat and vulnerability analysis processes and for selecting the most relevant security requirements to address the identified security weaknesses in a vehicle.

2.1.2. *Threat Analysis*

Threat analysis is an activity that identifies potential negative actions that affect the security mechanism in the vehicles [4]. Ref. [10] discusses an overview of the available solutions for the threat modeling process. The threats and risk assessment techniques are mentioned in several research topics. Ref. [13] reviews the available techniques in the vehicular sector of threats and risk evaluation; then, it presented an approach to classify security threats. [12] demonstrated that threat modeling, using existing tools, can be a helpful and effective analysis method for the automotive security engineering process in various stages in the automotive development lifecycle.

2.1.3. *Vulnerability Identification*

The vulnerability analysis is the process of exploring, defining, identifying, and prioritizing vulnerabilities or security weaknesses. Meanwhile, security mechanisms need to be used to avoid those threats that exploit existing vulnerabilities in system units. The security mechanism is composed of several types of defensive actions such as detective, preventive, corrective, recovery, or response [17]. A brief overview of security vulnerabilities and existing vulnerability databases in the automotive domain is discussed in [29]. Vulnerabilities can be found at hardware, software, or network level, an overview of a possible classification of vulnerabilities has been presented in [24].

2.2. *Attack Analysis*

The attack analysis aims to define the relationships between the detected threats and the discovered vulnerabilities. This analysis tries to trace a massive number of security threats that may exploit vulnerabilities to attack a vehicle; this process is called attack paths. Also, the attack paths process aims to collect and derive information about the paths that are used by the attacker to attack the vehicle. This information could also assist in the security testing process [29]. The endpoint of a attack analysis is a potential damage scenario, e.g. an attacker is able to violate a security property of an asset.

2.3. *Damage Scenario*

In order to identify potential damage scenarios all assets and their relevant security properties need to be identified. Assets can differ depending on the considered stakeholder. As example ISO/SAE 21434 (DIS) requires the identification of safety, financial, operational and privacy related assets from the viewpoint of the vehicle or road user. For different assets different security properties (Confidentiality, Integrity and Availability (CIA)) are relevant. As an example, for the braking signal from ECU to brakes, integrity and availability is relevant. Since the brake action is announced via the brake lights confidentiality is not relevant.

For the location data stored in the navigational system the situation is the opposite. If past location are no longer available this is mainly an inconvenience. But, depending on the content, this information needs to be kept confidential. Here also the different viewpoints and stakeholder needs consideration. Even if the vehicle user would be okay with a confidentiality violation of his location data this is not allowed in nations following the GDPR. Insufficient protection of localization data could lead to financial damages to the vehicle manufacturer.

In this step all relevant stakeholder needs consideration to identify all potential assets and their relevant security properties. Here violation of security properties can also be rated, e.g. the identification of the most critical asset with the most important security property. Figure 2 illustrates the sequence flow of the ISO/SAE 21434 risk management process.

The asset is defined as a valuable unit from the attacker's point of view. This asset has a set of security properties that are defined as a protection mechanism against different cyber attacks. A potential threat could utilize these security properties to exploit security weaknesses, which lead to a damage scenario. The damage scenario could cause different negative consequences to the vehicular network. The attack on a vehicle could be initiated from a single point in the vehicle such as a particular asset unit, or it could be a point in a full attack path that includes one or multiple weak points that an attacker follows to achieve a malicious goal. A cyberattack could have different levels of probability that an attack action happens. Therefore, the impact and the attack feasibility parameter values shall be calculated to evaluate the correct level of the risk severity to make it easy to define the appropriate risk treatment that able to handle existing risk.

2.4. *Risk Evaluation and Treatment*

Risk evaluation or risk assessment process is a systematic approach of identifying and analyzing the hazards (i.e., safety) or threats (i.e., security) and estimating a level of risk severity for each hazard or threat [22]. This activity is based on the parameters of impact and likelihood, which are used to evaluate the specific risk level. On the first hand, it is essential to ensure that different types of impacts do not damage the vehicle or cause other accident

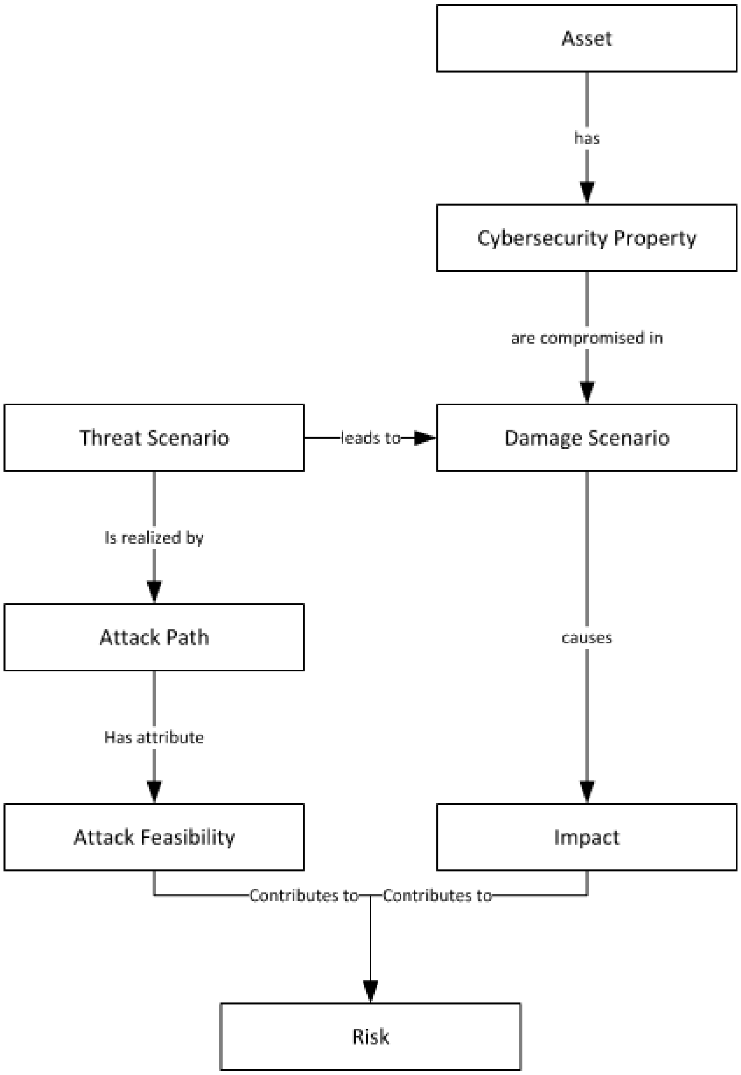

Fig. 2: The sequence flow of the risk management process by ISO/SAE 21434

or damage scenarios. Ref. [25] described four levels of impacts in the automotive domain:

- causes immediate damage to the environment or human lives (safety),
- causes the loss of control over personal information (privacy),
- causes financial damage (finance),
- negatively impacts the operation and traffic flow (operation).

In addition to that we can also consider impacts to other stakeholders, e.g. the vehicle manufacturer or the road operator. In this cases there are also impacts to topics like reputation of an organisation and scenarios impacting multiple stakeholder. Restricting the driving on an highway to a low limit by sending manipulated traffic information has a minor impact on the operation of the road user but a major impact on the reputation of the road operator. As it can seen with this example it is important to clearly define the scope of the impact assessment, which stakeholder are considered and how scenarios with multiple impacts are handled. In addition it is important to restrict the consideration also to direct impacts. In the scenario outlined above we could also consider impacts to a critical transport (e.g. emergency services) which is restricted and somebody suffering additional harm due to this scenario. Such scenarios needs to be cut off at a certain level.

We see here a relation between assets, system elements and damage scenarios:

- An asset is connected to one or more components of a system
- Violation of one or more security property of an asset can causes damage to one or more stakeholder thus leading to one or more damage scenarios
- A damage scenario has a certain level of impact on safety, financial, operational, privacy (SFOP) or more topics (SFOP+)

In a similar direction we have here also a relation between assets and threats:

- One or a combination of threats can cause a violation of security properties
- There is a certain degree of difficulty to one or a combination of threats

The evaluation of the likelihood considers the significant factor in the risk assessment process. The likelihood values represent how straightforward it is to exploit security weakness to attack a vehicle. Four different perspectives are proposed to evaluate the likelihood (i.e., attacker capabilities, ease of gaining information, accessibility of the system, and required equipment for an attack) [25]. Later, the level of severity of each of the detected potential threats is evaluated based on parameter values of the likelihood and impact level.

There might also be exploits of a security weakness which does not led to an impact, e.g. a security weakness in a system without an asset or exploits which does not violate a relevant security property.

The risk assessment process uses several risk methods for evaluating the vehicular risk level based on the parameter values of the likelihood and impact. The following formula is one of the most common risk assessment method:

$$Risk = Threat * Vulnerability * Consequence \tag{1}$$

where:

$$\begin{aligned} Threat * Vulnerability &= \text{Likelihood} \\ Consequence &= \text{Impact} \end{aligned}$$

The next steps are to address the unacceptable risk with applicable security requirements that reduce the risk severity level. Figure 3 depicts an example of the evaluated risks of the detected threats, as pointed on the graph. In this example, it is expected that the Tolerable Value (TV) or the risk acceptance threshold is four. The TV represents a security threshold;

all values above the TV need to be addressed by the suitable security requirements to mitigate the risk.

Security thresholds can be different for different aspects. A organisation might be willing to accept some financial impacts but might be more cautious with safety impacts. In order to support this consideration it is it is advisable to only summarize risks for the same topic and have separate risk mitigation processes.

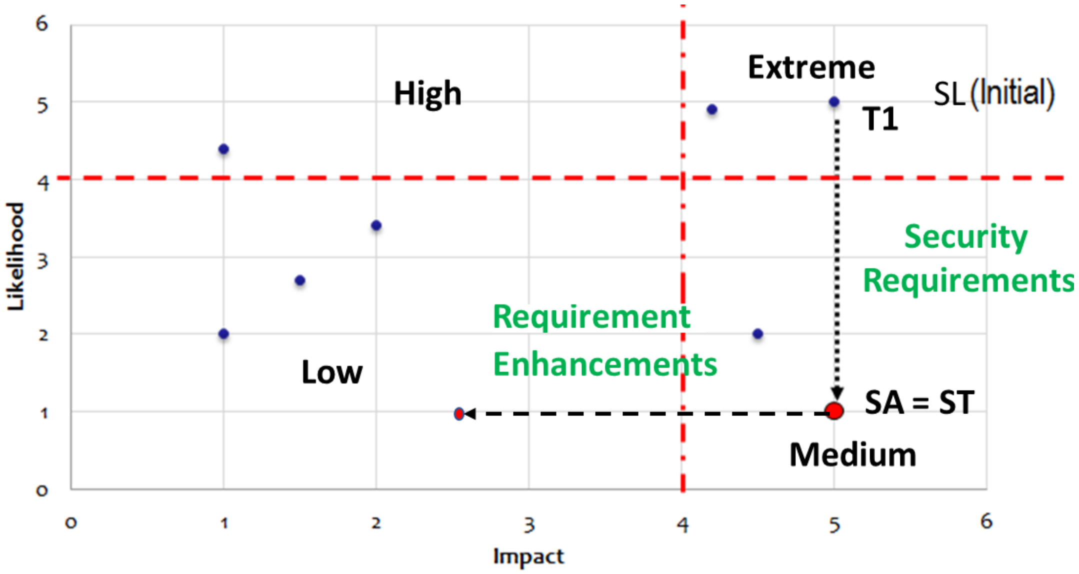

Fig. 3: Risk Mitigation Process [4]

For example, the threat (T1) on the graph is classified as an extreme severity level. The value of the Security Target (ST) is set during the concept phase, to define the specific security goal. Therefore, the security requirement(s) is/are used to mitigate the risk to an acceptable level. The resulting state after applying security requirements is called the Security Achieved (SA). This process completes only if SA = ST; otherwise, other security requirements (Requirement Enhancement (RE)) have to be applied to reduce the risk further to an acceptable level. [1] discussed in detail about security target, security achieved, and requirement enhancement.

In addition, the ontology approach is described in several research topics in cybersecurity. A CC Ontology tool is introduced as an ontology-based method to assist the evaluator at the certification process [8]. [30] introduced a security ontology for security requirements engineering that supports in the elicitation of security requirements. A security ontology is presented in [9] to provide a stable base for an applicable and holistic IT-security approach for small and medium-sized enterprises (SMEs), allowing low-cost risk management and threat analysis.

2.5. *Verification & Validation*

During and after the vehicular security engineering process, the vehicle must be checked to ensure that it is implemented according to the highest degree of protection level. Ref. [11] introduced a model-based security testing in the automotive industry; it discussed that the verification process of security requirements is integrated late in the development stages, where both time and budget are very restricting circumstances.

3. The Building Blocks of the Ontology Framework

This section discusses the building blocks of the proposed ontology-based model to manage security requirements against potential threats in the vehicular domain. The framework performs security verification and validation according to the current security status, and the actual security goal needs to be achieved. Figure 4 describes the building blocks of the proposed ontology framework.

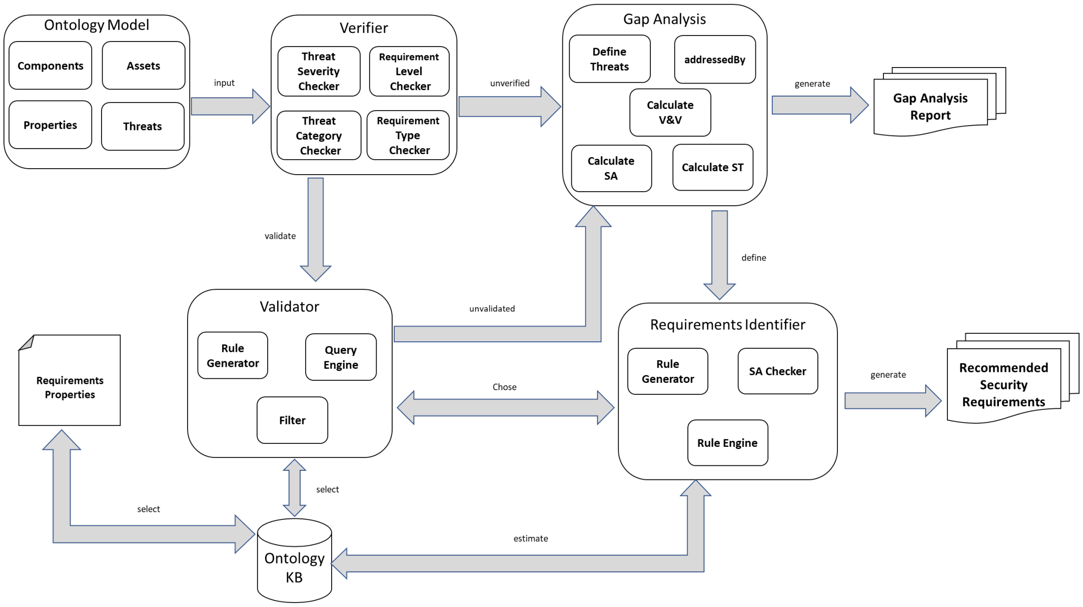

Fig. 4: The building blocks of the proposed framework

Reading Data: The block accepts the details of components, assets, potential threats, and selected security requirements. The structure of the input ontology model is described as semantic annotations (triples) in the form of (subject, predicate, and object); where the subject is the detected potential threat, the predicate is an object property assertion between threat and security requirements, and the object is security requirement. For example, a threat (T) can be addressed by a related security requirement (SR); so that it will be described as:

$$T \xrightarrow{addressedBy} SR$$

The predicate of the generated ontology is expressed as links between the threats hierarchical nodes and the security requirements nodes. That represents the selected security requirements can address one or more potential threat(s).

Verifier: The verifier part is one of the main blocks of the framework's design. That acts a peer review analysis to verify every single node in the ontology model to check the formal correctness or integrity, of a specific threat, that is addressed by security requirement(s). The verification process verifies if the specifications of the security requirements meet at the actual security level, which needs to be achieved to address a specific level of risk severity. For example, threat severity level plays an integral part in the risk treatment and V&V processes, because a threat with high severity level needs to be addressed with at least SL3 security requirement(s), as will be described in Section .

The verifier uses SPARQL query language to review the properties of the selected security requirement(s) and match the severity level of threats. The SPARQL language is applied to the ontology model to perform queries across different data sources(threats and security requirements) [23]. These queries are used to ensure that a vehicle is being developed based on standard security requirements, according to CCs. Additionally, to assures, the compliance of ToEs with PP meet the exact ST.

Validator: The validator part aims to investigate if the selected security requirements meet the ST. The validator block is considered as a rule-based approach consists of a set of "if-then" clauses to check which of the security requirements are validated or not. It uses SQWRL language (Semantic Query-Enhanced Web Rule Language) [21] that presents SQL-like operators for obtaining information from ontologies. The validator method construct SQWRL queries according to CC of security requirements are stored in an Ontology Knowledge Base (OKB). The CC is defined in a separate file "Requirement Properties" that represent the specific properties of threats and the related security requirements. The "Rule Generator" unit creates queries; then the "Query Engine" execute these queries to find security requirements able to address specific threats according to the CC. The "Filter" block selects the most suitable security requirements according to particular matching properties with threats.

Gap Analysis: The Gap Analysis method is applied to asses the differences in the SA before and after verifying and validating the selected security requirements. This estimates whether the selected security requirements meet the actual ST, and defines how to improve the current security state. This method calculates the values of SA and ST; then it generates reports that describe a complete view for describing the impact of the applied selected security requirements to the detected potential threats.

Requirements Identifier: The security requirement identification method uses the results of the gap analysis and performs a series of inference rules to select new security requirements from other PPs in the OKB to reach the actual ST. The "Rule Generator" generates logical rules that are typically conditional if-then clauses. The Semantic Web Rule Language (SWRL) [15] is applied to represent knowledge that select new security requirements from the OKB according to particular CC to address threats and achieve the required ST. The generated rules are applied to the "Rule Engine" to infer the logical consequences of the defined threats and security requirements properties. Then, it suggests/recommends a new set of security requirements suitable according to specific CC to address particular security weaknesses.

4. Case-Study: Potential Threats - Security Requirements for Automotive Assets

Automobiles are no longer mechanical units; the modern vehicles contain a massive number of interconnected electronic components networked together for controlling and monitoring the state of the vehicle. Modern vehicles consist of around 50 connected Electronic Control Units (ECUs) [16]. The increase in connectivity and interaction between multiple devices leads to the rise of new hazards. Figure 5 shows a simple design of a modern vehicle that contains numerous interconnected units.

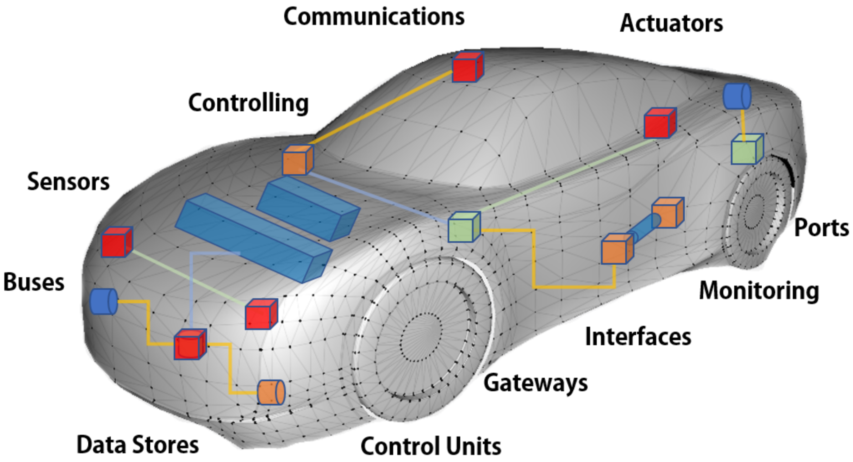

Fig. 5: Interconnected units in a modern vehicle

This case study investigates the security weaknesses and the applicable security requirements of a vehicular asset. The vehicle-to-anything Hardware Security Module (V2X HSM) is used in this case study as ToE, which is used for key management and cryptographic operations in the Vehicle C-ITS (Cooperative Intelligent Transport System and Services) Station (VCS) [6]. The ToE contains about seven assets are collected from version 2018 and 2019 of the "Protection Profile V2X Hardware Security Module" [5] [6]. The assets are describeds as follows [5] [6]:

- **Cryptographic keys:** the TOE Security Functionality (TSF) handles this asset.
- **VCS data:** data of users that exchange between Vehicle C-ITS Station (VCS) and ToE.
- **Secure Services:** TSF provides security services to the users.
- **HSM Software:** this asset regulates the action of the ToE.
- **Enrolment Private Keys:** private keys corresponding to public keys to be used in signing authorization tickers certificate requests.

- **Module Authentication Private Keys:** this is used to sign certificate request of the enrollment credentials.

- **Authorization Private Keys:** private keys corresponding to public keys are used to sign messages.

Figure 6 depicts the ontology representation model of the V2X HSM with relevant assets and some selected security properties to illustrate how the interaction is defined between the component, assets, and security properties.

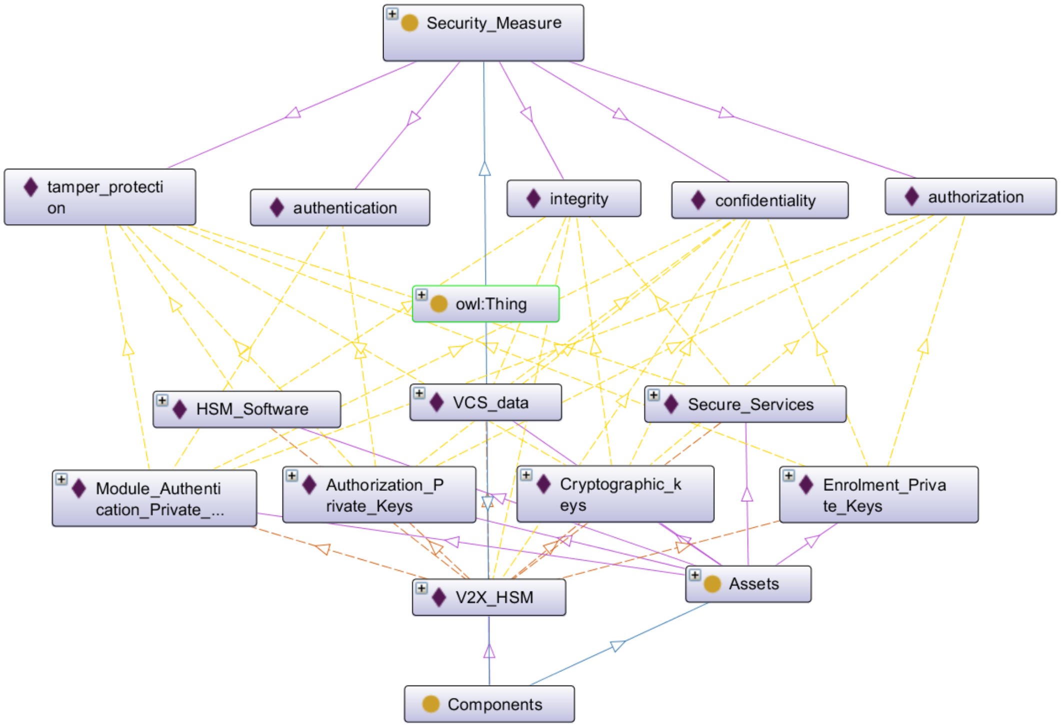

Fig. 6: Ontology model of the V2X HSM ToE

The proposed framework receives an ontology input in the form of vehicle components, assets, related security properties, and security requirements (if previously selected). Figure 7 illustrates the ontology structure of the VCS data asset as an input example to be handled in this case study, with the connection to related security properties. A threat (T13_6) is identified as potential threat violates the asset's security mechanism, such as tampering protection, integrity, and confidentiality. Threats could be identified by any threat analysis tools like ThreatGet [3] [10], or selected manually based on user experience. As the same as the security requirements, the ontology model may contain a set of selected security requirements that are chosen based on some knowledge of vehicular system design. These requirements could be managed by security requirement management tools such as MORETO [27]. Once the framework receives the input data, it begins applying a series of procedures to verify and validate the specified security requirements against identified potential threats. It then defines a list of possible threats to check and select a correct set of security requirements that shall be part of the asset security mechanism to protect it from various cyberattacks. There are two threats are defined for the selected asset (VCS data) according to the protection profile [6]; these threats are T.VCS_DATA_MODIF and T.VCS_DATA_DISCLOSE, re-named as T13_6 and T13_7, respectively. As shown in the figure, the identified threat (i.e., T13_6) in the ontology model is specified in the input, but the other threat is not defined (i.e., T13_7). Therefore, the fretwork applies a set of logical rules to infer new threats that exploits the asset's security mechanisms. The rule engine in the proposed security framework inferred T13_7 as the second expected threat that may have negative effects on the asset itself. These threats are described as a malicious sequence of events that adversely affect vehicle activity. However, no specified security requirements are identified as input to handle these malicious events. Therefore, the verification and validation process fails because the proposed framework investigates the integrity of the ontology relationships between individuals to see which threat is handled by the applicable security requirements. The framework would also take care of this process by choosing and outlining appropriate security requirements to resolve the existing security gaps. The framework then introduces a new set of rules to define the security requirements that could be expected as a set of recommended security requirements need to be part of the vehicle design (possibly within a component/asset design) to protect a specific critical point in the vehicle from cyberattacks.

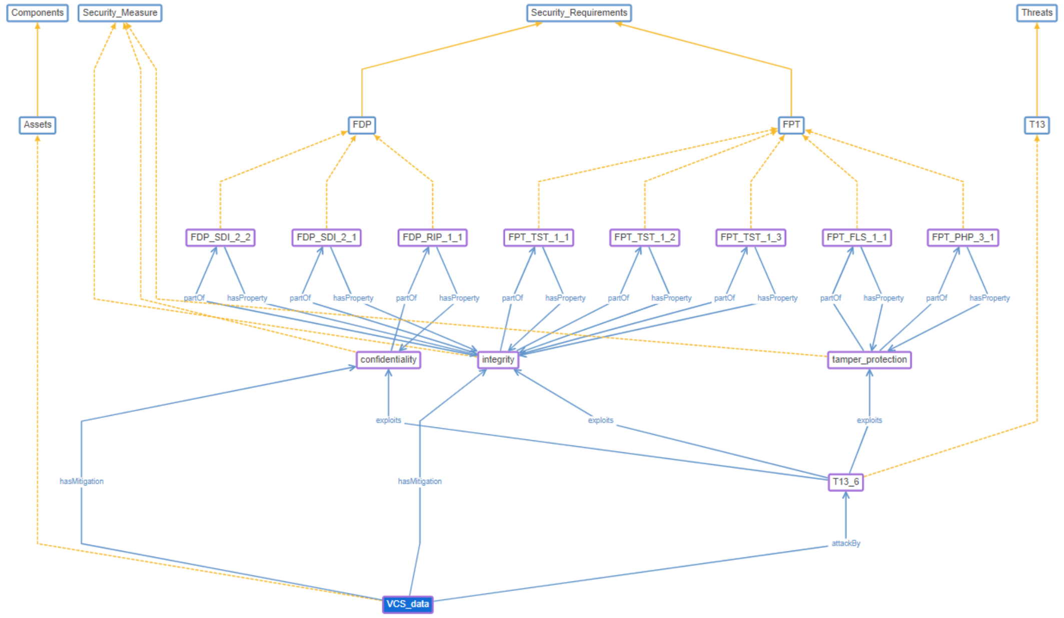

Fig. 7: The ontology model as an input to the proposed framework

According to the ontology model, no security requirements are selected to address the identified threat and protect the asset. It is important to define proper security requirements to be part of the "VCS data" asset to achieve a specific security objective. Therefore, the process of analyzing security requirements plays an important role in determining the security requirement(s) to solve existing security issues. Therefore, the framework applies a set of logical rules to identify security requirements to fill security gaps in vehicle design, particularly in components/assets. After applying the created rules, new relationships will be identified and integrated with the ontology model, which represents a complete taxonomy of the asset/component vehicle design. The taxonomy structure assists in outline a complete map of the vehicle system with all relevant details (i.e., threats, security measures, components, assets, security requirements, and risks). That helps to observe exiting security vulnerabilities in vehicle design (as problems) and perceive the relevant security requirements (as solutions).The SWRLAPI [b]is used to support semantic reasoning in defining a new set of security requirements engine. The engine uses the created rules to infer a new set of security requirements stored in security requirements knowledge-based. The newly identified security requirements are then incorporated with the ontology model to extend the vehicle taxonomy with all relevant security information. Figure 8 depicts how the effect of the inferred rules on the ontology structure of the asset's connections with other ontology instances (e.g., threats, security requirements, security properties, etc.).

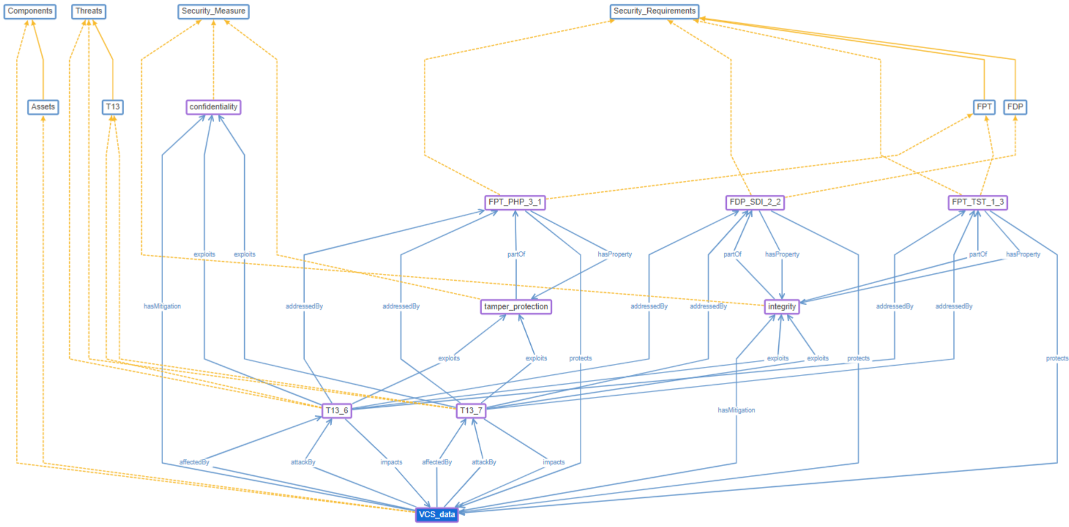

Fig. 8: A part of the new inferred results with the ontology model

The relationships "impacts," "protects," and "addressedBy" are identified and incorporated within the vehicle taxonomy, as is depicted in Figure 8. These relationships are described as:

- **Impacts:** the relationship represents a direct connection from a threat to affected component/asset.
- **protects:** the security requirement(s) are identified to fulfill prerequisites security mech-

[b] https://github.com/protegeproject/swrlapi

Table 1: Comparison between the inferred security requirements by the proposed security framework and the identified ones based on the V2X HSM protection profile

Threats	**Inferred Results**	**Security Requirements**
	FDP_SDI_2_2	
	FDP_SDI_2_1	
T.VCS_DATA_MODIF	FPT_TST_1_3	FDP_SDI_2
	FPT_TST_1_2	FPT_TST_1
	FPT_TST_1_1	FDP_PHP_3
T.VCS_DATA_DISCOSE	FDP_PHP_3_1	FPT_FLS_1
	FPT_FLS_1_1	
	FDP_RIP_1_1	

anisms need to protect a vehicular component/asset. Therefore, the "protects" relationship is defined to represent the relationship between a component/asset and a selected security requirement.

- **addressedBy:** security requirements are chosen to address a particular risk; this relationship is then defined between the security requirement and a particular threat.

Our findings on the VCS_data asset, according to the protection profile [6], this asset is impacted by two threats. The first threat is T.VCS_DATA_MODIF (is named T13_6 in this experiment), which exploits the asset's integrity, where the second threat is T.VCS_DATA_Disclose (that is renamed to T13_7 in this work), which breaches the confidentiality of the asset. The T13_6 was an input to the proposed framework, but the T13_7 was not included in the ontology input. The proposed framework finds and detects the missing threat (i.e., T13_7), which implies that the proposed framework is associated not only with the security requirements but also with managing the security issues that could have a negative impact on the system model.

In the protection profile [6] there are a set of security requirements that are defined as a set of security requirements for addressing identified threats and protecting "VCS data" asset. These security requirements are defined and selected according to the common criteria. The framework manages these security requirements to check the input ontology model and identify the proper set of security requirements that can fill the security gap in the system model. Our framework analyses the input ontology model and performs a set of logical rules in order to correlate the input with relevant security requirements. A set of security requirements have been inferred according to the common security measures between the security requirements, assets, and potential threats. This set is considered as a group of suggested or recommended security requirements, which assist the system designer in selecting and finding the most proper security requirements that help to fulfill the exiting security gap in vehicular design. The framework finds eight security requirements out of 23 are defined and explained in the protection profile [6]. Table 1 illustrates the obtained results by the proposed framework.

4.1. *Evaluation of the Results*

The framework gives a spot on the most proper security requirements that contains the common security measures with threats and particular assets. Our findings on security requirements at least hint that the frameworks provide a newly proposed concept of managing security issues in the vehicular domain by providing complete automation actionable to save times and efforts that are spent by the system architect. The system architect typically spends a lot of time and effort to match the common security properties between threat, assets, and security requirements and fill the exiting security gap in the system design. This process is achieved successfully by the proposed framework in a short time; the second column in Table 1 represents the set of identified security requirements by the proposed framework, where the third column represents the security requirements are defined in the protection profile [6]. Most of the results lead to a similar matching between the framework results, and security requirements are defined in the protection profile. The other identified security requirements are defined because they have common properties between the tested asset (i.e., VCS data) and the potential threats (i.e., T.VCS_DATA_MODIF and T.VCS_DATA_Disclose). The system or vehicular designer could check these results of the identified security requirements to decide which could be selected or ignored.

5. Summary, Conclusions and Future Work

Modern vehicles are consist of a massive numbers of interconnected units communicating through a network. The relationship between safety and security is considered a directly proportional because any injected malicious code to the vehicular components or busses could lead to damage or malfunction, which threaten the functional safety in a vehicle. The work presented an ontology framework for the security requirements management process to verify and validate the security requirements of the vehicular components and assets to assure that these requirements are fulfilled. The model applies a sequence of logical queries to the ontology model to determine whether or not the security requirements are able to handle risks in a vehicle.

A vehicular asset is used in this work as a case-study to investigate both potential threats and security requirements. The framework verifies and validates the selected security requirements, then compensates the detected security gaps by inferring a new set of security requirements. These security requirements are considered a set of recommended that need to be a part of the vehicular design (or probably component/asset) to protect the target unit from different forms of cyberattacks.

Future work will include verifying and validating security requirements on the vehicle model's component/asset level, based on various forms of security requirements (security standards and common criteria). The future plan also includes testing the proposed framework's ability to manage various types of input models, defining the potential threats, and choose the security under different vehicle data availability.

Acknowledgements

This work has received funding from the iDev40 project. This project is co-funded by the consortium members and ECSEL Joint Undertaking under grant agreement No 783163. The JU receives support from the European Union's Horizon 2020 research and innovation programme, national grants from Austria, Belgium, Germany, Italy, Spain and Romania as well as the European Structural and Investement Funds.

References

1. IEC 62443-3-3: Industrial communication networks – network and system security – part 3-3: System security requirements and security levels
2. ISO 15408, information technology - security techniques - evaluation criteria for IT security (common criteria)
3. Abdelkader Magdy, S., Christoph, S.: Threatget: New approach towards automotive security-by-design pp. 413–419 (2020)
4. Abdelkader Magdy Shaaban, Christoph Schmittner, A.B.: The design of a divide-and-conquer security framework for autonomous vehicles (2019)
5. Car 2 Car Communication Consortium: Protection Profile V2X Hardware Security Module. Protection profile, Car 2 Car Communication Consortium (2018), https://www.car-2-car.org/fileadmin/documents/Basic_System_Profile/Release_1.3.0/C2CCC_PP_2056_HSM.pdf
6. Car 2 Car Communication Consortium: Protection Profile V2X Hardware Security Module. Protection profile, Car 2 Car Communication Consortium (2019), https://www.car-2-car.org/fileadmin/documents/Basic_System_Profile/Release_1.4.0/C2CCC_PP_2056_HSM.pdf
7. Chakraborty, S., Al Faruque, M.A., Chang, W., Goswami, D., Wolf, M., Zhu, Q.: Automotive cyber-physical systems: A tutorial introduction. IEEE Design & Test 33(4), 92–108 (2016)
8. Ekclhart, A., Fenz, S., Goluch, G., Weippl, E.: Ontological mapping of common criteria's security assurance requirements. In: IFIP International Information Security Conference. pp. 85–95. Springer (2007)
9. Ekelhart, A., Fenz, S., Klemen, M., Weippl, E.: Security ontologies: Improving quantitative risk analysis. In: 2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07). pp. 156a–156a. IEEE (2007)
10. El Sadany, M., Schmittner, C., Kastner, W.: Assuring compliance with protection profiles with threatget. In: International Conference on Computer Safety, Reliability, and Security. pp. 62–73. Springer (2019)
11. KASTEBO, M., NORDH, V.: Model-based Security Testing in Automotive Industry. Master's thesis, Department of Computer Science and Engineering - UNIVERSITY OF GOTHENBURG, Gothenburg, Sweden (2017)
12. Ma, Z., Schmittner, C.: Threat modeling for automotive security analysis (2016)
13. Macher, G., Armengaud, E., Brenner, E., Kreiner, C.: Threat and risk assessment methodologies in the automotive domain. Procedia computer science 83, 1288–1294 (2016)
14. McAfee: Automotive security best practices. Tech. rep., McAfee (June 2016), recommendations for security and privacy in the era of the next-generation car
15. Member, W.: Swrl: A semantic web rule language. https://www.w3.org/Submission/SWRL/ (2004), accessed: 2019-10-18
16. Miller, C., Valasek, C.: Adventures in automotive networks and control units. Def Con 21, 260–264 (2013)
17. Mozzaquatro, B.A., Jardim-Goncalves, R., Agostinho, C.: Towards a reference ontology for security in the internet of things. In: Measurements & Networking (M&N), 2015 IEEE International Workshop on. pp. 1–6. IEEE (2015)

18. MUTSCHLER, A.S.: Data storage issues grow for cars. https://semiengineering.com/data-issues-grow-for-cars/, accessed: 19-10-2019
19. NASA: Your device has more computing power. https://www.nasa.gov/mission_pages/voyager/multimedia/vgrmemory.html, accessed: 18.10.2019
20. NHTSA: Vehicle cybersecurity. https://www.nhtsa.gov/technology-innovation/vehicle-cybersecurity, accessed: 17.10.2019
21. O'Connor, M.J., Das, A.K.: Sqwrl: A query language for owl. In: OWLED. vol. 529 (2009)
22. Ramesh, R., Prabu, M., Magibalan, S., Senthilkumar, P.: Hazard identification and risk assessment in automotive industry. International Journal of ChemTech Research 10(4), 352–358 (2017)
23. Recommendation, W.: Sparql query language for rdf. https://www.w3.org/TR/rdf-sparql-query/, accessed: 19.10.2019
24. Schmittner, C., Gruber, T., Puschner, P., Schoitsch, E.: Security application of failure mode and effect analysis (fmea). In: International Conference on Computer Safety, Reliability, and Security. pp. 310–325. Springer (2014)
25. Schmittner, C., Latzenhofer, M., Abdelkader Magdy, S., Hofer, M.: A proposal for a comprehensive automotive cybersecurity reference architecture. In: VEHICULAR 2018, The Seventh International Conference on Advances in Vehicular Systems, Technologies and Applications (2018)
26. Schoitsch, E., Schmittner, C., Ma, Z., Gruber, T.: The need for safety and cyber-security co-engineering and standardization for highly automated automotive vehicles. In: Advanced Microsystems for Automotive Applications 2015, pp. 251–261. Springer (2016)
27. Shaaban, A.M., Kristen, E., Schmittner, C.: Application of iec 62443 for iot components. Springer (2018)
28. Shaaban, A.M., Schmittner, C., Gruber, T., Mohamed, A.B., Quirchmayr, G., Schikuta, E.: Ontology-based model for automotive security verification and validation. In: Proceedings of the 21st International Conference on Information Integration and Web-Based Applications &amp; Services. p. 73–82. iiWAS2019, Association for Computing Machinery, New York, NY, USA (2019), https://doi.org/10.1145/3366030.3366070
29. Sommer, F., Dürrwang, J., Kriesten, R.: Survey and classification of automotive security attacks. Information 10(4), 148 (2019)
30. Souag, A., Salinesi, C., Mazo, R., Comyn-Wattiau, I.: A security ontology for security requirements elicitation. In: International symposium on engineering secure software and systems. pp. 157–177. Springer (2015)