A semantic-based approach to analyze the link between security and safety for Internet of Vehicle (IoV) and Autonomous Vehicles (AVs)

Maria Assunta Cappelli, Giovanna Di Marzo Serugendo, Anne-Francoise Cutting-Decelle, Martin Strohmeier

A semantic-based approach to analyze the link between security and safety for Internet of Vehicle (IoV) and Autonomous Vehicles (AVs)

Maria Assunta Cappelli, Giovanna Di Marzo Serugendo, Anne-Françoise Cutting-Decelle
Centre Universitaire d'Informatique (CUI), University of Geneva, CH
Maria.Cappelli@unige.ch, Giovanna.DiMarzo@unige.ch, Anne-Francoise.Cutting-Decelle@unige.ch

Martin Strohmeier
armasuisse Science and Technology, Thun, CH
Martin.Strohmeier@armasuisse.ch

***Abstract*—Current technological developments have led to a large quantity of embedded sensors, connected objects, and their related networks and communication to be present in the transport area involving modern cars, autonomous vehicles (AVs), aircraft, trains, as well as road infrastructures. Various types of signals and connections occurring on the Internet of Vehicles (IoV) are vulnerable to security attacks, which can cause the system to fail with serious consequences on the user's safety. Research on IoV security focuses on securing the communication among nodes. Only a few studies investigate the relationships between security and safety in IoV. Our approach addresses this gap by providing a semantic-based analysis exploring jointly safety and security. We propose an ontology, named SSIoV, - representing both security-safety knowledge - together with axioms and rules. Our aim is to perform reasoning and inferences on security vulnerabilities and their impact on safety risks, on the basis of actual data sets extracted from real scenarios.**

***Index Terms*—Internet of vehicle (IoV), Autonomous vehicles (AVs), Semantic approach, Ontology, Cyber Security, Security vulnerability, Safety risk**

I. Introduction

A large quantity of embedded sensors, connected objects, and their related networks and communication are present in everyday life. This also occurs in the transport domain with modern cars equipped with electronics on board, e-cars, autonomous vehicles (AVs), aircraft, trains, street lights, roadside units, Internet of things (IoT), Vehicular ad hoc network (VANET) and Internet of Vehicles (IoV).

IoV is an IoT application but also a large-scale distributed system featuring wireless communication and information exchange on internet between AVs, road, and users. IoV is the internet-based network where the vehicles are central nodes, with computational and storage abilities. Its network model also encompasses various types of communication enabling connected vehicles to gather and share their data among each other, with the road infrastructure, with various sensors [1]; or with the driver [2]. They all involve a huge amount of dynamic real-time data exchange.

The connectivity in IoV is prone to hackers' attack such as: sending commands to the vehicle for stealing data, tracking AVs, controlling cars' sensors or actuators; tampering with electric signals; diverting non-safety or safety critical functions, and so on [3]. Cybersecurity attacks due to *security* breaches can have catastrophic consequences in terms of *safety* as, for example: spoofing which can impact the human life of the "road users" provoking an accident; controlling cars' sensors or actuators, preventing steering or braking; tampering with electric signals; modifying signals in order to perturb a platoon stability; etc. In the automotive field, safety and cybersecurity regulations rely on the ISO 26262 and the ISO/SAE FDIS 21434 standards respectively. However, both standards do not deal with all aspects of AVs.

Most research work in this area focuses on securing communication through various means, such as network segmentation or cryptography. Several ontologies exist for safety and/or security for IoT, or for AVs cybersecurity. A few of them address both safety and security for IoV or AVs. Only a few studies combine the use of an ontology with reasoning rules for investigating the link between safety and security.

This paper presents the semantic-based approach we propose with a preliminary ontology, which allows us to perform reasoning and inferences in order to analyze the link between security vulnerabilities and safety risks. The approach relies on: (a) a high-level ontology which combines safety and security concepts, relations, axioms, and rules. We leverage existing ontologies from the IoT, risk, safety and security areas, and design a new ontology (SSIoV) focusing on the safety-security link for the automotive domain; (b) the instantiation of current datasets from the AVs area into the ontology (concepts, axioms and rules), through a graph database (e.g., GraphDB), that integrates both the ontology and the actual datasets; (c) the analysis of the security vulnerabilities and safety risks, by exploiting the inference abilities provided by the graph database, identifying rules that demonstrate incompatibilities with both safety and security.

II. State of the art

Conventional methods propose security solutions, which aim at detecting specific cyber-security attacks in networks

and do not involve safety [4]. Semantic approaches provide instead a holistic perspective [5], [6].

Semantic approaches to cyber-security. de Franco Rosa et al. [7] develop a Security Assessment Ontology (SecAOnto), which includes concepts for countermeasures, assets, and attacks.

Semantic approaches in the transport sector. Debbech [8] introduces an ontological approach for safety critical railways systems. Klotz et al. [9] present VSSO which utilizes a Vehicle Signal Specification (VSS) taxonomy for adapting the Sensor, Observation, Sample, and Actuator framework to the vehicle domain. Viktorovic et al. [10] propose the Connected Traffic Data Ontology (CTDO) on the foundations of SOSA ontology [11], to represent vehicles within the traffic ecosystem. Corsar et al. [12] make the Transport Disruption ontology for modelling travel and transport related events that have a disruptive impact on an agent's planned travel.

Semantic approaches to IoT. Bermudez et al. [13] develop IoT-Lite, that is a lightweight ontology to represent Internet of Things (IoT) resources, entities and services. Elsaleh et al. [14] propose IoT-Stream - a lightweight extension of SOSA ontology to annotate Stream Data on the Internet of Things (IoT) context.

Approaches for joint analysis of safety and security in transport field. Pereira et al. [15] provide a unified STAMP-based ontology representing the safety and security knowledge in order to help safety and security engineers to identify the mitigation needed to address the identified hazards for complex systems. Martin et al. [16] provide a pattern for a joint use of safety and security analysis in the automotive domain, without using ontologies.

The above studies provide a partial view of the problem we consider (IoT but not IoV, security without safety, transport but not automotive, joint safety and security but not ontology). Our work addresses this gap by providing a semantic analysis exploring jointly safety and security in IoV, and applying it to real data sets. To do so, we combine, adapt and extend some of the above ontologies, namely: IoT-Lite [13], VSSO [9], Pereira's ontology [15].

III. Research Approach and Methodology

In this section, we discuss the six specific steps of our research approach, which leads to a methodology for providing a semantic analysis of the link between security vulnerabilities and safety risks in the automotive domain. We illustrate our discussion on the following **Running Example - Spoofing message leading to a collision:** AVs broadcast beacon GPS signal messages to inform of their presence. An *attacker* sends a falsified *GPS signal* (a type of *GNSS* [17] signal) about its own position to the *target vehicle*. The *spoofing* attack here threatens the *authenticity* of the *sensors* signal.The GPS signal (falsely) mentions that the position of the attacker is very close to that of the target vehicle. The latter then applies a safety measure (*emergency stopping maneuver*) for ensuring a *safety property* (*safe stopping distance*) that leads to a *rear-end collision* with the vehicle behind it (*hazard*).

1. Developing an ontology unifying safety and security in the AVs domain. We use the Protégé software [18] to formalize the ontology. The security-safety ontology, named SSIoV, is a complete ontology referring to IoV and AV, which builds on existing ontologies. We extract and define the portion of the ontologies useful for this work, specifically linked to security vulnerabilities and safety risks involving signals, sensors, actors and organisational aspects (possibly aligning some of the concepts). The ontology defines with a common vocabulary, the concepts and their relationships and identifies causal relationships. It encompasses: *IoV organization* (e.g. assets; object; system; service; etc.), *safety components* (e.g. near collision, deviation, safe stopping distance; emergency stopping maneuver; etc.), and *security components* (e.g. threats, attacks, etc.). Table II and Figure 1 show an excerpt of the above concepts and their relationships focusing on our running example.

2. Modelling relationships between concepts; writing rules and axioms for safety risks and security vulnerabilities. We concentrate on events and rules, where security has an impact and a causal relationship on safety. Axioms for security vulnerabilities model various security breaches and describe how they impact signals or sensors. Axioms for safety risks model the various cases of how, from a deviation from normal operation, the system can reach a failure. We combine these two types of axioms to create security-safety rules expressing the causal relationships from security to safety.

Table I defines the following events linked to safety and security for our running example:

Name	Event	Explanation
Security-Breach	Security breach (attack)	An attacker generates falsified GPS signals and transmits it to the target vehicle
Safety-Rule	Safety rule (trigger)	The target vehicle takes an emergency stopping maneuver - slowing down suddenly
Safety-Cons	Safety rule consequence (fact)	The minimum safe stopping distance with the vehicle behind is not maintained
Safety-Issue	Safety issue (Consequence)	The target AV suffers a rear-end collision with the vehicle ahead

TABLE (I) Causal events between security and safety - Running example

To identify the causal relationships, we use the Systems-Theoretic Process Analysis (STPA) that is a safety analysis method on the System-Theoretic Accident Model and Processes (STAMP) model [19]. STPA allows describing the accident scenario in order to remove or control hazards in complex systems. STPA-Sec is a security extension of STPA, which extends it from safety to cybersecurity analysis [20], while STPA-SafeSec is a unified approach combining both safety and security analysis [21]. Some researchers applied the STPA approach to AVs [22]–[24]. Their research outcomes will enrich our ontology, since we transform these results into rules formalized and entered into Protégé .

To identify the rules and axioms, we use the existing regulation about the automotive domain. The existing sources are the cyber security best practices which provide guidance on the implementation of automotive cyber-security principles [17] [25] [26]; recommendation on cyber security [27];

3. Verifying the ontology consistency through a reasoning engine. We perform analytical reasoning for verifying the consistency of the developed unifying ontology, the safety and security axioms, and the security-safety rules. Once the consistency of our ontology and rules has been confirmed, we can move on to the next step.

4. Instantiating datasets into the ontology (concepts, axioms and rules). This instantiation is achieved through a graph database (e.g. GraphDB), that integrates both the ontology and actual data. Vehicular Reference Misbehavior (VeReMi) [28] is a current dataset which evaluates the misbehavior detection mechanisms for VANETs. This dataset consists of message logs of on-board units and a labelled ground truth, generated from a simulation environment, and also malicious messages intended to trigger incorrect application behavior. The integration allows detecting the spoofing attack that can cause a rear end-collision.

5. Querying the graph database. This task follows the ontology-based data access method (OBDA)[1]. It allows us to design, implement and execute specific queries and inferences on the graph database. Concerning our example above: (a) we query the system in order to select all spoofing attacks (the security breach); (b) we query the system to select all rules involving spoofing attacks that have an impact (causal relationships) on the safety (safety rule and safety rule consequences); (c) the system answers with all cases found in datasets involving this rule (safety issue).

Based on Table I and Figure 1, the reasoning then leads to the following conclusions for our running example:

$$\textbf{Security-Breach} \Rightarrow \textbf{Safety-Rule}$$
$$\textbf{Safety-Rule} \Rightarrow \textbf{Safety-Cons}$$
$$\textbf{Safety-Cons} \Rightarrow \textbf{Safety-Issue}$$

The spoofing attack (**Security-Breach**) with falsified GPS ultimately leads to a rear-end collision (**Safety-Issue**), we conclude that **Security-Breach** $\Rightarrow$ **Safety-Issue**.

6. Analyzing, evaluating and validating the outcomes. We identify and list the sets of rules incompatible with both security and safety and those that instead demonstrate no such incompatibility. We will identify an incompatibility when: (1) ontological reasoning shows that some data violates the rules (e.g., in the above scenario, the car did not brake soon enough). This means the rule or its expression is not sufficient for ensuring safety in all cases; (2) ontological reasoning identifies some risks involved even if no data violate the rules; (3) manual analysis of risks and rules incompatibility for remaining cases. Finally, we verify and validate our results (false positive and false negative).

[1]See http://optique-project/

IV. Security-Safety IoV ontology

The Security-Safety IoV (SSIoV) ontology we are developing encompasses four core parts: (a) IoV concepts and relationships (as an extension of IoT-Lite); (b) vehicle's signals and sensors (as an adaptation of VSSo); (c) safety components; (d) cyber security components. SSIoV ontology includes the main concepts and relationships which represent the central core of our ontology, as shown in Table II.

CONCEPT	RELATIONSHIP	CONCEPT
Asset	has	Vulnerabilities
Attack	threatens	Asset
Attack	exploits	Vulnerabilities
Attack	threatens	Safety Properties
Attack	causes	Hazard
Attack	threatens	Security Property
Hazard	damages	Asset

TABLE (II) Main concepts and relationships of SSIoV ontology

The three columns capture concepts and relationships of a cyber attack scenario. The *asset*'s *vulnerabilities* enable the *attack* exploiting the *asset*. This *attack* can cause *hazards*.

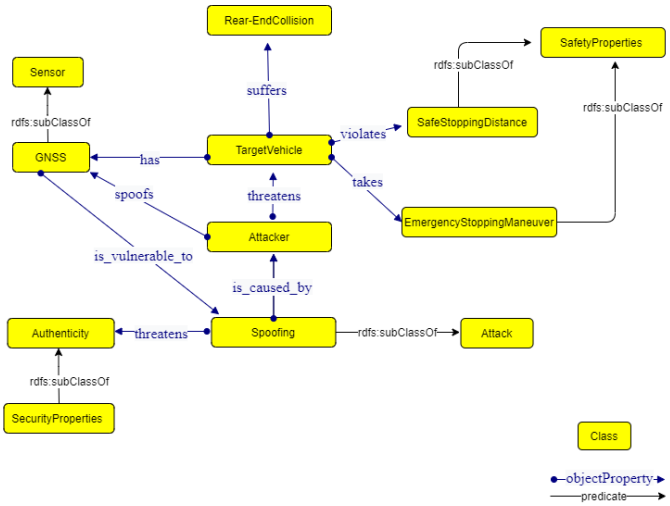

Fig. (1) Formalization of SSIoV: concepts and relationships of the first running example with Graffoo[2]

Starting from these simple relationships among concepts, we develop the SSIoV ontology, as shown in Figure 1 (excerpt focusing on our running example). It shows a portion of the ontology corresponding to our running example. The figure represents a *spoofing attack* propagated by an *attacker* against a *target vehicle*. The figure contains the main concepts and relationships shown in Table II : Target Vehicle and GPS are *Assets* [29]; spoofing is an *Attack*; Authenticity is a *Security Property*; Safe Stopping Distance and Emergency Stopping Maneuver are *Safety Properties*; Rear end-Collision is the *Hazard*. The SSIoV ontology currently under development, contains 278 Classes, 120 Object Properties, 54 Object

[2]See https://essepuntato.it/graffoo/

Property Domains, 18 Individual, 1304 Axioms, 430 Logical Axioms.

V. Conclusion

IoV has become the core network for making the autonomous driving scenario. However, to take advantage of this network, we need to face the security challenges raised from the IoV connectivity and their impact on safety. We developed a methodology that uses an ontology together with reasoning rules to investigate the link between safety and security, specifically targeting AVs.

In this paper, we have introduced preliminary results of our research, which aims at providing a semantic approach for enhancing the cyber security in the automotive domain. This work aims at providing a tool for improving preventive cyber defence capabilities in the IoV and AVs area. Based on an integrated security and safety rules ontology, together with corresponding rules, the tool highlights cyber security vulnerabilities leading to safety risks. This work contributes to improve security of critical road infrastructures for IoV. Our work can contribute to security and transport infrastructure, in terms of cars in the mid-term, aviation and railway in the long-term. This research also has the potential of improving and influencing the current standards that are being produced in the IoV and AV domains.

Future work involves the definition of safety and security rules, and evaluation with real data sets based on actual security-safety scenarios, investigating reverse resilience cases where safety rules may lead to security issues.

It would be interesting to see to what extent our approach might feed the FMEA Risk Analysis[3] carried out in the automotive domain to cope with safety analysis, particularly for practitioners in order to understand how the approach can be integrated in their common analysis methodologies [16].

References

[1] N. Sharma, N. Chauhan, and N. Chand, "Security challenges in internet of vehicles (iov) environment," in *2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC)*. IEEE, 2018, pp. 203–207.

[2] R. Gasmi and M. Aliouat, "Vehicular ad hoc networks versus internet of vehicles-a comparative view," in *2019 International Conference on Networking and Advanced Systems (ICNAS)*. IEEE, 2019, pp. 1–6.

[3] Y. Sun, L. Wu, S. Wu, S. Li, T. Zhang, L. Zhang, J. Xu, Y. Xiong, and X. Cui, "Attacks and countermeasures in the internet of vehicles," *Annals of Telecommunications*, vol. 72, no. 5-6, pp. 283–295, 2017.

[4] S. Sharma and B. Kaushik, "A survey on internet of vehicles: Applications, security issues et solutions," *Vehicular Communications*, vol. 20, p. 100182, 2019.

[5] T. Takahashi, Y. Kadobayashi, and H. Fujiwara, "Ontological approach toward cybersecurity in cloud computing," in *Proceedings of the 3rd international conference on Security of information and networks*, 2010, pp. 100–109.

[6] P. Torr, "Demystifying the threat modeling process," *IEEE Security & Privacy*, vol. 3, no. 5, pp. 66–70, 2005.

[7] F. de Franco Rosa, M. Jino, and R. Bonacin, "Towards an ontology of security assessment: A core model proposal," in *Information Technology-New Generations*. Springer, 2018, pp. 75–80.

[8] S. Debbech, "Ontologies pour la gestion de sécurité ferroviaire: intégration de l'analyse dysfonctionnelle dans la conception," Ph.D. dissertation, Ecole centrale de Lille, 2019.

[9] B. Klotz, R. Troncy, D. Wilms, and C. Bonnet, "Vsso-a vehicle signal and attribute ontology (short paper)," in *SSN Workshop at ISWC. CEUR Workshop Proceedings*, 2018.

[10] M. Viktorović, D. Yang, and B. d. Vries, "Connected traffic data ontology (ctdo) for intelligent urban traffic systems focused on connected (semi) autonomous vehicles," *Sensors*, vol. 20, no. 10, p. 2961, 2020.

[11] A. Haller, K. Janowicz, S. Cox, M. Lefrançois, K. Taylor, D. Le Phuoc, J. Lieberman, R. García-Castro, R. Atkinson, and C. Stadler, "Sosa: A lightweight ontology for sensors, observations, samples, and actuators," *Semantic Web Journal*, 2018.

[12] D. Corsar, M. Markovic, P. Edwards, and J. D. Nelson, "The transport disruption ontology," in *International Semantic Web Conference*. Springer, 2015, pp. 329–336.

[13] M. Bermudez-Edo, T. Elsaleh, P. Barnaghi, and K. Taylor, "Iotlite ontology. w3c member submission," *World Wide Web Consortium*, 2015.

[14] T. Elsaleh, M. Bermudez-Edo, S. Enshaeifar, S. T. Acton, R. Rezvani, and P. Barnaghi, "Iot-stream: a lightweight ontology for internet of things data streams," in *2019 Global IoT Summit (GIoTS)*. IEEE, 2019, pp. 1–6.

[15] D. P. Pereira, C. Hirata, and S. Nadjm-Tehrani, "A stamp-based ontology approach to support safety and security analyses," *Journal of Information Security and Applications*, vol. 47, pp. 302–319, 2019.

[16] H. Martin, Z. Ma, C. Schmittner, B. Winkler, M. Krammer, D. Schneider, T. Amorim, G. Macher, and C. Kreiner, "Combined automotive safety and security pattern engineering approach," *Reliability Engineering & System Safety*, vol. 198, p. 106773, 2020.

[17] ENISA. (2019) Code of practice, good practices for security of smart cars. [Online]. Available: https://www.enisa.europa.eu/publications/smart-cars

[18] M. A. Musen, "The protégé project: a look back and a look forward," *AI matters*, vol. 1, no. 4, pp. 4–12, 2015.

[19] N. G. Leveson, *Engineering a safer world: Systems thinking applied to safety*. The MIT Press, 2016.

[20] W. Young and N. G. Leveson, "An integrated approach to safety and security based on systems theory," *Communications of the ACM*, vol. 57, no. 2, pp. 31–35, 2014.

[21] I. Friedberg, K. McLaughlin, P. Smith, D. Laverty, and S. Sezer, "Stpa-safesec: Safety and security analysis for cyber-physical systems," *Journal of information security and applications*, vol. 34, pp. 183–196, 2017.

[22] A. Abdulkhaleq, S. Wagner, D. Lammering, H. Boehmert, and P. Blueher, "Using stpa in compliance with iso 26262 for developing a safe architecture for fully automated vehicles," *arXiv preprint arXiv:1703.03657*, 2017.

[23] L. Shan, C. Loiseaux, N. Marko, and J. C. Triginer, "Safety-security co-analysis with stpa: A case study on connected cars."

[24] S. Placke, J. Thomas, and D. Suo, "Integration of multiple active safety systems using stpa," SAE Technical Paper, Tech. Rep., 2015.

[25] N. H. T. S. A. NHTSA, "Cybersecurity best practices for modern vehicles," *Report No. DOT HS*, vol. 812, no. 333, pp. 17–20, 2016.

[26] E. A. M. A. ACEA. (2017) Acea principles of automobile cybersecurity. [Online]. Available: https://www.acea.be/uploads/publications/ACEA_Principles_of_Automobile_Cybersecurity.pdf

[27] N. UNECE, "Proposal for recommendation on cyber security," 2019. [Online]. Available: https://www.unece.org/fileadmin/DAM/trans/doc/2019/wp29grva/ECE-TRANS-WP29-GRVA-2019-02e.pdf

[28] R. W. van der Heijden, T. Lukaseder, and F. Kargl, "Veremi: A dataset for comparable evaluation of misbehavior detection in vanets," in *International Conference on Security and Privacy in Communication Systems*. Springer, 2018, pp. 318–337.

[29] R. Ross, M. McEvilley, and J. Oren, "Systems security engineering: Considerations for a multidisciplinary approach in the engineering of trustworthy secure systems," National Institute of Standards and Technology, Tech. Rep., 2016.

[3] See https://en.wikipedia.org/wiki/Failure_mode_and_effects_analysis