Automated Right of Way for Emergency Vehicles in C-ITS: An Analysis of Cyber-Security Risks

Lucie Langer[1(✉)], Arndt Bonitz[1], Christoph Schmittner[1], and Stefan Ruehrup[2]

[1] Austrian Institute of Technology, Vienna 1210, Austria
{lucie.langer,arndt.bonitz,christoph.schmittner}@ait.ac.at
[2] ASFINAG, Vienna 1120, Austria
stefan.ruehrup@asfinag.at

Abstract. Cooperative Intelligent Transport Systems (C-ITS) provide comprehensive information and communication services to enable a more efficient and safe use of transport systems. Emergency vehicles can benefit from C-ITS by sending preemption requests to traffic lights or other connected road users, thus reducing their time loss when approaching an emergency. This, however, depends on a secure and reliable communication between all involved parties. Potential risks involve cyber-attacks and acts of sabotage. A major issue is the security process applied to provide C-ITS vehicles with the authorisations to exercise the right of way intended for emergency vehicles.

This paper presents results from the research project *EVE (Efficient right of way for emergency vehicles in C-ITS)*: Following the lifecycle and processes of the emergency vehicle and its on-board unit from installation to decommissioning, relevant use cases are subjected to an extended Failure Mode and Effects Analysis (FMEA) to assess inherent flaws that could be exploited by cyber-attacks. The results show that, while the technical provisions foreseen by the relevant standards in general provide strong security, detailed security management processes need to be specified.

Keywords: C-ITS · SSP · Risk analysis · FMEA · Emergency vehicle

1 Introduction

In our future transport systems vehicles will interact both with road infrastructure and with each other: Intelligent Transport Systems (ITS) are defined as "systems in which information and communication technologies are applied in the field of road transport, including infrastructure, vehicles and users, and in traffic management and mobility management, as well as for interfaces with

The work described in this paper was carried out as part of the project EVE funded by the Austrian Security Research Programme KIRAS.

© Springer Nature Switzerland AG 2020
A. Casimiro et al. (Eds.): SAFECOMP 2020 Workshops, LNCS 12235, pp. 148–160, 2020.
https://doi.org/10.1007/978-3-030-55583-2_11

other modes of transport" [18]. ITS use digital communication to exchange information about road works, hazardous locations, traffic rules etc., partially based on data provided by various sensors. Cooperative ITS (C-ITS) place additional demands on the communication equipment: "Cooperative" means that each ITS station (on-board or roadside) must be able to communicate ad hoc with other ITS stations and exchange relevant information in a trusted domain.

Currently emergency vehicles indicate the urgency of their mission by warning lights and siren. On a rescue mission they usually have the right of way, and may disregard traffic lights. However, exercising this right can be challenging for the driver, especially with dense urban traffic or multi-lane roads, and requires a significant slow-down. There are systems for traffic signal preemption that change the signal to give way to the approaching emergency vehicle. These systems are also used for public transport, and are implemented in different ways, resulting in country- or even city-specific solutions.

The Austrian research project *EVE (Efficient right of way for emergency vehicles in C-ITS)*[1] investigates how this situation could be improved by C-ITS: At signalised intersections (see Fig. 1) the emergency vehicle can send a preemption request to the traffic light controller or other connected vehicles. On a motorway, the efficiency of forming a rescue lane may be enhanced by announcing an approaching emergency vehicle. To prevent misuse, so-called Service-Specific Permissions (SSPs) limit the use of preemption requests to authorised parties.

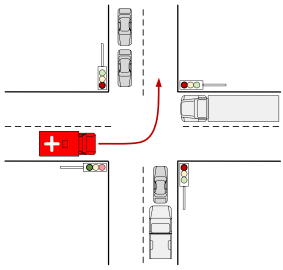

Fig. 1. Traffic signal preemption for emergency vehicles.

As C-ITS relies heavily on ad-hoc communication between the different participants, cybersecurity aspects play an important role: Tampering with C-ITS messages could, for example, cause drivers to react to fake events or follow incorrect rules, resulting in undesired or even unsafe driving behaviour. If an attacker obtains the Service-Specific Permissions reserved for emergency vehicles, he could use them for his own prioritisation or to disturb the overall traffic situation. C-ITS are therefore embedded in a comprehensive security and trust architecture to ensure the authorised use of C-ITS services. However, a high level

[1] https://kiras.at/en/financed-proposals/detail/d/eve-effiziente-bevorrangung-von-einsatzfahrzeugen-im-automatisierten-strassenverkehr/.

of security and safety of the target system can be ensured only by performing a comprehensive risk analysis and implementing according countermeasures.

This work presents a threat and risk analysis for prioritised emergency vehicles in C-ITS. Following the lifecycle of the emergency vehicle and its on-board unit from installation to decommissioning, relevant use cases have been subjected to an extended Failure Mode and Effects Analysis (FMEA) as part of the EVE project. The FMEA procedure and results are presented along the core use case, i.e., traffic signal preemption.

The paper is structured as follows: Sect. 2 summarises the state of the art in C-ITS, focusing on security aspects. Section 3 explains the methodology used for the risk analysis in the EVE project. Section 4 describes the risk analysis and evaluation results along the core use case of traffic signal preemption. Section 5 concludes the paper and provides an outlook on future work.

2 State of the Art

2.1 Status of C-ITS in Europe

C-ITS applications are currently being rolled out in Europe in mass production vehicles and in infrastructure deployments in several countries. The CAR-2-CAR Communication Consortium (C2C-CC) [28] has published profiles for C-ITS in vehicles based on standards and specifications from European Telecommunications Standards Institute (ETSI), European Committee for Standardization/International Organization for Standardization (CEN/ISO), Society of Automotive Engineers (SAE), and Institute of Electrical and Electronics Engineers (IEEE). For the infrastructure deployment, 18 EU Member states have joined the C-ROADS Platform which aims at cross-border harmonisation and interoperability for the roll-out C-ITS services. C-ROADS published a set of profiles that determine which ITS standards and which data elements and options should be used for the so-called Day-1 services, i.e., C-ITS services which should be available in the short term due to their expected societal benefits and technology maturity [1]. The profiles of C2C-CC and C-ROADS are coordinated to form a harmonised basis for Day-1 C-ITS services in Europe.

C-ROADS pilot deployments play an important role to launch the Europe-wide infrastructure roll-out. C-ROADS built on the experience from corridor projects, such as the Cooperative ITS Corridor between Rotterdam and Vienna [29], where the Austrian part ECo-AT [30] was characterised by a large set of use cases including road works and hazardous location warnings, as well as In-Vehicle Information (IVI) and Intersection Safety (ISS). In France, the SCOOP@F [31] project has equipped five pilot regions in France with C-ITS equipment since 2014. While most deployments target Day-1 or -1.5 use cases involving normal passenger vehicles, the specialised emergency vehicles and their specific use cases have only gained little attention.

The ITS Directive [18] provides the legal and technical framework for ITS within the European Union. It was followed by the European strategy on Cooperative Intelligent Transport Systems [5]. Based on this, the EC has initiated the

C-ITS platform in Phase I (2014–2016) [4] as a cooperative framework for developing a common European vision for the interoperable deployment of C-ITS. In Phase II (2016–2017) [6], the common vision for C-ITS was further developed towards Cooperative, Connected and Automated Mobility (CCAM).

2.2 Relevant C-ITS Services and C-ITS Security

ETSI TR 102 638 [13] defines a Basic Set of Applications (BSA) that reflect the main user needs and requirements. In the context of emergency vehicles, the following three services are important: The **Cooperative Awareness (CA) Basic Service** [11] allows road users to inform each other about their current position, velocity and other attributes. This service could be used by a vehicle to indicate its type (i.e., emergency vehicle) to other road users. The **Decentralised Environmental Notification (DEN) Basic Service** [10] supports informing road users about road hazards or abnormal traffic conditions, for example an approaching emergency vehicle or closed lanes on a motorway after an accident. Regarding infrastructure elements, [17] provides a set of services, including the **Traffic Light Control (TLC) Service** which enables the prioritisation of public transport and public safety vehicles at traffic lights.

The C-ITS **security architecture** defined in ETSI TS 102 940 and TS 102 941 [15,16] details a set of security requirements and a security (lifecycle) management system to establish the C-ITS trust model for the general communication architecture [9]. This trust model is based on a fully defined public key infrastructure (PKI), including concepts regarding Certificate Trust Lists with multiple Root Certificate Authorities and the revocation of certifications via Certificate Revocation Lists. With TS 103 097, ETSI also gives guidance on how to secure communication between road users and infrastructure elements [14]. For example, the **Service-Specific Permissions (SSPs)** transmitted as part of every ITS message ensure that only authorised ITS stations disseminate certain messages (for example, only an emergency vehicle may generate the DEN message *emergency vehicle approaching*). The PKI-based Certificate Policy [19] includes legal and technical requirements for the management of PKI certificates for C-ITS applications and all entities participating in the European C-ITS.

3 Methodology

With regard to EVE's focus on the ITS-S lifecycle and related processes, the risk analysis was performed through a process-based FMEA, which is an established method to systematically analyse each process step for potential risks, and has already been used for security analysis [23]. The attacks were classified according to the STRIDE model [22,24].

The first step of the analysis was to determine the lifecycle of the ITS station (ITS-S) from provisioning to decommissioning. Next, the processes defining each phase of the lifecycle were broken down into process steps and visualised in activity diagrams. This output was subsequently used for the process-based FMEA. Each of these steps is described in more detail in the following.

3.1 Lifecycle Definition

From a security point of view, the lifecycle of an ITS-S includes the initial configuration, enrolment, authorisation, operation[2], and end of life (see Fig. 2): The **initial configuration** of the ITS-S is done as part of the manufacturing process, and establishes information and key material in the ITS-S and the Enrolment Authority (see [16] for details). This information includes the designated *appPermissions* for the ITS-S, i.e. the C-ITS services that this ITS-S is permitted to use. For emergency vehicles, these may include sending DEN messages such as *emergency vehicle approaching* (cf. Sect. 2).

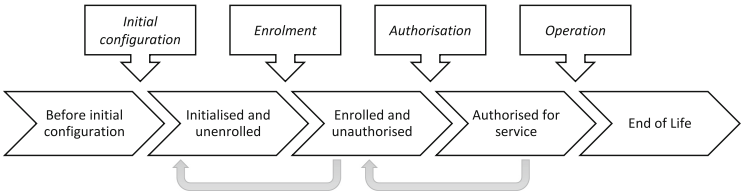

Fig. 2. ITS-S security lifecycle (cf. [16]).

In the **enrolment** phase, the initialised ITS-S requests its enrolment credential from the Enrolment Authority. For **authorisation**, the enrolled ITS-S uses this credential to request authorisation tickets from the Authorisation Authority, who checks with the Enrolment Authority whether the requested authorisations correspond to the approved *appPermissions* for that ITS-S.

During **operation**, the ITS-S communicates with other ITS-S. For each transmitted message the ITS-S uses an Authorisation Ticket to prove to the receiver that it is entitled to send that message and use the corresponding C-ITS service without revealing its identity. For the operation phase of the ITS-S lifecycle, two specific scenarios were considered for an emergency vehicle ITS-S: (i) requesting traffic signal pre-emption in urban areas (see Sect. 4) and (ii) requesting the formation of an ad-hoc emergency corridor on motorways (beyond the scope of this paper).

If the ITS-S has been compromised or has otherwise reached its **end of life**, it is passively revoked, i.e. the Enrolment Authority rejects any further authorisation requests for this ITS-S.

3.2 Process Analysis

For each of the ITS-S lifecycle phases, a process analysis was performed to identify the individual steps required to accomplish the target state. In order to ensure a structured procedure and to obtain an easily comprehensible overview of the processes, this breakdown into individual process steps was done by using

[2] Maintenance is not considered here.

UML activity diagrams for modelling (see Fig. 3) followed by a (textual) description of each process step. This analysis provided the basis for the subsequent process-based FMEA.

3.3 FMEA

The security analysis focuses on the processes relevant to the operation of emergency vehicles in a C-ITS environment. It is based on an extended FMEA, a structured technique that examines failure modes and effects. The aim is to identify potential weaknesses and improve the reliability, availability or safety of a system. The system or process under examination is hierarchically broken down into its basic elements and steps. Subsequently, the failure modes (i.e., error causes) of the elements are examined for causes and effects [21].

Originally, FMEA was aimed at the reliability or safety of hardware. It was later extended to cover additional topics like process analysis and security. The FMEA type used in this work is a process-based FMEA, which aims to identify possible weaknesses in production or performance processes. Since the focus is on security aspects, the FMEA method is applied in a slightly modified variant: If the failure of a component is caused by an attack, it is treated as a malfunction [27]. The main difference to the method presented in ETSI TR 102 893 "Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA)" [12] is our focus on the process and lifecycle of the system which requires a different approach than the more technical system-focused approach presented in [12].

The FMEA is based on the outcomes of the process analysis (see Sect. 3.2). Each process step is analysed for potential attacks. For each attack, the potential causes and effects (or attack vectors) are listed. Control measures defined by the relevant ETSI specifications are considered as well as additional security measures that supplement or refine these provisions.

The risk assessment, i.e. determining the risk level pertaining to a certain attack vector, is based on the factors **likelihood, severity** and **detection probability**. Each factor is assigned a numerical value[3], and the product of these values gives a risk priority number (RPN), as standardised in [8]. In recent years there have been some reservations against the use of the RPN [2,3]; it is, however, a familiar concept and widely used in the automotive industry. While there are differing risk curves, depending on the multiplication or addition of the contributing values, the FMEA standard IEC 60812 [21] proposes to use multiplication for obtaining the RPN. In addition, with regard to our focus on the security of the underlying lifecycle processes, [7] supports using multiplication for RPN when assessing process-related risk.

The risk assessment was conducted by a group of experts from the EVE consortium and discussed in multiple workshops. To provide a structured assessment, two additional elements were considered: A classification of the attack

[3] The range is from *low* (1) to *high* (10) for severity and likelihood, and vice versa for detection probability.

according to the Microsoft STRIDE model [22,24], and an assessment of the most probable adversaries. Here, attacker profile archetypes, as defined by [26], have been used to guide the assessment. These profiles include *Basic User* (low skill, low resources, no direct aim to attack the system), *Cybercriminal* (advanced ICT skill, low skills for physical attacks, advanced tools, average financial resources), *Insider* (advanced system knowledge, access to physical properties, dedicated tools, but low financial resources), *Nation State* (high offensive skills, resources and determination, advanced tools, focus on stealth), and *Terrorist* (low offensive skills, average resources, focus on physical availability).

Since an exact assessment could not always be achieved for the three determining factors, the resulting RPN often is a number *range* rather than a single value: This is also due to the fact that severity depends strongly on the distribution of autonomous or semi-autonomous vehicles that can react automatically to falsified ITS messages and thus cause greater damage. Similar scenarios are also conceivable for likelihood and detection probability. Depending on the distribution of ITS-enabled road users, the probability of an attack and its detection increases. The resulting risk priority score nevertheless provides a good basis to point out potentially critical process steps.

4 Exemplary Use Case

This section describes the procedure and outcomes of our risk analysis for one specific use case part of the lifecycle phase *operation*: An emergency vehicle approaches an intersection with ITS-enabled traffic lights and requests signal preemption (cf. the *Emergency Vehicle Approaching* use case from the SCOOP project [20]). This use case focuses on two infrastructure services, the **Road and Lane Topology (RLT)** and **Traffic Light Maneuver (TLM)** services [17], with two main components: (i) the on-board unit (OBU) of the emergency vehicle and (ii) the road-side unit (RSU) of the traffic light installation at the intersection.

4.1 Exemplary Process Analysis

The first step is a process analysis (see Sect. 3.2) including a visual representation of all required process steps (see Fig. 3). Each process step is then described in more detail (see Table 1) to facilitate the FMEA.

4.2 Exemplary FMEA

Since presenting the full FMEA table for this example would exceed the scope of this paper, the individual results are presented in a simplified list below. For each process step, possible attack vectors are listed including a first classification according to STRIDE, followed by effects and causes (in this order), see Sect. 3.3.

- **PS-001 Drive towards intersection**: Out of scope as we only considered cyber-security attacks.

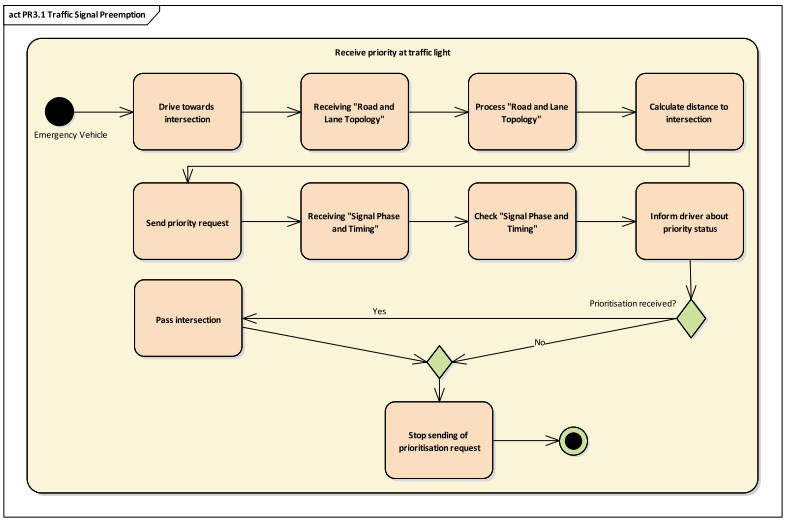

Fig. 3. UML activity diagram: traffic signal preemption for emergency vehicles.

Table 1. Process steps (PS) of the traffic signal preemption use case.

Process step	Description
PS-001 Drive towards intersection	Vehicle is approaching an intersection intending to cross it
PS-002 Receive “Road and Lane Topology”	OBU receives the road and lane topology transmitted by the RSU (Signal Phase And Timing Extended Message, SPATEM)
PS-003 Process “Road and Lane Topology”	OBU receives the topology information and checks it for correctness (authenticity)
PS-004 Calculate distance to intersection	OBU calculates distance to intersection using the topology information
PS-005 Send priority request	OBU sends priority request with Estimated Time of Arrival (ETA) to the RSU (Signal Request Extended Message, SREM)
PS-006 Receive “Signal Phase and Timing”	OBU receives “Signal Phase and Timing” of the RSU (Signal request Status Extended Message, SSEM)
PS-007 Check “Signal Phase and Timing”	OBU checks “Signal Phase and Timing” information for priority and authenticity status
PS-008 Inform driver about priority status	OBU informs driver via on-board display about status of prioritisation
PS-009 Pass intersection	Vehicle passes intersection
PS-010 Stop sending preemption request	OBU stops sending the preemption request once the intersection has been successfully crossed

- **PS-002 Receive "Road and Lane Topology"**:
  1. Denial of Service: OBU cannot receive topology information from RSU; Cause: attacker interferes with radio signal of the RSU
  2. Spoofing: OBU receives falsified topology information for the intersection and cannot calculate a correct prioritisation request; Cause: attacker sends out faulty or modified messages (for example after having compromised a RSU)
- **PS-003 Process "Road and Lane Topology"**:
  1. Denial of Service: either (i) RLT information is incorrect and cannot be distributed or (ii) the stability of the OBU could be affected; Cause: attacker has distributed (invalid) modified RLT
  2. Tampering: RLT model in OBU incorrect; Cause: attacker has distributed (valid) modified RLT
- **PS-004 Calculate distance to intersection**:
  - Tampering: Distance to intersection calculated incorrectly; Cause: attacker has distributed (valid) modified RLT
- **PS-005 Send priority request**:
  1. Denial of Service:
     (a) RSU cannot receive priority request; Cause: attacker interferes with radio signal of the OBU
     (b) RSU has incorrect arrival time, possible consequences for traffic; Cause: attacker modifies ETA on OBU side
  2. Elevation of Privilege: Vehicle is illegitimately prioritised; Cause: attacker pretends to be a vehicle on a rescue mission
- **PS-006 Receive "Signal Phase and Timing"**:
  1. Denial of Service: OBU cannot receive signal phase and timing (SPAT) information from RSU, vehicle cannot pass intersection; Cause: attacker interferes with radio signal (of the RSU)
  2. Spoofing: (i) Vehicle cannot pass intersection (ii) Vehicle attempts to pass intersection without prioritisation; Cause: attacker sends out faulty or modified SPAT information (must spoof signature)
- **PS-007 Check "Signal Phase and Timing"**:
  - Denial of Service: Could possibly affect the stability of the OBU; Cause: attacker has distributed modified RLT
- **PS-008 Inform driver about priority status**:
  - Tampering: Driver tries to pass an intersection assuming that he has been granted priority treatment; Cause: attacker modifies on-board display and shows incorrect prioritisation status (i.e., pretends that priority has been granted)
- **PS-009 Pass intersection**: Out of scope as we only considered cybersecurity attacks.
- **PS-010 Stop sending of prioritisation request**:
  - Denial of Service: RSU continues to give priority, traffic disruption; Cause: attacker continues to send preemption requests

4.3 Risk Assessment and Results

Based on these attack vectors the actual risk assessment was performed by determining likelihood, severity and detection probability for each individual attack scenario (see Fig. 4 as an example for process steps PS-002, PS-003 and PS-006). The attacker profile and security measures provided for by the relevant ETSI specifications were taken into account as these can affect the individual values: For example, the use of cryptographically signed messages reduces the likelihood of a successful attack. In many cases it was difficult to pin down the individual scores to one exact number due to the lack of real-world large-scale C-ITS implementations which could provide reliable data. Therefore, number ranges were used instead (cf. Fig. 4). Risk priority scores with a particularly wide range were additionally discussed in expert workshops within the EVE consortium in order to narrow the range.

Process Step	Attacks			Control & Mitigation	Attacker Profile	Likelihood	Severity	Detection Probability	RPN
	Classification	*Effects*	*Causes*						
PS-002 Receive Road and Lane Topology	Spoofing	OBU receives wrong topology information and fails to submit a valid preemption request	Attacker sends incorrect or modified messages (e.g., after having compromised a RSU)	Cryptographic protection of ITS messages (time stamps, signatures)	C	3-4	6-7	5-6	90-168
	Denial of Service	OBU cannot receive topology information from the RSU	Attacker jams radio signal from the RSU	n/a	T	5-6	4	3-4	36-96
PS-003 Process "Road and Lane Topology"	Denial of Service	RLT information is incorrect and cannot be distributed	Attacker has distributed (invalid) modified RLT	Cryptographic protection of ITS messages (time stamps, signatures)	C	3-4	4	3-4	36-64
		Could possibly affect the stability of the OBU			C	3-4	5-7	3-4	45-112
	Tampering	RLT model in OBU incorrect	Attacker has distributed (valid) modified RLT		C	2-4	8	3-4	54-144
PS-006 Receive Signal Phase and Timing	Denial of Service	OBU is unable to receive SPAT information from the RSU	Attacker jams RSU radio signal	n/a	T	5-6	3	7-8	104-144
	Spoofing	1. Vehicle cannot pass intersection 2. Vehicle tries to pass intersection without prioritization	Attacker sends out incorrect / modified SPAT information (must forge signature, therefore low probability of occurrence)	Cryptographic protection of ITS messages (time stamps, signatures)	C	2	4-6	5-6	40-72

Fig. 4. Analysis of process step PS-002 *Receive "Road and Lane Topology"*, PS-003 *Process "Road and Lane Topology"* and PS-006 Receive *"Signal Phase and Timing"*; Attacker Profile *C* refers to *Cybercriminal* and *T* to *Terrorist*, cf. Sect. 3.3.

The attack vectors with the highest risk priority scores of this exemplary use case apply to process steps **PS-002** (Receive "Road and Lane Topology"), **PS-003** (Process "Road and Lane Topology") and **PS-006** (Receive "Signal Phase and Timing"), see underlined values in Fig. 4: The risk posed by compromised road-side infrastructure is in general higher than the risk associated with compromised on-board units. While road infrastructure is more prone to tampering due to its easier accessibility, it is still managed by an infrastructure provider, and manipulations will probably be quickly detected. However, successful attacks may affect many other road users and therefore tend to be more severe than those targeted at on-board units of individual vehicles.

The relevant standards and guidelines suggest a number of countermeasures to minimise the risk from (cyber) threats. Additional countermeasures were defined as part of the process-based FMEA in EVE. Suggested countermeasures for the exemplary use case include system hardening of the ITS-S, i.e., removing all software components and functions that are not absolutely necessary for the ITS-S to perform its intended task. Secure software development techniques (e.g., input validation and sanitation) should be used to create the ITS-S software. Validating the achieved security level, for example through penetration tests and code reviews, can also help to ensure that the measures taken have been effectively implemented. Another countermeasure that applies specifically to the attack vector in process step PS-006 is anomaly detection for RSUs: Attacks to road-side infrastructure could be detected more efficiently by using systems that automatically report anomalies in the communication traffic between RSUs and OBUs. For example, an alarm could be triggered if no Common Awareness Messages (CAMs) from the OBUs of passing vehicles have been received by an RSU for several minutes at peak hours, possibly indicating a Denial of Service attack.

5 Conclusion and Outlook

Emergency vehicles can use the novel information and communication services provided by C-ITS to request right of way from infrastructure components or other connected road users, thus reducing the time loss when approaching an emergency. Cyber-attacks and acts of sabotage can, however, pose a significant risk to these scenarios, for example when attackers get hold of the credentials used for prioritisation. Our process-based FMEA shows that, while existing specifications and standards foresee a high level of security and reliability in general, they fall short of providing a full specification of security processes. Detailed procedures need to be defined for secure provisioning and decommissioning to ensure that unauthorised persons do not get hold of sensitive material. For Example, the Enrolment Authority must be informed in case an ITS-S has reached its end of life to prevent that it is used in an unauthorised way beyond the end of its lifecycle.

In addition, while there are standards, concrete guidance regarding security for infrastructure operators, automotive original equipment manufacturers (OEMs) and emergency fleet management organisations is still missing. One notable progress in this area is the recently published and approved Common Criteria Protection Profile for the C-ITS communication gateway in road work warning units [25]. This document provides not only guidance on the security measures the technical system should possess, it also includes Organisational Security Policies aimed at ensuring secure processes. While the Protection Profile for the C-ITS communication gateway in road work warning units has a rather restricted application area, it can provide the basis for a more general Protection Profile for C-ITS stations. Countermeasures that resulted from the process-based FMEA presented herein can be helpful when developing recommendations for such an extended Protection Profile.

References

1. C-ITS Platform Final Report, January 2016. https://ec.europa.eu/transport/sites/transport/files/themes/its/doc/c-its-platform-final-report-january-2016.pdf
2. Certa, A., Enea, M., Galante, G.M., La Fata, C.M.: An alternative to the risk priority number. ELECTRE TRI-based approach to the failure modes classification on the basis of risk parameters. Comput. Ind. Eng. **108**, 100–110 (2017)
3. Ciani, L., Guidi, G., Patrizi, G.: A critical comparison of alternative risk priority numbers in failure modes, effects, and criticality analysis. IEEE Access **7**, 92398–92409 (2019)
4. Commission, European: C-ITS Platform, Phase I. Final Report, Technical report (2016)
5. European Commission. COM 2016/766 A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility (2016)
6. Commission, European: C-ITS Platform, Phase II. Final Report, Technical report (2017)
7. Bundesministerium des Innern/Bundesverwaltungsamt. Handbuch für Organisationsuntersuchungen und Personalbedarfsermittlung, February 2018
8. DIN EN ISO 13485:2010–01, Medizinprodukte – Qualitätsmanagementsysteme – Anforderungen für regulatorische Zwecke (2016)
9. ETSI EN 302 665 Intelligent Transport Systems (ITS); Communications Architecture V1.1.1. European Standard (2010)
10. ETSI EN 302 637–3 Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications, Part 3: Specifications of Decentralized Environmental Notification Basic Service V1.2.1. European Standard (2014)
11. ETSI EN 302 637–2 Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications, Part 2: Specifications of Cooperative Awareness Basic Service V1.4.1. European Standard (2019)
12. ETSI TR 102 893 Intelligent Transport Systems (ITS); Threat, Vulnerability and Risk Analysis (TVRA) V1.2.1. Technical Report (2017)
13. ETSI TS 102 637–1 Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 1: Functional Requirements V1.1.1. Technical Specification (2010)
14. ETSI TS 103 097 Intelligent Transport Systems (ITS); Security; Security header and certificate formats V1.3.1. Technical Specification (2017)
15. ETSI TS 102 940 Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management V1.3.1. Technical Specification (2018)
16. ETSI TS 102 941 Intelligent Transport Systems (ITS); Security; Trust and Privacy Management V1.3.1. Technical Specification (2019)
17. ETSI TS 103 301 Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Facilities layer protocols and communication requirements for infrastructure services V1.3.1. Technical Specification (2020)
18. Directive 2010/40/EU of the European Parliament and of the Council of 7: on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport. Official J. Eur. Union L **207**(296–308), 2010 (2010)
19. European Commission. Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS)

20. Ministry for an Ecological, Transport Solidary Transition – Directorate General for Infrastructure, and the Sea (DGITM). C-ITS French Use Cases Catalog Functional descriptions. Technical Report
21. IEC 60812: Analysis techniques for system reliability: Procedure for failure mode and effects analysis (FMEA). International Standard (2006)
22. Kohnfelder, L., Garg, P.: The threats to our products. Microsoft Interface **33** (1999)
23. Lai, L.K.H., Chin, K.S.: Development of a failure mode and effects analysis based risk assessment tool for information security. Ind. Eng. Manag. Syst. **13**(1), 87–100 (2014)
24. Microsoft. The STRIDE Threat Model. https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)
25. Niehöfer, B., Wagner, M., Berndt, S.: Protection Profile for a Road Works Warning Gateway v1.1. Common Criteria Protection Profile (2019)
26. Rocchetto, M., Tippenhauer, N.O.: On attacker models and profiles for cyber-physical systems. In: Askoxylakis, I., Ioannidis, S., Katsikas, S., Meadows, C. (eds.) European Symposium on Research in Computer Security, vol. 9879, pp. 427–449. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-319-45741-3_22
27. Schmittner, C., Gruber, T., Puschner, P., Schoitsch, E.: Security application of failure mode and effect analysis (FMEA). In: Bondavalli, A., Di Giandomenico, F. (eds.) SAFECOMP 2014. LNCS, vol. 8666, pp. 310–325. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-10506-2_21
28. CAR 2 CAR Communication Consortium. https://www.car-2-car.org
29. Cooperative ITS Corridor. http://c-its-korridor.de/
30. ECo-AT. http://www.eco-at.info/
31. SCOOP@F Project. http://www.scoop.developpement-durable.gouv.fr/en/