IoT4CPS – Trustworthy IoT for CPS

FFG - ICT of the Future
Project No. 863129

Deliverable D4.1
Automotive Ethernet protection profile

The IoT4CPS Consortium:
AIT – Austrian Institute of Technology GmbH
AVL – AVL List GmbH
DUK – Donau-Universität Krems
IFAT – Infineon Technologies Austria AG
JKU – JK Universität Linz / Institute for Pervasive Computing
JR – Joanneum Research Forschungsgesellschaft mbH
NOKIA – Nokia Solutions and Networks Österreich GmbH
NXP – NXP Semiconductors Austria GmbH
SBA – SBA Research GmbH
SRFG – Salzburg Research Forschungsgesellschaft
SCCH – Software Competence Center Hagenberg GmbH
SAGÖ – Siemens AG Österreich
TTTech – TTTech Computertechnik AG
IAIK – TU Graz / Institute for Applied Information Processing and Communications
ITI – TU Graz / Institute for Technical Informatics
TUW – TU Wien / Institute of Computer Engineering
XNET – X-Net Services GmbH

For more information on this document or the IoT4CPS project, please contact:
Mario Drobics, AIT Austrian Institute of Technology, mario.drobics@ait.ac.at

Document Control

Title: Automotive Ethernet protection profile
Type: public
Editor(s): Edin Arnautovic
E-mail: edin.arnautovic@tttech.com
Author(s): Wilfried Steiner, Edin Arnautovic, Christoph Schmittner
Doc ID: D4.1

Amendment History

Version	Date	Author	Description/Comments
V0.1	24.1.2019	Edin Arnautovic	Initial version prepared
V0.2	01.02.2019	Wilfried Steiner	Core content
V.05	22.2.2019	Stefan Jaksic	Review inputs
V0.8	27.2.2019	Christoph Schmittner	Review and contributions
V1.0	28.2.2019	Edin Arnautovic	Final version integration
V1.1	1.3.2019	Edin Arnautovic	Minor updates
V1.2	5.3.2019	Mario Drobics	Formating

The IoT4CPS project is partially funded by the "ICT of the Future" Program of the FFG and the BMVIT.

Content

Abbreviations

ASIL	Automotive Safety Integrity Level
CC	Common Criteria
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation

Executive Summary

This deliverable analyses security aspects of future, Ethernet-based automotive networks with the focus on Time Sensitive Networking (TSN) and an associated CAN-Ethernet gateway which is used to bridge legacy CAN networks and Ethernet. It develops a first version of a Protection Profile according the Common Criteria. The deliverable introduces the general automotive Ethernet technology as well as TSN and its security characteristics. It then den follows with the definition of the protection profile on the example of the CAN-Ethernet gateway. The protection profile covers threats, security objectives, and formal security functional requirements for automotive Ethernet. Furthermore, the protection profile maintains traceability between threats, objectives and requirements.

1. Introduction

The importance of security and in particular its interdependencies with safety has been impressively demonstrated in July 2015 by a remote attack on a Jeep. By exploiting a vulnerability in the head unit, the attackers have been able to get control not only over non-critical functions, but also over critical automotive control functions [1]. With the growing connectivity of the car as well as with the increasing use of information technology (IT) it becomes clear that security becomes more and more the focus of automotive developments.
Ideally, OEMs and suppliers engage in joint security discussions and, indeed, they do. Recently a standard for cybersecurity in cyber-physical vehicle systems (SAE J3061) has been published. However, while SAE J3061 focuses on integration of cybersecurity in automotive processes, it falls short in addressing and enumerating threats and their mitigation strategies. We argue that an open discussion of these threats and mitigation strategies would greatly reduce the overall automotive security risk and that the Common Criteria (CC) should be used as a tool to structure such a discussion. The CC have various benefits: they provide a generic framework that can be tailored towards automotive use, they have been applied to numerous projects in various industries, including safety-critical applications, and, finally, they provide a thorough catalogue of security functions and security assurance methods that target completeness and correctness of a security solution with scalable assurance levels. Indeed, the CC have been argued for applicability to automotive systems before and even set in context to ASIL [2]. We include in this deliverable an evaluation of ISO 26262 and CC.
In this deliverable we develop an experimental protection profile for Deterministic Ethernet which is intended, among others, for automotive use [3]. Ethernet is attractive for automotive use for two main reasons: first with IEEE 802.3 100BASE-T1 and 1000BASE-T1 cost-effective automotive physical layers are now available and, secondly, IEEE 802.1 AVB (Audio/Video Bridging) and IEEE 802.1 TSN (Time-Sensitive Networking) have improved Ethernet's real-time and robustness properties. We have selected Ethernet, because it is currently gaining more and more significance as the next in-vehicle automotive network bus and there is a pressing need for security solutions. In this deliverable we will, thus, outline the path towards a protection profile (PP) according to the CC for Automotive Ethernet.

1.1 Common Criteria for Automotive Use

It is the aim of this document to serve as a draft Protection Profile to get an understanding if the Common Criteria are suitable for application to automotive in-vehicle networks and, potentially, to automotive information technology in general.
On the differentiation between PP and ST, the CC state as follows:

- Whereas an ST always describe a specific TOE (e.g., a MinuteGap v18.5 Firewall), a PP is intended to describe a TOE type (e.g., firewalls). The same PP may therefore be used as a template for many different STs to be used in different evaluations.

The common criteria allow for the following workflow [CC1]:

- An organization seeking to acquire a particular type of IT security product develops their security needs into a PP (protection profile), then has this evaluated and publishes it.
- A developer takes this PP, writes an ST (security target), that claims conformance to the PP and has this ST evaluated.
- The developer then builds a TOE (target of evaluation) (or uses an existing one) and has this evaluated against the ST.

The CC consists of three parts:

- Part1, Introduction and general model, is the introduction to the CC. It defines the general concepts and principles of IT security evaluation and presents a general model of evaluation.

- Part 2, Security functional components, establishes a set of functional components that serve as standard templates upon which to base functional requirements for TOEs. CC Part 2 catalogues the set of functional components and organizes them in families and classes.
- Part 3, Security assurance components, establishes a set of assurance components that serve as standard templates upon which to base assurance requirements for TOEs. CC Part 3 catalogues the set of assurance components and organizes them into families and classes. CC Part 3 also defines evaluation criteria for PPs and STs and presents seven pre-defined assurance packages which are called the *Evaluation Assurance Levels (EALs)*.

The ST demonstrates that:

- The SFRs meet the security objectives for the TOE;
- The security objectives for the TOE and the security objectives for the operational environment counter the threats;
- And, therefore, the SFRs and the security objectives for the operational environment counter the threats.

1.2 Common Criteria and automotive cybersecurity engineering

They automotive industry is aware that security is a new challenge and is in the process of addressing these issues. Superseding the already mentioned SAE J3061 the automotive domain is developing a novel cybersecurity engineering standard ISO/SAE 21434 “road vehicles – cybersecurity engineering”. Like the SAE J3061 this standard focus on the development of secure automotive systems, not their evaluation or assurance of achieved security. Compared to ISO 26262 which offers a detailed list of test methods and concepts, based on the ASIL, these standards focus more on the engineering and management process. Based on the current status of the standards in development, there is still a need to consider how to assure and evaluate the engineered security which can be covered by Common Criteria.
In (Schmittner & Zhendong, 2014) we compared the Common Criteria EAL with the ASIL level from ISO 26262 based on the required methods and formalism. Based on this we identified the following rough overlap:

Table 1: Comparison of safety integrity level and evaluation assurance levels

ASIL	A	B	C	D
EAL	3	4	5	6

In addition to that we also compared work products from ISO 26262 and Common Criteria. Here the focus was not on the coverage of requirements, but on the coverage of similar topics and objectives to determine how a combined description could look like. This table does not yet contain a complete study of ISO/SAE 21434. We identified overlaps between the ISO 26262 and the ISO/SAE 21434 item, but due to the draft status of ISO/SAE 21434 we did not yet conduct a complete survey.

ISO 14508	**ISO 26262**	**ISO/SAE 21434**
A.4.1 ST reference and TOE reference	Part3-5: Item definition	Item definition
A.4.2 TOE overview Part3-5: Item definition		
A.4.3 TOE description		
A.5 conformance claims	-	
A.6.2 Threats	Part3-7.5.1: Hazard analysis and risk assessment	
A.6.3 Organizational security policies	Part2-5: Overall safety management,	
	Part2-5.5.1: Organization specific rules and processes for functional safety	
	Part2-7: Safety management after release for production,	
	Part2-7.5: Evidence of a field monitoring process	

A.6.4 Assumptions	Only for Safety element out of Context	
A7.2.1 Security objectives for the TOE	Part3.7.5.2: Safety Goals	
A7.2.2 Security objectives for the operational environment	-	
A7.3. Relation between security objectives and the security problem definition	-	
A.8 Extended components definition	Part3-7.5.3: Verification review of hazard analysis and risk assessment and safety goals	
A.9.1 Security functional requirements	Part3-8.5.1: Functional safety concept	
A.9.2 Security assurance requirements	Part2-6: Safety management during development of the item,	
	Part2-6.5.5: Conformation plan	
	Part6-11: Verification of software safety requirements	
	Part6-11.5.1: Software verification plan	
A.9.3 Security requirements rationale	-	
A.10 TOE summary specification	Part2-6.5.3: Safety Case	

Based on a rough survey we believe that with the application of ISO 26262 and ISO/SAE 21434 many of the documentation requirements of the Common Criteria are resolved and the additional documentation effort can be greatly reduced. Due to the fact that there is no guidance on assurance methods in ISO/SAE 21434, there will still be some additional work in applying the common criteria.

2. Protection Profile Introduction

Protection profile contains the overview of the Target of Evaluation (TOE), security problem definition, security objectives and requirements.

2.1 TOE Overview

2.1.1 General Introduction

Computer networks shape our modern lives. On the one hand the Internet, home, and office networking are omnipresent and help us in our daily work as well as entertainment. On the other hand, computer networks ensure the correct operation of complex machineries such as automobiles, airplanes, or industrial automation systems. As of today, different technologies are used to realize these two types of computer networks as they need to fulfill different sets of requirements. While the first type primarily targets high communication speed and efficient network utilization, the second category focuses on guaranteed data delivery often intertwined with real-time demands. Automotive in-vehicle networks belong to this second category of computer networks. An example network of interest, an automotive network, is depicted in Figure 1. Here, sensors and actuators connect to three switches, where Switch 3 also acts a gateway between the Ethernet (represented with a double line) and the CAN network (represented with a single line). For simplicity we assume that switches 1 and 2 also incorporate processing elements like CPUs or GPUs. In real automotive networks switches, end points, sensors and actuators will be partially integrated in single ECUs. Thus, the network below should be regarded as a simplified example only.

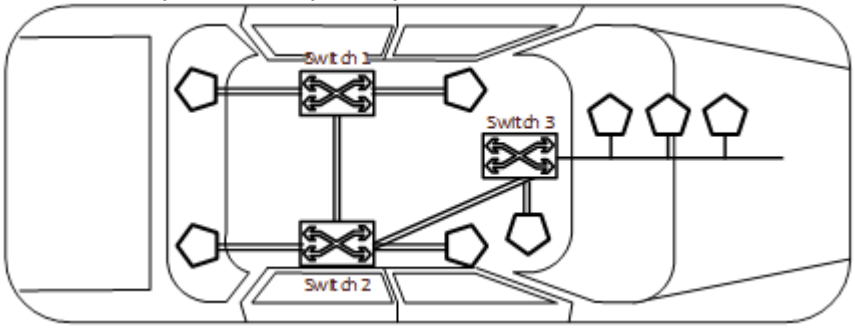

Figure 1: Example automotive in-vehicle network

One way for a network to achieve guaranteed data delivery while preserving real-time communication is to implement the time-triggered paradigm [1]. Here, the devices, i.e., switches and end points (that incorporate the sensors and actuators) synchronize their local clocks to establish a system-wide synchronized time. The communication in the network then follows a communication schedule that is defined at system design time and is locally pre-configured in the devices.
Current trend for automotive networks goes towards Time Sensitive Networking (TSN). TSN is a collective name for a set of standards and projects, published or under development by the TSN task group of the IEEE 802.1 Working Group. The TSN standards define mechanisms to provide deterministic services through IEEE 802 networks, such as, guaranteed packet transport with bounded latency, low packet delay variation, and low packet loss. IEEE 802.1Qbv defines schedule-driven, time-triggered (TT) communication, i.e., to leverage synchronized time in transmission and forwarding decisions for messages in the network. The core principle of TT communication is rather simple: the system designer generates a communication schedule that instructs the end stations when to send frames to the network. This communication schedule (or parts of it) is distributed to the end stations and bridges as part of their configuration, and a scheduling function at the end station (and potentially also in bridges) executes the communication schedule. As a key concept unique to IEEE 802.1, Qbv does not directly schedule frame transmissions, but schedules the activation and deactivation of queues. Said queues are both the traffic class queues in bridges as introduced earlier as well as the transmit queues in end stations.

2.1.2 Definition of the TOE

The TOE consists of Ethernet switches and CAN gateways and the wire harness that connects the switches to each other as well as the wire harness connecting the user to the TOE.
Ethernet switches (including CAN gateways) receive messages from the operational environment and either consume these messages (for example to update their internal configuration) or forward them to other switches or end stations that are attached to switches.
As an example we take the deterministic Ethernet (DE) switch that is designed for application development and evaluation of Deterministic Ethernet for in-vehicle network architectures considering multiple communication standards, including, Audio-Video Bridging (AVB), Time-Sensitive Networking (TSN), and Time-Triggered Ethernet in combination with a BroadR-Reach® physical layer.

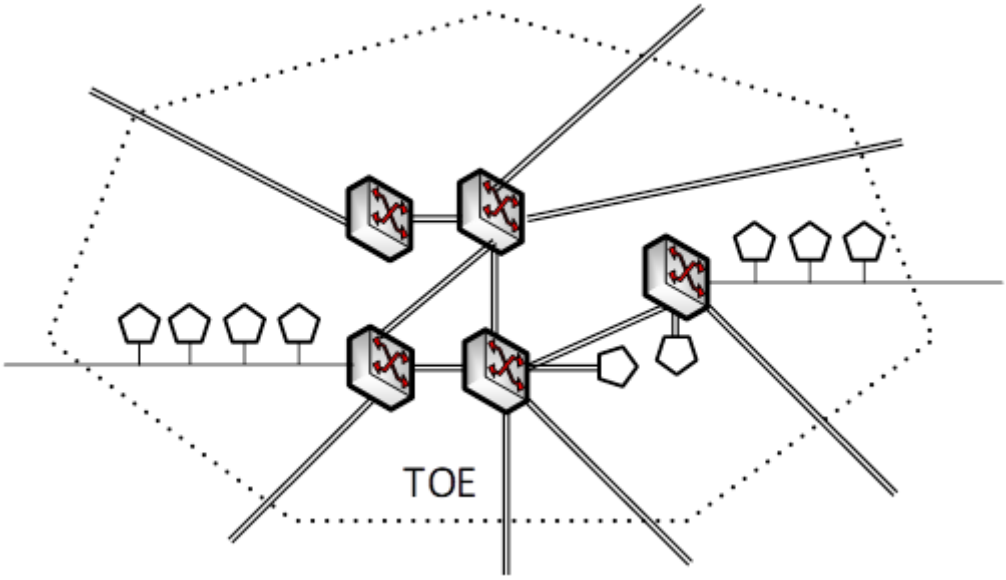

Figure 2: TOE

The DE-Switch contains also standard interfaces, such as CAN and FlexRay™, and such can serve as a gateway between the networks using these interfaces an Ethernet. Figure 3 shows the architecture of this switch. The Switch also contains the Management CPU (AURIX) which covers all the control and monitoring features of the system. The CPU also loads and stores the configuration for the

Ethernet Switch. The device is responsible for the correct setting of the peripherals, which includes the configuration of the switch and the physical layer and the control of the digital and analog I/Os and communication interfaces.
Ethernet switches can also generate and send messages to each other or to the operational environment. They are able to distinguish messages from each other by class identifiers and/or stream identifiers. In particular, some messages are considered critical by the TOE and perceive preferred treatment in terms of transmission latency. In this PP we call these critical messages the real-time messages and all these real-time messages have stream identifiers that are known to the TOE. Messages that are not real-time messages are called best-effort messages. Best-effort messages also have stream identifiers, but these stream identifiers are not necessarily known to the TOE. The TOE will classify those Ethernet messages that do not have a listed stream identifier for real-time messages, as best-effort messages.

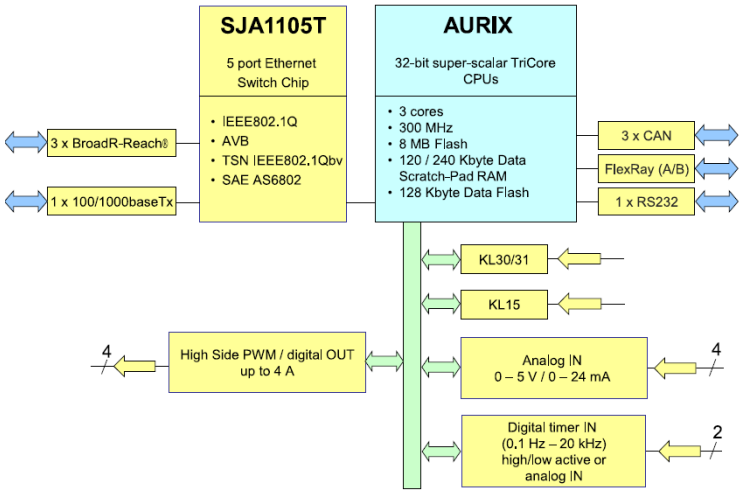

Figure 3: Deterministic Ethernet Switch

Switches forward Ethernet messages only based on their stream identifier. All paths of all Ethernet messages are static and can only be changed by an explicit change in the configuration of a switch.
Ethernet switches implement physical ports at which they receive messages. A switch can use this port information (i.e., the identifier of the physical port a message is received on) for its forwarding decisions. In particular, a switch can accept a message with a certain stream identifier at a certain port. However, it may be configured to discard the same message when it receives it on another port.
Users are components that connect to the TOE through Ethernet wires. Each user may use one or many stream identifiers for their Ethernet messages that they communicate to the TOE. The stream identifiers, thus, serve as security attributes for the SFRs. The users are subjects that use the services of the TOE.
This PP is primarily concerned with the following TOE objects:

- Buffers in the switches used to store Ethernet messages
- Communication bandwidth on the Ethernet wires in between the switches of the TOE
- Time slots for the communication of time-triggered messages
- Switch configuration data

The payload of Ethernet frames is considered as User Data. The Ethernet header is considered as TSF Data.
Each switch in the TOE holds configuration data that control how each switch is executing its services. This configuration data can be changed by users providing new configuration data to the switch through best-effort Ethernet messages.

Note that CAN is a broadcast protocol, so every node “receives” the message, but only receivers (as we have defined them) should accept the message.

2.1.3 Definition of the Operational Environment

The TOE is completely located inside a car and the car may be used anywhere in the world.
There are three roles of users:

- Regular users, are users of the TOE during regular operation of the vehicle. Regular users may be for example, cameras, pedals, body electronics, sensors, actuators, etc. The functionality of regular users will typically be implemented in ECUs (Electronic Control Units).
- Maintenance users, are of administrative nature. They connect directly to the TOE by means of an Ethernet wire. For example, a maintenance user may connect to the TOE by means of an on-board diagnosis (OBD) connection.
- Remote users, are all users that do not directly connect to the TOE, but connect through a wireless connection.

In this PP we consider that configuration of the TOE is only allowed by a maintenance user, i.e., from a well-defined port that requires physical presence at the car.
When configuration of the TOE would have to be done by a remote user, a separate PP for a wireless-wired gateway (and potential firewall) could be developed, such that this wireless-wired gateway could serve as a maintenance user in accordance with this PP.

3. Security Problem Definition

In this section we aim to provide a definition of a Security Problem, in the context of Protection Profile.

3.1 Threats

There are several classes of security threats that we tackle:
T_INSERT_DELAY: The threat agent sources messages into the Ethernet network thereby delaying real-time messages for more than the length of one maximum sized Ethernet frame.
T_MASQUERADING: The threat agent inserts real-time messages into the Ethernet network that masquerade other real-time messages.
T_INTERCEPTION: The threat agent modifies the TOE such that it receives real-time messages from the TOE that it shall not receive.
T_DEGRADE_SYNCHRONIZATION: The threat agent sends messages on the TOE user interface that cause the network-wide synchronized time for more than x% of the precision in the system.
T_CHANGE_CONFIG: The threat agent modifies the Ethernet switch configuration.
T_SWITCH_FAILURE: A switch becomes faulty.
T_LINK_FAILURE: A link in the TOE becomes unavailable.
UNAUTHORIZED_ALTERATION_OF SWITCH_MANAGEMENT_SOFTWARE: The threat agent modifies the management software of TOE
T_REPLAY_ATTACK: The threat agent records protocol packets and replays them at a later time without any modification.
T_CAN_FRAME_FABRICATION: The threat agent generates additional data (e.g, a sender node creates a new frame with an ID that the node is not authorized to transmit).
T_CAN_FLOODING: The threat agent floods the CAN bus with spoofed messages.

3.2 Organizational Security Policies

ORG_PRIVILEDGED_PORT: A user of the TOE shall not be directly connected to a privileged port of a switch of the TOE that accepts re-configuration attempts.
Guidance: The operational procedure for re-configuration of the TOE requires a trusted engineer to physically connect to the TOE by means of a wired Ethernet connection. Note that this restriction on

connectivity to privileged ports is only for edge switches. Switches that are not directly connected to a user may not be required to configure ports in privileged mode.
ORG_STRICTLY_INTERNAL_SYNC: The TOE shall be configured such that synchronized time inside the TOE does not use information provided on the user interface.
ORG_PORT_BASE_ACCESS_ONLY: A user may interact with the TOE only by means of the Ethernet links connected to edge switches.

4. Security Objectives (Countermeasures)

Security objectives consist of security objectives for the TOE and Operational Environment, as well as objectives rationale and extended component definition.

4.1 Security objectives for the TOE

O_MSG_WHITELISTING: The TOE shall ensure that only whitelisted real-time messages are communicated in the Ethernet network.
Threats: T_INSERT_DELAY, T_MASQUERADING, T_DEGRADE_SYNCHRONIZATION
SFRs: FIA_AFL.1.1, FIA_AFL.1.2, FIA_UID.1.1, FIA_UAU.1.1, FIA_UAU.5.2, FIA_UAU.6.1, FIA_UAU.7.1
O_MSG_RATE_CONTROL: The TOE shall ensure that the whitelisted real-time messages do not exceed a configured maximum rate.
Threats: T_INSERT_DELAY
SFRs: FRU_RSA.1.1, FRU_RSA.2.2
O_MSG_BOUND_URT_TRAFFIC: The TOE must be configured such that the overall amount of unsynchronized real-time traffic is sufficiently bounded and the individual end-to-end latency requirements of the unsynchronized real-time traffic are met.
Threats: T_INSERT_DELAY
SFRs: FRU_RSA.1.1, FRU_RSA.2.2
O_BOUND_BEST_EFFORT_INTERFERENCE: The TOE shall ensure that real-time messages can only be delayed by non-real-time messages for one maximum sized Ethernet frame.
Threats: T_INSERT_DELAY
SFRs: FRU_PRS.1.1, FRU_PRS.1.2
O_STATIC_CONFIGURED_IO: The TOE shall statically configure the communication paths of all real-time messages.
Threats: T_INTERCEPTION
SFRs: FRU_RSA.1.1
O_BLOCK_SYNC_MSGS: The TOE shall not accept synchronization messages from any user.
Threats: T_DEGRADE_SYNCHRONIZATION
SFRs: FIA_UAU.5.2
O_PRIVILEDGED_PORT_PROTECTION: The TOE will only accept re-configuration attempts on privileged ports.
Threats: T_INTERCEPTION, T_CHANGE_CONFIG
SFRs: FIA_UAU.5.2
O_REDUNDANT_CONNECTIVITY: The TOE will provide redundant communication paths between users for critical real-time messages.
Threats: T_SWITCH_FAILURE, T_LINK_FAILURE
SFRs: FRU_FLT.1.1

4.2 Security Objectives Rationale

Discussion if all the security objectives are achieved then the security problem is solved.

5. Security Functional Requirements

5.1 Class FIA: identification and Authentication

5.1.1 Authentication failures (FIA_AFL)

FIA_AFL.1 Authentication failure handling
Hierarchical to: No other components.
Dependencies: FIA_UAU.1 Timing of authentication
FIA_AFL.1.1 The TSF shall detect when [selection: *[assignment: positive integer number], an administrator configurable positive integer within[assignment: range of acceptable values]*] unsuccessful authentication attempts occur related to [assignment: *list of authentication events*].
FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [selection: *met, surpassed*], the TSF shall [assignment: *list of actions*].
FIA_AFL.1.1 The TSF shall detect when [*an administrator configurable positive integer within [assignment: range of acceptable values]*] unsuccessful authentication attempts occur related to [*assignment: list of authentication events*].
FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *met*, the TSF shall

- *stop to accept real-time messages from the physical port to which the user attaches that caused the unsuccessful authentication attempts,*
- *record an error message.*

5.1.2 User identification (FIA_UID)

FIA_UID.1 Timing of identification
Hierarchical to: No other components.
Dependencies: No dependencies.
FIA_UID.1.1 The TSF shall allow [assignment: *list of TSF-mediated actions*] on behalf of the user to be performed before the user is identified.
FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
FIA_UID.1.1 The TSF shall allow

- *the acceptance of best-effort traffic*

on behalf of the user to be performed before the user is identified.
Guidance: a user of the TOE may send arbitrary best-effort traffic to the TOE. The TOE is free to actually forward or to discard best-effort traffic for communication based on the current buffer saturation of the switch.

5.1.3 User authentication (FIA_UAU)

FIA_UAU.1 Timing of authentication
Hierarchical to: No other components.
Dependencies: FIA_UID.1 Timing of identification
FIA_UAU.1.1 The TSF shall allow [assignment: *list of TSF mediated actions*] on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
FIA_UAU.1.1 The TSF shall allow

- *the acceptance of best-effort traffic*

on behalf of the user to be performed before the user is authenticated.
Guidance: a user of the TOE may send arbitrary best-effort traffic to the TOE. The TOE is free to actually forward or to discard best-effort traffic for communication based on the current buffer saturation of the switch.

FIA_UAU.5 Multiple authentication mechanisms
Hierarchical to: No other components.
Dependencies: No dependencies.
FIA_UAU.5.1 The TSF shall provide [assignment: *list of multiple authentication mechanisms*] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [assignment: *rules describing how the multiple authentication mechanisms provide authentication*].
FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to

- *for real-time messages the Ethernet MAC destination address has a specific value which is stored in the switch configuration,*
- *for real-time messages the VLAN ID has a specific value out of a set of permitted values as stored in the switch configuration*
- *for real-time messages the Priority Code Point in the VLAN tag has a specific value out of a set of permitted values as stored in the switch configuration*
- *for real-time messages the physical port at which the switch receives the message complies with the physical port that the switch expects the message to be received,*
- *no synchronization message shall be authenticated,*
- *re-configuration messages are only accepted at privileged ports.*

FIA_UAU.6 Re-authenticating
Hierarchical to: No other components.
Dependencies: No dependencies.
FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions [assignment: *list of conditions under which re-authentication is required*].
FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions

- *that a new real-time message is received.*

FIA_UAU.7 Protected authentication feedback
Hierarchical to: No other components.
Dependencies: FIA_UAU.1 Timing of authentication
FIA_UAU.7.1 The TSF shall provide only [assignment: *list of feedback*] to the user while the authentication is in progress.
FIA_UAU.7.1 The TSF shall provide only

- *the feedback that messages are being accepted*

to the user while the authentication is in progress.
Guidance: No error messages shall be fed back to the user. This also excludes the behavior that the TOE terminates the communication on physical layer, e.g., in the case of unsuccessful authentication requests exceeding a certain threshold.

5.2 Class FRU: Resource utilization

5.2.1 Priority of service (FRU_PRS)

FRU_PRS.1 Limited priority of service
Hierarchical to: No other components.
Dependencies: No dependencies.
FRU_PRS.1.1 The TSF shall assign a priority to each subject in the TSF.
FRU_PRS.1.2 The TSF shall ensure that each access to [assignment: *controlled resources*] shall be mediated on the basis of the subjects assigned priority.
FRU_PRS.1.1 The TSF shall assign a priority to each subject in the TSF.
Guidance: each stream of messages is considered to be a subject.
FRU_PRS.1.2 The TSF shall ensure that each access to

- *the TOE switch memory*
- *the communication bandwidth between any two switches in the TOE and between switches and users in the TOE*

shall be mediated on the basis of the subjects assigned priority.
Guidance: real-time messages will always have higher priority than best-effort messages.

5.2.2 Resource allocation (FRU_RSA)

FRU_RSA.1 Maximum quotas

Hierarchical to: No other components.
Dependencies: No dependencies.
FRU_RSA.1.1 The TSF shall enforce maximum quotas of the following resources:
[assignment: *controlled resources*] that [selection: *individual user, defined group of users, subjects*] can use [selection: *simultaneously, over a specified period of time*].
FRU_RSA.1.1 The TSF shall enforce maximum quotas of the following resources:

- *the TOE switch memory*
- *the communication bandwidth between any two switches in the TOE and between switches and users in the TOE*
- *time slots in time-triggered communication*

that *real-time messages* can use *over a specified period of time*.

FRU_RSA.2 Minimum and maximum quotas
Hierarchical to: FRU_RSA.1 Maximum quotas
Dependencies: No dependencies.
FRU_RSA.2.1 The TSF shall enforce maximum quotas of the following resources [assignment: *controlled resources*] that [selection: *individual user, defined group of users, subjects*] can use [selection: *simultaneously, over a specified period of time*].
FRU_RSA.2.2 The TSF shall ensure the provision of minimum quantity of each [assignment: *controlled resource*] that is available for [selection: *an individual user, defined group of users, subjects*] to use [selection: *simultaneously, over a specified period of time*].
FRU_RSA.2.2 The TSF shall ensure the provision of minimum quantity of each

- *the TOE switch memory*
- *the communication bandwidth between any two switches in the TOE and between switches and users in the TOE*
- *time slots in time-triggered communication*

that is available for *real-time messages* to use *over a specified period of time*.

FRU_FLT.1 Degraded fault tolerance
Hierarchical to: No other components.
Dependencies: FPT_FLS.1 Failure with preservation of secure state
FRU_FLT.1.1 The TSF shall ensure the operation of [assignment: *list of TOE capabilities*] when the following failures occur: [assignment: *list of type of failures*].

FRU_FLT.1.1 The TSF shall ensure the operation of the TOE delivering critical real-time messages in time when the following failures occur:

- *one switch of the TOE fails*
- *one link in the TOE fails.*

6. Security Assurance Requirements

A vendor implementing this protection profile will decide the appropriate EAL case by case. The EAL will typically follow from the safety criticality of the applications using the TOE as well as the economic impact of low availability of the TOE.

7. Security Requirements Rationale

Discussion that if all SFRs are satisfied then all security objectives for the TOE are achieved.

8. Summary and conclusion

In this deliverable we defined a first version of a protection profile for automotive networks based on Ethernet including gateways to CAN bus. This protection profile defines threats, security objectives, as well as formal Security Functional Requirements (SFRs) for such networks. Furthermore, we established traceability between the threats, objectives and requirements.

9. Bibliography

[1] Greenberg, Andy. "Hackers remotely kill a jeep on the highway—with me in it." Wired, 21 July (2015).
[2] Robinson-Mallett, C.; Kaiser, B.; Grossmann, J.: Berührungspunkte und übergreifende Risiken des Security- und Safety Engineering durch die Vernetzung elektronischer Automobilsysteme mit Internet-Konnektivität. VDI/VW-Gemeinschaftstagung für Automotive Security, Kassel, 2013
[3] Matheus, Kirsten, and Thomas Königseder. Automotive Ethernet. Cambridge University Press, 2014.
[4] Common Criteria – Part 1
[5] Common Criteria – Part 2