SPARTA

D5.4 Appendix F

Protection Profile for a Safety and Security Platooning Management Module including a firewall

Project number	830892
Project acronym	SPARTA
Project title	Strategic programs for advanced research and technology in Europe
Start date of the project	1st February, 2019
Duration	36 months
Programme	H2020-SU-ICT-2018-2020

Deliverable type	Report
Deliverable reference number	SU-ICT-03-830892 **/** D5.4 **/** V1.0 **/** Appendix F
Work package contributing to the deliverable	WP5
Due date	Jan 2022 – M36
Actual submission date	2nd February, 2022

Responsible organisation	CETIC
Editor	Sebastien Dupont
Dissemination level	PU
Revision	V1.0

Abstract	Proposal of Protection Profile for Secure Communications in Automotive scenario, where the platooning module is protected by a firewall.
Keywords	Protection Profile, Firewall, Automotive, Certification

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 830892.

Editor

Sébastien Dupont (CETIC)

Contributors (ordered according to beneficiary numbers)

Guillaume Ginis, Philippe Massonet (CETIC)

Mirko Malacario, Claudio Porretti (LEO)

Reviewers (ordered according to beneficiary numbers)

Maximilian Tschirschnitz (TUM)

Rimantas Zylius (L3CE)

Disclaimer

Executive Summary

This Protection Profile is based on the “Protection Profile for a Safety and Security Platooning Management Module” [4]. It extends the PP in order to include a firewall in the Target Of Evaluation (TOE).

Firewall has been introduced in the TOE in order to protect the communication with the Platooning Module (SafeSecPMM) running in the vehicles.

The PP “Profil de protection - Firewall à Exigences Elevées” [5] has been taken as reference for this document security objectives and requirements for firewalls.

The objective of this document is to have a reference for performing an Impact Analysis against the changes occuring to the hypothetical TOE already certified in conformance with this PP.

Table of Content

List of Figures

List of Tables

Chapter 1 Introduction

This document defines a base Protection Profile (PP) for a Safety and Security Platooning Management Module (**SafSecPMM**). This module addresses cyber-attacks on a formed platoon that exploit the communication and sensing interfaces of a vehicle by, in particular, sending incorrect information about the state of the world, e.g., wrong speed, position of vehicles in the platoon. Such attacks can lead honest vehicles to potentially make wrong decisions that may affect the safety of passengers, e.g., accelerate when it should not, thus placing the platoon in an unsafe state. See [4] for the general context. The vehicles involved in a platoon need many communications amongst them and with the outside world.

With this in mind has been introduced the usage of a firewall in order to protect the SafeSecPMM module from threats conveyed through the communications.

1.1 PP reference

Protection Profile for a Safety and Security Platooning Management Module, version 1.0, SPARTA project, Vivek Nigam, Estibaliz Amparan; Angel López, and Cristina Martínez, January 31, 2021. [4]

Profil de protection - Firewall à Exigences Elevées - V2.2, Groupe de travail DGA, September, 1998. [5]

1.2 TOE Overview

The TOE is composed of a set of software modules: the firewall and the platooning management module (SafeSecPMM).

The TOE module, firewall of the Safety and Security Platooning Management Module (FW), is used to ensure the secure communication of vehicle platoons.

The TOE is intended to be used in vehicles.

The TOE has an interface towards the Vehicle Communication System (VCS), the Hardware Security Modules (HSM), and the Vehicle Control Module (VCM). Figure 3 illustrates the interfaces of the TOE with the VCS, HMS and VCM.

Only the communication with the VCS and the HSM are protected by the firewall modules as the interfaces with the VCM are not network based.

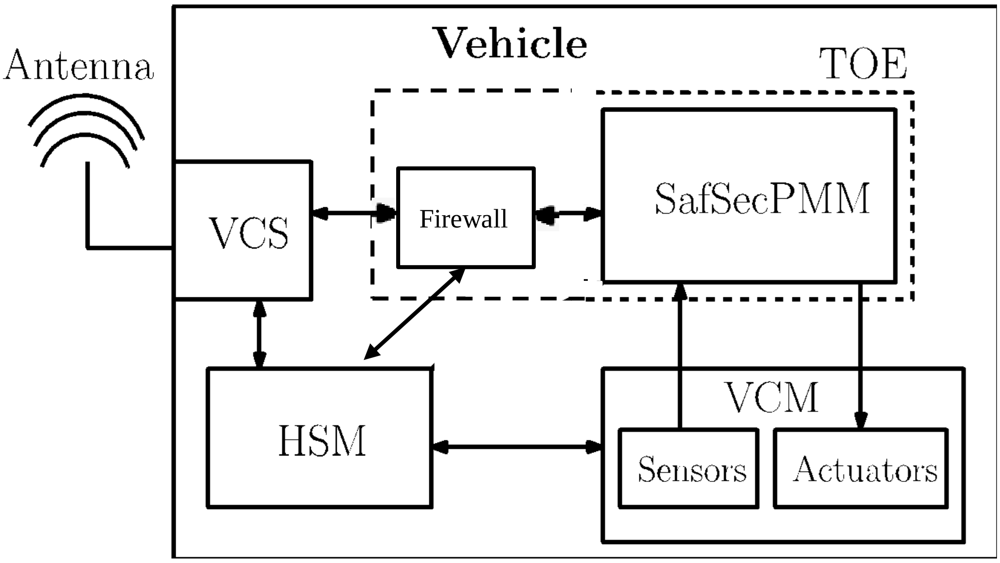

Figure 1: TOE Interfaces.

The TOE boundary is a tamper resistant hardware module including the software required for its functionality, that is, we are assuming that hardware attacks are not possible. However, logical attacks that exploit the software vulnerabilities are considered.

The SafSecPMM receives data from the VCS through the firewall (TOE), using HSM to decrypt any encrypted messages, or to check their integrity. The SafSecPMM also uses sensing data available in the VCM, such as information about the distance to any object, speed and localization. The sensor information from the VCM may be signed by HSM to guarantee communication integrity.

Moreover, based on the data collected, the SafSecPMM communicates necessary data to other vehicles and stationary deployments through the firewall and the VCS. Communication may be signed/encrypted using HSM. The TOE's SafSecPMM also sends commands to the VCM actuators, to guarantee the safe and secure operation of the vehicle and the platoon, such as commands setting the speed and the direction vector.

Chapter 2 Conformance Claims

2.1 CC conformance claim

The Protection Profile is conformant to Common Criteria:

- Part 1: Introduction and general model [1]
- Part 2: Security Functional Components [2]
- Part 3: Security Assurance Components [3]

2.2 PP conformance claim

The Protection Profile does not claim compliance to any Protection Profile.

However this document extend the content of Protection Profile for a Safety and Security Platooning Management Module [4].

2.3 Conformance rationale

As the PP does not claim conformance to any other Protection Profile, a conformance rationale is not required.

2.4 Conformance statements

The Protection Profile requires strict conformance by any ST or PP claiming conformance to it.

Chapter 3 Security Problem definition

The security problem definition is related to threats, security policy and assumptions that can lead to damage of the TOE assets, such as safety-related problems, user-sensitive data, and data used for accountability.

3.1 Assets

Assets are entities that the owner of the TOE presumably places value upon. The following TOE assets have been identified: the “Security service - Firewall (SS_FW)” asset has been added to the assets already identified in [4].

Asset	Description
Platoon Management Service (PMS) – provided by TOE-SF to users	The TOE is responsible for the safety of the vehicle user and co-responsible for the safety of other vehicle users in the platoon. Several types of services are provided by the TOE: ● **Lane following** function ensuring that the vehicle is within the bounds of the road lane used by the platoon as close as possible to the middle of the lane. ● **Safe distance** function ensures that the vehicle is not dangerously close to other vehicles. This function uses data sent by other vehicles, and data collected from sensors to decide the behaviour of the vehicle, e.g., which speed and direction to move. ● **Data sharing** function ensures that sound data, e.g., speed, direction, and position, is sent to vehicles that require that data, e.g., other vehicles that are part of the platoon. These assets must be protected at least in integrity, and ideally also by authenticity and availability.
SafSecPMM Software (PMM_SW)	Encoded instructions that regulate the behaviour of the TOE. The TOE software must be protected in integrity and authenticity.
Logs and Other Accountability Data (ACC_DATA)	The TOE stores data that can be used to trace the activities carried out by the vehicle, e.g., the data that has been received through the VCS or from the available sensor in the VCM, and the messages transmitted by the VCS and the commands sent to the VCM.

Asset	Description
	This data must be protected in integrity and authenticity.
Security service - Firewall (SS_FW)	The TOE is responsible for providing security services (a firewall) to manage network traffic. The firewall authorizes or blocks communications according to security policy, e.g. communications from or to an unnecessarily open port. These assets must be protected in integrity, authenticity and availability

Table 1: TOE Assets

3.2 Users

Users are the same as in [4].

Users are human or IT entities possibly interacting with the TOE from outside of the TOE boundary. The following TOE users have been identified.

User	Description
Vehicles and infrastructure stations	Vehicles that are in the platoon formation or vehicles. The infrastructure stations, such as stations collecting information about the platoon vehicles and also informing these vehicles about traffic conditions.
VCM	The VCM contains the sensors and actuators of the vehicle.
Driver	The vehicle driver is the person that is in control of the wheel and other functionalities.
VCS	The VCS contains the hardware enabling the communication with other vehicles.
Administrator	Administrators manage the TOE lifecycle (update, monitor) in the operation phase.

Table 2: TOE Users

3.3 Threats Agents

Threat agents are the same as in [4].

A threat agent is an entity that can adversely act on assets. The following Threat Agents have been identified for the TOE.

Agent	**Description**
Local Attacker	Attacker with physical access to the TOE, either legal owner of the vehicle or not; such attacker does not have an authorized access to TOE services. Local attackers can run hardware or software attacks through both physical or logical TOE interfaces.
Remote Attacker	Attacker incurring through the VCS or the sensors in the VCM. Remote attackers can run software attacks through logical TOE interfaces only.

Table 3: TOE Threat Agents.

3.4 Threats

Threats are based on the ones in [4] (grey text) and other specific ones have been added (black text).

We describe a threat as an adverse action performed by the threat agents on the assets that the TOE has to protect. Attackers will have two main objectives:

- Be able to track the vehicle. By tracking a vehicle, the attacker can, for example, determine the route of goods transported by vehicles, which may help them steal the goods.
- Cause a safety hazardous situation. For example, the attacker can place the passengers in the vehicles in danger. Script kiddies may have motivation to do so, only to show that they can, while professional cyber-attacks may be motivated to place passengers and vehicles in danger for financial motivations, e.g., carry out ransomware-type attacks.

The following threats against the TOE have been identified.

Name	Threat against TOE	Asset / Protection
Communication Data Spoofing (T.COM_SPF)	The attacker may inject data in the communication channel by, for example, carrying out replay attacks. For another example, if the attacker possesses valid secret encryption keys, stored in the vehicle's HSM, then Sybil attacks can cause the vehicle to infer that there is a vehicle that does not actually exist.	PMS / Authenticity
VCM Data Spoofing (T.SEN_SPF)	The attacker can carry environmental attacks that may confuse sensors causing the vehicle to perform incorrectly, e.g., accelerate the vehicle placing its passengers in danger.	PMS / Authenticity
Communication DoS (T.COM_DOS)	The attacker can carry out denial of service attacks on the communication channels used.	PMS / Availability
VCM DoS (T.VCM_DOS)	The attacker may deny the service of a sensor by, for example, covering the lenses of a camera/LIDAR used to infer objects.	PMS / Availability
SafSecPMM Software Tamper (T.SW_TAMPER)	The attacker may tamper with the software installed in the TOE causing the attacker to control the vehicle.	PMM_SW / Authenticity
Exploit Service Defects	The attacker may take advantage of a TOE	PMS / Integrity

Name	Threat against TOE	Asset / Protection
(T.SW_DEFECTS)	malfunction/defect of the Platooning Management Service.	
Tamper Accountability Data (T.ACC_TAMPER)	The attacker may tamper the accountability data, thus avoiding attacks that have been carried to be accounted for.	ACC_DATA / Integrity, Non-repudiation
Attack Software Update Mechanism (T.SW_UPDATE)	The attacker may attack the mechanisms used by vehicles to update the TOE software to install malwares or other malicious software.	PMS / Authenticity
Attack system access (T.ECU_ACCESS)	The attacker may get unauthorized access to the vehicle ECU via the network getting the control of the vehicle, e.g., Brute-force password attack.	PMS / Confidentiality, Integrity and Authenticity
Network Intrusion (T.NETWORK_INTRUSION)	a user of one of the external networks accesses SafeSecPMM internal network with malicious intent	PMM/Firewall Confidentiality, Integrity and Authenticity
TOE Intrusion T.FIREWALL_INTRUSION	an attacker obtains unauthorized remote access to the firewall. He could change the configuration, add unauthorized accesses, modify audit traces, and saturate the firewall.	PMM/Firewall Confidentiality, Integrity and Authenticity
Firewall compromission T.FIREWALL_COMPROMISE	as the firewall is a reused open source component, an attacker can corrupt the update channel of the firewall to compromise the TOE.	PMM/Firewall Confidentiality, Integrity and Authenticity

Table 4: Threats against TOE

3.5 Organizational security policies

Organizational Security Policies are based on the ones in [4] (grey text) and other specific ones have been added (black text).

Organisational Security Policies (OSPs) are security rules, procedures, or guidelines imposed (or presumed to be imposed) now and/or in the future by an actual or hypothetical organisation in the operational environment. OSPs can apply to the TOE and/or the operational environment of the TOE. The OSPs that are to be enforced by the TOE are defined in the following table.

Name	Organisational Security Policies
P.LANE_KEEPING	The TOE shall ensure that the vehicle does not leave the platooning lane for the duration when the vehicle belongs to a platoon.
P.DATA_INTEGRITY	The TOE environment shall communicate data to other vehicles of the platoon, e.g., its speed, direction, position, with integrity and authenticity. Moreover, this communication is done periodicity small enough to ensure the safe operation of the vehicle.
P.ACCOUNTABILITY	The TOE shall be able to store securely (preserving the integrity) all the data necessary to reproduce the logical steps used by the TOE to the decisions taken.
P.SAFETY_DISTANCE	The TOE shall ensure a distance greater than a minimal distance to other vehicles in the platoon so that the vehicles are safe. The exact minimal distance will depend on among other factors on the speed of the platoon, the operation mode (emergency brake, following, etc).
P.FIREWALL_ENABLED	The TOE shall ensure that the firewall is enabled and filtering traffic in and out of the TOE.
P.FIREWALL_SECURE_CONFIG	The TOE shall ensure that the firewall is configured with security rules implementing a secure profile. e.g. ensure unneeded network ports are closed

Table 5: Organizational security policies

3.6 Assumptions

Assumptions are based on the ones in [4] (grey text) and other specific ones have been added (black text).

The following table establishes assumptions that are made on the TOE operational environment in order to be able to provide security functionality. Assumptions are on physical and connectivity of the TOE operational environment. During the evaluation these assumptions are considered to be true, i.e. they are not tested in any way.

Name	Assumptions on the TOE operational environment
A.PLATOON_FORMATION	We assume that the platoon is formed, that is, we are not assuming manoeuvres where the vehicles need to join or split a platoon.

Name	Assumptions on the TOE operational environment
A.HIGHWAY	We assume that the platoon is moving on a highway with a dedicated lane, where other vehicles may not navigate. Moreover, there are no crossroads nor junctions.
A.OPERATION_MODES	A vehicle in a platoon is either a leader or a follower. The TOE shall support both modes of operation.
A.COMM_INTEGRITY	We assume that the communication between the VCM and TOE and between VCS and TOE have integrity.
A.INTEGRATION	We assume that appropriate technical and/or organisational security measures in the Platform Integration have been taken to guarantee the integrity, confidentiality and authenticity of the TOE assets.
A.FIREWALL_PHYSICAL_PROTECTION	the TOE firewall is protected against all unauthorized access attempts (tamper resistant hardware module)
A.FIREWALL_TRUSTED_ADMINISTRATOR	The assumption that the Security Administrator is trusted
A.FIREWALL_REGULAR_UPDATES	The assumption that the devices firmware and software is updated regularly
A.FIREWALL_ADMIN_CREDENTIALS_SECURE	The assumption that the Security Administrator’s credentials are protected by the platform they are stored on
A.FIREWALL_COMPONENTS_RUNNING	The assumption that each component of the firewall system is functioning properly

Table 6: Assumptions on the TOE operational environment

Chapter 4 Security Objectives

The security objectives are a concise and abstract statement of the intended solution to the problem defined by the Security Problem definition (see Chapter 3). They provide a high-level, natural language solution of the problem.

Security Objectives are based on the ones in [4] and other specific ones have been added (NETWORK or FIREWALL).

4.1 Security Objectives for the TOE

The following table defines the security objectives for the TOE, i.e. the set of objectives that the TOE should achieve in order to solve its part of the problem.

Security Objective	**Description**
OT.VCS_DATA	The TOE shall provide periodically to the VCS data about the vehicle, e.g., speed, direction, position. This data shall reflect the actual state of the vehicle.
OT.INCORRECT_VCM_DATA	The TOE shall be able to detect when data incoming from the VCM is incorrect, i.e., it differs from the actual state of the world.
OT.INCORRECT_VCS_DATA	The TOE shall be able to detect when data incoming from the VCS is incorrect, i.e., it differs from the actual state of the world.
OT.SENSOR_FAIL	The TOE shall be able to guarantee the safety of the vehicle even if a sensor fails, either due to an attack or due to some component failure.
OT.COMM_FAIL	The TOE shall be able to guarantee the safety of the vehicle even if a communication channel fails, either due to a DoS attack or due to some component failure, e.g., by going to a safe-mode and informing the driver.
OT.VCM_DATA	The TOE shall provide periodically to the VCM data to be consumed by the VCM actuators. The data shall be used to ensure the safety of the vehicle, e.g., keep the platoon lane and a safe distance to all other vehicles.
OT.TOE_SELF-PROTECTION	The TOE shall be able to protect itself and its assets from manipulation including physical and software tampering. Moreover, the following is assumed by the TOE: ● Messages outgoing from the VCS shall be digitally signed by the HSM. ● The digital certificate of messages in incoming flows from the VCS shall be checked by the HSM.
OT.ACCOUNTABILITY	The TOE shall provide accountability for all the decisions made that affect the behaviour of the vehicle. The TOE shall provide proof of the integrity and origin in order any message

Security Objective	Description
	stored in the memory can be said to be genuine with high confidence.
OT.NETWORK_ACCESS	The TOE must supply access control between two connected networks that filters access according to security policy rules. For access to certain services authentication of users is required. The rules should cover user identity, the nature of applications, the actions performed and their options, the flow of control.
OT.FIREWALL_ROLES	The TOE must not allow operators to perform operations they are not authorised to perform.
OT.FIREWALL_DATA_PROTECT	Information/Configuration specific to the TOE, user information stored temporarily in the TOE and the TOE binaries themselves (at rest or in transit during the update process) must be protected against attacks targeting their confidentiality, integrity and availability.

Table 7: Security Objectives for the TOE.

4.2 Security Objectives for the Operational Environment

The following table defines the security objectives for Operational Environment, i.e. the set of statements describing the goals that the operational environment should achieve.

Security Objective	Description
OE.SECURE_COMM	The TOE operational environment shall implement protections for the integrity, authenticity and confidentiality of the data exchanged between vehicles and between vehicles and stationary deployments.
OE.CORRECT_IMP	The TOE operational environment shall ensure that the TOE software does not have defects, such as, software bugs that can be exploited by the attacker, e.g., to carry-out buffer overflows, badly configured access control.
OE.INTEGRATION	Appropriate technical and/or organisational security measures shall be in place during platform integration phase.
OE.TOE_ACCESS	The TOE environment shall implement security measures to ensure that the TOE is only accessible from the VCS and the VCM by deploying measures for authenticity and access control.
OE.VCM_SEN_FAIL	The VCM must be able to detect when a sensor has failed and inform the sensor fail to the TOE whenever this occurs.
OE.VCS_CMM_FAIL	The VCS must be able to detect when a communication link to other vehicles/infrastructure stations fails and inform which link failed to the TOE whenever this occurs.

Security Objective	Description
OE.EXT_PERSON	An external person having access to the TOE, should only be able to do so in accordance with the security policy in place.
OE.FIREWALL_INSTALL	The TOE must be delivered, installed and updated securely so that security policies about network interconnection are respected
OE.FIREWALL_PROTECT	The TOE must be located in a protected enclosure. The means implemented must be in accordance with the security policy governing the interconnection of networks.

Table 8: Security Objectives for the Operational Environment

4.3 Security Objectives Rationale

The objective of this section is to establish a relation between the TOE Security Objectives and the Security Problem definition and provide a set of justifications that shows that all threats, OSPs and assumptions are effectively addressed by the security objectives.

4.3.1 Security Objectives Coverage

The following table provides a tracing showing which Security Objectives (see Sections 4.1 and 4.2) address which threats, OSPs, and assumptions of the firewall module of the TOE described in the Security Problem definition (see Chapter 3) for the additional Firewall objectives. The other ones are fully covered in [4].

As shown in the table, each security objective traces to at least one threat, OSP or assumption; each threat, OSP and assumption has at least one security objective tracing to it; and security objectives for the TOE do not trace back to assumptions.

	OT.NETWORK_ACCESS	OT.FIREWALL_ROLES	OT.FIREWALL_DATA_PROTECT	OE.FIREWALL_PLATFORM	OE.EXT_PERSON	OE.FIREWALL_INSTALL	OE.FIREWALL_PROTECT
T.NETWORK_INTRUSION	X		X				
T.FIREWALL_INTRUSION	X		X				
T.FIREWALL_COMPROMISE			X				
P.FIREWALL_ENABLED	X		X				
P.FIREWALL_SECURE_CONFIG		X	X				
A.FIREWALL_PHYSICAL_PROTECTION	▨	▨	▨	X	X		X
A.FIREWALL_TRUSTED_ADMINISTRATOR	▨	▨	▨		X		
A.FIREWALL_REGULAR_UPDATES	▨	▨	▨			X	
A.FIREWALL_ADMIN_CREDENTIALS_SECURE	▨	▨	▨		X		
A.FIREWALL_COMPONENTS_RUNNING	▨	▨	▨			X	

Table 9: Security Objectives coverage – Firewall

4.3.2 Security Objectives Sufficiency

The security objectives rationale demonstrates that the tracing is effective, i.e. all the given threats, OSPs and assumptions are addressed if all security objectives tracing to a particular threat, OSP or assumption are achieved.

Threat/OSP/Assumption	Security Objective	Rationale
T.NETWORK_INTRUSION	OT.NETWORK_ACCESS	The objectives' aim is to cover this threat (preventing access from one network to the other).
T.FIREWALL_INTRUSION	OT.FIREWALL_DATA_PROTECT	The firewall shall be protected against any gathering or modification of the information/configuration it uses.
	OT.NETWORK_ACCESS	As the firewall can be considered as an equipment of the network, the firewall shall also protect itself from any intrusion with the same mechanism used against T.Network_intrusion (reject unauthorized traffic).
T.FIREWALL_COMPROMISE	OT.FIREWALL_DATA_PROTECT	Verifying the firewall integrity shall prevent any compromise of its software or configuration.
P.FIREWALL_ENABLED	OT.NETWORK_ACCESS	The firewall shall be enabled to allow network access.
	OT.FIREWALL_DATA_PROTECT	The firewall shall be enabled to modify information/configuration it uses.
P.FIREWALL_SECURE_CONFIG	OT.FIREWALL_ROLES	The firewall shall guarantee that the configuration is secure to apply roles.
	OT.FIREWALL_DATA_PROTECT	The firewall shall guarantee that the configuration is secure to modify information/configuration it uses.
A.FIREWALL_PHYSICAL_PROTECTION	OE.FIREWALL_PLATFORM	The assumption of physical protection of the firewall is addressed by the OE that requires the TOE to run on a trusted Hardware.
	OE.EXT_PERSON	The assumption of physical protection of the firewall is addressed by the OE that requires the TOE can only be accessed according to security policies..
	OE.FIREWALL_PROTECT	The assumption of physical protection of the firewall is addressed by the OE that requires the TOE is located in a protected enclosure.

Threat/OSP/Assumption	Security Objective	Rationale
A.FIREWALL_TRUSTED_ADMINISTRATOR	OE.EXT_PERSON	The assumption of trusted administration is addressed by the OE that requires the TOE can only be accessed according to security policies.
A.FIREWALL_REGULAR_UPDATES	OE.FIREWALL_INSTALL	The firewall shall be updated according to the installation procedures and policies.
A.FIREWALL_ADMIN_CREDENTIALS_SECURE	OE.EXT_PERSON	The assumption of secure admin credentials is addressed by the OE that requires that the TOE can only be accessed according to security policies.
A.FIREWALL_COMPONENTS_RUNNING	OE.FIREWALL_INSTALL	The assumption of firewall components running is addressed by the OE that requires the TOE to be installed and updated according to security policies..

Table 10: Security Objectives sufficiency

4.4 Security Objectives Conclusion

We can conclude that all the security objectives are achieved, therefore the security problem as defined in Security problem definition (see Chapter 3) is solved: all threats are countered, all OSPs are enforced, and all assumptions are upheld.

Chapter 5 Security Requirements

The security requirements consist of two groups of requirements that are discussed in the following sections:

a) Security functional requirements (SFRs): a translation of the security objectives for the TOE into a standardised language.

b) Security assurance requirements (SARs): a description of how assurance is to be gained that the TOE meets the SFRs.

SFR from [4] are valid also for this PP.

5.1 Formatting conventions

The CC defines the following operations on SFRs: assignments, refinements, selections and iterations. This document uses the following font conventions to identify those operations:

- Assignment: Indicated with **[*italic bold text*]** surrounded by square brackets;
- Selection: Indicated with **[underlined bold text]** surrounded by brackets;
- Refinement: Indicated with ***italic bold text*** and ~~strikethroughs~~, if necessary;
- Iteration: Indicated by appending the iteration number in parenthesis, e.g., (1), (2), (3); and

Besides that, extended SFRs are identified by having a label ‘EXT’ after the requirement name for TOE SFRs.

5.2 Security Functional Requirements

This section describes the SFRs that must be satisfied by the TOE. These requirements are a translation into a standardized language of the security objectives defined for the TOE (see Chapter 4).

We focus on relevant requirements for the base operation of the firewall in our use case, other requirements (for example FMT_MSA.1 Management of security attributes, FMT_MSA.2 Secure security attributes, FMT_MSA.3 Static attribute initialisation) could be included in a more detailed protection profile.

5.2.1 CLASS FDP: User Data Protection

5.2.1.1 Security Attribute based access control (FDP_ACF.1)

FDP_ACF.1.1 The TSF shall enforce the **[assignment: *access control SFP*]** to objects based on **[assignment: *security attributes, named groups of security attributes*].**

Hierarchical to: No other components.
Dependencies: No dependencies.

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **[assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]**.

Hierarchical to: No other components.
Dependencies: No dependencies.

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]**.

Hierarchical to: No other components.
Dependencies: No dependencies.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the **[assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]**.

Hierarchical to: No other components.
Dependencies: No dependencies.

5.2.1.2 Simple Security Attributes (FDP_IFF.1)

FDP_IFF.1.1 The TSF shall enforce the **[assignment: *information flow control SFP*]** based on the following types of subject and information security attributes: [

- network origin identity of the communication flow (e.g., IP address) ;
- network destination identity of the communication flow (e.g., IP address) ;
- user origin identity of the communication flow (user name) (for authentication) ;
- user destination identity of the communication flow (user name) ;
- type of application (e.g., FTP, SQL, HTTP, SMTP, TELNET,...) ;
- type of application command requested (e.g., FTP «get», SQL «select»,...) ;
- format of the commands (e.g. lowercase, uppercase, length of commands,...);
- date / time of the access ;
- number, frequency and throughput of communication flow ;
- labels;
- any other multiple attributes will be specified by the ST author].

Hierarchical to: No other components.
Dependencies: No dependencies.

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: **[assignment: *for each operation, the security attribute-based relationship that must hold between subject and information security attributes*]**.

Hierarchical to: No other components.
Dependencies: No dependencies.

FDP_IFF.1.3 The TSF shall enforce the **[assignment: *additional information flow control SFP rules*]**.

Hierarchical to: No other components.
Dependencies: No dependencies.

FDP_IFF.1.4 The TSF shall provide the following **[assignment: *list of additional SFP capabilities*]**.

Hierarchical to: No other components.
Dependencies: No dependencies.

FDP_IFF.1.5 The TSF shall explicitly authorise an information flow based on the following rules: **[assignment*: rules, based on security attributes, that explicitly authorise information flows*].**

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: **[assignment*: rules, based on security attributes, that explicitly deny information flows*]**.

Hierarchical to: No other components.
Dependencies: No dependencies.

5.2.1.3 Partial elimination of illicit information flows (FDP_IFF.4)

FDP_IFF.4.1 The TSF shall enforce the **[assignment: *information flow control SFP*]** to limit the capacity of **[assignment: *non-empty list of types of illicit information flows*]** to a **[assignment: *maximum capacity*]**.

Hierarchical to: No other components.
Dependencies: No dependencies.

FDP_IFF.4.2 The TSF shall prevent the following types of **[assignment: *non-empty list of types of illicit information flows*]**.

Hierarchical to: No other components.
Dependencies: No dependencies.

5.3 Security Assurance Requirements

The Security Assurance Requirements (SARs) are a description in a standardized language of how the TOE is to be evaluated.

The Security Assurance Requirements will be based on the ones from [4].

5.4 Security Requirements Rationale

5.4.1 Security Functional Requirements Dependencies

	Dependencies	Comment
FDP_ACF.1	None	No Dependencies are defined as these security requirements are self contained.
FDP_IFF.1	None	No Dependencies are defined as these security requirements are self contained.
FDP_IFF.4	None	No Dependencies are defined as these security requirements are self contained.

Table 11: Security Functional Requirements dependencies

5.4.2 Security Assurance Requirements Dependencies

See [4] for the Security Assurance Requirements Dependencies.

5.4.3 Security Functional Requirements Coverage

Figure 13 shows how the SFRs trace back to the security objectives for the TOE (see Chapter 4) as follows: each SFR traces back to at least one security objective and each security objective for the TOE has at least one SFR tracing to it.

Please note that multiple SFRs may trace to the same security objective for the TOE, indicating that the combination of those security requirements meets that security objective for the TOE.

	OT.NETWORK_ ACCESS	OT.FIREWALL_ROLES	OT.FIREWALL_DAT A_PROTECT
FDP_ACF.1.1	X	X	X
FDP_ACF.1.2	X	X	X
FDP_ACF.1.3	X	X	X
FDP_ACF.1.4	X	X	X
FDP_IFF.1.1	X	X	X
FDP_IFF.1.2	X	X	X
FDP_IFF.1.3	X	X	X
FDP_IFF.1.4	X	X	X
FDP_IFF.1.5	X	X	X
FDP_IFF.1.6	X	X	X
FDP_IFF.4.1	X	X	X
FDP_IFF.4.2	X	X	X

Table 12: Security Functional Requirements coverage

5.4.4 Security Functional Requirements Sufficiency

This section provides a set of justifications that shows that all security objectives for the TOE are effectively addressed by the SFRs, i.e. if all SFRs tracing to a particular security objective for the TOE are satisfied, that security objective for the TOE is achieved.

Objective	SFR	Rationale
OT.NETWORK_ACCESS	FDP_IFF.1.1 FDP_IFF.1.2 FDP_IFF.1.3 FDP_IFF.1.4 FDP_IFF.1.5 FDP_IFF.1.6 FDP_IFF.4.1 FDP_IFF.4.2	All these requirements cover the basic functionalities of the firewall which aim is to satisfy its first objectives : supply access control based on rules, security attributes, user identity, nature of applications, ...
OT.FIREWALL_ROLES	FDP_ACF.1.1 FDP_ACF.1.2 FDP_ACF.1.3 FDP_ACF.1.4 FDP_ACC.1	All these requirements are necessarily related to roles so that the configuration/information managed by the firewall are not accessible to anyone.
OT.FIREWALL_DATA_PROTECT	FDP_ACF.1.1 FDP_ACF.1.2 FDP_ACF.1.3 FDP_ACF.1.4	All these requirements cover the basic functionalities of the firewall which shall also protect itself against attacks.

Objective	SFR	Rationale
	FDP_IFF.1.1 FDP_IFF.1.2 FDP_IFF.1.3 FDP_IFF.1.4 FDP_IFF.1.5 FDP_IFF.1.6 FDP_IFF.4.1 FDP_IFF.4.2 FDP_ACC.1	

Table 13: Security Functional Requirements sufficiency

5.4.5 Justification of the Chosen Evaluation Assurance Level

This part should be explained in the Security Target that is based on this Protection Profile and it should be coherent for the global TOE (Firewall + SafeSecPMM).

5.5 Security Requirements: Conclusion

Since all SFRs and SARs are satisfied and all security objectives for the operational environment are achieved, then there exists assurance that the security problem as defined in Chapter 3 is solved: all threats are countered, all OSPs are enforced, and all assumptions are upheld.

Chapter 6 List of Abbreviations

Abbreviation	Translation
ACC	Adaptative Cruise Control
C-ITS	Cooperative Intelligent Transport System
CACC	Cooperative Adaptive Cruise Control
DoS	Denial of Service
HSM	Hardware Security Module
OSP	Organisational Security Policy
PMM	Platoon Management Module
PMS	Platoon Management Service
PP	Protection Profile
SafSecPMM	Safe and Secure Platoon Management Module
SAR	Security Assurance Requirements
SF	Security Functionality
SFR	Security Functional Requirement
SFP	Security Function Policies
ST	Security Target
SW	Software
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSP	TOE Security Policy
VCS	Vehicle Communication System
VCM	Vehicle Control Module

Chapter 7 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1, revision 5, April 2017. Part 1: Introduction and general model

[2] Common Criteria for Information Technology Security Evaluation, Version 3.1, revision 5, April 2017. Part 2: Functional security components.

[3] Common Criteria for Information Technology Security Evaluation, Version 3.1, revision 5, April 2017. Part 3: Assurance security components.

[4] Protection Profile for a Safety and Security Platooning Management Module, version 1.0, SPARTA project, Vivek Nigam, Estibaliz Amparan; Angel López, and Cristina Martínez, January 31, 2021.

[5] Profil de protection - Firewall à Exigences Elevées - V2.2, Groupe de travail DGA, September, 1998.