Task Force Sécurité

Delivrable 1 : Common Criteria for C-ITS stations

Auteurs : Emilien Bourdy, Ramzi Boutahala, Hacène Fouchal, Sophie Bourdy-Liebart, Geoffrey Wilhelm, ,

Version : 0.4

Date : 6 Mai 2024

[Reference documents 5](#_Toc150327658)

[Abbreviation 5](#_Toc150327659)

[1-Preliminaries 6](#_Toc150327660)

[2- Introduction 6](#_Toc150327661)

[3-Requirements 6](#_Toc150327662)

[3.1 Software integrity requirements 6](#_Toc150327663)

[Secure boot (reference to CC1 of C-ITS CC) 6](#_Toc150327664)

[Self-Protection (reference to CC1 of C-ITS CC) 7](#_Toc150327665)

[Req\_SofInt\_SelfProt\_001 7](#_Toc150327666)

[ADV\_ARC.1.4C 8](#_Toc150327667)

[Req\_SofInt\_SelfProt\_002 8](#_Toc150327668)

[ADV\_ARC.1.4C 8](#_Toc150327669)

[ADV\_ARC.1.4C 8](#_Toc150327670)

[ADV\_ARC.1.4C 8](#_Toc150327671)

[3.2 Attack surface requirements 8](#_Toc150327672)

[Bypass prevention 8](#_Toc150327673)

[Error management 11](#_Toc150327674)

[Req\_AttSur\_ErrMan\_001 11](#_Toc150327675)

[ADV\_FSP.2.5C 11](#_Toc150327676)

[Req\_AttSur\_ErrMan\_002 11](#_Toc150327677)

[ADV\_FSP.2.5C 11](#_Toc150327678)

[Req\_AttSur\_ErrMan\_003 12](#_Toc150327679)

[3.3 Documentation requirements 12](#_Toc150327680)

[Interfaces 12](#_Toc150327681)

[Users 13](#_Toc150327682)

[Mode of operation 15](#_Toc150327683)

[Unique identification 16](#_Toc150327684)

[System 17](#_Toc150327685)

[CMDB 17](#_Toc150327686)

[Security Objectives 19](#_Toc150327687)

[Tests 20](#_Toc150327688)

[Req\_Doc\_Test\_001 20](#_Toc150327689)

[ATE\_FUN.1.1C 20](#_Toc150327690)

[Req\_Doc\_Test\_002 21](#_Toc150327691)

[ATE\_FUN.1.2C 21](#_Toc150327692)

[Req\_Doc\_Test\_003 21](#_Toc150327693)

[ATE\_FUN.1.3C 21](#_Toc150327694)

[Req\_Doc\_Test\_004 21](#_Toc150327695)

[ATE\_FUN.1.4C 21](#_Toc150327696)

[3.4 Installation requirements 21](#_Toc150327697)

[Installation Steps 22](#_Toc150327698)

[Req\_Install\_Steps\_001 22](#_Toc150327699)

[AGD\_PRE.1.2C 22](#_Toc150327700)

[Req\_Install\_Steps\_002 22](#_Toc150327701)

[AGD\_PRE.1.2C 22](#_Toc150327702)

[Req\_Install\_Steps\_003 22](#_Toc150327703)

[AGD\_PRE.1.2C 22](#_Toc150327704)

[Req\_Install\_Steps\_004 22](#_Toc150327705)

[AGD\_PRE.1.2C 22](#_Toc150327706)

[Req\_Install\_Steps\_005 23](#_Toc150327707)

[AGD\_PRE.1.2C 23](#_Toc150327708)

[Req\_Install\_Steps\_006 23](#_Toc150327709)

[AGD\_PRE.1.2C 23](#_Toc150327710)

[Preparation 23](#_Toc150327711)

[Req\_Install\_Prep\_001 23](#_Toc150327712)

[AGD\_PRE.1.2C 23](#_Toc150327713)

[Req\_Install\_Prep\_002 23](#_Toc150327714)

[AGD\_PRE.1.2C 23](#_Toc150327715)

[3.5 Log Management requirements 23](#_Toc150327716)

[Req\_Log\_Priv\_001 24](#_Toc150327717)

[Req\_Log\_Login\_001 24](#_Toc150327718)

[AGD\_PRE.1.2C 24](#_Toc150327719)

[Req\_Log\_ErrID\_001 24](#_Toc150327720)

[AGD\_PRE.1.2C 24](#_Toc150327721)

[Req\_Log\_Forbid\_001 24](#_Toc150327722)

[AGD\_PRE.1.2C 24](#_Toc150327723)

[ADV\_FSP.2.4C 24](#_Toc150327724)

[3.6 Input Validation requirements 25](#_Toc150327725)

[Req\_Input\_Verif\_001 25](#_Toc150327726)

[3.7 Evaluation requirements 25](#_Toc150327727)

[Audit 25](#_Toc150327728)

[Req\_Eval\_Audit\_001 25](#_Toc150327729)

[ADV\_FSP.2.2E 25](#_Toc150327730)

[Req\_Eval\_Audit\_002 25](#_Toc150327731)

[ADV\_FSP.2.2E 25](#_Toc150327732)

[Process 25](#_Toc150327733)

[Req\_Eval\_Proc\_001 26](#_Toc150327734)

[AGD\_PRE.1.1C 26](#_Toc150327735)

[Req\_Eval\_Proc\_002 26](#_Toc150327736)

[ASE\_REQ.2.7C 26](#_Toc150327737)

[Req\_Eval\_Proc\_003 26](#_Toc150327738)

[ASE\_REQ.2.8C 26](#_Toc150327739)

[Req\_Eval\_Proc\_004 26](#_Toc150327740)

[AVA\_VAN.2.2E 26](#_Toc150327741)

[Req\_Eval\_Proc\_005 27](#_Toc150327742)

[AVA\_VAN.2.3E 27](#_Toc150327743)

[Req\_Eval\_Proc\_006 27](#_Toc150327744)

[AVA\_VAN.2.4E 27](#_Toc150327745)

[Security Maintenance 27](#_Toc150327746)

[Req\_Eval\_Maint\_001 27](#_Toc150327747)

[ALC\_DEL.1.1C 27](#_Toc150327748)

[Req\_Eval\_Maint\_002 27](#_Toc150327749)

[ALC\_DEL.1.1C 27](#_Toc150327750)

[Tests 28](#_Toc150327751)

[Req\_Eval\_Test\_001 28](#_Toc150327752)

[ATE\_COV.1.1C 28](#_Toc150327753)

[Req\_Eval\_Test\_002 28](#_Toc150327754)

[ATE\_COV.1.1C 28](#_Toc150327755)

[Req\_Eval\_Test\_003 28](#_Toc150327756)

[ATE\_IND.2.1C / ATE\_IND.2.2C 28](#_Toc150327757)

[Req\_Eval\_Test\_004 29](#_Toc150327758)

[ATE\_IND.2.1C / ATE\_IND.2.2C 29](#_Toc150327759)

[Req\_Eval\_Test\_005 29](#_Toc150327760)

[ATE\_IND.2.2E 29](#_Toc150327761)

[Req\_Eval\_Test\_006 29](#_Toc150327762)

[ATE\_IND.2.3E 29](#_Toc150327763)

[3.8 Risk analysis requirements 29](#_Toc150327764)

[Req\_Risk\_Analy\_001 29](#_Toc150327765)

[ASE\_REQ.2.1C 29](#_Toc150327766)

[Req\_Risk\_Analy\_002 29](#_Toc150327767)

[ASE\_REQ.2.1C 29](#_Toc150327768)

[Req\_Risk\_Analy\_003 30](#_Toc150327769)

[ASE\_REQ.2.6C 30](#_Toc150327770)

[Req\_Risk\_Analy\_004 30](#_Toc150327771)

[AGD\_OPE.1.4C 30](#_Toc150327772)

[Req\_Risk\_Analy\_005 30](#_Toc150327773)

[AGD\_OPE.1.4C 30](#_Toc150327774)

[3. Preliminary risk analysis 31](#_Toc150327775)

# **Reference documents**

|  |  |  |
| --- | --- | --- |
| Reference | Name of the document | Link of the document |
| [DR1] | Common criteria | https://www.ssi.gouv.fr/uploads/2015/01/ccpart3v3.1r5.pdf |
| [DR2] | EN 303 645 | https://www.etsi.org/deliver/etsi\_en/303600\_303699/303645/02.01.01\_60/en\_303645v020101p.pdf |
| [DR3] | TS 103 701 | https://www.etsi.org/deliver/etsi\_ts/103700\_103799/103701/01.01.01\_60/ts\_103701v010101p.pdf |

# Abbreviation

|  |  |
| --- | --- |
| Acronym | Signification |
| **CM** | Configuration Management |
| **CMDB** | Configuration Management Database |
| **CVE** | Common Vulnerabilities and Exposures |
| **CVSS** | Common Vulnerability Scoring System |
| **PP** | Protection Profile |
| **SAR** | Suspicious Activity Report |
| **SFR** | Security Functional Requirements |
| **SO** | Security Objectives |
| **ST** | Security Target |
| **TOE** | Target of Evaluation |
| **TSF** | TOE Security Functionality |
| **TSFI** | TSF interfaces |

# 1-Preliminaries

The security task force (TF security) has worked on many aspects related to the security of C-ITS devices.

The first deliverable “TF-security- L1 requirements” describes the requirements to be respected by devices in order to be totally in conformance with the L1 security level. This deliverable is a set of detailed requirements on the device and its functioning in external environment which could be hostile.

The second deliverable “TF-security- Current situation” describes the situation of French devices regarding these requirements. In addition to that, the document describes the missing items to reach Level L1 and the situation of deployed Road Side Unit in France. Finally the current situation of the “Hardware Security Module” HSM of the deployed devices.

The third deliverable “TF-security- French C-ITS Protection Profile” describes the security requirements of all French C-ITS equipments to be deployed. In this document, the list of intrusion test is also detailed.

The risk study is achieved and the split into two parts. The risks regarding Level pre-L1 and L1 are proposed as an appendix of the deliverable “TF-security- L1 requirements” and a complementary risk study is input as an appendix of the deliverable “TF-security- French C-ITS Protection Profile”.

# 2- Introduction

This document gives a set of requirements which should be respected by all C-ITS stations be deployed in a secure environment. These requirements are split in 8 categories:

Software integrity; Attack surface; Documentation; Installation; Log Management; Input Validation; Evaluation and Risk analysis.

# 3-Requirements

## **3.1 Software integrity requirements**

### Secure boot (reference to CC1 of C-ITS CC)

The following criteria are related to ADV\_ARC.1.3C (The security architecture description shall describe how the TSF initialization process is secure) of [DR1]. For the C-ITS CC, it is related to criteria 1 which states : “Secure initialization process of the TOE (e.g. Secure Boot, Runtime-Level) is sufficient”.

|  |  |
| --- | --- |
| Id | Req\_SofInt\_SecBoot\_001 |
| CC-ID | ADV\_ARC.1.3C |
| Requirement purpose | A secure boot needs to be implemented |
| Additional Information 1 |  |
| Requirement Comment 1 | If SoC is used, secure boot is guaranteed. |

|  |  |
| --- | --- |
| Id | Req\_SofInt\_SecBoot\_002 |
| CC-ID | ADV\_ARC.1.3C |
| Requirement purpose | The secure boot needs to be implemented with hardware root of trust |
| Additional Information 1 |  |
| Requirement Comment 1 | The function u-boot checks the signature of the Linux kernel.  It computes the root hash. |
| Requirement Comment 2 | What is in write mode and what needs to be in read only mode? |
| Requirement Comment 3 | The purpose is to optimize the verification of the signature. |
| Requirement Comment 4 | Dual boot could be an issue for some providers |

|  |  |
| --- | --- |
| Id | Req\_SofInt\_SecBoot\_003 |
| CC-ID | ADV\_ARC.1.3C |
| Requirement purpose | Tampering detection system needs to be implemented |
| Additional Information 1 |  |
| Requirement Comment 1 | In case of modification detection, the signature will not be the right one and the CPU will refuse to boot. This requirement will be covered by the solution of the previous one. |
| Requirement Comment 2 | Tempering detection is possible only if the ITS Station is on |

|  |  |
| --- | --- |
| Id | Req\_SofInt\_SecBoot\_004 |
| CC-ID | ADV\_ARC.1.3C |
| Requirement purpose | Tampering detection system needs to send alert |
| Additional Information 1 |  |
| Requirement Comment 1 | Tempering detection alert is possible only if the ITS Station is on |

|  |  |
| --- | --- |
| Id | Req\_SofInt\_SecBoot\_005 |
| CC-ID | ADV\_ARC.1.3C |
| Requirement purpose | In case of logical tampering detection, the system needs to migrate / restore in safe state |
| Additional Information 1 |  |
| Requirement Comment 1 | The station is blocked until the right OS will be flashed again |
| Requirement Comment 2 | We cannot upload a non valid OS image |

### Self-Protection (reference to CC1 of C-ITS CC)

The following criteria are related to ADV\_ARC.1.4C (The security architecture description shall demonstrate that the TSF protects itself from tampering). For the C-ITS CC, it is related to criteria 2 stating: “Self-Protection of the TOE (physical protection, integrity protection mechanisms…) is sufficient”

|  |  |
| --- | --- |
| Id | Req\_SofInt\_SelfProt\_001 |
| CC-ID | ADV\_ARC.1.4C |
| Requirement purpose | In case of logical tampering detection, the system needs to migrate / restore in safe state |
| Additional Information 1 | There are several solutions for the detection: Magnet; Physical sensor; Switches; etc. |

|  |  |
| --- | --- |
| Id | Req\_SofInt\_SelfProt\_002 |
| CC-ID | ADV\_ARC.1.4C |
| Requirement purpose | In case of physical tampering detection, the system needs to lock himself |
| Additional Information 1 | For example, using a physical fuse, etc. |
| Requirement Comment 1 | A solution could be to delete the HSM keys stored to make impossible the signature of the messages. |

|  |  |
| --- | --- |
| Id | Req\_SofInt\_SelfProt\_003 |
| CC-ID | ADV\_ARC.1.4C |
| Requirement purpose | Enclose need to implement opening detection system |
| Additional Information 1 |  |
| Requirement Comment 1 |  |

|  |  |
| --- | --- |
| Id | Req\_SofInt\_SelfProt\_004 |
| CC-ID | ADV\_ARC.1.4C |
| Requirement purpose | In case o physical tampering detection, the system needs to lock all the applications |
| Additional Information 1 |  |
| Requirement Comment 1 |  |

## **3.2 Attack surface requirements**

### Bypass prevention

The following criteria are related to ADV\_ARC.1.5C (The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality. For C-ITS CC, It is related to CC 3 stating : “Security Functionality cannot be bypassed (e.g. by exploiting debug interfaces, causing buffer-overflows, altering boot-order, …) »

|  |  |
| --- | --- |
| Id | Req\_AttSur\_ByPass\_001 |
| CC-ID | ADV\_ARC.1.5C |
| Requirement purpose | No ongoing features must be deployed on the system in production mode. |
| Additional Information 1 |  |
| Requirement Comment 1 | Need to check dev and prod versions, e.g., features that could not be implemented due to time constraints should be removed from the product. |

|  |  |
| --- | --- |
| Id | Req\_AttSur\_ByPass\_002 |
| CC-ID | ADV\_ARC.1.5C |
| Requirement purpose | The system needs to implement certificate pining protections |
| Additional Information 1 |  |
| Requirement Comment 1 | Authentication is guaranteed by the certificates |
| Requirement Comment 2 | Exchange with servers without threatening the confidentiality |

|  |  |
| --- | --- |
| Id | Req\_AttSur\_ByPass\_003 |
| CC-ID | ADV\_ARC.1.5C |
| Requirement purpose | If possible due to hardware limitation, the memory needs to be protected by ASLR (Adress Space Layout Randomization) |
| Additional Information 1 |  |
| Requirement Comment 1 | Randomize memory addresses using ASLR: possibility to restart a code after knowing its location in memory. |
| Requirement Comment 2 | For Linux, one can use kernel.randomize\_va\_space=2 |
| Requirement Comment 3 | PKI’s root certificate needs to be protected |
| Requirement Comment 4 | OS x509 certificates are managed by the OS and are Read-Only files |

|  |  |
| --- | --- |
| Id | Req\_AttSur\_ByPass\_004 |
| CC-ID | ADV\_ARC.1.5C |
| Requirement purpose | Communications between chips (ex.: EEPROM 🡨🡪 CPU) needs to be encrypted to limit possibility of data sniffing |
| Additional Information 1 |  |
| Requirement Comment 1 | A solution could be the usage of a physical architecture with several printed wire connection layers, while putting those with important data in the hidden layers to make the access to them more complex. |
| Requirement Comment 2 | HSM---CPU connexions are usually protected by secure physical links |
| Requirement Comment 3 | RAM—CPU connexion is not protected |
| Requirement Comment 4 | FLASH—CPU connexion is not protected |

|  |  |
| --- | --- |
| Id | Req\_AttSur\_ByPass\_005 |
| CC-ID | ADV\_ARC.1.5C |
| Requirement purpose | If sensitive information are stored on the device, electromagnetic shield needs to be implemented. |
| Additional Information 1 |  |
| Requirement Comment 1 | The objective is to slow the intruder when he tries to recover sensitive data in memory e.g., a transistor that would change to 1, following a fault injection and would put the system in debug mode. |
| Requirement Comment 2 | Some solutions could be: using passwords, private keys, secrets, sensitive logs, etc. |

|  |  |
| --- | --- |
| Id | Req\_AttSur\_ByPass\_006 |
| CC-ID | ADV\_ARC.1.5C |
| Requirement purpose | The system needs to activate only operational services on production mode |
| Additional Information 1 |  |
| Requirement Comment 1 | Activate only services of the production version |

|  |  |
| --- | --- |
| Id | Req\_AttSur\_ByPass\_007 |
| CC-ID | ADV\_ARC.1.5C |
| Requirement purpose | In every data exchange, choose the encryption mode by default. |
| Additional Information 1 | Authentication and/or the encryption |
| Requirement Comment 1 | Before any exchange: we need to verify if it is sensitive? Does the provider have the technical means to protect it? |
| Requirement Comment 2 | For example, the HTTPS is available but not always used.  With self-signed certificates and ignoring the error.  To be checked also, if the encryption between the tablet and the UEVg is mandatory in the specification? |
| Requirement Comment 3 | Closed system: it is difficult to check the validity of the certificates, without https it is impossible to exchange. |
| Requirement Comment 4 | General comment for the L1: can we allow http flow to pass through the network due to the old architecture of the DIRs who does not use https today? |

|  |  |
| --- | --- |
| Id | Req\_AttSur\_ByPass\_008 |
| CC-ID | ADV\_ARC.1.5C |
| Requirement purpose | Deprecated encryption protocol needs to be removed for support |
| Additional Information 1 | Ex: TLS1.1 |
| Requirement Comment 2 | Provide a procedure for migrating to an updated version |
| Requirement Comment 3 | Consideration of all components that collaborate in the station, check the exchanges between the OBU/RSU and the outside. All external links could potentially be affected. |

|  |  |
| --- | --- |
| Id | Req\_AttSur\_ByPass\_009 |
| CC-ID | ADV\_ARC.1.5C |
| Requirement purpose | In case of manipulation or GPDR data, the “need to know concept” needs to be always considered. |
| Additional Information 1 |  |
| Requirement Comment 1 | Consideration of ISO 27701, which completes the 27001 for the RGPD.  The permission to access to a data does not give the right to access it. |
| Requirement Comment 2 | A solution could be the usage Declaration on honor to not access any other data than those required. |
| Requirement Comment 4 | In case of restriction, we can send them from the HMI |

|  |  |
| --- | --- |
| Id | Req\_AttSur\_ByPass\_010 |
| CC-ID | ADV\_ARC.1.5C |
| Requirement purpose | Telemetry data needs to include only generic and no user related data. |
| Additional Information 1 |  |
| Requirement Comment 1 | Already managed with usage of pseudonyms and the aggregation within the RSUs. |

|  |  |
| --- | --- |
| Id | Req\_AttSur\_ByPass\_011 |
| CC-ID | ADV\_ARC.1.5C |
| Requirement purpose | Telemetry data needs to protect privacy (ex.: putting together all data of user cannot permit to discover his behavior) |
| Additional Information 1 |  |
| Requirement Comment 1 | The correlation is already impossible for the data with the identity |

### Error management

The following criteria are related to ADV\_FSP.2.5C (All possible error messages, a TOE might reply on the defined actions above are documented sufficiently and are understandable); For C-ITS CC, it is related to criteria 7 stating: ”For each SFR-enforcing TSFI, the functional specification shall describe direct error messages resulting from processing associated with the SFR-enforcing actions”

|  |  |
| --- | --- |
| Id | Req\_AttSur\_ErrMan\_001 |
| CC-ID | ADV\_FSP.2.5C |
| Requirement purpose | The system needs to implement error management system to catch all error. |
| Additional Information 1 |  |

|  |  |
| --- | --- |
| Id | Req\_AttSur\_ErrMan\_002 |
| CC-ID | ADV\_FSP.2.5C |
| Requirement purpose | In case of showing error to user, no technical information must be displayed |
| Additional Information 1 |  |

|  |  |
| --- | --- |
| Id | Req\_AttSur\_ErrMan\_003 |
| CC-ID | AVA\_VAN.2.2E |
| Requirement purpose | From CMDB (Configuration management database) of system component, a specific technical monitoring needs to list all affected Common Vulnerabilities and Exposures (ex.: libraries). Automated system link snyk.io can be implemented. |
| Additional Information 1 |  |

## **3.3 Documentation requirements**

### Interfaces

The following criteria are related to ADV\_FSP.2.2C (The functional specification shall describe the purpose and method of use for all TSF). For C-ITS CC, it is related to criteria 4 stating : Method of use and purpose of each external logical interface is described sufficiently.

|  |  |
| --- | --- |
| Id | Req\_Doc\_Inter\_001 |
| CC-ID | ADV\_FSP.2.2C |
| Requirement purpose | Each network protocol needs to be detailed with source and destination |
| Additional Information 1 |  |
| Requirement Comment 1 | A solution could be to set the flow matrix of all the used protocols |
| Requirement Comment 2 | To be confirmed if the RGPD matrix of the DIR is sufficient.  This is specific for each deployment, then fall rather on the responsibility of the road operators than the providers?  Check if the flows are protected by the provider by default or through a set of parameters to be configured by the road operator? |
| Requirement Comment 3 | Is the protection profile different for each operator?  This is in contradiction with the idea of having a unique profile used by all. |
| Requirement Comment 4 | The supplier must provide a matrix with generic entities to be provided for all stations. |

|  |  |
| --- | --- |
| Id | Req\_Doc\_Inter\_002 |
| CC-ID | ADV\_FSP.2.2C |
| Requirement purpose | Each network protocols needs to be detailed with generating method |
| Additional Information 1 | Ex: user interaction / system internal workflow |
| Requirement Comment 2 | The source of generation of each of the flows should be known and detailed in the matrix. |

The following criteria are related to ADV\_FSP.2.3C (The functional specification shall identify and describe all parameters associated with each TSFI). For C-ITS CC, it is related to criteria 5 stating : All parameters for each external logical interface shall be described sufficiently.

|  |  |
| --- | --- |
| Id | Req\_Doc\_Inter\_003 |
| CC-ID | ADV\_FSP.2.3C |
| Requirement purpose | All configuration parameters to customize standard behavior needs to be detailed |
| Additional Information 1 |  |

The following criteria are related to ADV\_OPE.1.2C (The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner).For C-ITS CC, it is related to criteria 6 stating : “The use of all available interfaces for each user role is defined sufficiently.”

.”

|  |  |
| --- | --- |
| Id | Req\_Doc\_Inter\_004 |
| CC-ID | AGD\_OPE.1.2C |
| Requirement purpose | Each interface needs to describe user interaction with expected parameters. |
| Additional Information 1 |  |
| Requirement Comment 1 | This is very complex due to the infinite situations, for example in SSH access or in Web admin is difficult to be delimited |
| Requirement Comment 2 | Different accesses are possible: SSH/admin web interface; Tablet interface on the UEVg; etc. |

### Users

The following criteria are related to ADV\_FSP.2.4C (For each SFR-enforcing TSFI, the functional specification shall describe the SFR-enforcing actions associated with the TSFI). For the C-ITS CC, it is related to criteria 6 stating “All actions related to the security relevant behaviour of the TOE are defined sufficiently. (e.g. access rights, used cryptographic algorithms, managed security functionality, ….)”.

|  |  |
| --- | --- |
| Id | Req\_Doc\_User\_001 |
| CC-ID | ADV\_FSP.2.4C |
| Requirement purpose | User’s roles need to be described |
| Additional Information 1 |  |
| Requirement Comment 1 | Different possibilities: no user on the RSU; Root in ssh; web interface for administration; No normal user mode; etc. |
| Requirement Comment 2 | Does all the users have the same permissions than the root? |

|  |  |
| --- | --- |
| Id | Req\_Doc\_User\_002 |
| CC-ID | ADV\_FSP.2.4C |
| Requirement purpose | User’s privileges need to be described |
| Additional Information 1 |  |
| Requirement Comment 1 | Need to specify the different permissions |

|  |  |
| --- | --- |
| Id | Req\_Doc\_User\_003 |
| CC-ID | ADV\_FSP.2.4C |
| Requirement purpose | In case of cryptography usage, related mathematical analysis needs to be added to the documentation corpus |
| Additional Information 1 |  |
| Requirement Comment 1 | Refer to the mathematical concepts related to cryptographic operations |
| Requirement Comment 2 | Is a direct link to Wikipedia for example enough? |

The following criteria are related to AGP\_OPE.1.1C (The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings). For C-ITS CC, it is related to criteria 9 stating : “For each role and interface, all accessible functions and privileges including corresponding warnings and error messages are defined.”

|  |  |
| --- | --- |
| Id | Req\_Doc\_User\_004 |
| CC-ID | AGD\_OPE.1.1C |
| Requirement purpose | The documentation needs to have association between interface and corresponding privilege |
| Additional Information 1 | (ex.: interface #1 requires level 2 privilege) |
| Requirement Comment 1 | The problem is that in general the providers give only two accesses via SSH or web administration and both are allowed to do everything |

The following criteria are related to AGP\_OPE.1.2C (The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner). For the C-ITS CC, it is related to criteria 10 stating : “The use of all available interfaces for each user role is defined sufficiently

|  |  |
| --- | --- |
| Id | Req\_Doc\_User\_005 |
| CC-ID | AGD\_OPE.1.2C |
| Requirement purpose | Each interface needs to describe user interaction with expected parameters. |
| Additional Information 1 |  |
| Requirement Comment 1 | This is very complex due to the infinite situations, for example in SSH access or in Web admin is difficult to be delimited. |
| Requirement Comment 2 | Different accesses are possible: SSH/admin web interface; Tablet interface on the UEVg; etc. |

|  |  |
| --- | --- |
| Id | Req\_Doc\_User\_006 |
| CC-ID | AGD\_OPE.1.2C |
| Requirement purpose | Each interaction with user land needs to be caught with a special process. |
| Additional Information 1 |  |
| Requirement Comment 1 | Using the WEB interface and for each execution of a code, could we imagine that it will be checked on the server befor its execution? |

The following criteria are related to AGP\_OPE.1.3C (The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate). For the C-ITS CC, it is related to criteria 11 stating : “All available functions and the corresponding interface for each user role is documented sufficiently”.

|  |  |
| --- | --- |
| Id | Req\_Doc\_User\_007 |
| CC-ID | AGD\_OPE.1.3C |
| Requirement purpose | The documentation needs to map interface with the minimum level of privilege. |
| Additional Information 1 |  |
| Requirement Comment 1 | In general, SSH is root and WEB user is root also. |

The following criteria are related to AGP\_OPE.1.7C (The operational user guidance shall be clear and reasonable). In C-ITS CC, it is related to criteria 15 stating :” The user guidance is clear and reasonable.”

|  |  |
| --- | --- |
| Id | Req\_Doc\_User\_008 |
| CC-ID | AGD\_OPE.1.7C |
| Requirement purpose | Interfaces need to be user friendly like implementing info popup in case of error |
| Additional Information 1 |  |
| Requirement Comment 1 | This is possible for the Web interface, not for the SSH access. |
| Requirement Comment 2 | An error message could be sent to the console but for bugs only like segmentation error or stack overflow. |

|  |  |
| --- | --- |
| Id | Req\_Doc\_User\_009 |
| CC-ID | AGD\_OPE.1.6C |
| Requirement purpose | Less privilege policy needs to be implemented on the global system |
| Requirement Comment 1 |  |

### Mode of operation

The following criteria are related to AGP\_OPE.1.5C (The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation). In the C-ITS CC, it os related to criteria 13 stating : “All modes of operation of the TOE are defined clearly and understandably, including their consequences (e.g. secure mode, normal operation, …..)”.

|  |  |
| --- | --- |
| Id | Req\_Doc\_Operation\_001 |
| CC-ID | AGD\_OPE.1.5C |
| Requirement purpose | The documentation corpus needs to implement system state change schema |
| Additional Information 1 |  |
| Requirement Comment 1 | Generalize as much as possible to define the main states (those concerning security issues) |
| Requirement Comment 2 | Define a state system and predict all possible states.  Are all the failures to be defined?  What is the level of granularity to be used?  Do we need to aggregate the groups of states or do we need to detail all possible situations? |

### Unique identification

The following criteria are related to ALC\_CMC.2.1C (The TOE shall be labeled with its unique reference). For C-ITS CC, it is related to criteria 19 stating: “The TOE is labelled with a unique reference”.

|  |  |
| --- | --- |
| Id | Req\_Doc\_UniqueID\_001 |
| CC-ID | ALC\_CMC.2.1C |
| Requirement purpose | The system needs to be labeled with a trigram related to its version: MAJOR-MINOR-SUBMINOR |
| Additional Information 1 |  |

The following criterias are related to ALC\_CMC.2.2C (The CM documentation shall describe the method used to uniquely identify the configuration items) and ALC\_CMC.2.3C (The CM system shall uniquely identify all configuration items). For the C-ITS CC they are related to criteria 20 stating : “All configuration items shall be uniquely defined.”

|  |  |
| --- | --- |
| Id | Req\_Doc\_UniqueID\_002 |
| CC-ID | ALC\_CMC.2.2C / ALC\_CMC.2.3C |
| Requirement purpose | Each component configuration needs to be labeled with a trigram related to its version: MAJOR-MINOR-SUBMINOR |
| Additional Information 1 |  |
| Requirement Comment 1 | To be clarified for which level of detail (which configuration elements are concerned) |

|  |  |
| --- | --- |
| Id | Req\_Doc\_UniqueID\_003 |
| CC-ID | ALC\_CMS.2.2C |
| Requirement purpose | Each configuration items can be labeled with unique ID like md5 (name+version) |
| Additional Information 1 |  |
| Requirement Comment 1 | To be clarified for which level of detail (which configuration elements are concerned) |
| Requirement Comment 2 | Each Feature has its own code |

### System

The following criteria are related to ALC\_CMC.2.1C (The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; and the parts that comprise the TOE). For the C-ITS CC, it is related to criteria 21 stating :” The configuration list includes the TOE itself, and all parts the TOE is comprised of”.

|  |  |
| --- | --- |
| Id | Req\_Doc\_System\_001 |
| CC-ID | ALC\_CMS.2.1C |
| Requirement purpose | The documentation of system component needs to be exhaustive |
| Additional Information 1 |  |
| Requirement Comment 1 | Does this concern the supplier or the design office? |

The following criteria are related to ASE\_INT.1.1C (The ST introduction shall contain an ST reference, a TOE reference, a TOE overview and a TOE description). For the C-ITS CC, it is related to criteria 25 stating : “A unique reference of the developer deliverables and the TOE itself is given”.

|  |  |
| --- | --- |
| Id | Req\_Doc\_System\_002 |
| CC-ID | ASE\_INT.1.1C |
| Requirement purpose | Each configuration items can be labeled with unique ID like md5 (name+version) |
| Additional Information 1 |  |

The following criteria are related to ASE\_INT.1.3C (The TOE reference shall uniquely identify the TOE). For the C-ITS CC, it is related to criteria 26 stating “The developer deliverables clearly identify the TOE”.

|  |  |
| --- | --- |
| Id | Req\_Doc\_System\_003 |
| CC-ID | ASE\_INT.1.3C |
| Requirement purpose | The documentation needs to include a dedicated part for presenting the system |
| Additional Information 1 |  |
| Requirement Comment 1 | Model configuration list / CMDB to be provided at national level? |

### CMDB

The following criteria are related to ALC\_CMS.2.3C (For each TSF relevant configuration item, the configuration list shall indicate the developer of the item). For the C-ITS CC, it is related to criteria 23 stating “The configuration list shall indicate the developer of the item”.

|  |  |
| --- | --- |
| Id | Req\_Doc\_CMDB\_001 |
| CC-ID | ALC\_CMS.2.3C |
| Requirement purpose | Each configuration needs to refer developer in comments and in the CMDB |
| Additional Information 1 |  |
| Requirement Comment 1 | Is this model needed to be provided at national level? |
| Requirement Comment 2 | Provide a national template to have a simple document to be managed globally |

The following criteria are related to ASE\_INT.1.6C (The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE). For the C-ITS CC, it os related to criteria 27 stating :” The developer deliverables clearly identify any necessary non-TOE hardware/software/firmware”.

|  |  |
| --- | --- |
| Id | Req\_Doc\_CMDB\_002 |
| CC-ID | ASE\_INT.1.6C |
| Requirement purpose | All component of the system needs to be included in the CMDB |
| Additional Information 1 |  |
| Requirement Comment 1 | Is this Model configuration list/CMDB needed to be provided at national level? |

The following criteria are related to ASE\_INT.1.7C (The ToE description shall describe the physical scope of the ToE.). For the C-ITS CC, it is related to criteria 28 stating “All physical external interfaces are defined”.

|  |  |
| --- | --- |
| Id | Req\_Doc\_CMDB\_003 |
| CC-ID | ASE\_INT.1.7C |
| Requirement purpose | All physical components need to be listed into a CMDB with associated version. If applicable, developer and seller information need to be added. |
| Additional Information 1 |  |
| Requirement Comment 1 | Is this Model configuration list/CMDB needed to be provided at national level? |

|  |  |
| --- | --- |
| Id | Req\_Doc\_CMDB\_004 |
| CC-ID | ASE\_INT.1.7C |
| Requirement purpose | For each physical component, the end-of-life and maintenance program need to be detailed. |
| Additional Information 1 |  |
| Requirement Comment 1 | Is this Model configuration list/CMDB needed to be provided at national level? |

The following criteria are related to ASE\_INT.1.8C (The TOE description shall describe the logical scope of the TOE). For the C-ITS CC, it is related to criteria 29 stating:” All external logical interfaces are defined”.

|  |  |
| --- | --- |
| Id | Req\_Doc\_CMDB\_005 |
| CC-ID | ASE\_INT.1.8C |
| Requirement purpose | All logical components need to be listed into a CMDB with implemented version. If applicable, developer information and Snyk (snyk.io) link needs to be added. |
| Additional Information 1 |  |
| Requirement Comment 1 | Is this Model configuration list/CMDB needed to be provided at national level? |

The following criteria are related to ASE\_INT.1.2E (The evaluator shall confirm that the TOE reference, the TOE overview, and the TOE description are consistent with each other). In the C-ITS CC it is related to criteria 30 stating: “Versioning and naming is consistent through all developer documentations”.

|  |  |
| --- | --- |
| Id | Req\_Doc\_CMDB\_006 |
| CC-ID | ASE\_INT.1.2E |
| Requirement purpose | The CMDB needs to be updated in case of update of the system. |
| Additional Information 1 |  |

|  |  |
| --- | --- |
| Id |  |
| CC-ID | ASE\_INT.1.1C |
| Requirement purpose | The title of documentation needs to include the version of the system. |
| Additional Information 1 |  |

The following criteria are related to ASE\_SPD.1.2C (All threats shall be described in terms of a threat agent, an asset, and an adverse action). For the C-ITS CC, it is related to criteria 37 stating: “All assets are clearly defined”.

|  |  |
| --- | --- |
| Id | Req\_Doc\_CMDB\_007 |
| CC-ID | ASE\_SPD.1.2C |
| Requirement purpose | The CMDB needs to be exhaustive |
| Additional Information 1 | Enumerate all the configs with their values of the different parameters.  Is this enough?  It is not too complex to be done? |

### Security Objectives

The following criteria are related to ASE\_OBJ.2.1C (The statement of security objectives shall describe the security objectives for the TOE and the security objectives for the operational environment). For the C-ITS CC, it is related to criteria 31 stating: “Statement of security objectives for the TOE and for the operation environment”.

|  |  |
| --- | --- |
| Id | Req\_Doc\_SecObj\_001 |
| CC-ID | ASE\_OBJ.2.1C |
| Requirement purpose | The documentation corpus needs to include the Security Assurance Plan |
| Additional Information 1 |  |
| Requirement Comment 1 | Is a model needed to be provided at national level or it is specific for each deployment? |

The following criteria are related to ASE\_REQ.2.9C (The statement of security requirements shall be internally consistent). For the C-ITS CC, it is related to criteria 36 stating : “All statements in security requirement definition is internally consistent”.

|  |  |
| --- | --- |
| Id | Req\_Doc\_SecObj\_002 |
| CC-ID | ASE\_REQ.2.9C |
| Requirement purpose | Each statement of security needs to be associated to applicable referential |
| Additional Information 1 |  |
| Requirement Comment 1 | Associate a unique identifier to each point |

The following criteria are related to ASE\_TSS.1.1C (The TOE summary specification shall describe how the TOE meets each SFR). ;For the C-ITS CC, it is related to criteria 38 stating: “All security objectives for the TOE are implemented in the TOE”.

|  |  |
| --- | --- |
| Id | Req\_Doc\_SecObj\_003 |
| CC-ID | ASE\_TSS.1.1C |
| Requirement purpose | The documentation needs to check if all security objectives have related technical response. |
| Additional Information 1 |  |
| Requirement Comment 1 | Is a model needed to be provided at national level or it is specific for each deployment? |

### Tests

The following criteria are related to ATE\_FUN.1.1C (The test documentation shall consist of test plans, expected test results and actual test results). For the C-ITS CC, it is related to criteria 40 stating : “The developer provided a developer test suite and a corresponding documentation including Test plans, expected results and actual results”.

|  |  |
| --- | --- |
| Id | Req\_Doc\_Test\_001 |
| CC-ID | ATE\_FUN.1.1C |
| Requirement purpose | The documentation corpus needs to include the test plan |
| Additional Information 1 |  |
| Requirement Comment 1 | Who should provide the test plan? Is it the evaluator?  Are the tests common to all suppliers? |

The following criteria are related to ASE\_FUN.1.2C (The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests). For the C-ITS CC, it is related to the criteria 41 stating: “The provided developer test plan identifies the tests and the scenario for performing each tests”.

|  |  |
| --- | --- |
| Id | Req\_Doc\_Test\_002 |
| CC-ID | ATE\_FUN.1.2C |
| Requirement purpose | The test plan, included in the documentation corpus, needs to describe test cases and give testing scripts with corresponding parameters. |
| Additional Information 1 |  |
| Requirement Comment 1 | Who should provide the test plan? Is it the evaluator?  Are the tests common to all suppliers? |

The following criteria are related to ASE\_FUN.1.3C (The expected test results shall show the anticipated outputs from a successful execution of the tests). For the C-ITS CC, it is related to criteria 41 stating :” The expected test results shall show the anticipated outputs from a successful execution of the tests”.

|  |  |
| --- | --- |
| Id | Req\_Doc\_Test\_003 |
| CC-ID | ATE\_FUN.1.3C |
| Requirement purpose | Each test in the test plan needs to give success and fail score. |
| Additional Information 1 |  |
| Requirement Comment 1 | Who should provide the test plan? Is it the evaluator?  Are the tests common to all suppliers? |

The following criteria are related to ASE\_FUN.1.4C (The actual test results shall be consistent with the expected test results). For the C-ITS CC, it is related to criteria 43 stating :” All actual results are consistent with the expected ones, or an appropriate explanation for the deviations is given”.

|  |  |
| --- | --- |
| Id | Req\_Doc\_Test\_004 |
| CC-ID | ATE\_FUN.1.4C |
| Requirement purpose | The test plan needs to be in relation with security objectives |
| Additional Information 1 |  |
| Requirement Comment 1 | Who should provide the test plan? Is it the evaluator?  Are the tests common to all suppliers? |

## **3.4 Installation requirements**

### Installation Steps

The following criteria are related to AGD\_PRE.1.2C (The preparation procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST). In the C-ITS CC, it is related to criteria17 statng :” All steps for secure installation of the TOE and for the secure preparation of the environment are defined sufficiently”.

|  |  |
| --- | --- |
| Id | Req\_Install\_Steps\_001 |
| CC-ID | AGD\_PRE.1.2C |
| Requirement purpose | The installation process needs to implement changing default / hardcoded passwords |
| Additional Information 1 |  |
| Requirement Comment 1 | Need to disable the default passwords. |

|  |  |
| --- | --- |
| Id | Req\_Install\_Steps\_002 |
| CC-ID | AGD\_PRE.1.2C |
| Requirement purpose | The installation process needs to implement “OneTimePassword” elements in case of one-way setup. |
| Additional Information 1 |  |
| Requirement Comment 1 | To be clarified more: probably possible to use a 2 Factor Authentication (2FA), but we may be careful in case of time synchronization problems. |
| Requirement Comment 2 | E.g., “Google Authenticator” could be used to generate passwords valid on a time window for SSH access and/or for the web access as well. However, it needs to be coded and integrated. |

|  |  |
| --- | --- |
| Id | Req\_Install\_Steps\_003 |
| CC-ID | AGD\_PRE.1.2C |
| Requirement purpose | The installation process needs to implement remove / deactivate debug interfaces |
| Additional Information 1 |  |
| Requirement Comment 1 | After the first installation in debug mode, the reboot must switch to non-debug mode and disable all the debug interfaces. |

|  |  |
| --- | --- |
| Id | Req\_Install\_Steps\_004 |
| CC-ID | AGD\_PRE.1.2C |
| Requirement purpose | At the end of the installation process, generic account / anonymous accounts need to be removed or deactivated. |
| Additional Information 1 |  |
| Requirement Comment 1 | The root user must not be reachable after the installation. In case of a problem, a new installation is necessary. |
| Requirement Comment 2 | Removing the root account is not feasible in general, as we understand the requirement, changing the generic password is generally sufficient. |

|  |  |
| --- | --- |
| Id | Req\_Install\_Steps\_005 |
| CC-ID | AGD\_PRE.1.2C |
| Requirement purpose | The installation process needs to implement Bios / bootloader access limitation. This limitation can be physical or logical. |
| Additional Information 1 |  |
| Requirement Comment 1 | Access with password for example. |

|  |  |
| --- | --- |
| Id | Req\_Install\_Steps\_006 |
| CC-ID | AGD\_PRE.1.2C |
| Requirement purpose | The installation process needs to implement read only mode for firmware |
| Additional Information 1 |  |
| Requirement Comment 1 | Generally, C-ITS stations could not use read-only mode, for example: configs change regularly, configs and pseudonyms need regular changes. |

### Preparation

The following criteria are related to AGD\_PRE.1.2C (The evaluator shall apply the preparation procedures to confirm that the TOE can be prepared securely for operation). For the C-ITS CC, it is related to criteria 18 which states: “The TOE can be prepared securely for operation with the defined methods ».

|  |  |
| --- | --- |
| Id | Req\_Install\_Prep\_001 |
| CC-ID | AGD\_PRE.1.2C |
| Requirement purpose | The installation process needs to implement a checklist for all secure installation process |
| Additional Information 1 |  |
| Requirement Comment 1 | An installation procedure must be provided. |

|  |  |
| --- | --- |
| Id | Req\_Install\_Prep\_002 |
| CC-ID | AGD\_PRE.1.2C |
| Requirement purpose | The installation process needs to remove authorization to boot on alternative devices (ex.: USB keys) |
| Additional Information 1 |  |
| Requirement Comment 1 | Using password to access to the u-boot |

## **3.5 Log Management requirements**

The following requirements are related to some others items. The log management is an additional task for the former requirements.

|  |  |
| --- | --- |
| Id | Req\_Log\_Priv\_001 |
| CC-ID | AGD\_OPE.1.3C |
| Requirement purpose | The installation process needs to implement read only mode for firmware |
| Additional Information 1 |  |
| Requirement Comment 1 | Generally, C-ITS stations could not use read-only mode, for example: configs change regularly, configs and pseudonyms need regular changes. |

|  |  |
| --- | --- |
| Id | Req\_Log\_Login\_001 |
| CC-ID | AGD\_PRE.1.2C |
| Requirement purpose | The log system needs to implement success and failure on login |
| Additional Information 1 |  |
| Requirement Comment 1 | This could allow the beginning of compromise detection |

|  |  |
| --- | --- |
| Id | Req\_Log\_ErrID\_001 |
| CC-ID | AGD\_PRE.1.2C |
| Requirement purpose | Each error needs to be labeled with unique ID to easily find them in log system. |
| Additional Information 1 |  |
| Requirement Comment 1 | The equipment must display only few information to the user (useful especially in case of intruder). Error messages should be hidden if they contain sensitive data. |
| Requirement Comment 2 | This need to be implemented in the ITS stack and in each one of the software modules. |

|  |  |
| --- | --- |
| Id | Req\_Log\_Forbid\_001 |
| CC-ID | AGD\_PRE.1.2C |
| Requirement purpose | Non legitimate access to the interface without the required privilege needs to generate log. |
| Additional Information 1 |  |
| Requirement Comment 1 | Physical interfaces can be used in the same way as any other interface. So, they need to be protected also. |
| Requirement Comment 2 | Different accesses are possible: SSH/admin web interface; Tablet interface on the UEVg; etc. |

|  |  |
| --- | --- |
| Id |  |
| CC-ID | ADV\_FSP.2.4C |
| Requirement purpose | The system needs to generate log related to user behavior and privilege usage. |
| Requirement Comment 1 |  |

## **3.6 Input Validation requirements**

The following criteria are related to AGD\_OPE.1.7C which has been described in a former section.

|  |  |
| --- | --- |
| Id | Req\_Input\_Verif\_001 |
| CC-ID | AGD\_OPE.1.7C |
| Requirement purpose | All input needs to be verified before processing them on server side |
| Additional Information 1 |  |
| Requirement Comment 1 | Possible for the web interface, not really for SSH access. |
| Requirement Comment 2 | Mainly doable for the web pages to be checked locally. |

## **3.7 Evaluation requirements**

### Audit

The following criteria are related to ADV\_FSP.2.2E (The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs). In the C-ITS CC, it is related to criteria 8 which states: “The given developer documentation is an accurate and complete instantiation of the SFRs defined at Level 1 evaluation task no. 32 ».

|  |  |
| --- | --- |
| Id | Req\_Eval\_Audit\_001 |
| CC-ID | ADV\_FSP.2.2E |
| Requirement purpose | Evaluator needs to prove usage of well-known methodology |
| Additional Information 1 | (ex.: OWASP / OSSTMM) |
| Requirement Comment 1 | Is this Model configuration list/CMDB needed to be provided at national level? |

|  |  |
| --- | --- |
| Id | Req\_Eval\_Audit\_002 |
| CC-ID | ADV\_FSP.2.2E |
| Requirement purpose | Each evaluation needs to have audit plan and audit criteria |
| Additional Information 1 | (ex.: attacker posture) |
| Requirement Comment 1 | It concerns mainly the evaluator.  Does it concern the supplier or the design office?  If it is the supplier, then this point should be probably developed, or at least explained |

### Process

The following criteria are related to AGD\_PRE.1.1C (The preparation procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures). In the C-ITS CC, it is related to criteria 16 which states: “All steps for the secure acceptance of the delivered TOE in accordance with line 25 are defined”.

|  |  |
| --- | --- |
| Id | Req\_Eval\_Proc\_001 |
| CC-ID | AGD\_PRE.1.1C |
| Requirement purpose | The evaluation process needs to implement referential. |
| Additional Information 1 |  |
| Requirement Comment 1 | This part is mainly for the evaluator and his checking procedures. |

The following criteria are related to ASE\_REQ.2.7C (The security requirements rationale shall demonstrate that the SFRs meet all security objectives for the TOE). In the C-ITS CC, it is related to criteria 34 which states :” The defined SFRs sufficiently cover the SOs for the TOE defined in XXX”

|  |  |
| --- | --- |
| Id | Req\_Eval\_Proc\_002 |
| CC-ID | ASE\_REQ.2.7C |
| Requirement purpose | The evaluation process needs to assess all security objective |
| Additional Information 1 |  |
| Requirement Comment 1 | Provide test plan to prove that the safety objectives were respected. |
| Requirement Comment 2 | Who should provide this? Is it the evaluator or the supplier? |

The following criteria are related to ASE\_REQ.2.8C (The security requirements rationale shall explain why the SARs were chosen). In the C-ITS CC, it is related to criteria 35 which states :” The necessary SARs are clearly defined including the reason why those are chosen”.

|  |  |
| --- | --- |
| Id | Req\_Eval\_Proc\_003 |
| CC-ID | ASE\_REQ.2.8C |
| Requirement purpose | The evaluation process needs to assess all security requirements |
| Additional Information 1 |  |
| Requirement Comment 1 | This point should be common to all suppliers and defined at the national level (it is not the suppliers who will decide the level of security to reach) |
| Requirement Comment 2 | What are the levels of requirements? Who defines them, i.e., the supplier or by the project at national level? |

The following criteria are related to AVA\_VAN.2.2E (The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE). In the C-ITS CC, it is related to criteria 47 which states that “The TOE does not contain any soft- or hardware parts which include relevant critical CVEs (critical according to CVSS:3.0)”.

|  |  |
| --- | --- |
| Id | Req\_Eval\_Proc\_004 |
| CC-ID | AVA\_VAN.2.2E |
| Requirement purpose | Each vulnerability identified during system security evaluation process needs to be associated to Common Vulnerability Scoring System (CVSS) score (ex.: first.org) |
| Additional Information 1 |  |
| Requirement Comment 1 | Does this task concern the evaluator? |

The following criteria are related to AVA\_VAN.2.3E (The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE). In the C-ITS CC, it is related to criteria 48 which states :” The evaluation body performed an independent vulnerability analysis of the TOE based on the knowledge of the TOE derived by all aspects given above”.

|  |  |
| --- | --- |
| Id | Req\_Eval\_Proc\_005 |
| CC-ID | AVA\_VAN.2.3E |
| Requirement purpose | The evaluation process needs to take care about the system documentation. |
| Additional Information 1 |  |
| Requirement Comment 1 | Does this task concern the evaluator? |

The following criteria are related to AVA\_VAN.2.4E (The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential). For the C-ITS CC, it is related to criteria 49 which states: ”The evaluation body conducted penetration testing to the TOE based on identified potential vulnerabilities”.

|  |  |
| --- | --- |
| Id | Req\_Eval\_Proc\_006 |
| CC-ID | AVA\_VAN.2.4E |
| Requirement purpose | The evaluation process needs to be at least a penetration test on black box and grey box mode. |
| Additional Information 1 |  |
| Requirement Comment 1 | To be defined with the evaluators. |

### Security Maintenance

The following criteria are related to ALC.DEL.1.1.C (The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer). For the C-ITS CC, it is related to criteria 24 which states: “The delivery procedure (from production side until start of normal operation of the TOE) shall maintain security of the TOE. (e.g. seal, personal hand-over, fix transportation time, ….) ».

|  |  |
| --- | --- |
| Id | Req\_Eval\_Maint\_001 |
| CC-ID | ALC\_DEL.1.1C |
| Requirement purpose | In case of releasing a minor version, a security audit on changelog needs to be performed before going to production |
| Additional Information 1 |  |
| Requirement Comment 1 | This task could be expensive. |

|  |  |
| --- | --- |
| Id | Req\_Eval\_Maint\_002 |
| CC-ID | ALC\_DEL.1.1C |
| Requirement purpose | In case of releasing a major version, a security audit on global system needs to be performed before going to production |
| Additional Information 1 |  |
| Requirement Comment 1 | This task could be expensive. |

### Tests

The following criteria are related to ATE.COV.1.1C (The evidence of the test coverage shall show the correspondence between the tests in the test documentation and the TSFIs in the functional specification). For the C-ITS CC, it is related to criteria 39 which states : “All external logical interfaces are tested by the developer”.

|  |  |
| --- | --- |
| Id | Req\_Eval\_Test\_001 |
| CC-ID | ATE\_COV.1.1C |
| Requirement purpose | Unit test needs to be developed on each logical interface. |
| Additional Information 1 |  |
| Requirement Comment 1 | think the list as a whitelist and add to the list any scenario found. |
| Requirement Comment 2 | Who should provide the proof of success? Is it the evaluator? |

|  |  |
| --- | --- |
| Id | Req\_Eval\_Test\_002 |
| CC-ID | ATE\_COV.1.1C |
| Requirement purpose | Automated scan using well known scanner like AFL (Amercian Fuzzing Loop) Suite needs to be performed on each logical interface (in case of applicability) |
| Additional Information 1 |  |
| Requirement Comment 1 | A scanner must be adapted to the GeoNet protocol. The objective is to send payloads until it breaks. |
| Requirement Comment 2 | What about other type of interfaces (DATEX, logs, config, etc..)? |
| Requirement Comment 3 | How to assist the evaluator to extract the possible faults. |

The following criteria are related to ATE.IND.2.1C (The TOE shall be suitable for testing.

) and ATE.IND.2.2C (The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF). For the C-ITS CC, it is related to criteria 44 which states:” A TOE suitable for testing and access (physical or remote) to the test environment necessary to perform developer tests is provided to the evaluation body ».

|  |  |
| --- | --- |
| Id | Req\_Eval\_Test\_003 |
| CC-ID | ATE\_IND.2.1C / ATE\_IND.2.2C |
| Requirement purpose | The development process for the system needs to implement testing slots. |
| Additional Information 1 |  |
| Requirement Comment 1 | To be better clarified |

|  |  |
| --- | --- |
| Id | Req\_Eval\_Test\_004 |
| CC-ID | ATE\_IND.2.1C / ATE\_IND.2.2C |
| Requirement purpose | The test slot needs to be done on the version which will be pushed to production. |
| Additional Information 1 |  |

The following criteria are related to ATE.IND.2.2E (The evaluator shall execute a sample of tests in the test documentation to verify the developer test results). For the C-ITS CC, it is related to criteria 45 which states :” The evaluation body repeats a subset of developer tests”.

|  |  |
| --- | --- |
| Id | Req\_Eval\_Test\_005 |
| CC-ID | ATE\_IND.2.2E |
| Requirement purpose | The evaluation process needs to include all developers’ tests |
| Additional Information 1 |  |

The following criteria are related to ATE.IND.2.3E (The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified). For the C-ITS CC, it is related to criteria 46 which states:” The evaluation body performs some independent tests to the TOE”.

|  |  |
| --- | --- |
| Id | Req\_Eval\_Test\_006 |
| CC-ID | ATE\_IND.2.3E |
| Requirement purpose | The evaluation process needs to be done by third party like an audit company |
| Additional Information 1 |  |
| Requirement Comment 1 | Is this about SOG-IS? |

## **3.8 Risk analysis requirements**

The following criteria are related to ASE\_REQ.2.1C (The statement of security requirements shall describe the SFRs and the SARs). For the C-ITS CC, it is related to criteria 32 which states :” All SFRs within the TOE and all SARs are defined”.

|  |  |
| --- | --- |
| Id | Req\_Risk\_Analy\_001 |
| CC-ID | ASE\_REQ.2.1C |
| Requirement purpose | The Security Assurance Plan needs to implement security objective section |
| Additional Information 1 |  |
| Requirement Comment 1 | Is there any model to be provided at the national level? |

|  |  |
| --- | --- |
| Id | Req\_Risk\_Analy\_002 |
| CC-ID | ASE\_REQ.2.1C |
| Requirement purpose | The Security Assurance Plan needs to implement security requirements and associated answer in technical terms |
| Additional Information 1 |  |
| Requirement Comment 1 | Prove that the development is secure and that it takes in consideration the security in the development (security by design). |
| Requirement Comment 2 | Describe here technically everything that has been implemented: how secure boot is implemented, what encryption is used for each communication flow (of which GeoNet is part of, config loading, log sending, etc.) |

The following criteria are related to ASE\_REQ.2.6C (The security requirements rationale shall trace each SFR back to the security objectives for the TOE). For the C-ITS CC, it is related to criteria 33 which states: “All SOs for the TOE are covered by SFRs.”.

|  |  |
| --- | --- |
| Id | Req\_Risk\_Analy\_003 |
| CC-ID | ASE\_REQ.2.6C |
| Requirement purpose | The Security Assurance Plan needs to include map to associate each security objective with a related security requirement. |
| Additional Information 1 |  |
| Requirement Comment 1 | Is there any model to be provided at the national level? |

The following criteria are related to AGD\_OPE.1.4C (The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF). For the C-ITS CC, it is related to criteria 12 which states :” All events/actions that are necessary for the security functionality are clearly defined for each user-role ».

|  |  |
| --- | --- |
| Id | Req\_Risk\_Analy\_004 |
| CC-ID | AGD\_OPE.1.4C |
| Requirement purpose | A risk impact analysis needs to be done on the system. This document must identify threat scenario related to the system |
| Additional Information 1 |  |
| Requirement Comment 1 | Does it concern the supplier or the design office? |
| Requirement Comment 2 | The analysis is required at the project level for all stations. |

|  |  |
| --- | --- |
| Id | Req\_Risk\_Analy\_005 |
| CC-ID | AGD\_OPE.1.4C |
| Requirement purpose | Each threat scenario identified during the risk analysis needs to be associated to log generation system. For example, if two user roles are forbidden, setting role functionality needs to produce detailed log. |
| Additional Information 1 |  |
| Requirement Comment 1 | Does this concern the supplier or the design office? |

# 3. Preliminary risk analysis

These requirements are supposed to protect devices when they are deployed on open roads in normal environments where attackers could be active with regular devices used by “common users”. This protection could be not sufficient if the adversaries use high level devices are those used by strong countries for large scale operations. The actions described in this document may not resist against strong equipements which are able to collect data from very tiny wires on mother board of computers or which could extract private keys from certificates which huge computers using quantic computers.

Main weakness:

* Access to physical connection between HSM and CPU
* Discovering the private key of the Long-Term Certificate of the device
* Discovering of the private key of the secure boot