



## JRC Technical Report

# Security Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS)

*EU C-ITS Security Policy  
Release 3.0 – September 2023.*

This publication is a Technical report by the Joint Research Centre (JRC), the European Commission's science and knowledge service. It aims to provide evidence-based scientific support to the European policymaking process. The contents of this publication do not necessarily reflect the position or opinion of the European Commission. Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use that might be made of this publication. For information on the methodology and quality underlying the data used in this publication for which the source is neither Eurostat nor other Commission services, users should contact the referenced source. The designations employed and the presentation of material on the maps do not imply the expression of any opinion whatsoever on the part of the European Union concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.

Contact information  
Email: [JRC-CPOC@ec.europa.eu](mailto:JRC-CPOC@ec.europa.eu)

EU Science Hub  
<https://joint-research-centre.ec.europa.eu>

JRC133795

Ispra: European Commission 2023

© European Union, 2023



The reuse policy of the European Commission documents is implemented by the Commission Decision 2011/833/EU of 12 December 2011 on the reuse of Commission documents (OJ L 330, 14.12.2011, p. 39). Unless otherwise noted, the reuse of this document is authorised under the Creative Commons Attribution 4.0 International (CC BY 4.0) licence (<https://creativecommons.org/licenses/by/4.0/>). This means that reuse is allowed provided appropriate credit is given and any changes are indicated.

All content © European Union 2023

How to cite this report: "Security Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS) - Release 3.0" European Commission, Ispra, 2023, JRC133795

# Contents

Contents .....	i
Abstract .....	1
1 Introduction.....	2
1.1 Scope and Objectives .....	2
1.2 Target audience .....	2
2 C-ITS Security Policy .....	3
2.1 Information security/cybersecurity management .....	3
2.2 Information classification .....	3
2.3 Risk assessment .....	5
2.3.1 General .....	5
2.3.2 Risk criteria.....	5
2.3.3 Risk identification.....	5
2.3.4 Risk analysis.....	6
2.3.5 Risk evaluation.....	7
2.4 Risk treatment .....	7
2.4.1 General .....	7
2.4.2 Controls for C-ITS stations.....	7
2.4.2.1 Generic controls .....	7
2.4.2.2 Controls for communication between C-ITS stations.....	7
2.4.2.3 Controls for C-ITS stations as an end-entity.....	9
2.4.3 Controls for EU CCMS participants .....	9
2.5 Compliance with this security policy.....	9
3 Conclusions .....	11
List of abbreviations .....	14
List of definitions .....	15
List of tables.....	17

## Abstract

This document is the Security Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS). The purpose of this policy is to provide a framework for the management of information security for the deployment and operation of the European Cooperative Intelligent Transport System (C-ITS). It defines how to manage information security, incl. the definition of security policies for individual stakeholders and the operation of an information security management system. It defines the policy requirements for information security management for all organisational entities that process C-ITS data or manufacture equipment that will process C-ITS data. The C-ITS system is a distributed system with many stakeholders and many actors processing parts of the C-ITS data which makes information security not only a responsibility of the individual organisations but also a joint and shared responsibility.

The document is the Release 3.0 and it is an update of Release 2.0 prepared for the C-ITS Delegated Act proposal in 2019. Release 3.0 is based on the contributions and active review by the members of the Editing Team of the sub-group on Cooperative Intelligent Transport Systems of the Commission Expert Group on Intelligent Transport Systems (E01941).

# 1 Introduction

Since the adoption of the European Commission's Communication COM 2016/766 on "A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility" on 30th of November 2016, the Commission has worked, together with all relevant stakeholders in the C-ITS domain, to steer the development of a common security and certificate policy and other accompanying documents needed for the deployment and operation of C-ITS in Europe.

This document is the Release 3.0 of the Security Policy for Deployment and Operation of European C-ITS, which was approved by the sub-group on Cooperative Intelligent Transport Systems of the Commission Expert Group on Intelligent Transport Systems (E01941) in June 2023.

## 1.1 Scope and Objectives

This document specifies the C-ITS Security Policy in Europe and it has been agreed upon by all involved stakeholders. It is strongly linked to the latest version of the Certificate Policy [1], and together these documents lay the foundation for the deployment of secure and interoperable C-ITS services in Europe. More specifically, the Security Policy aims to provide a framework for the management of information security for the deployment and operation of the European C-ITS. It defines how to manage information security, incl. the definition of security policies for individual stakeholders and the operation of an information security management system.

C-ITS services are cooperative per definition and therefore often require a complete trust chain from start to end of the respective service. The trust elements that are not part of the C-ITS domain (i.e. those elements not defined in [1], [2], [3], [4], [5], [6]) are outside the scope of this document. The intention is to cover these external trust elements in later policies if needed.

After an introduction presenting the policy context and the overall content, the core of the Security Policy (Chapter 2) is divided into five sub-chapters, providing information on:

- The Information security/cybersecurity management system to be operated by the C-ITS station operations;
- Minimum requirements for information classification;
- The risk assessment to be periodically conducted;
- Risk treatment;
- The certification needed to be compliant with this Security Policy.

A brief outlook on the impact of this work and future actions is also provided at the end of the document. Indeed, this Security Policy is subject to future change and will hence be updated whenever required and consequently published as a new release.

## 1.2 Target audience

The target audience of this document are all the stakeholders involved in the deployment and operation of C-ITS in Europe, including the European Commission, Member States' competent authorities, notably the Ministries for Transport, road infrastructure operators responsible, vehicle manufacturers implementing and deploying C-ITS, C-ITS station manufacturers, C-ITS PKI service providers, and sectorial/Industry associations (e.g. Car2Car Communication Consortium, C-ROADS).

## 2 C-ITS Security Policy

### 2.1 Information security/cybersecurity management

- (1) C-ITS station operators shall operate a certified information security management system according to ISO-27001 [7] that ensures the security of all of their C-ITS stations and the processed data.

Instead of the ISMS [7], vehicle C-ITS stations may be covered by a CSMS that is certified in accordance with UN Regulation 155 [8] and EU Regulation 2022/1398 [9]. Systems and infrastructure that are not covered by the CSMS (including all interfaces) and that process data from C-ITS trust model elements [1] shall be certified against ISO-27001 [7].

C-ITS Station operators that operate an essential road transport service according to the NIS [10] or NIS 2 [11] Directives may apply the security measures and security requirements defined by the national transposition of the NIS [10] or NIS 2 [11] Directives instead.

- (2) The scope of the management system (ISMS/CSMS) shall include all the operated C-ITS stations.
- (3) C-ITS station operators shall determine external and internal issues relevant to C-ITS, including:
  - COM(2016) 766 final [12];
  - the GDPR [13].
- (4) C-ITS station operators shall determine the parties that are relevant to the ISMS/CSMS, including all relevant C-ITS stakeholders, and the relevant requirements of those interested parties.
- (5) C-ITS station operators shall ensure that their applicable security/cybersecurity policies are consistent with this policy.

C-ITS station operators shall ensure that their security objectives include and are consistent with the security objectives (as per Table 1) and high-level requirements in this policy.

- (6) C-ITS station operators shall classify the information referred to in section 2.2, and shall use this classification as input to the risk management strategy.
- (7) C-ITS station operators shall apply an security risk assessment process as set out in section 2.3 at planned intervals or when significant changes are proposed or occur.
- (8) C-ITS station operators shall ensure that requirements are determined for treating security risks identified in the security risk assessment process, according to section 2.4.
- (9) C-ITS station operators shall ensure that C-ITS stations are designed, developed and assessed so as to ensure that they meet applicable requirements in [2] and [3].
- (10) C-ITS station operators shall operate C-ITS stations and all other information-processing systems that implement appropriate security risk treatment controls according to section 2.4

### 2.2 Information classification

This section lays down the minimum requirements for information classification. This does not prevent any C-ITS stakeholder from applying more stringent requirements.

C-ITS station operators shall classify handled information. The acceptable values for potential impact are low, moderate and high, as summarised Table 1.

Table 1: Potential impact definitions for each security objective of confidentiality, integrity and availability

Security objective	Potential impact		
	LOW	MODERATE	HIGH
<b>Confidentiality</b> Preserving authorised restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information	The unauthorised disclosure of information could be expected to have a limited adverse effect on organisational operations, organisational assets or individuals.	The unauthorised disclosure of information could be expected to have a serious adverse effect on organisational operations, organisational assets or individuals.	The unauthorised disclosure of information could be expected to have a severe or catastrophic adverse effect on organisational operations, organisational assets or individuals.
<b>Integrity</b> Guarding against improper information modification or destruction; this includes ensuring information non-repudiation and authenticity	The unauthorised modification or destruction of information could be expected to have a limited adverse effect on organisational operations, organisational assets or individuals.	The unauthorised modification or destruction of information could be expected to have a serious adverse effect on organisational operations, organisational assets or individuals.	The unauthorised modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organisational operations, organisational assets or individuals.
<b>Availability</b> Ensuring timely and reliable access to and use of information	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organisational operations, organisational assets or individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organisational operations, organisational assets or individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organisational operations, organisational assets or individuals.

- (11) The following information classification impact types shall be considered in terms of the degree of damage or costs to the C-ITS service and C-ITS stakeholders caused by an security incident:
- safety — where the impact places road users or any of the C-ITS stakeholders at imminent risk of injury;
  - operational impacts — where the impact is substantially negative for road traffic efficiency, or other societal impact such as environmental footprint and organised crime;
  - financial — where the impact results in direct or indirect monetary costs for one or more of the C-ITS stakeholders;
  - privacy – the GDPR having both legal and financial impact;
- (12) C-ITS stakeholders shall respect the following minimum impact values for the information handled:

Table 2: Impacts

	Information originated by fixed C-ITS stations	Information originated by mobile C-ITS stations
Confidentiality	CAM: low DENM: low IVIM: low MAPEM: low SPATEM: low SSEM: low	CAM: low DENM: low SREM: low personal data contained in any of the three messages: moderate
Integrity	CAM: moderate DENM: moderate IVIM: moderate MAPEM: moderate SPATEM: moderate SSEM: moderate	CAM: moderate DENM: moderate SREM: moderate
Availability	CAM: low DENM: low IVIM: low MAPEM: low SPATEM: low SSEM: moderate	CAM: low DENM: low SREM: moderate

## 2.3 Risk assessment

### 2.3.1 General

- (13) Risk assessment shall be periodically conducted. It shall include appropriate documentation of:
- the scope of the risk assessment, i.e. the system being assessed and its boundaries and system purpose, and the information that is handled;
  - the risk criteria;
  - risk assessment, including risk identification, analysis and evaluation.

### 2.3.2 Risk criteria

- (14) Risk impact criteria to be used to assess the impact of the incident/threat scenarios shall be determined in the light of the information classification impact types referred to in section 2.2.
- (15) Risk acceptance criteria shall include the identification of risk levels that are unacceptable, by including the criteria in 2.3.5.

### 2.3.3 Risk identification

- (16) C-ITS station operators shall identify risks in accordance with the guidelines of ISO/IEC 27005 [14] or ISO/SAE 21434 [15]. The following minimum requirements shall apply:
- the main assets to be protected are C-ITS messages as referred to in section 2.1;



- supporting assets should be identified, including:
  - information used for C-ITS messages (e.g. local dynamic map, time, protocol control, etc.);
  - C-ITS stations and their software, configuration data and associated communication channels;
  - central C-ITS control assets;
  - relevant entities within the EU CCMS;
- threats to those assets under the control of the C-ITS station operator, and their sources, shall be identified;
- existing and planned controls shall be identified;
- vulnerabilities that can be exploited by threats to cause harm to assets or to the C-ITS stakeholders shall be identified and described as incident/threat scenarios;
- the possible consequences of security incidents/threats on the assets shall be identified on the basis of the information classification.

#### 2.3.4 Risk analysis

(17) The following minimum requirements apply to risk analysis:

- the impact of the identified security incidents on the C-ITS service and the C-ITS stakeholders shall be assessed on the basis of the information and information system security category, using at least the three levels set out in section 2.2;

The highest level shall be taken as total impact;

- the likelihood of the identified incident/threat scenarios shall be assessed using at least the following three levels:
  - unlikely (value 1) – the incident/threat scenario is unlikely to occur / difficult to realise or the motivation for an attacker is very low;
  - possible (value 2) – the incident/threat scenario may occur/ is possible to realise or the motivation for an attacker is reasonable;
  - likely (value 3) – the incident/threat scenario is likely to occur / easy to realise and the motivation for an attacker is high;
- the levels of risk shall be determined for all identified incident/threat scenarios on the basis of the product of impact and likelihood, resulting in at least the following risk levels: low (values 1,2), moderate (values 3,4) and high (values 6,9), defined as follows:

Table 3: Risk levels

Risk levels as product of impact and likelihood		Likelihood		
		unlikely (1)	possible (2)	likely (3)
Impact	low (1)	low (1)	low (2)	moderate (3)
	moderate (2)	low (2)	moderate (4)	high (6)
	high (3)	moderate (3)	high (6)	high (9)

### 2.3.5 Risk evaluation

- (18) Levels of risk shall be compared against risk acceptance criteria to determine what risks shall be subject to treatment. At least moderate- or high-level risks applicable to the C-ITS service and C-ITS network shall be treated, according to section 2.4

## 2.4 Risk treatment

### 2.4.1 General

- (19) Risks shall be treated in one of the following ways:
- risk modification by using controls identified in section 2.4.2 or 2.4.3, so that the residual risk can be reassessed as being acceptable;
  - risk retention (where the level of risk meets the risk acceptance criteria);
  - risk avoidance;
  - risk sharing or transfer.
- (20) Risk sharing or transfer to mitigate risk shall not be transferred to other actors in the C-ITS network in such a way as to create unacceptable residual risks.
- (21) Risk treatment shall be documented according to the applicable standard.

### 2.4.2 Controls for C-ITS stations

#### 2.4.2.1 *Generic controls*

- (22) C-ITS stations shall implement appropriate countermeasures to mitigate risk, according to section 2.4.1. Those countermeasures should implement controls as defined in ISO/IEC 27001 and ISO/IEC 27002 or in Annex 5 of UN Regulation 155 [8] for vehicle C-ITS stations.

#### 2.4.2.2 *Controls for communication between C-ITS stations*

- (23) The following minimum mandatory controls shall be implemented on the sender side:

Table 4: Controls on the sender side

	Information originated by fixed C-ITS stations	Information originated by mobile C-ITS stations
Confidentiality	-	The personal data contained in messages shall be secured using an adequate AT change procedure to ensure a level of security adequate to the risk of re-identification of drivers based on their transmitted data. Therefore, C-ITS stations shall change ATs adequately when sending messages and shall not re-use ATs after a change, except in cases of non-average <sup>1</sup> driver behaviour.
Integrity	C-ITS messages shall be signed in accordance with TS 103 097 [4].  In cases where C-ITS stations communicate with each other over IP (internet protocol), any of the C-ITS stations may use ETSI ITS certificates and session security based on a future ETSI ITS standard (when available) profiling ISO 21177 [5].	C-ITS messages shall be signed in accordance with TS 103 097 [4].  In cases where C-ITS stations communicate with each other over IP (internet protocol), any of the C-ITS stations may use ETSI ITS certificates and session security based on a future ETSI ITS standard (when available) profiling ISO 21177 [5].
Availability	-	-

(24) The following minimum mandatory controls shall be implemented on the receiver side:

Table 5: Controls on the receiver side

	Information originated by fixed C-ITS stations	Information originated by mobile C-ITS stations
Confidentiality		Received messages containing personal data shall be treated in compliance with GDPR.
Integrity	The integrity of C-ITS messages used by ITS applications shall be validated in accordance with TS 103 097 [4].  In cases where C-ITS stations communicate with each other over IP (internet protocol), any of the C-ITS stations may use ETSI ITS certificates and session security based on a future ETSI ITS standard (when available) profiling ISO 21177 [5].	The integrity of C-ITS messages used by ITS applications shall be validated in accordance with TS 103 097 [4].  In cases where C-ITS stations communicate with each other over IP (internet protocol), any of the C-ITS stations may use ETSI ITS certificates and session security based on a future ETSI ITS standard (when available) profiling ISO 21177 [5].
Availability	-	A received SREM shall be processed and produce an SSEM broadcast to the originator of the SREM.

<sup>1</sup> The definition of average driving behaviour shall be based on relevant statistical analysis of the driving behaviour in the European Union, e.g. based on data from the German Aerospace Centre (DLR).

- (25) To support the security requirements of confidentiality, integrity and availability set out in the tables above, C-ITS station operators shall operate C-ITS stations that have been assessed and certified using security assessment criteria against a certified protection profile as specified in the 'common criteria'<sup>2</sup> / ISO 15408 [16] and approved by the CPA. Due to the different features of the different types of C-ITS station and different location privacy requirements, different protection profiles may be defined.

Only as long as C-ITS station protection profiles certified against 'common criteria' / ISO 15408 [16] are not yet available, C-ITS station operators shall be allowed to have their C-ITS stations assessed and certified against a security target with a similar or higher evaluation assurance level (EAL 2+ or higher) instead. C-ITS station operators may still operate C-ITS stations (type/model/version) that have been certified this way after a protection profile has been certified.

The list of CPA approved C-ITS station protection profiles (and security targets with a similar or higher evaluation assurance level) and associated services will be maintained in an annex published on the same website as this policy.

- (26) All protection profiles and related documents applicable for the security certification of the C-ITS stations shall be evaluated, validated and certified according to ISO 15408 [16], applying the Mutual Recognition Agreement of information technology security evaluation certificates of the Senior Officials Group on Information Systems Security (SOG-IS)<sup>3</sup>, or an equivalent European cybersecurity certification scheme under the relevant European cybersecurity framework. In the development of such protection profiles, the scope of the security certification of the C-ITS station may be defined by the manufacturer, subject to assessment and approval of the CPA and a SOG-IS conformity assessment body or at least equivalent as described in the next paragraph.
- (27) Security certificates for C-ITS stations shall be issued under the common criteria certification scheme (ISO 15408 [16]) by a conformity assessment body recognised by the management committee in the framework of the SOG-IS agreement, or issued by a conformity assessment body accredited by a national cybersecurity certification authority of a Member State. Such a conformity assessment body shall provide at least equivalent conditions of security evaluation as envisaged by the SOG-IS Mutual Recognition Agreement.

#### 2.4.2.3 Controls for C-ITS stations as an end-entity

- (28) C-ITS stations shall comply with the applicable requirements of the certificate policy [1] according to their role as an EU CCMS end-entity.
- (29) In addition to the provisions of the NIS 2 Directive [11], C-ITS stakeholders shall establish a procedure for the coordinated management of security incidents with potential impact on the C-ITS service delivery or other stakeholders. C-ITS station shall provide a set of logging evidence for security-related events for the incident analysis.

#### 2.4.3 Controls for EU CCMS participants

- (30) EU CCMS participants shall comply with the certificate policy [1] according to their role in the EU CCMS.

### 2.5 Compliance with this security policy

- (31) Consistently with 2.1 (1), C-ITS station operators shall maintain a valid certification for compliance with this policy following the guidelines for an ISO 27001 audit [17] or the certification process of a CSMS according to UN Regulation 155 [8] for vehicle C-ITS stations or a valid evaluation for compliance for the road operators subject to the NIS [10] and NIS 2 [11] Directives.

---

<sup>2</sup> 'Common criteria' portal: <http://www.commoncriteriaportal.org/cc/>

<sup>3</sup> In the road transport sector, SOG-IS has already been involved in the smart tachograph security certification, for example. The SOG-IS Agreement is currently the only scheme in Europe that can support the harmonisation of security certification of electronic products. At this stage, SOG-IS supports only the 'common criteria' process, so the C-ITS stations must be assessed and certified according to the 'common criteria'; see <https://www.sogis.org/>

- (32) Consistently with 2.1 (1), the auditing body for this policy shall be accredited and certified by a member of European Accreditation against ISO 27001 [7] and ISO 27006 [18], or it shall be a Technical Service accredited for UN Regulation 155 [8] under EU Regulation 2018/858 [19] (article 73), or it shall be an auditing body accredited by National Authorities for compliance evaluation
- (33) against the NIS [10] and NIS 2 [11] Directives.

### 3 Conclusions

The contents of Release 3.0 of the Security Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS) were approved by the sub-group on Cooperative Intelligent Transport Systems of the Commission Expert Group on Intelligent Transport Systems (E01941) in June 2023.

The aim of this document is to lay down, together with the Certificate Policy, the rules of the European Union C-ITS Security Credential Management System (EU CCMS), the common trust model for the exchange of C-ITS messages. The information contained in this document is expected to have a positive impact on the whole C-ITS ecosystem, providing clear rules and guidelines especially to C-ITS stations manufactures and operators, for their certification and deployment, meeting the IT security and privacy highest requirements.

Until a dedicated entity is appointed as C-ITS Certificate Policy Authority (CPA), the sub-group on Cooperative Intelligent Transport Systems of the Commission Expert Group on Intelligent Transport Systems (E01941) will continue to manage future updates of this policy.

The latest version of this document is published online in the documentation section of the C-ITS Point of Contact website: <https://cpoc.jrc.ec.europa.eu/Documentation.html>

## References

The following references are used in this Security Policy:

- [1] European Commission, “Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS), Release 3.0,” 2023.
- [2] *C-ROADS Harmonised C-ITS specifications for Europe - Release 2.0 or newer.*
- [3] Car 2 Car Communication Consortium, “Basic System Profile - v1.6 or newer,” [Online]. Available: <https://www.car-2-car.org/documents/basic-system-profile/>.
- [4] European Telecommunications Standards Institute, *ETSI TS 103 097 V1.4.1 or V2.1.1. Intelligent transport systems (ITS) security; security header and certificate formats.*
- [5] International Organization for Standardisation, *ISO/TS 21177:2019 Intelligent transport systems — ITS station security services for secure session establishment and authentication between trusted devices*, Geneva, Switzerland, 2019.
- [6] European Telecommunications Standards Institute, *ETSI EN 302 665 V1.1.1 Intelligent transport systems (ITS), Communications architecture.*
- [7] International Organization for Standardization, “ISO/IEC 27001:2022: Information technology — security techniques – information security management systems – requirements,” Geneva, Switzerland, 2022.
- [8] *UN Regulation No 155 – Uniform provisions concerning the approval of vehicles with regards to cybersecurity and cybersecurity management system [2021/387]*, OJ L 82/30, 2021.
- [9] Commission Delegated Regulation (EU) 2022/1398 of 8 June 2022 amending Regulation (EU) 2019/2144 of the European Parliament and of the Council to take into account technical progress and regulatory developments concerning amendments to Vehicle Regulations, adopted in the context of the United Nations Economic Commission for Europe, OJ L 213/1, 2022.
- [10] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. (NIS Directive), OJ L 194/1, 2016.
- [11] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148. (NIS 2 Directive), OJ L 333/80, 2022.
- [12] European Commission, *A European strategy on cooperative intelligent transport systems – a milestone towards cooperative, connected and automated mobility*, COM(2016) 766, 30 November 2016.
- [13] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L119/1, 2016.
- [14] International Organization for Standardization, “ISO/IEC 27005:2022 Information technology – security techniques – information security risk management,” Geneva, Switzerland, 2022.
- [15] International Organization for Standardization, “ISO/SAE 21434:2021: Road vehicles — Cybersecurity engineering,” Geneva, Switzerland, 2021.

- [16] International Organization for Standardization, *ISO 15408-1:2022: Information security, cybersecurity and privacy protection - Evaluation criteria for IT security / Common Criteria*, Geneva, Switzerland, 2022.
- [17] International Organization for Standardization, *ISO/IEC 27007:2020 Information technology — Security techniques — Guidelines for information security management systems auditing*, Geneva, Switzerland, 2020.
- [18] International Organization for Standardization, *ISO/IEC 27006:2015 Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems*, Geneva, Switzerland, 2015.
- [19] Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC (Text with EEA relevance), OJ L 151/1.
- [20] International Organization for Standardization, “ISO/IEC 27000:2022: Information security, cybersecurity and privacy protection — Information security controls,” Geneva, Switzerland, 2022.



## List of abbreviations

C-ITS	Cooperative Intelligent Transport Systems
CAM	Cooperative Awareness Message
CP	Certificate Policy
CPA	Certificate Policy Authority
CSMS	Cybersecurity Management System
DENM	Decentralised Environmental Notification Message
EU CCMS	European Union C-ITS Security Credential Management System
ISMS	Information Security Management System
IVIM	Infrastructure-to-Vehicle Information Message
MAPEM	MAP (topology) Extended Message
SPATEM	Signal Phase and Timing Extended Message
SREM	Signal Request Extended Message
SSEM	Signal Request Status Extended Message

## List of definitions

Availability	Being accessible and usable on demand by an authorised entity (ISO 27000) [20]
C-ITS	(or cooperative intelligent transport systems) is defined as intelligent transport systems that enable ITS users to cooperate by exchanging secured and trusted C-ITS messages using the EU C-ITS security credential management system.
C-ITS messages	<p>Protocol data units that comply with [2] and [3]:</p> <ul style="list-style-type: none"> <li>- CAM</li> <li>- DENM</li> <li>- IVIM</li> <li>- SPATEM</li> <li>- MAPEM</li> <li>- SSEM</li> <li>- SREM</li> </ul> <p>Others to be added in the future</p> <p>Note: C-ITS Messages are sent by C-ITS stations that implement the requirements of [2] or [3].</p>
C-ITS service	An ITS service provided through C- ITS messages
C-ITS station	A set of hardware and software components required to generate and transmit and/or receive, collect, store, and process secured and trusted C-ITS messages in order to enable the provision of a C-ITS service. This includes personal, central, vehicle and roadside ITS stations as defined in EN 302 665 [6]
C-ITS station operator	The organisation that is responsible for monitoring and controlling the operation of one or more C-ITS Stations in order to provide a C-ITS service
C-ITS infrastructure	System of facilities, equipment and applications needed for the operation of an organisation that provides C-ITS services related to central or fixed C-ITS stations
C-ITS stakeholders	Individual, group or organisation with a role and responsibility in the C-ITS network
Confidential information	Information that is not to be made available or disclosed to unauthorised individuals, entities or processes (ISO 27000) [20]
Central C-ITS station	It is realized by a set of hardware and/or software components installed in the backoffice of the C-ITS service provider e.g. a Traffic Management Center or a Fleet Management Center
Fixed C-ITS station	It means a C-ITS station installed in a central system or roadside infrastructure
Information security	Preservation of the confidentiality, integrity and availability of information (ISO 27000) [20]
Information security incident	An unwanted or unexpected information security event, or series of events, that has a significant probability of compromising business operations and threatening information security
Integrity	Property of accuracy and completeness (ISO 27000) [20]

Local dynamic map (LDM)	An in-vehicle C-ITS station's dynamically updated repository of data relating to local driving conditions; it includes information received from on-board sensors and from CAM and DENM messages
Mobile C-ITS station	It means a C-ITS station installed in a vehicle (e.g. also a roadworks warning trailer) or a personal device.
Protocol control	The protocol control assets select an appropriate message transfer protocol for an outgoing message request and send the message to the lower layers of the protocol stack in a format that can be processed by those layers. Incoming messages are converted into a format that can be handled within the C-ITS station and passed to the relevant functional asset for further processing
Risk analysis	Process to comprehend the nature of risk and to determine the level of risk
Risk assessment	Overall process of risk identification, risk analysis and risk evaluation (ISO 27000) [20]
Risk evaluation	Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable (ISO 27000) [20]
Risk identification	Process of finding, recognizing and describing risks (ISO 27000) [20]
Risk criteria	Terms of reference against which the significance of risk is evaluated (ISO 27000) [20]
Risk treatment	Process to modify risk (ISO 27000) [20]

## List of tables

Table 1: Potential impact definitions for each security objective of confidentiality, integrity and availability.....	4
Table 2: Impacts.....	5
Table 3: Risk levels.....	6
Table 4: Controls on the sender side .....	8
Table 5: Controls on the receiver side.....	8

## GETTING IN TOUCH WITH THE EU

### In person

All over the European Union there are hundreds of Europe Direct centres. You can find the address of the centre nearest you online ([european-union.europa.eu/contact-eu/meet-us\\_en](https://european-union.europa.eu/contact-eu/meet-us_en)).

### On the phone or in writing

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

- by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),
- at the following standard number: +32 22999696,
- via the following form: [european-union.europa.eu/contact-eu/write-us\\_en](https://european-union.europa.eu/contact-eu/write-us_en).

## FINDING INFORMATION ABOUT THE EU

### Online

Information about the European Union in all the official languages of the EU is available on the Europa website ([european-union.europa.eu](https://european-union.europa.eu)).

### EU publications

You can view or order EU publications at [op.europa.eu/en/publications](https://op.europa.eu/en/publications). Multiple copies of free publications can be obtained by contacting Europe Direct or your local documentation centre ([european-union.europa.eu/contact-eu/meet-us\\_en](https://european-union.europa.eu/contact-eu/meet-us_en)).

### EU law and related documents

For access to legal information from the EU, including all EU law since 1951 in all the official language versions, go to EUR-Lex ([eur-lex.europa.eu](https://eur-lex.europa.eu)).

### Open data from the EU

The portal [data.europa.eu](https://data.europa.eu) provides access to open datasets from the EU institutions, bodies and agencies. These can be downloaded and reused for free, for both commercial and non-commercial purposes. The portal also provides access to a wealth of datasets from European countries.

# Science for policy

The Joint Research Centre (JRC) provides independent, evidence-based knowledge and science, supporting EU policies to positively impact society



**EU Science Hub**

[joint-research-centre.ec.europa.eu](https://joint-research-centre.ec.europa.eu)



@EU\_ScienceHub



EU Science Hub - Joint Research Centre



EU Science, Research and Innovation



EU Science Hub



@eu\_science