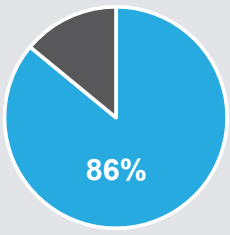
Cyber Security Signposting Guidance

We are entering into a world where equipment in vehicles and on the road can communicate with each other and in turn exchange vast amounts of data. This data and digitally rich environment offers great potential but also exposes us to huge risks, particularly that of cyber attacks. The impact of a security breach could be devastating, with incorrect information and unavailability of technology resulting in dangerous scenarios or potential fatalities.

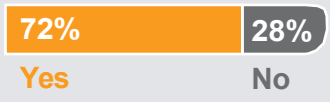
It is now of critical importance that global standards related to cyber secure systems are fully understood and included in any procurement and maintenance activities. New cyber standards are being published almost monthly. However, in addition to standards, there are various other online resources available for reference. These are divided in 4 categories, named as “ITS-Intelligent Transport Systems”, “Vehicles”, “Communication” and “General”.
Signposting to these has been developed to help you navigate these resources.

A survey conducted at the TTF Conference March 2020*

Does cyber security worry you?



Is it difficult to find cyber-related information for your procurement needs?



**Response from 150+ delegates at TTF Conference March*

Why is this important?

- To help you navigate through the numerous online resources related to cyber in ITS
- To enable design, procurement, implementation and maintenance of cyber secure solutions
- To demonstrate to peers, support teams and vendors that you understand the importance of cyber safe solutions
- To ensure that our roads are cyber secure now and in the years to come

What is in the repository?

- The repository is a collation of various online resources including standards, guidelines, certifications, frameworks and directives
- Resources referenced include BSI, EN, ISO, ESTI, ITU, IEEE, NEMA, IEC
- Categorisation of resources based on the ITS eco-system (vehicle, infrastructure, communications) to help you navigate through the various resources

How can it be used?

- In procurement and vendor discussions
- In cyber baseline requirements
- In specifying equipment and maintenance
- For bench-marking against best practice when determining the best solution

Department for Transport

TRANSPORT TECHNOLOGY FORUM

ARUP

Signposted repository for cyber security resources related to ITS

REF#	CATEGORY	IDENTIFIER & TITLE	DESCRIPTION	LOCATION
1	ITS - Operations	**ISO 14827-1:2005 (ISO Standard)**	**ISO 14827-1:2005 Transport information and control systems — Data interfaces between centres for transport information and control systems — Part 1:** Message definition requirements Defines the format that should be used to document those end-application messages that are to be exchanged between/among central systems. The format is protocol-independent to the extent practical. For example, this one format can be used to define data exchanges that may apply to DATEX-ASN, CORBA, or other Application Protocols.	https://www.iso.org/standard/41361.html
2	ITS - Operations	**NEMA TS 8-2018 (NEMA Standard)**	**NEMA TS 8** addresses the following areas of concern: physical security, local access security, communications security (between field and central system), and central system security. For each of these areas, NEMA TS 8 identifies potential threat areas and the severity of their consequences, prevention and mitigation techniques that manufacturers can use to minimize their impacts, and methods to effectively rate security performance.	https://www.techstreet.com/nema/standards/nema-ts-8-2018?product_id=2012417#-jumps
3	Vehicles - GRC	**J3061_201601 (SAE Guideline)**	**Cybersecurity Guidebook for Cyber-Physical Vehicle Systems** This recommended practice establishes a set of high-level guiding principles for Cybersecurity as it relates to cyber-physical vehicle systems.	https://www.SAE.org/standards/content/j3061_201601/
4	Vehicles - Operations	**J3101_202002 (SAE Standard)**	**Hardware Protected Security for Ground Vehicles** This document presents a common set of requirements to be implemented in hardware-assisted functions to facilitate security-enhanced applications, to achieve an ideal system for hardware protection for ground vehicle applications.	https://www.SAE.org/standards/content/j3061_201601/
5	Vehicles - GRC	**DOT HS 812 073 (NIST Framework)**	**NIST - Cybersecurity Risk management framework applied to modern vehicles** The objective of this paper is to review the National Institute of Standards and Technology guidelines and foundational publications for cybersecurity risk management. This paper is a primer that provides an examination of cybersecurity risk management topics and is intended to provide readers with a better understanding of the NIST approach to cybersecurity. This NIST approach is often used as a baseline in industries and sectors to develop a more targeted risk management approach for the specific use cases and issues in those industries and sectors. This paper will establish for readers a baseline conceptual understanding of the NIST approach with foundational documents to establish a common vocabulary for discussing risk management for the vehicle sector.	https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/812073_natlinstitstandardstechcyber.pdf
6	Vehicles - GRC	**DOT HS 812 075 (NHTSA Guideline)**	**A Summary of Cybersecurity Best Practices** The National Highway Traffic Safety Administration performed a review of cybersecurity best practices and lessons learned in the area of safety-critical electronic control systems. This review was across a variety of industries in which electronic control systems are used in applications where breaches in cybersecurity could impinge on critical control functions and therefore could jeopardize safety of life.	https://www.hsdl.org/?view&-did=806518
7	Vehicles - Data Security	**ISO 24534-4:2010 (ISO Standard)**	**ISO 24534-4:2010 Automatic vehicle and equipment identification — Electronic registration identification (ERI) for vehicles — Part 4: Secure communications using asymmetrical techniques** Provides requirements for electronic registration identification (ERI) that are based on an identifier assigned to a vehicle (e.g. for recognition by national authorities) suitable to be used for: • electronic identification of local and foreign vehicles by national authorities; • vehicle manufacturing, in-life maintenance and end-of-life identification (vehicle life cycle management); • Adaptation of vehicle data (e.g. for international resales); • safety-related purposes; • crime reduction; • commercial services.	https://www.iso.org/standard/51852.html?browse=tc
8	Vehicles - Operations	**PAS 1881:2020 (BSI Standard)**	**Assuring the Safety of Automated Vehicle Trials and Testing - Specification** It is intended to support the safe testing and trials of CAVs. PAS 1881 specifies minimum requirements for safety cases for automated vehicle trials and development testing in the UK to demonstrate activities can be undertaken safely. This PAS is relevant to stakeholders including (but not limited to) trialling organizations, local authorities, highway authorities, road operators, landowners, leaseholders, insurers, test beds and licensing agencies.	https://www.bsigroup.com/en-GB/CAV/pas-1881/

REF#	CATEGORY	IDENTIFIER & TITLE	DESCRIPTION	LOCATION
9	Vehicles - Data Security	**ISO 15031-7:2013 (ISO Standard)**	**ISO 15031-7:2013 Road vehicles — Communication between vehicle and external equipment for emissions-related diagnostics — Part 7: Data link security** ISO 15031-7:2013 gives guidelines for the protection of road vehicle modules from unauthorized intrusion through a vehicle diagnostic data link. These security measures offer vehicle manufacturers the flexibility to tailor their security to their own specific needs and do not exclude other, additional measures.	https://www.iso.org/standard/62489.html
10	ITS - Data Security	**ISO 16461:2018 (ISO Standard)**	**ISO 16461:2018 Intelligent transport systems** — Criteria for privacy and integrity protection in probe vehicle information systems This document specifies the basic rules to be considered by service providers handling privacy in probe vehicle information services. This document is aimed at protecting the privacy as well as the intrinsic rights and interests of the probe data subjects specified in ISO 24100:2010.This document specifies the following items related to probe vehicle systems (PVS), i.e. systems collecting probe data from private vehicles and processing these probe data statistically towards useful information that can be provided to various end users: • architecture of the PVS in support of appropriate protection of data integrity and anonymity in the PVS; • security criteria and requirements for the PVS, specifically • requirements for data integrity protection and privacy; requirements for correct and anonymous generation and handling of probe data.	https://www.iso.org/standard/56791.html
11	ITS - GRC	**x.1373 series x (ITU Guideline)**	**x.1373 series x: Data networks, open system communications and security** Secure software update capability for intelligent transportation system communication devices - sets out the general specifications for the basic model for software updates, threat/risk analysis, definitions for security requirements, software update controls, and data format for update modules	https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1373-201703-I!!PDF-E&type=items
12	ITS - Operations	**ISO 15784-2:2015 (ISO Standard)**	**ISO 15784-2:2015 Intelligent transport systems (ITS) — Data exchange involving roadside modules communication — Part 2: Centre to field device communications using SNMP** Specifies a mechanism to exchange data and messages in the following cases: • between a traffic management centre(s) and roadside modules for traffic management; • between roadside modules used for traffic management.	https://www.iso.org/standard/55233.html
13	ITS - Operations	**DOT HS 812 073 (NIST Framework)**	**NIST - Cybersecurity Risk management framework applied to modern vehicles** The objective of this paper is to review the National Institute of Standards and Technology guidelines and foundational publications for cybersecurity risk management. This paper is a primer that provides an examination of cybersecurity risk management topics and is intended to provide readers with a better understanding of the NIST approach to cybersecurity. This NIST approach is often used as a baseline in industries and sectors to develop a more targeted risk management approach for the specific use cases and issues in those industries and sectors. This paper will establish for readers a baseline conceptual understanding of the NIST approach with foundational documents to establish a common vocabulary for discussing risk management for the vehicle sector.	https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/812073_natlinstitstandardstechcyber.pdf
14	ITS - Protocols	**ISO 10711:2012 (ISO Standard)**	**ISO 10711:2012 Intelligent Transport Systems — Interface Protocol and Message Set Definition between Traffic Signal Controllers and Detectors** ISO 10711:2012 defines protocols and message sets between traffic detectors and traffic signal controllers. It is applicable to the various types of traffic detector technologies currently in use for real-time traffic signal controls. It defines message sets that contain data collection and control protocol for three different types of detectors of traffic signal control systems	https://www.iso.org/standard/46069.html
15	ITS - Data Security	**ISO 24100:2010 (ISO Standard)**	**ISO 24100:2010 Intelligent transport systems — Basic principles for personal data protection in probe vehicle information services** States the basic rules to be observed by service providers who handle personal data in probe vehicle information services. This International Standard is aimed at protecting the personal data as well as the intrinsic rights and interests of probe data senders, i.e., owners and drivers of vehicles fitted with in-vehicle probe systems.	https://www.iso.org/standard/42017.html

REF#	CATEGORY	IDENTIFIER & TITLE	DESCRIPTION	LOCATION
16	ITS - Operations	**ASTM E2468 - 05(2018) (ASTM Standard)**	**Standard Practice for Metadata to Support Archived Data Management Systems** This standard is applicable to various types of operational data collected by intelligent transportation systems (ITS) and stored in an archived data management system.	https://www.astm.org/Standards/E2468.htm
17	ITS - Operations	**ISO/SAE DIS 21434 [SAE] (ISO Standard)**	**ISO/SAE DIS 21434 [SAE] Road vehicles — Cybersecurity engineering** This covers the topics such as Overall cyber security management, Project dependent cyber security management, Continuous cyber security activities etc.	https://www.iso.org/standard/70918.html
18	ITS - Operations	**https://www.iso.org/standard/70918.html**	**Intelligent Transport Systems (ITS); Security; Pre-standardization study on pseudonym change management** The purpose of the present document is to realize a pre-standardization study on pseudonyms management for C-ITS in order to provide guidance and recommendations for the future versions of related ETSI ITS specifications. Definition of relevant metrics that may be used to quantify the level of safety and privacy provided by the different strategies. The evaluation of the pseudonym change strategies then follows. Note that in the present document the evaluation itself is not available and will be added in the next release. However, the methodology of evaluation is basically described.	https://www.etsi.org/deliver/etsi_tr/103400_103499/103415/01.01.01_60/
19	ITS - Data Security	**ETSI TS 102 941 V1.2.1 (2018-05) (ETSI Standard)**	**Intelligent Transport Systems (ITS); Security; Trust and Privacy Management** The present document specifies the trust and privacy management for Intelligent Transport System (ITS) communications. Based upon the security services defined in ETSI TS 102 731 [1] and the security architecture defined in ETSI TS 102 940 [5], it identifies the trust establishment and privacy management required to support security in an ITS environment and the relationships that exist between the entities themselves and the elements of the ITS reference architecture defined in ETSI EN 302 665 [2].	https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/812073_natlinstitstandardstechcyber.pdf
20	ITS - Operations	**ETSI TS 103 600 V 1.1.1 (ETSI Standard)**	**Intelligent Transport Systems (ITS) - Testing - Interoperability test specifications for security** The present document contains specification of interoperability test descriptions to validate implementations of ETSI TS 103 097 [1], ETSI TS 102 941 [3] and ETSI TS 102 940.	https://www.etsi.org/deliver/etsi_ts/103600_103699/103600/01.01.01_60/
21	ITS - Operations	**IEC/TR 63069*CEI/TR 63069 (IEC Standard)**	**Industrial-process measurement, control and automation - Framework for functional safety and security** IEC TR 63069:2019 (E) explains and provides guidance on the common application of IEC 61508 (all parts) and IEC 62443 (all parts) in the area of industrial-process measurement, control and automation	https://webstore.iec.ch/publication/31421
22	ITS - Operations	**IEC/TR 63074*CEI/TR 63074 (IEC Standard)**	**Safety of machinery - Security aspects related to functional safety of safety- related control systems** IEC TR 63074:2019 gives guidance on the use of IEC 62443 (all parts) related to those aspects of security threats and vulnerabilities that could influence functional safety implemented and realized by safety- related control systems (SCS) and could lead to the loss of the ability to maintain safe operation of a machine.	https://webstore.iec.ch/publication/31572
23	ITS - GRC	**PAS 11281:2018 (BSI Standard)**	**Connected automotive ecosystems. Impact of security on safety.** This PAS aims to help organizations in the CAV ecosystem ensure that security-related risks in their products, services or activities don't pose an unacceptable safety risk in the physical world.	https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/812073_natlinstitstandardstechcyber.pdf
24	ITS - GRC	**FHWA-JPO-19-763 (US DoT Guideline**	**FHWA-JPO-19-763 : Cybersecurity and Intelligent Transportation Systems; A Best Practice Guide** The U.S. Department of Homeland Security Transportation Systems Sector Cybersecurity Framework Implementation Guidance provides guidelines for applying the framework to transportation systems [4] . The guidance describes how to apply the tenets of the NIST CSF to reduce cyber risks of critical transportation infrastructure such as an ITS.	https://rosap.ntl.bts.gov/view/dot/42461

REF#	CATEGORY	IDENTIFIER & TITLE	DESCRIPTION	LOCATION
25	ITS - Operations	**DIN SPEC 27072 (DIN Standard)**	**Information Technology - IoT capable devices - Minimum requirements for Information security** This DIN SPEC is sponsor by Bundesamt für Sicherheit in der Information Technik (BSI) and therefore available free of charge. This DIN specification contains requirements for connected devices within the small business-home Environment. Complying with these requirements reduces the likelihood, that comm attack vectors can used successfully against these devices. This specification does not intend to assure security of the devices. This specification can be used as Basis in procurement processes. This specification does not cover smartphones, Laptops or personal Computer.	https://www.beuth.de/en/technical-rule/din-
26	ITS - Operations	**“ISO 15764:2004 (ISO Standard)”**	**ISO 15764:2004 Road vehicles — Extended data link security** ISO 15764:2004 describes an extension of data link protocols for enhancing the security of data transfers between electronic control units (ECUs) connected by a communication network used in road vehicles. It is based on cryptographic methods that include encryption, digital signatures and message authentication codes (MACs). It provides a description of services to establish ECUs as trusted parties in respect of one another and to protect against specific threats. It is applicable to all data links between pairs of ECUs capable of storing and processing secret data so that unauthorised third parties are denied access to it. Parameters are provided to enable the level of security in the data link to be selected.	https://www.iso.org/standard/28775.html
27	ITS - Operations	**ISO 26262-1:2018 (ISO Standard)**	**ISO 26262-1:2018 Road vehicles — Functional safety — Part 1: Vocabulary** This document is intended to be applied to safety-related systems that include one or more electrical and/or electronic (E/E) systems and that are installed in series production road vehicles, excluding mopeds. This document does not address unique E/E systems in special vehicles such as E/E systems designed for drivers with disabilities.	https://www.iso.org/standard/68383.html
28	ITS - Operations	**ISO/PAS 21448:2019 (ISO Standard)**	**ISO/PAS 21448:2019 Road vehicles — Safety of the intended functionality** The absence of unreasonable risk due to hazards resulting from functional insufficiencies of the intended functionality or by reasonably foreseeable misuse by persons is referred to as the Safety Of The Intended Functionality (SOTIF). This document provides guidance on the applicable design, verification and validation measures needed to achieve the SOTIF. This document does not apply to faults covered by the ISO 26262 series or to hazards directly caused by the system technology (e.g. eye damage from a laser sensor).	https://www.iso.org/standard/70939.html
29	ITS - Operations	**ISO/TS 15638-4:2020 (ISO Standard)**	**ISO/TS 15638-4:2020 Intelligent transport systems — Framework for cooperative telematics applications for regulated commercial freight vehicles (TARV) — Part 4: System security requirements** Security requirements address both hardware and software aspects. This document addresses the security requirements for: • the transfer of TARV data from an IVS to an application service provider across a wireless communications interface; • the receipt of instructions from an application service provider to a TARV IVS; • the communications aspects of handling of software updates for the IVS over wireless communications.	https://www.iso.org/standard/72094.html
30	ITS - Operations	**PAS 1085:2018 (BSI Standard)**	**Manufacturing. Establishing and implementing a security-minded approach. Specification** It specifies requirements for the security-minded management of manufacturing organizations and their associated value chains wherever information, digital technologies and associated control systems for the design, production, operation, maintenance and disposal of products and systems are in use.	https://shop.bsigroup.com/ProductDe-
31	ITS - Operations	**ETSI TS 133 185 V15.0.0 (2018-07) (ETSI Standard)**	**LTE; 5G; Security aspect for LTE support of Vehicle-to-Everything (V2X) services (3GPP TS 33.185 version 15.0.0 Release 15)** The present document specifies the security aspects of V2X features in LTE, including security architecture, security requirements on the network entities that are used to support V2X services, as well as the procedures and solutions which are provided to meet those requirements.	https://www.etsi.org/deliver/etsi_ts/133100_133199/133185/15.00.00_60/

REF#	CATEGORY	IDENTIFIER & TITLE	DESCRIPTION	LOCATION
32	ITS - Data Security	**ETSI TS 103 097 V 1.3.1 (ETSI Standard)**	**Intelligent Transport Systems (ITS); Security; Security header and certificate formats** The present document specifies the secure data structure including header and certificate formats for Intelligent Transport Systems.	https://www.etsi.org/deliver/etsi_ts/103000_103099/103097/01.03.01_60/
33	ITS - GRC	**ETSI TS 102 723-8 V 1.1.1 (ETSI Standard)**	**Intelligent Transport Systems (ITS); OSI cross-layer topics; Part 8:** Interface between security entity and network and transport layer The present document specifies interfaces between the ITS security entity and the ITS network and transport layers including interface services and service primitives which are extensible in order to achieve general applicability. Additionally, it specifies related procedures and common parameters.	https://www.etsi.org/deliver/etsi_ts/102700_102799/10272308/01.01.01_60
34	ITS - Data Security	**ETSI TR 103 061-8 V1.1.1 (2015-09) (ETSI Standard)**	**Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS Security; Part 6: Validation report** The present document is the validation report of the ITS Security conformance tests defined in ETSI TS 103 096-3 [i.2] derived from ETSI TS 103 097 (V1.2.1) [i.1]. It provides statistics of executed and validated GeoNetworking conformance tests. The information provided has been produced by validation against at least two prototype implementations from industry.	https://www.etsi.org/deliver/etsi_tr/103000_103099/10306106/01.01.01_60
35	ITS - Protocols	**ETSI TS 102 867 (ETSI Standard)**	**Intelligent Transport Systems (ITS); Security; Stage 3 mapping for IEEE 1609.2** The present document specifies the use of the mechanisms of IEEE 1609.2 within the ITS communications architecture defined in EN 302 665 [3] to provide a stage 3 implementation for a subset of the security services defined in TS 102 731.	https://standards.globalspec.com/std/1529093/TS%20102%20867
36	ITS - Operations	**PAS 1885:2018 (BSI Standard)**	**The fundamental principles of automotive cyber security.** As vehicles get smarter and their connectivity and integration with outside systems increases, so too does the need for vehicle and vehicle systems-related cyber security. This PAS has been written to help all parties involved in the vehicle lifecycle and ecosystem understand better how to improve and maintain vehicle security and the security of associated intelligent transport systems (ITS).	https://shop.bsigroup.com/ProductDe
37	Communications Protocols	**IEC/TR 63069*CEI/TR 63069 (IEC Standard)**	**Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS PKI management; Part 1: Protocol Implementation Conformance Statement (PICS)** The present document provides the Protocol Implementation Conformance Statement (PICS) pro forma for the test specifications for security algorithms as specified in ETSI TS 102 941 [1] and in accordance with the relevant guidance given in ISO/IEC 9646-7 [i.2] and ETSI ETS 300 406 [i.3].	https://www.etsi.org/deliver/etsi_ts/103500_103599/10352501/01.01.01_60/
38	Communication GRC	**ETSI TS 103 096-2 V1.4.1 (2018-08) (ETSI Standard)**	**Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS Security; Part 2: Test Suite Structure and Test Purposes (TSS & TP)** The present document provides the Test Suite Structure and Test Purposes (TSS & TP) for Security as defined in ETSI TS 103 097 [1] in accordance with the relevant guidance given in ISO/IEC 9646-7 [i.6].	https://www.etsi.org/deliver/etsi_ts/103000_103099/10309602/01.04.01_60/
39	Communication GRC	**ETSI TS 103 096-3 V1.4.1 (2018-08) (ETSI Standard)**	**Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS Security; Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)** The present document provides parts of the Abstract Test Suite (ATS) for Security as defined in ETSI TS 103 097 [1] in accordance with the relevant guidance given in ISO/IEC 9646-7 [i.6]. The objective of the present document is to provide a basis for conformance tests for security communication over GeoNetworking equipment giving a high probability of interoperability between different manufacturers' equipment.	https://www.etsi.org/deliver/etsi_ts/103000_103099/10309603/01.04.01_60/

REF#	CATEGORY	IDENTIFIER & TITLE	DESCRIPTION	LOCATION
40	Communication Protocols	**J2735_201603 (SAE Standard)**	**Dedicated Short Range Communications (DSRC) Message Set Dictionary** This SAE Standard specifies a message set, and its data frames and data elements, specifically for use by applications intended to utilize the 5.9 GHz Dedicated Short Range Communications for Wireless Access in Vehicular Environments (DSRC/WAVE, referenced in this document simply as “DSRC”) communications systems.	https://www.sae.org/standards/content/j2735_201603/
41	Communication Cryptography	**ISO 20828:2006 (ISO Standard)**	**ISO 20828:2006 Road vehicles — Security certificate management** ISO 20828:2006 establishes a uniform practice for the issuing and management of security certificates for use in Public Key Infrastructure applications. Assuming that all entities, intending to set up a secure data exchange to other entities based on private and public keys, are able to provide their own certificate, the certificate management scheme guarantees that the entities get all additional information needed to establish trust to other entities, from a single source in a simple and unified format. The certificate management is flexible with respect to the relations between Certification Authorities, not requesting any hierarchical structure. It does not prescribe centralized directories or the like, being accessible by all entities involved. With these properties the management scheme is optimised for applications in the automotive domain.	https://www.iso.org/standard/41891.html
42	Communication Protocols	**ISO 26021-2:2008 (ISO Standard)**	**ISO 26021-2:2008 Road vehicles — End-of-life activation of on-board pyrotechnic devices — Part 2: Communication requirements** Defines the deployment process, the system architecture, CAN-based communication methods and system preconditions which have to be implemented to fulfil the use cases defined in ISO 26021-1. Additionally, the relationship to and use with other existing standards are defined.	https://www.iso.org/standard/45457.html
43	Communication - GRC	**J3138_201806 (SAE Standard)**	**Diagnostic Link Connector Security** This document describes some of the actions that should be taken to help ensure safe vehicle operation in the case that any such connected device (external test equipment, connected data collection device) has been compromised by a source external to the vehicle. In particular, this document describes those actions specifically related to SAE J1979, ISO 15765, and ISO 14229 standardized diagnostic services. Generally, the following forms of communication bus connection topologies are used in current vehicles: a - Open access to communication buses b - Communication buses isolated via a gateway c - Hybrid combinations of a. and b.	https://www.sae.org/standards/content/j3138_201806/
44	Communication - Data Security	**ISO 20078-3:2019 (ISO Standard)**	**ISO 20078-3:2019 Road vehicles — Extended vehicle (ExVe) web services — Part 3: Security** This document defines how to authenticate users and Accessing Parties on a web services interface. It also defines how a Resource Owner can delegate Access to its Resources to an Accessing Party. Within this context, this document also defines the necessary roles and required separation of duties between these in order to fulfil requirements stated on security, data privacy and data protection.	https://www.iso.org/standard/67579.html
45	Communication - Protocols	**ISO 10711:2012 (ISO Standard)**	**ISO 10711:2012 Intelligent Transport Systems — Interface Protocol and Message Set Definition between Traffic Signal Controllers and Detectors** ISO 10711:2012 defines protocols and message sets between traffic detectors and traffic signal controllers. It is applicable to the various types of traffic detector technologies currently in use for real-time traffic signal controls.	https://www.iso.org/standard/46069.html
46	Communication - Operations	**ISO 12813:2019 (ISO Standard)**	**ISO 12813:2019 Electronic fee collection — Compliance check communication for autonomous systems** This document defines requirements for short-range communication for the purposes of compliance checking in autonomous electronic fee collecting systems. Compliance checking communication (CCC) takes place between a road vehicle’s on-board equipment (OBE) and an interrogator (roadside mounted equipment, mobile device or hand-held unit), and serves to establish whether the data that are delivered by the OBE correctly reflect the road usage of the corresponding vehicle according to the rules of the pertinent toll regime.	https://www.iso.org/standard/75833.html

REF#	CATEGORY	IDENTIFIER & TITLE	DESCRIPTION	LOCATION
47	Communication - Operations	**ISO 12855:2015 (ISO Standard)**	**ISO 12855:2015 Electronic fee collection — Information exchange between service provision and toll charging** ISO 12855:2015 specifies: • the interfaces between electronic fee collection (EFC) systems for vehicle related transport services, e.g. road user charging, parking and access control; it does not cover interfaces for EFC systems for public transport; an EFC system can include any EFC system, e.g. including systems that automatically read licence plate numbers of vehicles passing a toll point, • an exchange of information between the central equipment of the two roles of service provision and toll charging, e.g. • charging related data (toll declarations, billing details), • administrative data, and • confirmation data, • transfer mechanisms and supporting functions, • information objects, data syntax and semantics, • examples of data interchanges (see Annex C and Annex D), and • an example on how to use this International Standard for the European Electronic Tolling Service (EETS) (see Annex F).	https://www.iso.org/standard/64127.html
48	Communication - Operations	**ISO 13141:2015 (ISO Standard)**	**ISO 13141:2015 Electronic fee collection — Localisation augmentation communication for autonomous systems** ISO 13141:2015 establishes requirements for short-range communication for the purposes of augmenting the localization in autonomous electronic fee collection (EFC) systems. Localization augmentation serves to inform on-board equipment (OBE) about geographical location and the identification of a charge object. This International Standard specifies the provision of location and heading information and security means to protect from the manipulation of the OBE with false roadside equipment (RSE).	https://www.iso.org/standard/64166.html
49	Communication - Operations	**ISO 12813 (ISO Standard)**	**ISO 12813 Electronic fee collection -- Compliance check communication for autonomous system** Security services for mutual authentication of the communication partners and for signing of data	https://www.iso.org/standard/75833.html
50	Communication - Protocols	**ISO 15662:2006(en) (ISO Standard)**	**ISO 15662:2006(en) Intelligent transport systems — Wide area communication — Protocol management information** Most of the application services in the ITS sector use a variety of wide area communication systems in order to connect user terminals and “Service Centres”. In addition, the application services that are currently being provided connect specific user terminals to specific service centres using specific wide area communications systems. In other words, the various conditions that must be established to provide services are fixed. However, when the future modes of service use are considered, it is assumed that a user will utilize the same terminal to access “Service Centre A” in some cases and “Service Centre B” in other cases. It can also be assumed that in some cases the user may be on foot and in others he or she may be travelling in a vehicle. It can also be assumed that some users may access the service centre from “smart phones”, while others may do so from navigation systems, while still others may do so using interactive TVs.	https://www.iso.org/obp/ui/fr/#iso:st-
51	Communication - Cryptography	**NTCIP 2202:2001 (A Joint Standard of AASHTO, ITE and NEMA)**	**NTCIP 2202:2001 Internet (TCP/IP and UDP/IP) Transport Profile** This standard specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information (hereafter referred to as sensitive information).	https://www.ntcip.org/wp-content/uploads/2018/11/NTCIP2202.pdf
52	Communication - Operations	**NTCIP 1209 v02 (A Joint Standard of AASHTO, ITE and NEMA)**	**"Object Definitions for Transportation Sensor Systems (TSS)** Communication between an ITS Management Centre or portable computer and a Transportation Sensor System (TSS) is accomplished by using NTCIP Application Layer services to convey requests to access or modify values of TSS data elements resident in the TSS via an NTCIP network. An NTCIP message consists of a specific Application Layer service and a set of data elements. An NTCIP message may be conveyed using any NTCIP defined class of service that has been specified to be compatible with the Simple Transportation Management Framework (STMF).	https://www.ntcip.org/wp-content/uploads/2018/11/NTCIP1209v-0218jp.pdf

REF#	CATEGORY	IDENTIFIER & TITLE	DESCRIPTION	LOCATION
53	Communica-tion - Operations	1609.11-2010 (IEEE Standard)	**IEEE Standard for Wireless Access in Vehicular Environments (WAVE)-- Over-the-Air Electronic Payment Data Exchange Protocol for Intelligent Transportation Systems (ITS)** This standard specifies the electronic payment service layer and profile for Payment and Identity authentication, and Payment Data transfer for Dedicated Short Range Communication (DSRC) based applications in Wireless Access in Vehicular Environments. This standard defines a basic level of technical interoperability (vehicle-to-roadside) for electronic payment equipment, i.e., onboard unit (OBU) and roadside unit (RSU) using WAVE.	https://stan-dards.ieee.org/stan-
54	Communica-tion Operations	ISO/TS 21177:2019 (ISO Standard)	**ISO/TS 21177:2019 Intelligent transport systems — ITS station security services for secure session establishment and authentication between trusted devices** This document contains specifications for a set of ITS station security services required to ensure the authenticity of the source and integrity of information exchanged between trusted entities: • devices operated as bounded secured managed entities, i.e. ""ITS Station Communication Units"" (ITS-SCU) and ""ITS station units"" (ITS-SU) specified in ISO 21217, and • between ITS-SUs (composed of one or several ITS-SCUs) and external trusted entities such as sensor and control networks.	https://www.iso.org/stan-dard/70056.html?browse=tc
55	Communica-tion - Protocols	ISO/TS 21185:2019 (ISO Standard)	**ISO/TS 21185:2019 Intelligent transport systems — Communication profiles for secure connections between trusted devices** This document specifies a methodology to define ITS-S communication profiles (ITS-SCPs) based on standardized communication protocols to interconnect trusted devices. These profiles enable secure information exchange between such trusted devices, including secure low-latency information exchange, in different configurations. The present document also normatively specifies some ITS-SCPs based on the methodology, yet without the intent of covering all possible cases, in order to exemplify the methodology.	https://www.iso.org/stan-dard/70058.html?browse=tc
56	Communi-cation - Data Security	ISO 24534-5:2011 (ISO Standard)	**ISO 24534-5:2011 Intelligent transport systems — Automatic vehicle and equipment identification — Electronic Registration Identification (ERI) for vehicles — Part 5: Secure communications using symmetrical techniques** ISO 24534 provides the requirements for an electronic registration identification (ERI) using symmetric encryption techniques that are based on an identifier assigned to a vehicle (e.g. for recognition by national authorities) suitable to be used for: • electronic identification of local and foreign vehicles by national authorities, • vehicle manufacturing, in-life maintenance and end-of-life identification (vehicle life-cycle management), • adaptation of vehicle data, e.g. in case of international re-sales, • safety related purposes, • crime reduction, • commercial services, and • adhering to privacy and data protection regulations.	https://www.iso.org/stan-dard/54570.html?browse=tc
57	Communica-tion - GRC	ETSI TR 102 893 V1.3.2 (ETSI Standard)	**Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA)** The present document summarizes the results of a Threat, Vulnerability and Risk Analysis (TVRA) of 5,9 GHz radio communications in an Intelligent Transport System (ITS). The analysis considers vehicle-to-vehicle and vehicle-to-roadside network infrastructure communications services in the ITS Basic Set of Applications (BSA) [i.3] operating in a fully deployed ITS.	https://www.etsi.org/deliver/etsi_tr/102800_102899/102893/01.02.01_60/
58	Communica-tion - Protocols	ETSI TR 102 638 V1.1.1 (2009-06) (ETSI Standard)	**Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions** The present document defines BSA mainly focusing on V2V, V2I and I2V communications in the V2X dedicated frequency band. However, it does not exclude using other access technologies such as cell networks (e.g. 2G, 3G, 4G), and / or broadcasting systems (DAB, T-DMB, DVB).	https://www.etsi.org/deliver/etsi_tr/102600_102699/102638/01.01.01_60/

REF#	CATEGORY	IDENTIFIER & TITLE	DESCRIPTION	LOCATION
59	Communi-cation - Data Security	**ETSI TS 102 943 V1.1.1 (ETSI Standard)**	**Intelligent Transport Systems (ITS); Security; Confidentiality services** The present document specifies services to ensure that that the confidentiality of information sent to and from an Intelligent Transport System (ITS) station can be maintained at a level that is acceptable to the users of the station.	https://www.etsi.org/deliver/etsi_ts/102900_102999/102941/01.03.01_60/
60	Communi-cation - Data Security	**ETSI TS 102 941 V 1.3.1 (ETSI Standard)**	**Intelligent Transport Systems (ITS); Security; Trust and Privacy Management** The present document specifies the trust and privacy management for Intelligent Transport System (ITS) communications. Based upon the security services defined in ETSI TS 102 731 and the security architecture defined in ETSI TS 102 940, it identifies the trust establishment and privacy management required to support security in an ITS environment and the relationships that exist between the entities themselves and the elements of the ITS reference architecture defined in ETSI EN 302 665.	https://www.etsi.org/deliver/etsi_ts/102900_102999/102941/01.03.01_60/
61	Communi-cation - Data Security	**ETSI TS 102 942 V1.1.1 (ETSI Standard)**	**Intelligent Transport Systems (ITS); Security; Access Control** The present document specifies authentication and authorization services to avoid unauthorized access to ITS services. It also specifies measures to ensure the required level of security and privacy for ITS message communication.	https://www.etsi.org/deliver/etsi_ts/102900_102999/102942/01.01.01_60/
62	Communica-tion - Cryptography	**ETSI TS 102 940 V1.3.1 (ETSI Standard)**	**Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management** The present document specifies a security architecture for Intelligent Transport System (ITS) communications. Based upon the security services defined in ETSI TS 102 731, it identifies the functional entities required to support security in an ITS environment and the relationships that exist between the entities themselves and the elements of the ITS reference architecture defined in ETSI EN 302 665.	https://www.etsi.org/deliver/etsi_ts/102900_102999/102940/01.03.01_60/
63	Communica-tion - Operations	**ETSI TS 103 097 V1.3.1 (ETSI Standard)**	**Intelligent Transport Systems (ITS); Security; Security header and certificate formats** The present document specifies the secure data structure including header and certificate formats for Intelligent Transport Systems.	https://www.iso.org/standard/54570.html?browse=tc
64	Communica-tion - Operations	**ETSI EN 302 665 V1.1.1 (2010-09) (ETSI Standard)**	**Intelligent Transport Systems (ITS); Communications Architecture** The present document specifies the International communication architecture of communications for Intelligent Transport Systems (ITSC). This version of the present document is dedicated to the road transport context.	https://www.etsi.org/deliver/etsi_en/302600_302699/302665/01.01.01_60/
65	Communi-cation - Data Security	**ETSI TS 102 731 V1.1.1 (ETSI Standard)**	**Intelligent Transport Systems (ITS); Security; Security Services and Architecture** The present document specifies mechanisms at the stage 2 level defined by ETS 300 387 [i.2] for secure and privacy-preserving communication in ITS environments. It describes facilities for credential and identity management, privacy and anonymity, integrity protection, authentication and authorization.	https://www.etsi.org/deliver/etsi_ts/102700_102799/102731/01.01.01_60/
66	Communi-cation - Data Security	**ISO 19790:2012 (ISO Standard)**	**ISO 19790:2012 Information technology — Security techniques — Security requirements for cryptographic modules** This International Standard defines four security levels for cryptographic modules to provide for a wide spectrum of data sensitivity (e.g. low value administrative data, million dollar funds transfers, life protecting data, personal identity information, and sensitive information used by government) and a diversity of application environments (e.g. a guarded facility, an office, removable media, and a completely unprotected location).	https://www.iso.org/standard/52906.html
67	Communica-tion - Cryptography	**ISO 24759:2017 (ISO Standard)**	**ISO 24759:2017 Information technology — Security techniques —** Test requirements for cryptographic modules This document also specifies the requirements for information that vendors provide to testing laboratories as supporting evidence to demonstrate their cryptographic modules' conformity to the requirements specified in ISO/IEC 19790:2012.	https://www.iso.org/standard/72515.html

REF#	CATEGORY	IDENTIFIER & TITLE	DESCRIPTION	LOCATION
68	Communica-tion - GRC	**ISO/TR 23786:2019 (ISO Standard)**	**ISO/TR 23786:2019 Road vehicles — Solutions for remote access to vehicle — Criteria for risk assessment** This document identifies criteria that can be considered for assessing the risks related to solutions for remote access to road vehicles, including extended vehicles (ExVe) and their implementation.	https://www.etsi.org/deliver/etsi_ts/102900_102999/10294 2/01.01.01_60/
69	Communica-tion - Protocols	**IEC 62351-3 (IEC Standard)**	**Power systems management and associated information exchange – Data and communications security – Part 3: Communication network and system security – Profiles including TCP/IP** IEC 62351-3:2014+A1:2018+A2:2020 specifies how to provide confidentiality, integrity protection, and message level authentication for SCADA and telecontrol protocols that make use of TCP/IP as a message transport layer when cyber-security is required. Although there are many possible solutions to secure TCP/IP, the particular scope of this part is to provide security between communicating entities at either end of a TCP/IP connection within the end communicating entities. This part of IEC 62351 reflects the security requirements of the IEC power systems management protocols.	https://web-store.iec.ch/publica-
70	Communica-tion - Cryptography	**ISO/IEC 18033-3:2010 [ISO/IEC 18033-3:2010] (IEC Standard)**	**ISO/IEC 18033-3:2010 [ISO/IEC 18033-3:2010] Information technology — Security techniques — Encryption algorithms— Part 3: Block ciphers** ISO/IEC 18033 specifies encryption systems (ciphers) for the purpose of data confidentiality.	https://www.iso.org/stan-dard/54531.html
71	Communica-tion - Cryptography	**FIPS 197 Advanced Encryption Standard (AES) (NIST Standard)**	**FIPS 197 Advanced Encryption Standard (AES)** The Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data.	https://nvl-pubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf
72	Communica-tion - Operations	**NTCIP 1103 V03 (A Joint Standard of AASHTO, ITE, and NEMA)**	**National Transportation Communications for ITS Protocol Transportation Management Protocols (TMP)** TMP defines a set of rules and procedures for exchanging transportation management information between transportation management applications and transportation equipment such that they interoperate with each other.	https://www.ntcip.org/doc-ument-num-bers-and-sta-tus/
73	Communica-tion - Protocols	**NTCIP 2103 V02 (A Joint Standard of AASHTO, ITE, and NEMA)**	**Point-to-Point Protocol over RS-232 Subnetwork Profile Published** The protocol stack described in NTCIP 2103 v02 is appropriate for the reliable exchange of data between processing equipment on switched data networks.	https://www.ntcip.org/doc-ument-num-bers-and-sta-tus/
74	Communica-tion - Protocols	**NTCIP 8004 V02 (A Joint Standard of AASHTO, ITE and NEMA)**	**Structure and Identification of Management Information (SMI)** NTCIP 8004 v02 specifies a set of rules and protocols for organizing, describing, and defining transportation management information to be exchanged between transportation management applications and/or transportation equipment such that they interoperate with each other.	https://www.ntcip.org/doc-ument-num-bers-and-sta-tus/
75	Communica-tion - Operations	**ETSI TS 118 103 V2.12.1 (2019-04) (ETSI Standard)**	**oneM2M; Security solutions (oneM2M TS-0003 version 2.12.1 Release 2A)** The present document defines security solutions applicable within the M2M (Machine to Machine) system.	https://www.etsi.org/deliver/etsi_ts/118100_118199/11810 3/02.12.01_60/
76	Communica-tion - GRC	**ETSI TS 133 102 V 15.1.0*3GPP TS 33.102 Version 15.1.0 Release 15 (ETSI Standard)**	**Digital cellular telecommunications system (Phase 2+) (GSM) - Universal Mobile Telecommunications System (UMTS) - 3G security - Security architecture (3GPP TS 33.102 version 15.1.0 Release 15)** This specification defines the security architecture, i.e., the security features and the security mechanisms, for the third generation mobile telecommunication system.	https://www.etsi.org/deliver/etsi_ts/133100_133199/13310 2/15.01.00_60/
77	Communica-tion - GRC	**ETSI TS 133 117 V 14.5.0*3GPP TS 33.117 Version 14.5.0 Release 14 (ETSI Standard)**	**Universal Mobile Telecommunications System (UMTS) - LTE - Catalogue of general security assurance requirements (3GPP TS 33.117 version 14.5.0 Release 14)** The present document contains objectives, requirements and test cases that are deemed applicable, possibly after adaptation, to several network product classes.	https://www.etsi.org/deliver/etsi_ts/133100_133199/13311 7/14.01.00_60/
78	Communica-tion - Operations	**ETSI TS 133 117 V 15.3.0*3GPP TS 33.117 Version 15.3.0 Release 15 (ETSI Standard)**	**Universal Mobile Telecommunications System (UMTS) - LTE - Catalogue of general security assurance requirements (3GPP TS 33.117 version 15.3.0 Release 15)** The present document specifies both the architectural and functional system requirements for Lawful Interception (LI) in 3GPP networks. The present document provides an LI architecture supporting both network layer based and service layer based Interception.	https://www.etsi.org/deliver/etsi_ts/133100_133199/13312 7/15.03.00_60/

REF#	CATEGORY	IDENTIFIER & TITLE	DESCRIPTION	LOCATION
79	Communica-tion - Operations	**ETSI TS 133 122 V 15.3.0*3GPP TS 33.122 Version 15.3.0 Release 15 (ETSI Standard)**	**LTE - 5G - Security aspects of Common API Framework (CAPIF) for 3GPP northbound APIs (3GPP TS 33.122 version 15.3.0 Release 15)** The present document specifies the architecture, procedures and information flows necessary for the CAPIF. The aspects of this specification include identifying architecture requirements for the CAPIF (e.g. registration, discovery, identity management) that are applicable to any service APIs when used by northbound entities, as well as any interactions between the CAPIF and the service APIs themselves. The common API framework applies to both EPS and 5GS, and is independent of the underlying 3GPP access (e.g. E-UTRA, NR).	https://www.etsi.org/deliver/etsi_ts/123200_123299/123222/15.03.00_60/
80	Communica-tion - Protocols	**ETSI TS 133 128 V 15.0.0*3GPP TS 33.128 Version 15.0.0 Release 15 (ETSI Standard)**	**LTE - 5G - Digital cellular telecommunications system (Phase 2+) (GSM) - Universal Mobile Telecommunications System (UMTS) - Security - Protocol and procedures for Lawful Interception (LI) - Stage 3 (3GPP TS 33.128 version 15.0.0 Release 15)** The present document specifies the protocols and procedures required to perform Lawful Interception within a 3GPP network. The present document addresses both internal interfaces used internally with a 3GPP network and external handover interfaces used to handover intercepted communications to law enforcement.	https://www.etsi.org/deliver/etsi_ts/133100_133199/133128/15.00.00_60/
81	Communica-tion Operations	**ETSI TS 133 179 V 13.8.0*3GPP TS 33.179 Version 13.8.0 Release 13 (ETSI Standard)**	**LTE - Security of Mission Critical Push To Talk (MCPTT) over LTE (3GPP TS 33.179 version 13.8.0 Release 13)** The present document specifies the security architecture, procedures and information flows needed to protect the mission critical push to talk (MCPTT) service. The architecture includes mechanisms for authentication, protection of MCPTT signalling and protection of MCPTT media. Security for both MCPTT group calls and MCPTT private calls operating in on-network and off-network modes of operation is specified.	https://www.etsi.org/deliver/etsi_ts/133100_133199/133179/13.08.00_60/
82	Communica-tion - Cryptography	**ETSI TS 133 210 V 15.2.0*3GPP TS 33.210 Version 15.2.0 Release 15 (ETSI Standard)**	**Digital cellular telecommunications system (Phase 2+) (GSM) - Universal Mobile Telecommunications System (UMTS) - LTE - 3G security - Network Domain Security (NDS) - IP network layer security (3GPP TS 33.210 version 15.2.0 Release 15)** The present document defines the security architecture for network domain IP based control planes, which shall be applied to NDS/IP-networks (i.e. 3GPP and fixed broadband networks). The scope of network domain control plane security is to cover the control signalling on selected interfaces between network elements of NDS/IP networks. . The present document furthermore serves as a central repository for cryptographic profiles for security above IP layer.	https://www.etsi.org/deliver/etsi_TS/133200_133299/133210/15.02.00_60/
83	Communica-tion - Operations	**ETSI TS 133 310 V 15.2.0*3GPP TS 33.310 Version 15.2.0 Release 15 (ETSI Standard)**	**Universal Mobile Telecommunications System (UMTS) - LTE - Network Domain Security (NDS) - Authentication Framework (AF)** (3GPP TS 33.310 version 15.2.0 Release 15) The scope of this Technical Specification is limited to authentication of network elements, which are using NDS/IP or TLS, and to Certificate Enrolment for Base Stations as described in the present document.	https://www.etsi.org/deliver/etsi_ts/133300_133399/133310/15.02.00_60/
84	Communica-tion - Data Security	**ETSI TS 133 107 V 15.5.0*3GPP TS 33.107 Version 15.5.0 Release 15 (ETSI Standard)**	**Universal Mobile Telecommunications System (UMTS) - LTE - Digital cellular telecommunications system (Phase 2+) (GSM) - 3G security - Lawful interception architecture and functions (3GPP TS 33.107 version 15.5.0 Release 15)** **The present document describes the architecture and functional** requirements within a Third Generation Mobile Communication System (3GMS) and the Evolved Packet System (EPS).	https://www.etsi.org/deliver/etsi_ts/133100_133199/133107/15.05.00_60/
85	Communi-cation - Data Security	**ETSI TS 133 108 V 15.4.0*3GPP TS 33.108 Version 15.4.0 Release 15 (ETSI Standard)**	**"Universal Mobile Telecommunications System (UMTS) - LTE - Digital cellular telecommunications system (Phase 2+) (GSM) - 3G security - Handover interface for Lawful Interception (LI) (3GPP TS 33.108 version 15.4.0 Release 15)** The present document specifies the handover interfaces for Lawful Interception (LI) of Packet-Data Services, Circuit Switched Services, Multimedia Services within the UMTS network and Evolved Packet System (EPS). The handover interface in this context includes the delivery of Intercept Related Information (IRI) through the Handover Interface 2 (HI2) and Content of Communication (CC) through the Handover Interface 3 (HI3) to the Law Enforcement Monitoring Facility (LEMF).	https://www.etsi.org/deliver/etsi_ts/133100_133199/133108/15.04.00_60/

REF#	CATEGORY	IDENTIFIER & TITLE	DESCRIPTION	LOCATION
86	Communica-tion - Operations	**ETSI TS 133 180 V 14.6.0*3GPP TS 33.180 Version 14.6.0 Release 14 (ESTI Standard)**	**"LTE - Security of the mission critical service (3GPP TS 33.180 version 14.6.0 Release 14)** The present document specifies the security architecture, procedures and information flows needed to protect the mission critical service (MCX). The architecture includes mechanisms to protect the Common Functional Architecture and security mechanisms for mission critical applications. This includes Push-To-Talk (MCPTT), Video (MCVideo) and Data (MCData). Additionally, security mechanisms relating to on-network use, off-network use, roaming, migration, interconnection, interworking and multiple security domains are described.	https://www.etsi.org/deliver/etsi_ts/133100_133199/133180/14.06.00_60/
87	Communica-tion - Operations	**ETSI TS 133 180 V 15.4.0*3GPP TS 33.180 Version 15.4.0 Release 15 (ETSI Standard)**	**LTE - Security of the mission critical service (3GPP TS 33.180 version 15.4.0 Release 15)** The present document specifies the security architecture, procedures and information flows needed to protect the mission critical service (MCX). The architecture includes mechanisms to protect the Common Functional Architecture and security mechanisms for mission critical applications. This includes Push-To-Talk (MCPTT), Video (MCVideo) and Data (MCData). Additionally, security mechanisms relating to on-network use, off-network use, roaming, migration, interconnection, interworking and multiple security domains are described.	https://www.etsi.org/deliver/etsi_ts/133100_133199/133180/15.04.00_60/
88	Communica-tion - Operations	**ETSI TS 133 401 V 15.7.0*3GPP TS 33.401 Version 15.7.0 Release 15 (ETSI Standard)**	**Digital cellular telecommunications system (Phase 2+) (GSM) - Universal Mobile Telecommunications System (UMTS) - LTE - 3GPP System Architecture Evolution (SAE) - Security architecture (3GPP TS 33.401 version 15.7.0 Release 15)** The present document specifies the security architecture, i.e., the security features and the security mechanisms for the Evolved Packet System and the Evolved Packet Core, and the security procedures performed within the evolved Packet System (EPS) including the Evolved Packet Core (EPC) and the Evolved UTRAN (E-UTRAN).	https://www.etsi.org/deliver/etsi_ts/133400_133499/133401/15.07.00_60/
89	Communica-tion - Operations	**ETSI TS 133 501 V 15.4.0*3GPP TS 33.501 Version 15.4.0 Release 15 (ETSI Standard)**	**5G - Security architecture and procedures for 5G System (3GPP TS 33.501 version 15.4.0 Release 15)** The present document specifies the security architecture, i.e., the security features and the security mechanisms for the 5G System and the 5G Core, and the security procedures performed within the 5G System including the 5G Core and the 5G New Radio.	https://www.etsi.org/deliver/etsi_ts/133500_133599/133501/15.04.00_60/
90	Communica-tion - Protocols	**ETSI ES 203 311-6 V 1.1.1 (ETSI Standard)**	**"Integrated broadband cable telecommunication networks (CABLE) - Fourth generation transmission systems for interactive cable television services - IP cable modems - Part 6: Security - DOCSIS® 3.1 [ANSI/SCTE 220-5 2016]** The present document specifies radio parameters, data link services and protocol data units, and application services and protocol data units which are necessary for the efficient use of the radio spectrum and for the purpose of DSRC based applications. This includes methods of measurements for verifying the limits stated in the present document.	https://www.etsi.org/deliver/etsi_es/203300_203399/20331106/01.01.01_50/es
91	Communica-tion - Cryptography	**ISO/IEC 18033-6 (IEC Standard)**	**ISO/IEC 18033-6 IT Security techniques - Encryption algorithms - Part 6: Homomorphic encryption** This document specifies the following mechanisms for homomorphic encryption. • Exponential ElGamal encryption; • Paillier encryption.	https://www.iso.org/standard/67740.html

REF#	CATEGORY	IDENTIFIER & TITLE	DESCRIPTION	LOCATION
92	Communica-tion Cryptograph	**ETSI TS 103 525-2 V1.1.1 (2019-03) (ETSI Standard)**	**Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS PKI management; Part 2: Test Suite Structure and Test Purposes (TSS & TP)** The present document provides the Test Suite Structure and Test Purposes (TSS & TP) for PKI management as defined in ETSI TS 102 941 [1] in accordance with the relevant guidance given in ISO/IEC 9646-7 [i.6]. The ISO standard for the methodology of conformance testing (ISO/IEC 9646-1 [i.3] and ISO/IEC 9646-2 [i.4]) as well as the ETSI rules for conformance testing (ETSI ETS 300 406 [i.7]) are used as a basis for the test methodology.	https://www.etsi.org/deliver/etsi_ts/103500_103599/10352502/01.01.01_60
93	Communica-tion Cryptography	**ETSI TS 103 525-3 V1.1.1 (2019-03) (ETSI Standard)**	**Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS PKI management; Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)** The present document provides parts of the Abstract Test Suite (ATS) for ITS PKI management as defined in ETSI TS 102 941 [2] in accordance with the relevant guidance given in ISO/IEC 9646-7 [i.6]. The objective of the present document is to provide a basis for conformance tests for security communication over GeoNetworking equipment giving a high probability of interoperability between different manufacturers' equipment.	https://www.etsi.org/deliver/etsi_ts/103500_103599/10352503/01.01.01_60/
94	Communica-tion Protocols	**ETSI TS 103 096-1 V1.4.1 (2018-08) (ETSI Standard)**	**Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS Security; Part 1: Protocol Implementation Conformance Statement (PICS)** The present document provides the Protocol Implementation Conformance Statement (PICS) pro forma for the test specifications for security algorithms as specified in ETSI TS 103 097 [1] and in accordance with the relevant guidance given in ISO/IEC 9646-7 [i.2] and ETSI ETS 300 406 [i.3].	https://www.etsi.org/deliver/etsi_ts/103000_103099/10309601/01.04.01_60/
95	Communi-cation - Data Security	**P1609.13 (IEEE Standard)**	**Wireless Access in Vehicular Environments - Reliable Data Transport Mechanisms for Multiple Receivers** This standard provides mechanisms for distribution of data within the Wireless Access in Vehicular Environments (WAVE) system. These mechanisms are optimized for use in the vehicular environment, where connectivity may be intermittent; for large data transfers; and for data which is of interest to a large number of system participants. Considerations addressed by the standard include image identification and versioning, discovery, distribution, error correction, and security.	https://stan-dards.ieee.org/proj-ect/1609_13.html
96	Communi-cation - Data Security	**1609.2-2016 (IEEE Standard)**	**IEEE Standard for Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages** This standard defines secure message formats and processing for use by Wireless Access in Vehicular Environments (WAVE) devices, including methods to secure WAVE management messages and methods to secure application messages. It also describes administrative functions necessary to support the core security functions.	https://stan-dards.ieee.org/stan-
97	Communi-cation - Data Security	**1609.4-2016 (IEEE Standard)**	**IEEE Standard for Wireless Access in Vehicular Environments (WAVE) -- Multi-Channel Operation** Multi-channel wireless radio operations, Wireless Access in Vehicular Environments (WAVE) mode, medium access control (MAC), and physical layers (PHYs), including parameters for priority access, channel switching and routing, management services, and primitives designed for multi-channel operations are described in this standard.	https://stan-dards.ieee.org/stan-
98	Communica-tion - Protocols	**1609.0-2019 (IEEE Standard)**	**IEEE Guide for Wireless Access in Vehicular Environments (WAVE) Architecture** The wireless access in vehicular environments (WAVE) architecture and services necessary for WAVE devices to communicate in a mobile vehicular environment are described in this guide. It is meant to be used in conjunction with the family of IEEE 1609 standards as of its publication date. These include IEEE Std 1609.2(TM), IEEE Standard Security Services for Applications and Management Messages; IEEE Std 1609.3(TM), Networking Services; IEEE Std 1609.4(TM), Multi-Channel Operation; IEEE Std 1609.11(TM), Over-the-Air Electronic Payment Data Exchange Protocol for Intelligent Transportation Systems (ITS); IEEE Std 1609.12(TM), Identifiers; and IEEE Std 802.11(TM) in operation outside the context of a basic service set.	https://stan-dards.ieee.org/stan-
99	Communica-tion - Protocols	**1609.12-2019 (IEEE Standard)**	**IEEE Standard for Wireless Access in Vehicular Environments (WAVE)--Identifiers** Wireless Access in Vehicular Environments (WAVE) is specified in the IEEE 1609 family of standards, within which certain identifiers are used. The use of these identifiers is described, and identifier values that have been allocated for use by WAVE systems are indicated.	https://stan-dards.ieee.org/stan-

REF#	CATEGORY	IDENTIFIER & TITLE	DESCRIPTION	LOCATION
100	Communication - Protocols	**ISO/IEC 19823-21 (IEC Standard)**	**ISO/IEC 19823-21 Information technology - Conformance test methods for security service crypto suites - Part 21: Crypto suite SIMON** This document describes methods for determining conformance to the security crypto suite defined in ISO/IEC 29167-21.	https://www.iso.org/standard/73468.html
101	Communication - Protocols	**ISO/IEC 19823-22 (IEC Standard)**	**ISO/IEC 19823-22 Information technology - Conformance test methods for security service crypto suites - Part 22: Crypto suite SPECK** This document describes methods for determining conformance to the security crypto suite defined in ISO/IEC 29167-22.	https://www.iso.org/standard/73467.html
102	Communication - Operations	**SAE J 1760 (SAE Standard)**	**Data Security Services** The scope of this SAE Recommended Practice is to require the use of the same Security Services as defined by the International Standard ISO/CD 15764, modified by the Class of Security as determined by the resource provider and referenced in Table 1, Extended Data Link Security References.	https://www.sae.org/standards/content/j1760_200112/
103	Communication - Operations	**SAE J 2186 (SAE Standard)**	**E/E Data Link Security** This SAE Recommended Practice establishes a uniform practice for protecting vehicle components from “”unauthorized”” access through a vehicle data link connector (DLC). The document defines a security system for motor vehicle and tool manufacturers. It will provide flexibility to tailor systems to the security needs of the vehicle manufacturer. The vehicle modules addressed are those that are capable of having solid state memory contents accessed or altered through the data link connector. Improper memory content alteration could potentially damage the electronics or other vehicle modules; risk the vehicle compliance to government legislated requirements; or risk the vehicle manufacturer’s security interests. This document does not imply that other security measures are not required nor possible.	https://www.sae.org/standards/content/j2186_199109/
104	General	**ISO/IEC 27001 (IEC Standard)**	**ISO/IEC 27001 Information Security Management System (ISMS)** Using this family of standards will help your organization manage the security of assets such as financial information, intellectual property, employee details or information entrusted to you by third parties. ISO/IEC 27001 is the best-known standard in the family providing requirements for an information security management system (ISMS).	https://www.iso.org/isoiec-27001-information-security.html
105	General	**ISO 22301:2019 (ISO Standard)**	**ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements** This updated international standard details the requirements of a business continuity management system (BCMS). It enables organizations to prepare for disruptive incidents that might otherwise prevent them from achieving their objectives. Users will be better prepared for disruptions and will recover more quickly, minimizing the impact on employees, customers and suppliers.	https://shop.bsigroup.com/ProductDe-
106	General	**ISO/IEC 20546:2019 (IEC Standard)**	**SO/IEC 20546:2019 - Information technology - Big Data - Overview and Vocabulary** Provides a set of terms and definitions needed to promote improved communication and understanding of this area. It provides a terminological foundation for big data-related standards, and a conceptual overview.	https://www.iso.org/standard/68305.html
107	General	**Federal information processing standards publication (Supersedes FIPS PUB 140-2) (NIST Standard)**	**Federal information processing standards publication (Supersedes FIPS PUB 140-2) Security requirements for cryptographic modules** This standard specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information (hereafter referred to as sensitive information). The standard provides four increasing.	https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf
108	General	**NIST Special publication 800-12 Rev1 (NIST Guideline)**	**NIST Special publication 800-12 Rev1 - An Introduction to Information Security** Organizations rely heavily on the use of information technology (IT) products and services to run their day-to-day activities. Ensuring the security of these products and services is of the utmost importance for the success of the organization. This publication introduces the information security principles that organizations may leverage to understand the information security needs of their respective systems.	https://nvlpubs.nist.gov/nistpubs/Special-Publications/NIST.SP.800-12r1.pdf
109	General	**NIST Special publication 800-37 Rev. 2 (NIST Guideline)**	**NIST Special publication 800-37 Rev. 2 Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy** Updated in 2010 provides a new risk approach:Guide for Applying the Risk Management Framework to Federal Information Systems	https://www.etsi.org/deliver/etsi_ts/133300_133399/133310/15.02.00_60/
110	General	**NIST Special publication 800-63-3 (NIST Guideline)**	**NIST Special publication 800-63-3 - Digital Identity Guidelines** Digital Identity Guidelines, Published June 2017 updated to include updates as of December 1, 2017, provides guidelines for implementing digital identity services, including identity proofing, registration, and authentication of users.	https://nvlpubs.nist.gov/nistpubs/Special-Publications/NIST.SP.800-63-3.pdf

REF#	CATEGORY	IDENTIFIER & TITLE	DESCRIPTION	LOCATION
111	General	**NIST Special Publication 800-82 Rev. 2 (NIST Guideline)**	**NIST Special Publication 800-82 Rev. 2 Guide to Industrial Control Systems (ICS) Security** Guide to Industrial Control System (ICS) Security, revised May 2015, describes how to secure multiple types of Industrial Control Systems against cyber attacks while considering the performance, reliability and safety requirements specific to ICS.	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf
112	General	**ISA-62443-1-1-2007 (ISA Standard)**	**Security for Industrial Automation and Control Systems Part 1-1: Terminology, Concepts, and Models** Formerly designated ANSI/ISA-99.00.01-2007, this is the first in a series of ISA standards that addresses the subject of security for industrial automation and control systems. The focus is on the electronic security of these systems, commonly referred to as cyber security. This Part 1 standard describes the basic concepts and models related to cyber security.	https://www.isa.org/store/products/product-detail/?productId=116720
113	General	**ISA–62443-2-1–2009 (ISA Standard)**	**Security for Industrial Automation and Control Systems:** Establishing an Industrial Automation and Control Systems Security Program Formerly designated ANSI/ISA-99.02.01-2009, this standard is part of a multipart series that addresses the issue of security for industrial automation and control systems. It has been developed by Working Group 2 of the ISA99 committee. This standard describes the elements contained in a cyber security management system for use in the industrial automation and control systems environment and provides guidance on how to meet the requirements described for each element. This standard has been developed in large part from a previous Technical Report produced by the ISA99 committee, ISA–TR99.00.02–2004, Integrating Electronic Security into the Manufacturing and Control Systems Environment. The majority of the contents of this Technical Report have been included in this standard and as such this standard supersedes the Technical Report. The ISA99 series addresses electronic security within the industrial automation and control systems environment. The series will serve as the foundation for the IEC 62443 series of the same titles, as being developed by IEC TC65 WG10, “Security for industrial process measurement and control - Network and system security.	https://www.isa.org/store/products/product-detail/?productId=116731
114	General	**ANSI/ISA-TR62443-2-3-2015 (ISA Standard)**	**Security for industrial automation and control systems Part 2-3: Patch management in the IACS environment** ISA-TR62443-2-3 describes requirements for asset owners and industrial automation and control system (IACS) product suppliers that have established and are now maintaining an IACS patch management program.	https://www.isa.org/store/isa-tr62443-2-3-2015,-security-for-industrial-automation-and-control-systems-part-2-3-patch-management-in-the-iacs-envi-
115	General	**ANSI/ISA-62443-2-4-2018 / IEC 62443-2-4:2015+AMD1:2017 CSV (ISA Standard)**	**Security for industrial automation and control systems, Part 2-4: Security program requirements for IACS service providers (IEC 62443-2-4:2015+AMD1:2017 CSV, IDT)** This part of ISA-62443 specifies a comprehensive set of requirements for security capabilities for IACS service providers that they can offer to the asset owner during integration and maintenance activities of an Automation Solution.	https://www.isa.org/store/ansi/isa-62443-2-4-2018-/-iec-62443-2-
116	General	**ANSI/ISA-62443-3-3 (99.03.03)-2013 (ISA Standard)**	**Security for industrial automation and control systems Part 3-3: System security requirements and security levels** This ISA99 standard, part of the ISA-62443 series, provides detailed technical control system requirements (SRs) associated with the seven foundational requirements (FRs) described in ISA-62443-1-1 (99.01.01) including defining the requirements for control system capability security levels, SL C (control system). These requirements would be used by various members of the industrial automation and control system (IACS) community along with the defined zones and conduits for the system under consideration (SuC) while developing the appropriate control system target SL, SL-T(control system), for a specific asset.	https://www.isa.org/store/products/product-detail/?productId=116785tail?p
117	General	**ANSI/ISA-62443-4-2-2018 (ISA Standard)**	**Security for industrial automation and control systems, Part 4-2: Technical security requirements for IACS components, 2nd Printing** This second printing contains an editorial corrigendum, which is detailed in the document preface. This document in the ISA-62443 series provides detailed technical control system component requirements (CRs) associated with the seven foundational requirements (FRs) described in ISA-62443-1-1 including defining the requirements for control system capability security levels and their components, SL C(component).	https://www.isa.org/store/ansi/isa-62443-4-2-2018,-security-for-industrial-automation-and-control-systems,-part-4-2-technical-2

REF#	CATEGORY	IDENTIFIER & TITLE	DESCRIPTION	LOCATION
118	General	**ANSI/ISA-62443-4-2-2018 (ISA Standard)**	**Security for industrial automation and control systems, Part 4-2: Technical security requirements for IACS components, 2nd Printing** This second printing contains an editorial corrigendum, which is detailed in the document preface. This document in the ISA-62443 series provides detailed technical control system component requirements (CRs) associated with the seven foundational requirements (FRs) described in ISA-62443-1-1 including defining the requirements for control system capability security levels and their components, SL C(component).	https://www.isa.org/store/ansi/isa-62443-4-2-2018,-security-for-industrial-automation-and-control-systems,-part-4-2-technical-security-requirements-for-iacs-components/62990952
119	General	**PCI DSS - Payment Card Industry Data Security Standard (PCI Security Standards Council Standard)**	**PCI DSS - Payment Card Industry Data Security Standard** Payment Card Industry (PCI) Data Security Standard - The Payment Card Industry Data Security Standard (PCI DSS) was developed to encourage and enhance cardholder data security.	https://www.pcisecuritystandards.org/
120	General	**The Directive on security of network and information systems (European Union Directive)**	**The Directive on security of network and information system** The NIS sets a range of network and information security requirements which apply to operators of essential services and digital service providers (DSPs). The “operators of essential services” referred to in the legislation include enterprises in the energy, transport, banking, financial market infrastructures, health, drinking water supply and distribution, and digital infrastructure sectors.	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uris-
121	General	**ANSI/ISA-TR624PAS 555:2013 (BSI Standard)**	**Cyber Security Risk - Governance and Management - Specification Standard.** The requirements of this PAS define the overall outcomes of effective cyber security. Importantly, it considers not only the technical aspects of cyber security, but also the physical, cultural and behavioural aspects, alongside effective leadership and governance.	https://shop.bsigroup.com/ProductDe-
122	General	**ISO/IEC 27033-4:2014 [ISO/IEC 27033-4:2014] (IEC Standard)**	**ISO/IEC 27033-4:2014 [ISO/IEC 27033-4:2014] Information technology — Security techniques — Network security — Part 4: Securing communications between networks using security gateways** ISO/IEC 27033-4:2014 gives guidance for securing communications between networks using security gateways (firewall, application firewall, Intrusion Protection System, etc.) in accordance with a documented information security policy of the security gateways, including: 1. identifying and analysing network security threats associated with security gateways; 2. defining network security requirements for security gateways based on threat analysis; 3. using techniques for design and implementation to address the threats and control aspects associated with typical network scenarios; and 4. addressing issues associated with implementing, operating, monitoring and reviewing network security gateway controls.	https://www.iso.org/standard/51583.ht-
123	General	**ISO/IEC 9594-8:2017(en) (ISO Standard)**	**ISO/IEC 7498-1:1994 [ISO/IEC 7498-1:1994] Information technology — Open Systems Interconnection — Basic Reference Model: The Basic Model** The model provides a common basis for the coordination of standards development for the purpose of systems interconnection, while allowing existing standards to be placed into perspective within the overall Reference Model. The model identifies areas for developing or improving standards. It does not intend to serve as an implementation specification.	https://www.iso.org/standard/20269.ht-
124	General	**ISO/IEC 7498-1:1994 [ISO/IEC 7498-1:1994] (IEC Standard)**	**Security for industrial automation and control systems, Part 4-2: Technical security requirements for IACS components, 2nd Printing** This second printing contains an editorial corrigendum, which is detailed in the document preface. This document in the ISA-62443 series provides detailed technical control system component requirements (CRs) associated with the seven foundational requirements (FRs) described in ISA-62443-1-1 including defining the requirements for control system capability security levels and their components, SL C(component).	https://www.iso.org/standard/20269.html

REF#	CATEGORY	IDENTIFIER & TITLE	DESCRIPTION	LOCATION
125	General	**ISO/IEC 27701:2019 [ISO/IEC 27701:2019] (IEC Standard)**	**ISO/IEC 27701:2019 [ISO/IEC 27701:2019] Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines** This document specifies requirements and provides guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS) in the form of an extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy management within the context of the organization.	https://www.iso.org/standard/71670.html
126	General	**BS 7858:2019 (BSI Standard)**	**Screening of individuals working in a secure environment. Code of practice** It details how to screen individuals who want to work in “secure” environments, defined as anywhere that an insider could steal or threaten the integrity of data, information, or other physical or intellectual assets; or threaten people’s safety.	https://shop.bsigroup.com/ProductDe-
127	General	**ISO/IEC 24760-1 (IEC Framework)**	**ISO/IEC 24760-1 IT Security and Privacy - A framework for identity management - Part 1: Terminology and concepts** This document defines terms for identity management, and specifies core concepts of identity and identity management and their relationships.	https://www.iso.org/standard/77582.html
128	General	**ISO/IEC 30111:2019 (IEC Standard)**	**ISO/IEC 30111:2019 Information technology — Security techniques — Vulnerability handling processes** This document provides requirements and recommendations for how to process and remediate reported potential vulnerabilities in a product or service.	https://www.iso.org/standard/69725.html
129	General	**DIN VDE 0175-110 (DIN Standard)**	**Cyber Security and Resilience Guidelines for the Smart Energy Operational Environment (IEC SyCSmartEnergy/106/DC:2019); Text in German and English** Cyber security has become an increasingly vital requirement for any business, particularly those responsible for critical infrastructures, such as power system operations responsible for managing the rapidly evolving electric system. These energy businesses must navigate their way through increasingly changing and risky business environments while continuing to provide and improve their services to end users. These business challenges include the transitions to clean energy resources and the increasing societal reliance on electrical energy. At the same time, evolving regulations, breath taking new technologies, and innovative market opportunities are impacting the existing business structures, including the interconnection of distributed energy resources owned and operated by third-parties, the rapidly expanded use of electrical vehicles, the reorganization of the power system with microgrids, availability of cloud services, and increased utilization of the Internet of Things (IoT) technologies.	https://www.vde-verlag.de/standards/1100603/e-din-vde-0175-110-
130	General	**BS 10754-1:2018 (BSI Standard)**	**Information technology. Systems trustworthiness. Governance and management specification** It provides a specification for improving the trustworthiness of systems, software and services. It’s intended to be a widely applicable approach that can be customized for any organization and software.	https://shop.bsigroup.com/ProductDe-
131	General	**ISO/IEC TS 17961:2013 [ISO/IEC TS 17961:2013] (ISO Standard)**	**ISO/IEC TS 17961:2013 [ISO/IEC TS 17961:2013] Information technology — Programming languages, their environments and system software interfaces — C secure coding rules** ISO/IEC TS 17961:2013 specifies rules for secure coding in the C programming language, and code examples. ISO/IEC TS 17961:2013 does not specify the mechanism by which these rules are enforced, or any particular coding style to be enforced. Each rule in this Technical Specification is accompanied by code examples. Two distinct kinds of examples are provided: noncompliant examples demonstrating language constructs that have weaknesses with potentially exploitable security implications; such examples are expected to elicit a diagnostic from a conforming analyser for the affected language construct; andcompliant examples are expected not to elicit a diagnostic.	https://www.iso.org/standard/61134.html
132	General	**ISO/IEC 27032:2012 [ISO/IEC 27032:2012] (ISO Standard)**	**ISO/IEC 27032:2012 [ISO/IEC 27032:2012] Information technology — Security techniques — Guidelines for cybersecurity** ISO/IEC 27032:2012 provides guidance for improving the state of Cybersecurity, drawing out the unique aspects of that activity and its dependencies on other security domains, in particular: information security, network security, internet security, and critical information infrastructure protection (CIIP). It covers the baseline security practices for stakeholders in the Cyberspace.	https://www.iso.org/standard/44375.html

REF#	CATEGORY	IDENTIFIER & TITLE	DESCRIPTION	LOCATION
133	General	**ISO/IEC 27035-1:2016 [ISO/IEC 27035-1:2016] (ISO Standard)**	**ISO/IEC 27035-1:2016 [ISO/IEC 27035-1:2016] Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management** ISO/IEC 27035-1:2016 is the foundation of this multipart International Standard. It presents basic concepts and phases of information security incident management and combines these concepts with principles in a structured approach to detecting, reporting, assessing, and responding to incidents, and applying lessons learnt.	https://www.iso.org/standard/60803.html
134	General	**ISO/IEC/IEEE 15026-1:2019(en) (ISO Standard)**	**ISO/IEC/IEEE 15026-1:2019(en) Systems and software engineering — Systems and software assurance — Part 1: Concepts and vocabulary** This document defines assurance-related terms and establishes an organized set of concepts and relationships to form a basis for shared understanding across user communities for assurance. It provides information to users of the other parts of ISO/IEC/IEEE 15026 including the combined use of multiple parts. The essential concept introduced by ISO/IEC/IEEE 15026 (all parts) is the statement of claims in an assurance case and the support of those claims through argumentation and evidence. These claims are in the context of assurance for properties of systems and software within life cycle processes for the system or software product.	https://www.iso.org/obp/ui/#iso:std:iso-iec-ieee:15026:-1:ed-1:v1:en-
135	General	**ISO/IEC/IEEE 15288:2015 [ISO/IEC/IEEE 15288:2015,ISO/IEC/IEEE 15288:2015] (ISO Standard)**	**ISO/IEC/IEEE 15288:2015 [ISO/IEC/IEEE 15288:2015,ISO/IEC/IEEE 15288:2015] Systems and software engineering — System life cycle processes** ISO/IEC/IEEE 15288:2015 establishes a common framework of process descriptions for describing the life cycle of systems created by humans. It defines a set of processes and associated terminology from an engineering viewpoint. These processes can be applied at any level in the hierarchy of a system's structure. Selected sets of these processes can be applied throughout the life cycle for managing and performing the stages of a system's life cycle. This is accomplished through the involvement of all stakeholders, with the ultimate goal of achieving customer satisfaction.	https://www.iso.org/standard/63711.html
136	General	**https://www.iso.org/standard/63711.html**	**ISO 28000:2007 Specification for security management systems for the supply chain** ISO 28000:2007 specifies the requirements for a security management system, including those aspects critical to security assurance of the supply chain. Security management is linked to many other aspects of business management. Aspects include all activities controlled or influenced by organizations that impact on supply chain security. These other aspects should be considered directly, where and when they have an impact on security management, including transporting these goods along the supply chain.	https://www.iso.org/standard/44641.html
137	General	**ISO/IEC 27037:2012 [ISO/IEC 27037:2012] (ISO Standard)**	**ISO/IEC 27037:2012 [ISO/IEC 27037:2012] Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence** ISO/IEC 27037:2012 provides guidelines for specific activities in the handling of digital evidence, which are identification, collection, acquisition and preservation of potential digital evidence that can be of evidential value. It provides guidance to individuals with respect to common situations encountered throughout the digital evidence handling process and assists organizations in their disciplinary procedures and in facilitating the exchange of potential digital evidence between jurisdictions.	https://www.iso.org/standard/44381.html
138	General	**ISO/IEC 27042:2015 [ISO/IEC 27042:2015] (ISO Standard)**	**ISO/IEC 27042:2015 [ISO/IEC 27042:2015] Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence** ISO/IEC 27042:2015 provides guidance on the analysis and interpretation of digital evidence in a manner which addresses issues of continuity, validity, reproducibility, and repeatability. It encapsulates best practice for selection, design, and implementation of analytical processes and recording sufficient information to allow such processes to be subjected to independent scrutiny when required. It provides guidance on appropriate mechanisms for demonstrating proficiency and competence of the investigative team.	https://www.iso.org/standard/44406.html
139	General	**ISO 22300:2018 (ISO Standard)**	**ISO 22300:2018 Security and resilience — Vocabulary** ISO 22300:2018 defines terms used in security and resilience standards.	https://www.iso.org/standard/68436.html
140	General	**ISO 55000:2014 (ISO Standard)**	**ISO 55000:2014 Asset management — Overview, principles and terminology** ISO 55000:2014 provides an overview of asset management, its principles and terminology, and the expected benefits from adopting asset management.	https://www.iso.org/standard/55088.html

REF#	CATEGORY	IDENTIFIER & TITLE	DESCRIPTION	LOCATION
141	General	**Introduction to Cyberspace (CPNI/ NCSC Online resource)**	**Introduction to Cyberspace** Provides Introduction- "Cyberspace" is the term used to describe the electronic medium of digital networks used to store, modify and communicate information. It includes the Internet but also other information systems that support businesses, infrastructure and services.	https://www.cpni.gov.uk/cyber https://www.youtube.com/user/UKCPNI
142	General	**10 steps to cyber security (NCSC Online resource)**	**10 steps to cyber security** Guidance on how organisations can protect themselves in cyberspace. Includes: • A board level responsibility • Common cyber attacks - reducing the impact • The 10 Steps	https://www.ncsc.gov.uk/collec-
143	General	**Small & medium sized organisations Cyber security advice (NCSC Online resource)**	**Small & medium sized organisations Cyber security advice** Cyber security advice for businesses, charities, clubs and schools with up to 250 employees.	https://www.ncsc.gov.uk/section/information-for/small-medium-sized-organisations
144	General	**Large organisations Cyber security advice (NCSC Online resource)**	**Large organisations Cyber security advice** Cyber security advice for businesses, charities and critical national infrastructure with more than 250 employees. You are likely to have a dedicated team managing your cyber security.	https://www.ncsc.gov.uk/section/information-for/large-organisations
145	General	**Public sector Cyber security advice (NCSC Online resource)**	**Public sector Cyber security advice** Cyber security guidance for public sector organisations employees.	https://www.ncsc.gov.uk/section/information-for/public-sector
146	General	**NCSC certification (NCSC Online resource)**	**NCSC certification** The NCSC, working with partners, offer certification that covers a range of products, services and organisations. This includes: • Certified Assisted Products (CAPS) • Penetration testing (CHECK) • Commercial Product Assurance (CPA) • Assured Services (CAS) • Cyber Incident Response (CIR)	https://www.ncsc.gov.uk/section/products-services/ncsc-certification
147	General	**Cyber Essentials (Cyber Essentials Online resource)**	**Cyber Essentials** Cyber Essentials helps to guard against the most common cyber threats and demonstrates commitment to cyber security: • Cyber Essentials • Cyber Essentials Plus	https://www.ncsc.gov.uk/cyberessentials/overview
148	General	**Guide to the General Data Protection Regulation (GDPR) (ICO Online resource)**	**Guide to the General Data Protection Regulation (GDPR)** The Guide to the GDPR is part of our Guide to Data Protection. It is for DPOs and others who have day-to-day responsibility for data protection. It explains the general data protection regime that applies to most UK businesses and organisations. It covers the General Data Protection Regulation (GDPR) as it applies in the UK, tailored by the Data Protection Act 2018.	https://ico.org.uk/for-organisations/guide-to-data-protection/
149	General	**Government Security Classifications (UK Government Online resource)**	**Government Security Classifications** Everyone who works with UK government has a duty to respect the confidentiality and integrity of any HMG information and data that they access, and is personally accountable for safeguarding assets in line with this policy. Government Departments and Agencies should apply this policy and ensure that consistent controls are implemented throughout their public sector delivery partners (i.e. NDPBs and Arms Length Bodies) and wider supply chain.	https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715778/May-2018_Government-Security-Classifications-2.pdf
150	General	**EU-US Privacy Shield (U.S. Department of Commerce and the European Commission and Swiss Administration Online resource)**	**EU-US Privacy Shield** The EU-U.S. and Swiss-U.S. Privacy Shield Frameworks were designed by the U.S. Department of Commerce and the European Commission and Swiss Administration to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the European Union and Switzerland to the United States in support of transatlantic commerce.	https://www.privacyshield.gov/welcome

REF#	CATEGORY	IDENTIFIER & TITLE	DESCRIPTION	LOCATION
151	General	**Cyber security and information risk guidance for Audit Committees (ETSI Online resource)**	**Cyber security and information risk guidance for Audit Committees** As government's guidance to audit committees makes clear, cyber security is now an area of management activity that audit committees should scrutinise 1 Together with the rapidly changing nature of the risk, this means that there is an important role for audit committees in understanding whether management is adopting a clear approach, if they are complying with their own rules and standards and whether they are adequately resourced to carry out these activities	https://www.etsi.org/committee/cyber
152	General	**Top tips for staying secure online (NCSC Online resource)**	**Top tips for staying secure online** General tip to stay secure online. This is online guidance.	https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online
153	General	**Cyber Security Toolkit for Boards (NCSC Online resource)**	**Cyber Security Toolkit for Boards** Resource used to help to develop your own cyber security board strategy - one that can adapt to fit your own unique cultures and business priorities. A general introduction to cyber security. Separate sections, each dealing with an important aspect of cyber security. For each aspect, we will: • explain what it is, and why it's important • recommend what individual Board members should be doing • recommend what the Board should be ensuring your organisation is doingprovide questions and answers which you can use to start crucial discussions with your cyber security	https://www.ncsc.gov.uk/collection/board-toolkit
154	General	**Cloud guidance (NCSC Online resource)**	**Cloud guidance** Guidance on how to configure, deploy and use cloud services securely	www.ncsc.gov.uk/guidance/cloud-security-standards-and-definitions
155	General	**Security frameworks (NCSC Online resource)**	**Security frameworks** Guidance to help organisations make decisions about cyber security risk.	www.ncsc.gov.uk/guidance/summary-risk-methods-and-frameworks
156	General	**Assessment of organisations information security maturity – previously centrally mandated but still used by many departments (NCSC Online resource)**	**Assessment of organisations information security maturity – previously centrally mandated but still used by many departments** HMG IA Maturity Model -No longer supported by the NCSC, but organisations may choose to continue to use the Maturity Model to assess and improve their security effectiveness. Services which were offered as part of the support for the Maturity Model - the independent review and the supported self-assessment - have been withdrawn.	www.ncsc.gov.uk/articles/hmg-ia-maturity-model-iamm
157	General	**Cyber Assurance of Physical Security Systems (CAPSS)– 2019 (CPNI/NCSC Online resource)**	**Cyber Assurance of Physical Security Systems (CAPSS) – 2019** This document describes the features, testing and deployment requirements necessary to meet CPNI CAPSS certification for physical security systems. It is intended for vendors, system architects, developers, evaluation and technical staff operating within the security arena. It describes minimum baseline requirements for physical security systems for evaluation and certification under CPNI's Cyber Assurance of Physical Security Systems (CAPSS) standard for inclusion in the Catalogue of Security Equipment (CSE) published by CPNI. Where there is no CSE chapter, the product only needs to be CAPSS evaluated. (https://www.cpni.gov.uk/cse-categories)	https://www.cpni.gov.uk/cyber-assurance-physical-security-systems-capss
158	General	**Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (NIST Framework)**	**Framework for Improving Critical Infrastructure Cybersecurity** This publication describes a voluntary risk management framework (""the Framework"") that consists of standards, guidelines, and best practices to manage cybersecurity-related risk. The Framework's prioritized, flexible, and cost-effective approach helps to promote the protection and resilience of critical infrastructure and other sectors important to the economy and national security. This release, Version 1.1, includes a number of updates from the original Version 1.0 (from February 2014), including: a new section on self-assessment; expanded explanation of using the Framework for cyber supply chain risk management purposes; refinements to better account for authentication, authorization, and identity proofing; explanation of the relationship between implementation tiers and profiles; and consideration of coordinated vulnerability disclosure.	https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11

REF#	CATEGORY	IDENTIFIER & TITLE	DESCRIPTION	LOCATION
159	General	**NCSC CPA Build Standard (NCSC Standard)**	**NCSC CPA Build Standard** CPA covers the independent testing of commercial products with security-enforcing functions for public sector use. The Commercial Product Assurance was set up to help companies demonstrate that the security functions of their products met NCSC standards, and help the UK public sector identify those products whose security claims were backed by independent testing.	https://www.ncsc.gov.uk/information/commercial-product-assurance-cpa
160	General	**CPNI Control Rooms Guidance (CPNI Online resource)**	**CPNI Control Rooms Guidance** It is general guidance only and needs to be adapted for use in specific situations. This guidance is issued by the UK's Centre for the Protection of National Security (CPNI) with the aim of helping organisations that make up the national infrastructure improve their protective security. It is general guidance only and needs to be adapted for use in specific situations.	https://www.cpni.gov.uk/system/files/documents/73/38/Control%20Rooms%20Guidance%20Dec%202016.pdf
161	General	**End User Device Security Collection (NCSC Online resource)**	**End User Device Security Collection** Guidance for organisations deploying a range of end user device platforms as part of a remote working solution. This guidance is for any organisation wishing to secure the EUDs they use, but it is primarily to help system administrators make informed decisions about the configuration, management and use of EUDs, and risk owners understand the overall risk to their networks presented by their use.	https://www.ncsc.gov.uk/collection/end-user-device-security
162	General	**NCSC Guidance – using IPsec to protect data (NCSC Online resource)**	**NCSC Guidance – using IPsec to protect data** Guidance for organisations wishing to deploy or buy network encryption, using IPsec. This guide is for the protection of information flows within a single organisation, or within a group of organisations, across bearer networks such as the Internet, a commercial WAN circuit, or the Public Services Network (PSN) for public sector organisations.	https://www.ncsc.gov.uk/guidance/using-ipsec-protect-data
164	General	**ISO 29147 (ISO Standard)**	**ISO 29147 Information technology — Security techniques — Vulnerability disclosure** This document provides requirements and recommendations to vendors on the disclosure of vulnerabilities in products and services. Vulnerability disclosure enables users to perform technical vulnerability management as specified in ISO/IEC 27002:2013, 12.6.1[1]. Vulnerability disclosure helps users protect their systems and data, prioritize defensive investments, and better assess risk. The goal of vulnerability disclosure is to reduce the risk associated with exploiting vulnerabilities. Coordinated vulnerability disclosure is especially important when multiple vendors are affected. This document provides: • guidelines on receiving reports about potential vulnerabilities; • guidelines on disclosing vulnerability remediation information; • terms and definitions that are specific to vulnerability disclosure; • an overview of vulnerability disclosure concepts; • techniques and policy considerations for vulnerability disclosure; • examples of techniques, policies (Annex A), and communications (Annex B).	https://www.iso.org/standard/72311.html
165	General	**Suitable list of compromised passwords (NCSC Online resource)**	**Suitable list of compromised passwords** A list of common compromised passwords. This is a guidance.	https://www.ncsc.gov.uk/static-assets/documents/PwnedPasswordsTop100k.txt
166	General	**NCSC Guidance – using TLS to protect data (NCSC Online resource)**	**NCSC Guidance – using TLS to protect data** Transport Layer Security (TLS) is a protocol which provides privacy between communicating applications and their users, or between communicating services. When a server and client communicate, well-configured TLS ensures that no third party can eavesdrop or tamper with any message.	https://www.ncsc.gov.uk/guidance/tls-external-facing-services
167	General	**The HMG Security policy framework (UK Government Online resource)**	**The HMG Security policy framework** Security policy framework: protecting government assets. The security policy framework describes the standards, best-practice guidelines and approaches that are required to protect UK government assets (people, information and infrastructure). It focuses on the outcomes that are required to achieve a proportionate and risk-managed approach to security that enables government business to function effectively, safely and securely.	https://www.gov.uk/government/publications/security-policy-framework

REF#	CATEGORY	IDENTIFIER & TITLE	DESCRIPTION	LOCATION
168	General	**Internet Engineering Task Force (IETF Online resource)**	**Internet Engineering Task Force** Internet Engineering Task Force is an open standards organization, which develops and promotes voluntary Internet standards, in particular the standards that comprise the Internet protocol suite.	https://www.ietf.org/standards https://www.ietf.org/topics/security/
169	General	**AESIN (Online resource)**	**AESIN** AESIN is a dedicated UK initiative focused on the advanced delivery of Electronic Systems into vehicles and infrastructure operated by the UK Trade .AESIN is a collaborative, non-profit, response to the Automotive Sector Revolution in complex Electronic Systems enabling technology for the more Electric Connected and Automated vehicles of tomorrow.	https://aesin.org.uk/work-streams/
170	General	**Integrated Transport Smartcard Organisation (ITSO Online resource)**	**Integrated Transport Smartcard Organisation** ITSO Ltd is a non-profit distributing technical, standardisation and interoperability membership organisation with objectives to: maintain and develop the ITSO specification for transport smartcards. ITSO Smart ticketing is a system that electronically stores a travel ticket on a microchip, which is then usually embedded on a smartcard. ITSO has received certification to the Government's Cyber Essentials scheme, demonstrating the continued commitment to cyber security best practice. ITSO Specification is the UK technical standard for interoperable smart ticketing.	https://www.itso.org.uk/
171	General	**The key principles of vehicle cyber security for connected and automated vehicles (UK Government Online resource)**	**The key principles of vehicle cyber security for connected and automated vehicles** The Department for Transport, in conjunction with Centre for the Protection of National Infrastructure (CPNI), have created the following key principles for use throughout the automotive sector, the CAV and ITS ecosystems and their supply chains.	https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles/the-key-principles-of-vehicle-cyber-security-for-connected-and-automated-vehicles
172	General	**UK Defence Standardization (UK Government Online resource)**	**UK Defence Standardization** Defence Standardization develops and pursues MOD's standardization policy, both nationally and internationally, with civil and military partners to support increased interoperability and more effective acquisition.	https://www.gov.uk/guidance/uk-defence-standardization
173	General	**Protocol security and Security (ITU Online resource)**	**Protocol security and Security** **Protocol security 2019 - QSTR-SS7-DFS - SS7 vulnerabilities and** mitigation measures for digital financial services transactions Security 2015 - Security in Telecommunications and Information Technology 2016 - XSTR-SUSS - Successful use of security standards 2014 - Current and new challenges for public-key infrastructure standardization	https://www.itu.int/pub/T-TUT
174	General	**How the USA department of transportation is protecting the connected transportation system from cyber threats. (U.S. Department of Transport Online resource)**	**How the USA department of transportation is protecting the connected transportation system from cyber threats.** Flyer on the different element of ITS and cyber security. This is a guidance.	https://www.its.dot.gov/factsheets/pdf/cybersecurity_factsheet.pdf
175	General	**Supply chain security guidance (NCSC Online resource)**	**Supply chain security guidance** Proposing a series of 12 principles, designed to help you establish effective control and oversight of your supply chain.	https://www.ncsc.gov.uk/collection/supply-chain-security
176	General	**Secure design principles (NCSC Online resource)**	**Secure design principles** Guides for the design of cyber secure systems	https://www.ncsc.gov.uk/collection/cyber-security-design-principles

REF#	CATEGORY	IDENTIFIER & TITLE	DESCRIPTION	LOCATION
177	General	**Crown Commercial Services - Cyber Security Services 3 Framework (Online Resource)**	**Framework for Procurement of Cyber Security Services** This framework provides a dynamic purchasing system (DPS) that allows public sector buyers to procure an extensive variety of cybersecurity services from a range of pre-qualified suppliers. Two distinct routes to finding pre-qualified suppliers ware provided. The first route provides the buyer with suppliers who are assured by the National Cyber Security Centre (NCSC). Using this filter will ensure that your supplier has been assessed by NCSC, the National Technical Authority for cyber security in the UK. The second route provides the buyer with a set of suppliers who provide similar services to those under the NCSC assured route but without the assurance the National Technical Authority provides.	https://www.crowncommercial.gov.uk/agreements/RM3764.3
178	General	**ISO 27001:2013 (ISO Standard)**	**ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements** ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization..	https://www.iso.org/standard/54534.html
179	General	**ISO 20000-1:2018 (ISO Standard)**	**ISO/IEC 20000-1:2018 Information technology — Service management** ISO/IEC 27001:2013 specifies requirements for an organization to establish, implement, maintain and continually improve a service management system (SMS). The requirements specified in this document include the planning, design, transition, delivery and improvement of services to meet the service requirements and deliver value.	https://www.iso.org/standard/70636.html