



Ministry of Electronics &
Information Technology
Government of India

DSCI
PROMOTING DATA PROTECTION
A NASSCOM® Initiative



National Centre
of Excellence
CYBERSECURITY TECHNOLOGY
AND ENTREPRENEURSHIP



CYBERSECURITY
CENTRE of EXCELLENCE
A joint initiative of DSCI & Government of Telangana

ROAD TO

IOT

STANDARDS

NOVEMBER

2022

TABLE OF CONTENTS

01	SECURITY STANDARDS: WHY DO THEY MATTER?	05
02	STANDARD BODIES	06
03	IOT SECURITY STANDARDS	08
	1.ISO/IEC 30141: IOT (INTERNET OF THINGS) - REFERENCE ARCHITECTURE	
	1.1. Generic characteristics of IoT systems	
	1.1.1.IoT system trustworthiness characteristics	
	1.1.2.IoT system architecture characteristics	
	1.1.3.IoT system functional characteristics	
	1.2.IoT Conceptual Model (CM)	
	1.3.IoT Reference Model (RM)	
	1.3.1.Entity-based RM	
	1.3.2.Domain-based RM	
	1.3.3.Relation between entity-based RM and domain-based RM	
	1.4.IoT Reference Architecture (RA) Views	
	1.4.1. IoT RA functional view	
	1.4.2. IoT RA system deployment view	
	1.4.3. IoT RA networking view	
	1.4.4. IoT RA usage view	
	2. ISO/IEC 27400: GUIDELINES FOR SECURITY AND PRIVACY IN IOT	26
	2.1 Issues that are addressed by this standard	
	2.2 Purpose and Justification	
	2.3 Stakeholders	
	2.4 Recommended Standards referred to in ISO/IEC 27400	
	2.5 ISO/IEC 27400 Identified Controls	
	3. ISO/IEC 27402: IOT SECURITY AND PRIVACY - DEVICE BASELINE REQUIREMENTS	31
	4. UNECE WP.29 CYBERSECURITY REGULATION (UN155): VEHICLE CYBER SECURITY MANAGEMENT SYSTEM & SECURE UPDATE MANAGEMENT SYSTEM	32
	4.1. Requirements for cyber security management	
	4.2. Requirements for vehicle types	
	4.3. List of provisions	



TABLE OF CONTENTS

5. ISO /SAE 21434: ROAD VEHICLE CYBERSECURITY ENGINEERING

40

- 5.1 Existing Policy and Upcoming Recommendations
- 5.2 Vulnerability Analysis
- 5.3 Vulnerability Management
 - 5.3.1 Risk Assessment Methods
- 5.4 Concept Phase
 - 5.4.1 Product Development
 - 5.4.2 Cybersecurity Validation
 - 5.4.3 Production
 - 5.4.4 Operations and Maintenance
 - 5.4.5 Cybersecurity Incident Response

6. ETSI EN 303645: CYBERSECURITY FOR CONSUMER IOT

49

- 6.1 Cybersecurity provisions for consumer IoT
 - 6.1.1 No universal default passwords
 - 6.1.2 Implement a means to manage reports of vulnerabilities
 - 6.1.3 Keep software updated
 - 6.1.4. Securely store sensitive security parameters
 - 6.1.5. Communicate securely
 - 6.1.6. Minimize exposed attack surfaces
 - 6.1.7. Ensure software integrity
 - 6.1.8. Ensure that personal data is secure
 - 6.1.9. Make systems resilient to outages
 - 6.1.10. Examine system telemetry data
 - 6.1.11. Make it easy for users to delete user data
 - 6.1.12. Make installation and maintenance of devices easy
 - 6.1.13. Validate input data
- 6.2. Data protection provisions for consumer IoT

7. ISA/IEC 62443: CYBERSECURITY FOR INDUSTRIAL AUTOMATION & CONTROL SYSTEMS

57

8. CYBERSECURITY FOR MEDICAL DEVICES

62

- 8.1 Current State of Cybersecurity Requirements for Medical Devices
- 8.2 Role of IEC 81001-5-1 in Strengthening Cybersecurity
- 8.3 MDCG 2019-16 Guidance on Cybersecurity for medical devices
- 8.4 US FDA 510 (K) Pre-Market Guidelines for Device Security – 2022

TABLE OF CONTENTS

	9. IMDRF	71
	9.1. Principles and Practices for Medical Device Cybersecurity –2020	
	9.2. IMDRF - Principles and Practices for Medical Device Cybersecurity of Legacy Devices 2022	
	10. FIDO Device Onboarding (FDO)	77
	11. Software Bill of Materials (SBOM)	83
04	CONCLUSION	89
05	ABBREVIATIONS	90
06	REFERENCES	92

SECURITY STANDARDS:

Why Do They Matter?

With the rise in cyber-attacks and data breaches, it is no doubt that we need to take better precautions to protect our digital assets. Any business or organization must take the necessary steps to protect itself.

Standards are largely trusted by stakeholders and businesses, and if anybody can show that their products meet these requirements, it gives them a lot of credibility. They offer the most reliable information and are updated from time to time.

A security standard is a guideline or a set of rules and regulations that determines how organizations use various methods to safeguard their data and prevent unauthorized access. Security standards help the organization identify and track what it needs to do to maintain its data integrity, confidentiality, and availability. They also provide a framework for organizations looking to adopt best practices for protection. They also serve as a set of requirements that helps organizations and individuals comply with laws and regulations.

The number of cyber security standards is growing. Governments and corporations require their deployment more frequently. These security standards play a significant role in risk management and security enhancement. They assist in defining the capabilities that are necessary for secure systems as well as standard security requirements. By fostering a shared understanding of security issues, security standards promote the exchange of information and best practices.

Security standards improve an organization's overall risk management and physical security in several ways. By fostering a shared understanding of conditions, terms, and definitions that can help avoid expensive mistakes, security standards also facilitate the exchange of knowledge and best practices.

In this document, we shall/will cover the different security standards for IoT and why they are essential for keeping digital data secure.

STANDARD BODIES

Following are a few standard bodies that formulate standards catering to various fields:

ISO:

The International Organization for Standardization (ISO) is a global organization that seeks to establish standardization across a wide range of products and businesses. ISO is a voluntary organization made up of standard-setting bodies from over 160 countries, with one standard-setting body representing each member country. Its primary purpose is to facilitate trade, but it is also concerned with process improvement, safety, and quality in various domains.

IEC:

The International Electrotechnical Commission (IEC) is a global standards body that develops and publishes international standards for all electrical, electronic, and related technology. IEC standards include a wide range of technologies, including power generation, transmission, and distribution, household appliances, semiconductors, fiber optics, batteries, solar energy, nanotechnology, and marine energy. The IEC also oversees four global conformity assessment systems, which certify whether equipment, systems, or components meet international standards. IEC standards also apply to all electro technologies, including energy generation and distribution, electronics, magnetics, multimedia, telecommunications, and medical technology, as well as related general disciplines such as terminology and symbols, electromagnetic compatibility, measurement and performance, dependability, design and development, safety, and the environment.

ETSI:

European Telecommunications Standards Institute is a non-profit organization aiming to develop telecommunications standards throughout Europe. ETSI standards may be approved as the technical basis for directives or regulations by the European Commission. The primary responsibility of ETSI is to eliminate all deviations from global standards and to focus on a defined, European-specific set of requirements. ETSI also ensures standard interoperability, such as Integrated Services Digital Network, GSM, and Universal Mobile Telecommunications System (UMTS).

US FDA:

The Food and Drug Administration of the United States (FDA or USFDA) is a federal agency of the Department of Health and Human Services. The FDA oversees protecting and promoting public health by regulating and supervising food safety, tobacco products, dietary supplements, prescription and over-the-counter pharmaceutical drugs, vaccines, electromagnetic radiation emitting devices (ERED), cosmetics, animal foods and feed, and veterinary products.

ISA:

International Society of Automation is a non-profit organization for technicians, management, and engineering professionals. Founded in 1945, it helps its members worldwide with services and programs on leadership, organizational, and communication skills. It plays a pivotal role in developing national and international standards, publishing books and technical articles, certifying industry professionals, and providing training. ISA has been acknowledged as the authoritative source for automation and control systems consensus industry standards since 1949.

UNECE:

United Nations Economic Commission for Europe, one of the five regional commissions of the United Nations was founded in 1947. UNECE is devoted to policy dialogue, capacity building, development of regulations, exchange and application of best practices, and technical cooperation for Eastern Europe, the Caucasus, and Central Asia countries. It focuses on the United Nations' global economic mandates in collaboration with other international players and important stakeholders, most notably the business sector.

NIST:

The National Institute of Standards and Technology, founded in 1901 in the USA, is one of the nation's oldest physical science laboratories. Currently, NIST measurements support technologies of all types and sizes, aiming to promote American innovation and industrial competitiveness. Its core competencies are Measurement Science, Rigorous traceability, and Development and Use of Standards. In cybersecurity, NIST develops standards, best practices, guidelines, and other resources that the US industries, agencies, and the public can follow.

ENISA:

The European Union Agency for Cybersecurity, founded in 2004, is the EU's agency that specifically thrives to achieve "a high common level of cybersecurity across Europe". It develops risk management and risk assessment methods, analyses data of emerging risks in Europe, helps in framing cyber policies in Europe, and organises knowledge-sharing, capability building, and awareness sessions.

BSI:

The British Standards Institution, also founded in 1901 as the Engineering Standards Committee, is the recognized National Standards Body of the UK. It is one of the largest certification bodies across the globe and played a key role in forming the ISO. It creates standards for technical and management purposes, including a wide range of industry sectors. It also awards the BSI Kitemark, a trademark that is highly known and trusted worldwide.

IOT SECURITY STANDARDS:

1. ISO/IEC 30141: IOT (INTERNET OF THINGS) - REFERENCE ARCHITECTURE

ISO/IEC 30141, IoT Reference Architecture stipulates an internationally standardized Internet of Things (IoT) Reference Architecture utilizing reusable designs, straightforward vocabulary, and industry best practices. ISO/IEC 30141 aims to provide a common framework for designers and developers of IoT applications and enable "trustworthy" systems that are reliable, safe, secure, respect privacy, and can withstand natural disasters and attacks.

This document has the following descriptions:

1.1. Generic characteristics of IoT systems

The document describes two types of characteristics: functional and non-functional.

These characteristics are also categorized into three types:

1.1.1. IoT system trustworthiness characteristics

Category - IoT System Trustworthiness	Characteristics
1.	Availability
2.	Confidentiality
3.	Integrity
4.	Protection of personally identifiable information
5.	Reliability
6.	Resilience
7.	Safety

1) Availability

- a) Availability means always being available for use and access by authorized entities.
- b) In IoT systems, the property of availability is regarded as a characteristic of devices, data, and services.

- Devices – in terms of network connectivity and operability
 - Data – in terms of the ability of the system to acquire data upon request
 - Services – in terms of the ability of the system to provide services with a pre-defined Quality of Service (QoS)
- c) Applicable in systems/applications like health monitoring or intrusion detection

2) Confidentiality

- a) The property of confidentiality ensures that authorized information is not disclosed to unauthorized entities.
- b) In IoT systems, confidentiality protection policies deter the leakage of sensitive information such as PII and ensure secure operation.
- c) Applicable in devices/ applications like IoT motion detection sensors and IoT smart meters, which collect the personal information of their users.

3) Integrity

- a) Integrity as a property ensures the accuracy and comprehensiveness of a system.
- b) In IoT systems, the collected information is generally used to make decisions. This property checks data alteration by malicious actors, faulty devices, or natural disasters.
- c) Applicable in systems where there are multiple nodes operating in each system.

4) Protection of personally identifiable information (PII)

- a) This document follows the definition of PII set by ISO/IEC 27018:2014, 3.2: “Any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal.”
- b) In IoT systems, the appropriate entities are people, technology, and processes. Any IoT systems that collect, receive, process, or share PII must ensure compliance with their respective judiciaries.
Local judiciary laws and compliance play an important role in IoT systems.

- c) The IoT system owner and operator act as the PII controller, independent of the IoT application.

5) Reliability

- a) Reliability refers to the system producing consistent results and premeditated behaviour.

The desired level of reliability and risk go together. Hence, the designer of an IoT system can evaluate the risk of changing the system using a risk management process as mentioned in ISO 31010.

- b) In IoT systems that are time-critical, reliability is highly essential. Incorrect or misleading information can corrupt the whole system/process.
- c) Applicable in applications/devices like industrial manufacturing operations and medical devices.

6) Resilience

- a) Resilience helps systems to remain adaptable and flexible to ad hoc changes and resistant to failures without loss of performance.
- b) Most IoT devices work in congregations and are prone to failures. IoT systems must be designed in a way that they can self-monitor and self-heal.
- c) Applicable in industrial control devices and networks.

7) Safety

- a) Here, safety relates to an acceptable level of risk of harm. It considers levels of failure to prevent or avoid harm.
- b) In most IoT systems, if failure modes are not addressed, then it might result in damage, loss, injury, or death.
- c) Applicable in applications like medical or health care applications, automotive applications, and environment monitoring.

1.1.2. IoT system architecture characteristics

Category – IoT System Architecture	Characteristics
1.	Composability
2.	Functional and management capability separation
3.	Heterogeneity
4.	Highly distributed systems
5.	Legacy support
6.	Modularity
7.	Network connectivity
8.	Scalability
9.	Shareability
10.	Unique identification
11.	Well-defined components

1) Composability

- a) It refers to the ability to integrate individual IoT components into an IoT system to fulfill a set of goals.
- b) System integration, interoperability, and composability provide information on building a fully functional IoT system. Composability is more stringent than interoperability, as it requires components that are both compatible and exchangeable.
- c) Applicable in devices like temperature sensors in buildings and vendor specific IoT controllers.

2) Functional and management capability separation

- a) A separation between the functional and management capabilities of an IoT component are observed because these capabilities are handled by different software components and work on different endpoints.
- b) Management capabilities and functional capabilities logically differ in terms of purposes, user roles, classification and types of data, access, and protocols, formats and life cycles. There are numerous situations where it is essential to restrict access to an IoT system or component to a select few of the entities with which the data is shared from that IoT system.

- c) Applicable to systems like HVAC or other building management systems.

3) Heterogeneity

- a) A broad range of Physical Entities and IoT system components that interact differently.
- b) IoT systems typically exist as cross-product, cross-domain, and cross-system. This brings a significant challenge to the heterogeneity of interconnected IoT systems.
- c) Examples of heterogeneity can be temperature sensors from different vendors with different specifications.

4) Highly distributed systems

- a) Such systems can be fully functionally integrated while also consisting of sub-systems that can be separated from each other and are usually connected by a communication link like a data bus.
- b) In the way that IoT systems can exist locally or globally, data can also be stored at the edge of the network, centrally, or both. Similarly, processing can also take place centrally or at the edge of the network.
- c) Applicable to the distributed assembly lines in the smart manufacturing systems of Industry 4.0.

5) Legacy support

- a) Components, protocols, devices, etc., that are outdated but still in use can be incorporated into IoT systems.
- b) Legacy systems are generally more susceptible to risk and vulnerabilities. Care must be taken when using these with newer devices/systems so that they do not hamper the security or performance of the device/system. Many IoT systems have a combination of legacy devices and updated devices.
- c) Example – migration from IPv4 compliance to IPv6 compliance

6) Modularity

- a) Modularity is a property where smaller components are combined to form larger systems. These modular components should be such that they can be removed or replaced without any disturbance to the system's operation.
- b) Standardized interfaces allow implementers flexibility in designing components and IoT systems.
- c) Applicable to devices like smart thermostats.

7) Network connectivity

- a) Components of an IoT system communicate via network links, using either wired or wireless media. It is at the core of IoT that these entities can communicate with other entities over a communications network.
- b) IoT systems exchange information using different inter-networked connections in a structured manner. The IoT network structure can be static or dynamic.
- c) Applicability depends on the scale of the IoT network.

8) Scalability

- a) When a system continues to work effectively despite increasing its size, volume of work, or complexity, then scalability is achieved.
- b) IoT systems use a variety of elements like devices, services, event reports, networks, etc. It is important to ensure that the system continues to operate effectively when the number of changes increases.
- c) An example is when the number of sensors attached to an IoT system varies over time.

9) Shareability

- a) It refers to the limit to which an individual component and its resources can be accessed.
- b) Most of the components in IoT systems end up underutilized as their capability is not realized or known. Using them to their capability can lead to increased efficiency.
- c) An example is that the temperature sensing for heating control can be used by the security system for fire detection and control.

10) Unique identification

- a) The components and entities of an IoT system must be associated with an individual name, code, symbol, or a number and must be referenced with the same.
- b) Like how most things are standardized to be understood globally, components of IoT systems must also be associated with unique identification to enable interoperability across heterogeneous systems.
- c) Applicable to individual hardware devices, software, and other entities.

11) Well-defined components

- a) Availability of relevant information and description of the capabilities and characteristics of IoT entities, along with their uncertainties, accounts for well-defined components.
- b) A lack of understanding of the capabilities of the IoT system components makes it difficult to understand the design goals of the system.
- c) Applicable to IoT components with varying amounts of memory or support.

1.1.3. IoT system functional characteristics

Category - IoT System Functional	Characteristics
1.	Accuracy
2.	Auto-configuration
3.	Compliance
4.	Content-awareness
5.	Context-awareness
6.	Data characteristics – volume, velocity, veracity, variability, and variety
7.	Discoverability
8.	Flexibility
9.	Manageability
10.	Network communication
11.	Network management and operation
12.	Real-time capability

13.	Self-description
14.	Service subscription

1) Accuracy

- a) It refers to the closeness between the measured values and actual values of an output.
- b) Varying levels of accuracy are required for different IoT systems based on their configuration, operation, and output expectation.
- c) Applicable in most scenarios but critical in applications in a medical or manufacturing context.

2) Auto-configuration

- a) The automatic configuration of devices based on the interworking of preset rules, which includes automatic networking, automatic service provisioning, and plug & play. Authorized components should only be auto-configured into the system.
- b) The configurations of large-scale IoT systems keep changing over time. Auto-configuration is key in such cases as they ease the process for users with heavy reliability requirements.
- c) An example is Zero Configuration Networking (Zeroconf™).

3) Compliance

- a) Compliance requires the IoT system and its components to abide by the predefined rules, laws, regulations, standards, or policies.
- b) Compliance in IoT systems includes regulations to assure interoperability, to ratify functionality or capability, to assess the functioning of an IoT device or system without causing trouble, etc.
- c) Applicable to categories like safety regulations, RF related regulations, and consumer protection regulations.

4) Content-awareness

- a) To be aware of the information in an IoT component and its associated metadata. Devices with content awareness are capable of locating services, increasing information retrieval accuracy, abstracting application data, etc.

- b) Based on criteria such as location, quality of service needs, and data sensitivity, content awareness supports suitable functional activities such as data routing, delivery speed, and security features such as encryption.
- c) Applicable to applications including health services, broadcasting, surveillance systems, and emergency services.

5) Context-awareness

- a) It is a characteristic of an IoT device or system to monitor the environment in which it is operating to determine the when, where, and what of the events.
- b) IoT devices are designed to be customizable and flexible to the user's choice. They are not meant to conform only to the rules set by their manufacturer. In this context, context-awareness allows customized and autonomic services of related IoT components.
- c) Applicable to services like location-based services and fire services.

6) Data Characteristics

- a) The five Vs of data are volume, velocity, veracity, variability, and variety. They are derived from big data systems but often, IoT systems produce large volumes of data sent at high speed through network links, the veracity of which must be checked, which might vary over time and contain a wide variety of data types from various IoT components.
- b) IoT systems spread globally generate large amounts of data. This data can be stored in a centralized location or distributed locations, which needs to be appropriately indexed, stored, processed, and secured.
- c) Applicable to companies using big data analytics and having multiple data points.

7) Discoverability

- a) In IoT systems, discoverability owes to a network endpoint being found dynamically and for it to report its services and capabilities through either a query mechanism or a self-advertising mechanism. Endpoints here may refer to IoT devices, services, applications, or users.

- b) IoT systems can use discovery/lookup services to find other devices, services, or systems based on attributes such as geographical location, capabilities, interfaces, accessibility, ownership, security policy, operational configuration, or other relevant variables.
- c) Examples include Hypercat and Consul.

8) Flexibility

- a) When an IoT system or component is flexible, it provides an array of functionality depending on the need or context.
- b) The document defines the flexibility distinction between the following kinds of components:
 - 1) a device that has fixed, nonprogrammable, non-extensible functionality – “hard-wired single purpose”;
 - 2) a device that has fixed hard-wired capability, but provides some amount of configurability within the single available format;
 - 3) a device that is both programmable and expandable in the hardware domain – such as adding memory, adding more computational capability, or adding RF channel capability;
 - 4) a family of devices, each of which might fall into categories 1) to 3), from which an integrator can select the one(s) which are appropriate for a given context;
 - 5) a family of devices such as in 4), where some of the options provide different amounts of composability or modularity at different levels of abstraction
- c) Example – thermostat

9) Manageability

- a) Device management, network management, system management, interface maintenance and alerts are all parts of manageability in IoT systems.
- b) Most IoT devices, networks, and systems are designed to work autonomously. Such systems must be manageable even when there are missing or faulty parts in the system.
- c) Example – smoke sensor deployed in various parts of a building.

10) Network communication

- a) IoT systems operate on various networks – limited range, low power networks, wide area networks, and wired and wireless networks. The communication protocols differ between these different types of networks.
- b) IoT systems are heavily dependent on connected networks to exchange information. Gateways can be used to connect multiple types of networks, often between proximity networks and wide-area networks.
- c) Applicable to protocols such as Netconf and IoT-specific 6LoWPAN.

11) Network management and operation

- a) The nature and purpose of network administration and operation are determined by network type, network ownership, and communication mode over the network. During the initial configuration and deployment of a network, management is necessary, including the handling of device identification and addresses, network profiles, and including dynamic management capabilities.
- b) IoT network management must cover both proximity networks and wide area networks and combine them into a cohesive system capable of serving the IoT system's aims. Where IoT systems rely on third-party general-purpose communication networks, their management and operational interfaces can be used.
- c) Applicable to Industry 4.0.

12) Real-time capability

- a) The capability of a system to perform computation in real-time when an external process occurs so that those results can be used to control, monitor, and respond to the process.
- b) Often, IoT systems function, exchange information, and provide feedback in real-time. Having real-time capability helps these systems monitor their processes efficiently.
- c) Applicable to process control systems.

13)Self-description

- a) The process in which the components of an IoT system let other components know of their capabilities for the purposes of composition, interoperability, and dynamic discovery.
- b) IoT systems are not just intra-connected but also interconnected. Therefore, providing a self-description eases the process for most components to work in confluence with others.
- c) Applicable to systems using Bluetooth or WiFi to connect to networks.

14)Service subscription

- a) Usually, IoT services are made available as subscriptions where users make payments and conform with applicable prerequisites. Subscribing to a service and developing new IoT applications might result in additional system safety requirements.
- b) A few IoT systems work on the subscription model. The manufacturers providing such services must ensure appropriate mechanisms to maintain the subscriptions.
- c) Example – personal fitness monitoring

1.2 IoT Conceptual Model (CM)

According to standard definitions, an IoT device is a digital entity that serves as a link between other digital entities in an IoT system and physical objects in the real world. One or more of the 185 networks are used by IoT devices to communicate with other entities. IoT devices can use data stores and expose one or more endpoints through which interactions can be made.

IoT devices include sensors and actuators. A sensor is a device that monitors a physical object by detecting and responding to some form of input from the physical environment and producing digital data that can be transferred via a network. Instead, an actuator is 190 a device that takes in digital inputs and modifies one or more physical attributes based on the input.

In our functional view, these three elements are responsible for implementing the Perception Layer's functionalities. IoT Gateways, a virtual object that serves as a means of tethering one or more IoT devices to a wide-area network, implement the Gateway (GW) access level functions. Short-range networks are used by IoT gateway

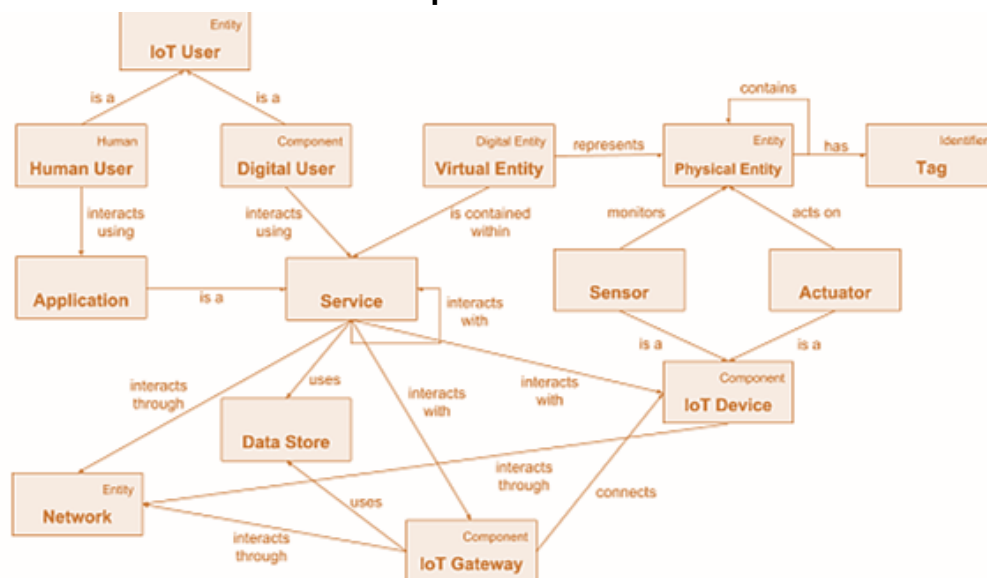
to communicate with IoT devices, while the network layer is used to communicate with services.

A service is a collection of unique capabilities made available by a software component through a specified interface and may include other services. One or more components work together to implement a service. The service platform and Enabler layer are made up of the services and the components that 200 implement them. Finally, an Internet of Things (IoT) application is a piece of software that provides a range of capabilities so that a user can carry out a task. It is important to note that an application is another example of the service idea and that it implements the features typical of the application domain in the context of the Internet of Things (eHealth, smart home, etc.)

Another example is an air conditioner acting as an actuator in Bluetooth communication between a smartphone app and an air conditioner to regulate the room's temperature.

Another instance is a smartphone with a barcode reading app. This app may use a locally installed database (local data store) to seek up the barcode details of a scanned object, or it may use the mobile network to connect to a remote service that hosts a catalogue. One type of tag that is connected to a physical object is the barcode.

Overview of IoT conceptual model in ISO/IEC 30141



Source: A Survey: Internet of Things Reference Architectures, Security, and Interoperability

The core IoT ideas found in the IoT CM are shown in the above picture, along with their linkages and interactions. The diagram is purposefully simplified and omits several of the IoT ideas that are covered in more detail in other pictures.

An Internet of Things (IoT) system is a system that includes devices that connect physical entities in the real world with digital entities, communicating with those digital entities via one or more networks over a large region. An IoT system contains all of the entities shown in Figure. Humans (human users) or non-humans (digital users), such as robots or automation services, which operate on behalf of human users, can both be IoT-Users. A digital user interacts with services via a communication network to consume them. Using applications of a specialized type of service is a form where a human user interacts. Some programmes/applications use the network to communicate with other services.

Here, a physical entity is a physical object that may be moved or measured by a sensor. Instead of the Physical Entity itself, the Physical Entity may have an attached tag that is tracked by a sensor. In the world of IT, a virtual entity stands in for a physical entity.

IoT devices will have direct or indirect contact with a physical entity which includes actuators and sensors. Digital Entities include virtual entities, tags, actuators, sensors, identifiers, IoT gateways, and IoT devices. A digital entity is a virtual being. IoT devices can be either actuators or sensors. IoT devices interact across a network and have the option of directly communicating broadly or connecting to an IoT gateway that also has this capability.

An actuator acts on (changes) a physical entity's property based on digital information that has been received. A sensor picks up certain physical entity properties and converts them into a communicable digital representation. One or more tags may be connected to a physical entity, and sensors may monitor the tag rather than the physical entity itself. Actuators and sensors are two categories of IoT devices that quantitatively translate fluctuations in one physical property into variations in another. Like the GPS position sensor and accelerometer in a smartphone, an IoT device can house many sensors.

Data related to IoT systems are kept in data stores. This data might come directly from IoT devices or via services acting on data from IoT devices.

1.3 IoT Reference Model (RM)

1.3.1. Entity-based RM

The entity-based RM consists of the following:

- a) Physical entities
- b) Tags of various types attached to physical entities
- c) IoT devices, including sensors and actuators
- d) Communication networks for IoT devices, including proximity networks and wide area networks
- e) IoT gateways, including local services and data
- f) Application and service sub-system
- g) Operation and management sub-system
- h) Resource access and Interchange sub-system
- i) IoT users, including humans, devices/HMI
- j) Peer systems, which are other IoT or non-IoT systems

1.3.2. Domain-based RM

This RM helps designers to focus on the essential tasks to be performed by subdividing them logically.

Following are the sub-divisions of the domain-based RM:

- a) User Domain (UD)
- b) Physical Entity Domain (PED)
- c) Sensing & Controlling Domain (SCD)
- d) Operations & Management Domain (OMD)
- e) Resource Access & Interchange Domain (RAID)
- f) Application & Service Domain (ASD)

1.3.3. Relation between entity-based RM and domain-based RM

When the entity-based RM and domain-based RM are mapped together, the relationship between the entities and their domains is as follows:

- a) IoT-Users belong to the User Domain
- b) Application & Service sub-systems belong to the Application & Service Domain
- c) Operations and Management sub-systems belong to the Operations & Management Domain

- d) The Resource Access & Interchange sub-system belongs to the Resource Access & Interchange Domain
- e) IoT devices and IoT gateway are entities in the Sensing & Controlling Domain
- f) Physical Entities exist in the Physical Entity Domain

1.4 IoT Reference Architecture (RA) Views

The IoT RA is divided into four types of views:

1.4.1. IoT RA functional view

This view is divided into the following concepts:

1) Intra-domain functional components

These components are divided as follows:

- a) Sensing & Controlling Domain (SCD)
- b) Application & Service Domain (ASD)
- c) Operations & Management Domain (OMD)
- d) Resource Access & Interchange Domain (RAID)

The RAID is further divided into two main functional groups: discovery and access data flow

- e) User Domain (UD)
- f) Physical Entity Domain (PED)

2) Cross-domain capabilities

These capabilities are divided as follows:

a) Network Connectivity

This is further categorized into:

- Proximity networking
- Access networking
- Service networking
- User networking

b) Trustworthiness

This is further categorized into:

- Safety
- Privacy and PII Protection
- Security

- Resilience
 - Reliability
- c) Dynamic Composition

1.4.2. IoT RA system deployment view

1) General

This view describes the following aspects:

- a) key physical components (e.g., sub-systems, devices, networks) of an IoT system;
 - b) the general implementation architecture of an IoT system, including the structure of an IoT system, the distribution of components, and the topology of the interconnectivity of the components;
 - c) 3) a technical description of its components, including behaviours and other properties
- 2) Systems/sub-systems in Physical Entity Domain (PED)
 - 3) Systems/sub-systems in Sensing & Controlling Domain (SCD)
 - 4) Systems/sub-systems in Application & Service Domain (ASD)
 - 5) Systems/sub-systems in Operation & Management Domain (OMD)
 - 6) Systems/sub-systems in User Domain (UD)
 - 7) Systems/sub-systems in Resource Access & Interchange Domain (RAID)

1.4.3. IoT RA networking view

1) Communication Networks

- a) General
- b) Proximity Network
- c) Access Network
- d) Services Network
- e) User Network

2) Communication Networks Implementation

1.4.4. IoT RA usage view

1) General description

This view addresses the following:

- a) Activities

- b) Roles and sub-roles
- c) Services and cross-cutting aspects
- 2) Description of the roles, sub-roles, and related activities

The three user groups in all IoT-related activities are:

- a) IoT service provider

Following are the sub-roles of an IoT service provider:

- IoT business manager
- IoT service delivery manager
- IoT system operator
- IoT security analyst
- IoT operations analyst
- IoT data scientist
- IoT chief privacy officer (CPO)/data protection officer (DPO)
- IoT network & infrastructure security manager
- IoT privacy analyst/privacy engineer
- IoT safety officer

- b) IoT service developer

Following are the sub-roles of an IoT service developer:

- IoT solution architect
- IoT development operations manager
- IoT application developer
- IoT device developer
- IoT system integrator
- IoT CPO/DPO

- c) IoT-User

Following are the sub-roles of an IoT user:

- Human user
- Digital user

2. ISO/IEC 27400: GUIDELINES FOR SECURITY AND PRIVACY IN IOT

IoT devices may connect to the Internet and communicate with one another. Insecure items, as opposed to more traditional IT systems (e.g., PCs, laptops, and servers), may jeopardize privacy and security. As a result, proper privacy and security safeguards are necessary. IoT systems will receive security and privacy recommendations as part of the standard. Furthermore, the standard may handle trustworthiness and be compatible with other IoT standards.

2.1 Issues that are addressed by this standard are:

- Impacts of a broad extent and type, potentially involving property damage and safety problems
- Some products have a long lifecycle, while others are inexpensive and disposable, implying a short life cycle. However, how long will these things last? Managing the version and change management (such as patching) are additional issues for IoT
- A lack of standardization presents complications in monitoring and organizing things, which may result in some becoming unmanaged
- Queries concerning interoperability and interaction among things and devices
- Some things have limitations in functionality and performance [Capacity]
- Potential connections or uses not anticipated by the designer or manufacturer

The standard includes general 'risk sources' and 'risk scenarios' applicable to IoT, a collection of instances to evaluate. There are several reservations regarding the choice and terminology (vulnerabilities are not dangers!). Controls that are missing or ineffective are not dangerous, suggesting a lack of comprehension of the underlying ideas. The other IoT security measures included in the standard do not appear to be directly tied to the dangers they are purportedly intended to minimize. Discussing important [information] concerns in ISO27k is a great start. Most ISO27K standards prescribe information security procedures immediately without identifying the hazards to information. Even if it is a modest step, this standard goes further than the "Just do this:" approach. This motivates users to find, investigate, and assess information hazards in their companies.

2.2 Purpose and Justification:

Things that are not safe can influence security and privacy in different ways than more traditional IT systems (e.g., desktops, laptops, and servers). To reduce unacceptable risks, suitable security and privacy standards are required.

Things can be thought of as standalone electrical devices as well as parts of more significant, more complicated "ecosystems," which may include:

- the operating systems and programmes they use, which provide a range of services;
- the network architecture (including local, wide-area, and personal networks);
- the physical environment that they communicate with via sensors and actuators;
- the individuals who designate, purchase, configure, use, and manage them;
- the businesses that create, produce, employ, and manage them;
- given that objects are "everywhere," society as a whole.

IoT designers/manufacturers and users, both individuals and organizations, may not be aware of the information risks and appropriate/necessary controls; as a result, the standard has a role in promoting trustworthiness and increasing maturity on both the supply (vendor) and demand (customer) sides.

2.3 Stakeholders:

According to the ISO/IEC 27400 standard, three stakeholders are accountable for the security of IoT systems, they are:

- IoT Service Provider – In charge of delivering services related to the functioning of the IoT ecosystem. They oversee networking, data collecting, and the management of deployed IoT devices/solutions.
- IoT Service Developer - This position oversees designing, implementing, and integrating IoT services. It is anticipated that the developer will adhere to best practices to safeguard the IoT ecosystem.
- IoT User - The IoT ecosystem's end user (both human and digital).

2.4 Recommended Standards referred to in ISO/IEC 27400:

Standard	Description
ISO/IEC 27000	Information Security Management System (ISMS) Widely used by the industry
ISO/IEC 27701	Extended requirements to ISMS for privacy information management
ISO/IEC 29134	Guidelines on privacy impact assessment
IEC 62443	Guidance in the domain of security of Industrial Automation and Control Systems (IACS)
ISO 31000	Guidelines on risk management
ISO/IEC 27005	Providing information security-specific guidelines for risk management

2.5 ISO/IEC 27400 Identified Controls:

ISO/IEC 27400 specifies 45 controls for securing deployed IoT applications. Furthermore, it explicitly states the objective of control, accountable stakeholders, domain, and instructions on safely integrating IoT solutions.

Controls related to	Responsible Stakeholders
IoT security policy	ISD/ISP
Responsibility for IoT security in an organization	ISD/ISP
Asset management	ISP
Equipment and assets located outside physically secured areas	ISP
Secure disposal or re-use of equipment	ISP
Learning from security incidents	ISD/ISP
Secure IoT system engineering principles	ISD
Secure development environment and procedures	ISD

Security of IoT systems in support of safety	ISD/ISP
Security in connecting varied IoT devices	ISD/ISP
Verification of IoT devices and systems design	ISD/ISP
Monitoring and logging	ISD/ISP
Protection of logs	ISD/ISP
Use of suitable networks for the IoT systems	ISD/ISP
Secure settings and configurations in the delivery of IoT devices and services	ISD/ISP
User and device authentication	ISD/ISP
Define provision of software and firmware updates	ISD/ISP
Sharing vulnerability information	ISD/ISP
Adapted security measures to the life cycle of IoT systems and services	ISD/ISP
Guidance for IoT users on the proper use of IoT devices and services	ISD/ISP
Determination of security roles for stakeholders	ISD/ISP
Management of vulnerable devices	ISP
Management of supplier relationships in IoT security	ISD/ISP
Secure disclosure of Information regarding the security of IoT devices	ISD
Contacts and support service	IU
Initial settings of IoT device and service	IU
Deactivation of unused devices	IU
Secure disposal or re-use of IoT device	IU
Prevention of privacy-invasive events	ISD/ISP

IoT privacy by default	ISD/ISP
Provision of privacy notices	ISP
Verification of IoT functionality	ISD/ISP
Consideration of IoT users	ISD/ISP
Management of IoT privacy controls	ISP
Unique device identity	ISD
Fail-safe authentication	ISD/ISP
Minimization of indirect data collection	ISP
Communication of privacy preferences	ISP
Verification of automated decision	ISP
Accountability for stakeholders	ISD/ISP
Unlinkability of PII	ISD/ISP
Sharing information on PII protection measures of IoT devices	IDD
Privacy controls for IoT users	IU
Purposeful use for connecting with other devices and services	IU/ISP/ISD
Certification/validation of PII protection	IU

3. ISO/IEC 27402: IOT SECURITY AND PRIVACY - DEVICE BASELINE REQUIREMENTS

The ISO/IEC 27402 standard is meant to specify a security baseline for IoT devices that support information security and privacy controls. This standard includes recommendations for the device manufacturer in terms of the development process (like risk assessment), and product declarations (like security features and vulnerability disclosure), along with the requirements for the security product (like secure storage, reset function). Its primary focus is “device” and partially covers its product and process aspects. It provides guidance on the fundamental security features anticipated in all IoT devices.

Following are a few examples of the topics that are covered in the baseline (information security) requirements:

- a. Unique Device Identifier that should be immutable and verifiable
- b. Factory Reset functionality
- c. Delete all user data functionality
- d. Data Protection
- e. Patching/updating capability for firmware and software

The technical committee intends to outline only a few essential information security and privacy controls in this standard, with the idea of producing additional standards that describe additional criteria for specific sectors or verticals, expanding on the generic baseline. Other security controls are necessary and might be included in future standards for certain applications.

At the time of writing, the standard “ISO/IEC 27402 CD (Committee Draft): Cybersecurity - IoT Security and Privacy - Device Baseline Requirements” is under development and at stage 30, under the purview of the Technical Committee “ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection”.

4. UNECE WP.29 CYBERSECURITY REGULATION (UN155): VEHICLE CYBER SECURITY MANAGEMENT SYSTEM & SECURE UPDATE MANAGEMENT SYSTEM

UN155 is to give requirements of the UN Regulation on provisions regarding the vehicles of reference to cyber security and cyber security management systems (UN Regulation No. 155) and provide details on what can be used to demonstrate compliance with those requirements. Vehicle manufacturers who submit systems for testing and the Technical Services who examine those systems are the primary audience for this paper. This document will assist in evaluations between different Technical Services/Approval Authorities UN155 intends to guide what information is acceptable to Technical Services/Approval Authorities and what amount of information should be provided. This document will be able to assist in evaluations between different Technical Services/Approval Authorities.

The Technical Service or Approval Authority should verify that:

- (a) The vehicle manufacturer has a CSMS;
- (b) The presented CSMS complies with the requirements listed below in this regulation.

For this requirement, the focus is on the manufacturer's processes and assessing if they are in place to get an overview of the manufacturer's capability to fulfill the requirements of the CSMS.

The following clarifications should be noted:

- (a) The CSMS may be a part of the organization's Quality Management System or be independent of it;
- (b) If the CSMS is part of the organization's QMS, it should be identifiable

The range of activities performed by the manufacturer to manage the cyber security of the development, production, and post-production phases of a vehicle type:

- (a) Organizational structure used to address cyber security;
- (b) Roles and Responsibilities regarding cybersecurity management incl. Accountability

4.1. Requirements for cyber security management

1. The vehicle manufacturer's Cyber Security Management System must be in place, and it must comply with this Regulation, according to the Approval Authority or its Technical Service, who must confirm this for the assessment.
2. The following elements must be covered by the cyber security management system:
3. The vehicle manufacturer must convince an approval authority that their cyber security management system is appropriate for the subsequent phases
 - A. Phase of development;
 - B. Phase of production;
 - C. Phase of post-production
4. The vehicle manufacturer must prove that the procedures followed by their Cyber Security Management System ensure security is properly considered, including risks and mitigations.
 - A. the mechanisms utilised to handle cyber security within the manufacturer's company;
 - B. the mechanisms used to identify risks associated with various vehicle types. In these processes, the dangers and other pertinent threat evaluation shall be done;
 - C. the procedures used to evaluate, classify, and manage the identified risks;
 - D. The procedures in place to ensure the identified risks are properly controlled;
 - E. the procedures used to evaluate a vehicle type's cyber security;
 - F. the procedures used to make sure the risk assessment is kept up to date;
 - G. The mechanism used to monitor for, identify, and react to cyber-attacks, cyber threats, and vulnerabilities related to different types of vehicles, as well

as the procedures used to determine whether the implemented cyber security measures are still effective considering newly discovered cyber threats and vulnerabilities;

H. procedures for supplying pertinent data to help analysis of attempted or successful cyberattacks.

5. The vehicle manufacturer must prove that the procedures utilised in their Cyber Security Management System will make sure that, depending on classification, cyber dangers are avoided. Any vulnerabilities that necessitate a response from the vehicle maker must be fixed in a timely manner.

6. The vehicle manufacturer must show that the procedures utilised in their Cyber Security Management System will guarantee that the monitoring will be ongoing. That includes,

A. Monitoring of the vehicles after first registration;

B. Include the capacity to analyse and find cyber threats, weaknesses, and assaults using vehicle data and records. This capacity must encompass all the drivers' or automobile owners' privacy rights, especially regarding consent.

7. The vehicle manufacturer will have to present evidence of how their system manages their cyber security dependencies with contractual suppliers and service providers.

The requirement should be considered unfulfilled if one of the following statements is true:

A. Processes are absent or incomplete.

B. Processes are not applied universally or consistently.

C. Processes are often or routinely circumvented to achieve business objectives.

D. The vehicle manufacturer's security governance and risk management approach have no bearing on its processes.

E. System security relies on users' careful and consistent application of manual security processes.

- F. Processes have not been reviewed in response to significant changes (e.g., technology or regulatory framework) or within a suitable period.
- G. Processes are not readily available to staff, too detailed to remember, or too hard to understand.

The requirement may be considered fulfilled if all the following statements are true:

1. The vehicle manufacturer thoroughly documents its overarching security governance and risk management approach, technical security practice, and specific regulatory compliance. Cyber security is integrated and embedded throughout these processes, and key performance indicators are reported to its executive management.
2. The vehicle manufacturer's processes are developed to be practical, usable, and appropriate for its policies and technologies.
3. Processes that rely on user behaviour are practical, appropriate, and achievable.
4. The vehicle manufacturer reviews and updates process regularly to ensure they remain relevant. This is in addition to reviews following a significant cyber security incident.
5. Any changes to the essential function or the threat it faces trigger a review of processes.
6. The vehicle manufacturer designs systems to remain secure even when user security policies and processes are not always followed. For such a claim, the manufacturer should provide justification.

Sources for risk identification:

- (a) Vulnerability/ Threats sharing platforms;
- (b) Lessons learned regarding risks and vulnerabilities.

The processes to mitigate them:

1. Identification of the relevance of a system to cybersecurity;
2. Description of the overall system concerning:

- (i) Definition of the system/function;
 - (ii) Boundaries and interactions with other systems;
 - (iii) Architecture;
 - (iv) Environment of operation of the system (context, constraints, and assumptions).
3. Identification of assets;
 4. Identification of threats;
 5. Identification of vulnerabilities.

4.2. Requirements for vehicle types

1. For the Cyber Security Management System pertinent to the vehicle type being certified, the manufacturer must have a current Certificate of Compliance.

However, if the vehicle manufacturer can show that the kind of vehicle could not be built in accordance with the CSMS, then the vehicle manufacturer must show that cyber security was appropriately considered during the development phase of the relevant vehicle type concerned.

2. For the vehicle type being certified, the vehicle manufacturer is responsible for identifying and managing risks associated to suppliers.
3. A thorough risk assessment for the vehicle type must be conducted by the vehicle manufacturer, and the hazards found therein must be adequately treated or managed. The distinct components of the vehicle type and their interconnections must be taken into account during the risk assessment. The risk evaluation must also consider interactions with any external systems. The vehicle manufacturer must take into account all threats, as well as any additional risks.
4. The vehicle manufacturer is responsible for defending the vehicle type against dangers noted in the risk analysis. The vehicle type shall be protected by proportionate mitigations.

In particular, if a mitigation measure is technically impractical for type approvals granted before July 1, 2024, the vehicle maker must make sure that another suitable mitigation is put into place. The maker must give the approval authority the appropriate technical feasibility evaluation.

5. The vehicle manufacturer must implement reasonable and proportionate security measures for specific situations depending on the vehicle type (if provided) for the execution and storage of third-party software, services, data, applications, etc
6. Prior to type of approval, the vehicle's manufacturer shall carry out the necessary and adequate testing to confirm the success of the security measures implemented.
7. The vehicle manufacturer shall implement certain policies and for the vehicle type to:
 1. identify and stop cyberattacks on the specific type of vehicle;
 2. support the vehicle manufacturer's monitoring system in identifying threats, weaknesses, and cyberattacks pertinent to the vehicle type;
 3. the ability to do data forensics to enable the study of attempted or successful cyberattacks
8. For the purposes of this Regulation, cryptographic modules must adhere to consensus criteria. The vehicle manufacturer must defend the usage of any cryptographic modules if they do not adhere to consensus requirements.

4.3. List of provisions:

The results of the vehicle manufacturer's monitoring actions shall be reported to the Approval Authority or the Technical Service at least once a year or more frequently if appropriate. This report must include pertinent details about new cyberattacks. Also, the vehicles manufacturer shall additionally validate that any new actions taken and report to the Technical Service or the Approval Authority the continued effectiveness of the cyber security mitigations adopted for their vehicle types.

The requirement should be considered unfulfilled if one of the following statements is true:

1. Risk identification is not based on a clearly defined set of assumptions.
2. Risk identification for vehicle types is a "one-off" activity (or not done at all).
3. Vehicle types are assessed in isolation without considering dependencies and interactions with other systems. (e.g., interactions between IT and OT environments).

The requirement may be considered fulfilled if all the following statements are true:

1. The vehicle manufacturer's organizational process ensures that security risks to vehicle types are identified, analyzed, prioritized, and managed.
2. The vehicle manufacturer's approach to risk is focused on the possibility of adverse impact on its vehicle types, leading to a detailed understanding of how much effect might arise because of attacker actions and the security properties of its networks and systems.
3. The vehicle manufacturer's risk identification is based on a clearly understood set of assumptions, informed by an up-to-date understanding of security threats to its vehicle types and its sector.
4. The vehicle manufacturer's risk identification is informed by an understanding of the vulnerabilities in its vehicle types.
5. The vehicle manufacturer performs detailed threat analysis and understands how this applies to your organization in the context of the threat to its vehicle types and sector.

The processes used for testing the cyber security of a vehicle type:

- (a) ISO/SAE 21434 can be used as the basis for evidencing and evaluating as required, especially based on [RQ-09-10], [RQ-10-01], [RQ-11-01], [RQ-11-02], [RQ-12-01];
- (b) BSI PAS 11281:2018 may be utilized for considering that the interaction of safety and security and processes for evidencing security outcomes are met.

- (c) Organization-specific rules for testing during development;
- (d) Processes for creation and execution of test strategies;
- (e) Processes for cybersecurity testing planning;
- (f) Processes for cybersecurity system design testing;
- (g) Processes for cybersecurity software unit testing;
- (h) Processes for cybersecurity hardware testing;
- (i) Processes for cybersecurity integration testing;
- (j) Processes for documentation of the results of testing;
- (k) Processes for handling vulnerabilities identified during testing;
- (l) Justification and requirements for cybersecurity tests, like Functional (requirements-based, positive and negative) testing, Interface Testing, Penetration Testing, Vulnerability scanning, and Fuzz testing, but not limited to the same.
- (m) Processes for testing to ensure the produced system has the cybersecurity 15 requirements, controls, and capabilities outlined in the production plan;
- (n) Processes for testing to ensure the produced item meets the cybersecurity specifications which are in accordance with the system in the development phase;
- (o) Processes for testing to assure that cybersecurity controls and configuration as cybersecurity specifications are enabled in the produced item;
- (p) Processes for documenting the test results and findings handling

5. ISO/SAE 21434 STANDARD FOR CONNECTED CARS' CYBERSECURITY

5.1 Existing Policy and Upcoming Recommendations

The upcoming recommendation ISO/SAE 21434 "Road vehicles – Cybersecurity engineering" sets standards specific to items for identification, such as the use of embedded controllers, the long lifecycle of vehicles, and the safety implications of these technologies in cars. It hopes to:

- Define a structured process to include cybersecurity in the design phase
 - Following a structured approach helps reduce the potential for a successful attack to minimize losses
 - A structured process provides the means to react to a continually changing threat landscape
- Maintain consistency across a global industry
- Be comprehensive and promote conscious decision-making. The standard recommendation itself stipulates no proposals for compliance. However, the recommendations, which apply to road vehicles, offer the following principles for all automotive industry vendors:
 - Ensure that the systems of road vehicles released in the market after that are reasonably secure
 - Ensure that automakers and suppliers can perform due diligence
 - Focus on automotive cybersecurity engineering based on current technologies and methodologies
 - Adopt a risk-oriented approach
 1. For determining action prioritization
 2. The basis for analyses of risk factors for methodical elicitation of cybersecurity requirements
- Use the standard as a basis for management activities for cybersecurity
- Identify guidelines for cybersecurity activities/processes across all phases of the vehicle lifecycle

1. Design and engineering
2. Production
3. Operation by customer
4. Maintenance and service
5. Decommissioning

The organization should implement management systems for cybersecurity and manage the tools for cybersecurity engineering, particularly a quality management system. In detail, it should:

- Define a cybersecurity policy and the organization-specific rules and processes for cybersecurity
- Assign the responsibilities and corresponding authorities required to perform/spearhead the cybersecurity activities
- Support the implementation of cybersecurity, including the provision of resources and the management of the cybersecurity processes and related procedures' interactions
- Institute and maintain a cybersecurity culture, including competence management, awareness management, and continuous improvement systems
- Perform an organizational cybersecurity audit
- Manage the sharing of cybersecurity information
- Institute and maintain management systems that support the cybersecurity activities, and provide evidence that the tool used does not adversely affect cybersecurity

5.2 Vulnerability Analysis

This process examines gaps and assesses whether the weakness can be exploited to launch an attack. These security flaws and events must be analyzed to identify vulnerabilities, examples of which are:

- Missing requirements or specifications
- Architectural or design weaknesses, including incorrect design of security protocols

- Implementation weaknesses and incorrect implementation of security protocols, including hardware and software bugs
- Weaknesses in the operational processes and procedures, including misuse and inadequate user training
- Use of outdated or deprecated functions, including cryptographic algorithms

5.3 Vulnerability Management

5.3.1 Risk Assessment Methods

This section deals with the possible evaluation measures to determine the impact of a threat to the car user. The procedure is as follows:

1. **Asset identification**: Identifying an item or component's possible scenarios and assets. The potential compromise of assets with cybersecurity properties and the respective damage scenarios must be evaluated. For example, an asset can be messages about vehicle velocity and deceleration received by an airbag unit, and the cybersecurity property is integrity. Damage scenario includes airbag deployment during a user's overtaking manoeuvre while in transit.
2. **Threat scenario identification**: Identifying the threat scenarios to the cybersecurity properties of the assets. One damage scenario cited can potentially correspond to multiple threat scenarios. For instance, spoofing messages on the CAN bus connected to the airbag ECU can lead to the loss of velocity integrity, and acceleration messages can potentially cause airbag deployment and loss of vehicle control.
3. **Impact rating**: Estimating the magnitude of damage and/or physical harm associated with a damage scenario. The damage scenarios must be assessed against potential adverse consequences to users in the independent impact categories of safety, financial, operational, and privacy (SFOP). If further impact categories are considered beyond SFOP, then those categories must be documented. While SFOP is the core category used to rate impact on users, additional categories of stakeholders can be extended, such as for the business or the performing organization. Additional examples of categories are loss of intellectual property, financial loss to the business, or the loss of brand image or reputation. The safety-related impact will be derived

from ISO 26262, and the impact rating of the damage scenario shall be determined to be one of the following:

- Severe
- Major
- Moderate
- Negligible

4. **Attack path analysis:** Identifying and linking potential attack paths to one or more threat scenarios. The threat scenarios shall be analyzed to describe possible attack paths, and the analysis must be documented.

The analysis approach can be based on:

- A. Top-down approaches, such as attack trees, attack graphs, taxonomy mnemonic-based approaches (e.g., STRIDE)
- B. Bottom-up approaches (e.g., the output of the vulnerability analysis)
- C. A combination of these approaches

5. **Attack feasibility rating:** Rating the ease of exploitation of the attack paths.

For each identified attack path, the attack feasibility rating must be determined as one of the following:

- High
- Medium
- Low
- Very low

The rating method should be based on one of the following assessment approaches depending on the phase in the lifecycle and available information:

- An attack potential-based approach should be based on core factors, including elapsed time, specialist expertise, knowledge of the item or component, the window of opportunity, and equipment.
- A Common Vulnerability Scoring System (CVSS)-based approach should be based on the exploit metrics of the base metrics, including attack vector, attack complexity, privileges required, and user interaction.
- An attack vector-based approach should evaluate the predominant attack vector of the attack path.

6. **Risk determination**: Defining the risk value of a threat scenario.

The risk value of a threat scenario must be determined from the impact of the associated damage scenario and the attack feasibility of the associated attack paths. The value assigns ranges from 1 to 5, with 5 being the highest risk. If the threat scenario corresponds to more than one attack path, the associated attack feasibility levels can be appropriately aggregated (e.g., the threat scenario is assigned the maximum feasibility level of the corresponding attack paths).

7. **Risk treatment decision**: Addressing the identified risks by selecting a suitable risk treatment option. A risk treatment option must be determined based on the impact categories, attack paths, and results from the risk determination

5.4 Concept Phase

5.4.1 Product Development

1. The cybersecurity engineering activities regarding refinement of cybersecurity requirements and architectural design include:

- Understanding and complying with the cybersecurity requirements from a higher level
- Preventing the introduction of new vulnerabilities
- Identifying and managing known vulnerabilities, if applicable

2. The cybersecurity engineering activities regarding integration and verification include:

- Verification of the cybersecurity requirements' fulfilment allocated to the system or component
- Verification that identified vulnerabilities have been successfully managed
- Searching for previously unidentified vulnerabilities and their management

3. The standard contains an extensive list of cybersecurity requirements related to the development phase. Below are examples:

- The interface/s between components of the refined architectural design in fulfilment of the refined cybersecurity requirements must be identified and described, the parameters and purposes and usage included. This requirement is related to interfaces as potential entry points for cybersecurity attacks. Proper validation of allowed data ranges incoming to the interface must be part of the coding. The interface specification can serve as an input to vulnerability analysis.
- Component testing should be performed to search for unidentified vulnerabilities. Test methods to search for flaws can include penetration testing, vulnerability scanning, and fuzz testing.

4. The standard also includes specific requirements related to coding and the selection of programming languages. When selecting a design, modelling, or programming language, the following should be considered:

- An unambiguous and comprehensible definition in both syntax and semantics
- Support for the achievement of modularity, abstraction, and encapsulation
- Support for the use of structured constructs
- Support for the use of secure design and coding techniques

5. Design principles for software unit design and implementation at the source code level should be applied to achieve the following characteristics:

- Correct order execution of subprograms and functions within the software units based on the architectural software design
- Consistency of the interfaces between the software units
- The correctness of data flow and control flow between and within the software units
- Low complexity
- Readability and comprehensibility
- Robustness
- Suitability for software modification (unless ease of software modification runs contrary to the cybersecurity requirements)
- Verifiability

5.4.2. Cybersecurity Validation

Validation activities must be performed to confirm:

1. The adequacy of the cybersecurity goals.
2. The completeness, consistency, correctness, and adequacy of the item and the cybersecurity requirements in the operational environment.
3. The cybersecurity goals of the item have been achieved, along with the validity of the cybersecurity claims, if applicable.

5.4.3. Production

This section covers the fabrication, assembly, and/or configuration of an item or component. A production control plan is created to:

- Ensure that cybersecurity requirements for post-development are applied to the item or component
- Ensure that it cannot be exploited during production
- Ensure that additional vulnerabilities cannot be added during production

5.4.4. Operations and Maintenance

This chapter describes the criteria for responding to cybersecurity incidents and deploying updates. A cybersecurity incident response occurs when a cybersecurity event escalates, and an organization needs to respond to it. Organizations can issue updates for various reasons, such as vulnerabilities, functional improvements, or safety issues.

5.4.5. Cybersecurity Incident Response

A cybersecurity incident response should include:

1. Remediation actions for the incident, as determined by the established vulnerability management procedure/s

2. A communication plan that involves internal parties, including communications teams (marketing and/ or public relations), product development teams, legal, customer relations, quality management, and purchasing
3. Assigned responsibilities for the remedial actions
4. A method for determining progress or remediation actions
5. Criteria for closure and actions upon closure

A range of connected and automated vehicles is already available, intensifying the usage of connectivity features and information sharing for vehicle maintenance and traffic safety features. The resulting highly connected networking amplifies the attractiveness level for hackers' attacks on vehicles and connected infrastructure. Therefore, efforts are being poured into developing an industry-standard capable of tackling automotive cybersecurity issues and protecting assets. The joint working group of the standardization organizations ISO and SAE has recently established and published a draft international specification of the "ISO/SAE DIS 21434 Road Vehicles - Cybersecurity Engineering" standard.

This Standard specifies engineering requirements for cybersecurity risk management regarding the concept, product development, production, operation, maintenance, and decommissioning of electrical and electronic (E/E) systems in road vehicles, including their components and interfaces.

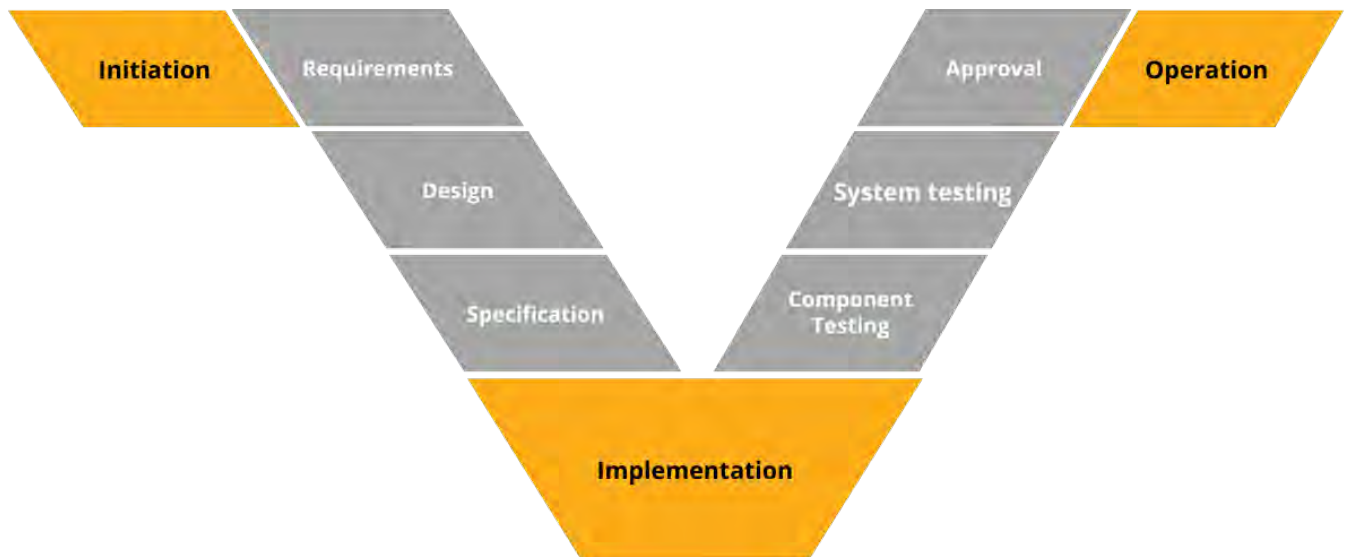
A framework is defined that includes requirements for cybersecurity processes and a common language for communicating and managing cybersecurity risk.

This document is applicable to series production road vehicle E/E systems, including their components and interfaces, whose development or modification began after the publication of this document.

The ISO/SAE DIS 21434 standard is designed for road cars and aims to establish basic standards for automotive cybersecurity engineering. A risk-based approach to prioritizing actions is advised, as is the systematic elicitation of cybersecurity measures.

This standard looks at the entire development process and life cycle of a vehicle. It follows the V-model. During all phases, including requirements engineering, design,

specification, implementation, test, and operations, one must consider all security aspects.



ISO/SAE 21434 follows the V-model 1

6. ETSI EN 303645: CYBERSECURITY FOR CONSUMER IOT

EN 303645 specifies high-level security and data protection provisions for consumer IoT devices connected to network infrastructure and interacting with their associated services. The related services are outside the scope of this document.

The following is a non-exhaustive list of consumer IoT device examples:

- Fitness trackers.
- Smart cameras, televisions, and sound systems.
- Connected baby monitors and children's toys.
- Home automation and connected detection systems, particularly their hubs and gateways.
- IoT gateways, hubs, and base stations that connect multiple devices.
- Connected appliances such as washers and refrigerators, as well as smart home assistants.
- Connected window sensors, smoke detectors, and door locks.

6.1 Cyber security provisions for consumer IoT

6.1.1. No universal default passwords

Many consumer IoT devices are sold with universal default usernames and passwords (such as "admin, admin") for user interfaces through network protocols. Continued usage of universal default values has been the source of many security issues in IoT, and the practice needs to be discontinued. The above provision can be achieved using pre-installed passwords that are unique per device and/or by requiring the user to choose a password that follows best practice as part of initialization or by some other method that does not use passwords.

- When pre-installed unique per-device passwords are being used, they must be generated using a mechanism that minimizes the likelihood of automated attacks against a specific class or type of device.

- When passwords are used, and in any state other than factory default, all consumer IoT devices must have individual passwords defined by the user or unique per device.
- When a user can authenticate against a device, the device must offer a user or administrator an easy way to modify the authentication value used.
- Authentication mechanisms to authenticate users against a device must employ industry-best cryptography appropriate to the technology's properties, risk, and usage.
- When the device is not constrained, it shall have a mechanism that makes brute force attacks on authentication mechanisms via network interfaces impracticable.

6.1.2. Implement a means to manage reports of vulnerabilities

A vulnerability disclosure policy must be made public by the manufacturer. This policy should include, at the very least:

- contact information for the reporting of issues and
- information on timelines for
 - 1) initial acknowledgement of receipt; and
 - 2) status updates until the resolution of the reported issues.

A vulnerability disclosure policy specifies the process through which security researchers and others can report issues. Such a policy can be updated as required to ensure further transparency and clarity in the dealings of the manufacturer with security researchers and vice versa.

6.1.3. Keep software updated

Developing and deploying security updates on time is one of the most important actions of a to protect its customers and the wider technology ecosystem. It is good practice that all software is kept updated and well maintained.

- In consumer IoT devices, all software components should be securely updateable.
- When the device is not constrained, it shall have to install updates securely.

- The user should be able to apply an update easily.
- Software updates should be done automatically.
- The device should check for security updates after initialization and then consistently.
- Suppose the device supports automatic updates and update notifications. In that case, these should be enabled and configurable so that the user can enable, disable, or halt the installation of security updates and update notifications.
- To facilitate secure update mechanisms, the device must use best practice cryptography.
- Security updates shall be timely.
- The device should validate software updates for authenticity and integrity.
- When updates are delivered over a network interface, the device must use a trust relationship to verify the authenticity and integrity of each update.
- The manufacturer should notify the user recognizably and straightforwardly that a security update is required and provide information on the risks mitigated by the update.
- When a software update interferes with the device's basic activity, the device should notify the user. The manufacturer shall publish the defined support period in an accessible way that is clear and transparent to the user.
- For constrained devices that can't update their software, the manufacturer should publish the reason for the lack of software updates, the period and approach of hardware replacement support, and a defined support period in an accessible, clear, and transparent manner to the user.
- The product should be hardware replaceable and isolable for constrained devices that can't have their software updated.
- The consumer IoT device's model designation must be easily identifiable, either through labelling on the device or through a physical interface.

6.1.4. Securely store sensitive security parameters

- The device must securely store sensitive security parameters in persistent storage.

- When a hard-coded unique per-device identity is utilized in a device for security reasons, it must be implemented to prevent tampering via physical, software, or electrical means.
- Critical security parameters that are hard coded in device software source code must not be used.
- Any critical security parameters used in device software to check the integrity and authenticity of software updates and protect communication with associated services must be unique per device and produced with a mechanism that lowers the risk of automated attacks.

6.1.5. Communicate securely

- The consumer IoT device must use reviewed or evaluated implementations to deliver network and security functionalities, particularly in cryptography.
- To communicate securely, the consumer IoT device must use best practice cryptography.
- Cryptographic algorithms and primitives should be updateable.
- Access to device functionality via an initialized network interface should be possible only after authentication upon the interface.
- Critical security parameters must be encrypted in transit, with encryption appropriate to the technology's properties, risk, and usage.
- The consumer IoT device must safeguard the confidentiality of sensitive security parameters communicated over remotely accessible network interfaces.
- Device functionality that facilitates security-relevant configuration changes via a network interface shall only be accessible after authentication. The exception is for network service protocols relied upon by the device and where the manufacturer cannot guarantee the configuration required for the device to operate.
- The manufacturer must adhere to secure management processes for critical device security parameters.

6.1.6. Minimize exposed attack surfaces

The "principle of least privilege" is a foundation of good security engineering, applicable to IoT as much as in any other field of application.

- Device hardware should not expose physical interfaces to attack unless necessary.
- A debug interface that is physically accessible must be disabled in software.
- All logical interfaces and unused networks must be disabled.
- The device's network interfaces must minimize unauthenticated disclosure of security-relevant information in the initialized state.
- Considering security and functionality, software should operate with the least necessary privileges.
- The code should be reduced to only the functionality required for the service/device to function.
- Only software services used or required for the device's intended use or operation should be enabled by the manufacturer.
- The manufacturer should use secure development processes when developing the software deployed on the device.
- The device should include a hardware-level access control mechanism for memory.

6.1.7. Ensure software integrity

- The software on the consumer IoT device should be validated using secure boot mechanisms.
- Presume an unauthorized change is detected in the software. In that case, the device should notify the user and administrator of the problem and not connect to networks other than those required to perform the notifying function.

6.1.8. Ensure that personal data is secure

- Sensitive personal data transmitted between the device and related services must be kept confidential, and cryptography suitable for the technology and envisioned use should be used.
- The device's external sensing capabilities must be documented clearly and transparently for the user.
- The confidentiality of private information transiting between a device and a service, particularly associated services, should be protected using best practice cryptography.

6.1.9. Make systems resilient to outages

The provisions in the present clause aim to ensure that IoT services are kept up and running as the adoption of IoT devices across all aspects of a consumer's life increases, including in functions relevant to personal safety. It is important to note that safety-related regulations can apply. However, the key is to avoid making outages the cause of impact on the user and to design products and services that provide a level of resilience to these challenges.

- Given the likelihood of data network and power outages, resilience should be built into consumer IoT devices and services.
- Consumer IoT devices should remain operational and locally functional in the event of a network outage and recover cleanly when power is restored.
- Given the infrastructure's capability, the consumer IoT device should connect to networks in a usual, stable, operational, and orderly manner.

6.1.10. Examine system telemetry data

- If telemetry data is collected from consumer IoT devices and services, such as usage and measurement data, it should be examined for security anomalies.

6.1.11. Make it easy for users to delete user data

- The user must be provided with the capabilities to delete user data from the device.
- Users should receive explicit confirmation that their personal information has been removed from services, devices, and applications.
- The device should include functionality that allows the consumer to remove personal data from associated services.
- Users should be given specific instructions on deleting their personal data.

6.1.12. Make installation and maintenance of devices easy

- Consumer IoT installation and maintenance should involve a few user decisions and adhere to usability and security best practices.
- The manufacturer should guide users on how to set up their devices securely.
- The manufacturer should provide users with guidance to check whether their device is securely set up.

6.1.13. Validate input data

- The consumer IoT device software must validate data entered through user interfaces, transferred through Application Programming Interfaces (APIs), or shared between networks in services and devices.

Systems can be subverted by incorrectly formatted data or code transferred across different types of interfaces. Attackers or testers can use automated tools such as fuzzes to exploit potential gaps and weaknesses that emerge because of not validating data.

6.2. Data protection provisions for consumer IoT

Many consumer IoT devices process personal data. It is expected that manufacturers provide features within consumer IoT devices that support the protection of such personal data. In addition, there exist laws and regulations relating to the protection of personal data in consumer IoT devices (for example, the GDPR). The present document intends to help manufacturers of consumer IoT

devices provide several features for protecting personal data from a strictly technical perspective.

- For each device and service, the manufacturer must provide consumers with clear and unambiguous information about what personal data is processed and how it's used. This also applies to third-party participants, such as advertisers.
- Where personal data is processed based on consumers' consent, this consent shall be obtained validly.
- Consumers who gave consent for processing their personal data shall be able to withdraw it at any time.
- Whenever telemetry data is collected from consumer IoT devices and services, personal data should be processed only to the extent required for the intended functionality.
- Suppose telemetry data from consumer IoT devices and services is collected. In that case, consumers must be given information about telemetry data and its use.

7. ISA/IEC 62443: CYBERSECURITY FOR INDUSTRIAL AUTOMATION & CONTROL SYSTEMS

ISA/IEC 62443 is a series of standards and technical reports that offers a comprehensive cybersecurity framework for industrial automation and control systems. It is developed by the ISA99 Committee and adopted by the IEC. It covers every stage of industrial cybersecurity, ranging from risk assessment to operations. This series of standards cater to the non-regulated category of industrial control systems. The purpose of the 62443 series is to increase the safety, availability, integrity, and confidentiality of IACS, as well as to offer criteria for acquiring and deploying secure IACS. Currently, it consists of nine standards, technical reports (TR), and technical specifications (TS).

The Security Program for the IACS must be integrated with the whole Information Security Management System (ISMS) of the organization. Although the IACS is different from IT systems so there are extra specifications and factors for its security program.

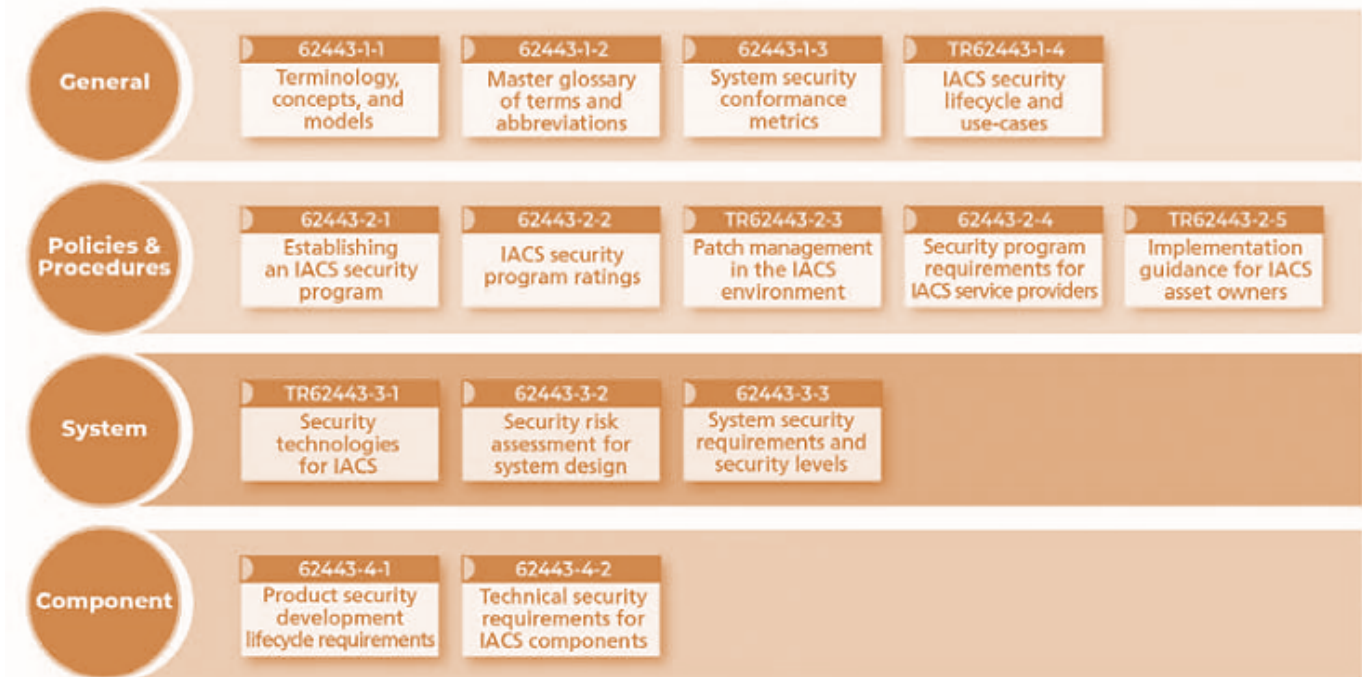
The technological security requirements for IACS Systems and Elements are specified and these prerequisites enable the Product Provider to Supply and Support a product with the capacity to satisfy the technological security specifications for a Capability for Security Level (SL-C).

The idea of security precautions is essential to become familiar with the ISA/IEC 62443 series.

A security measure is a technique, apparatus, a method, practise, or approach that lessens a threat, a weakness or an attack by removing or preventing it by reducing the damage it can cause, or by seeing and informing others of it that remedial action is possible. There are three different types of security measures

- Technical safety precautions include IACS hardware and software implementation normally perform without human intervention
- Security measures for any organization include someone who carries out one or more processes (Procedures and policies)

- Security measures that limits physical access to IACS components and systems through safety precautions like locking cupboards or doors



Source: ISAGCA-Security-Lifecycles-whitepaper

- Following are the 14 work products (Standards, Technical Specifications, and Technical Reports) that are grouped into 4 tiers:

1. General	IEC 62443-1-1	IEC TR-62443-1-2	IEC 62443-1-3	IEC 62443-1-4
	Terminology, Models, and Concepts	Master Glossary of Terms and Abbreviations	System Security Conformance Metrics	IACS Security Lifecycle and Use Cases

2. Policies and Procedures	IEC 62443-2-1	IEC TR-62443-2-2	IEC TR-62443-2-3	IEC TR-62443-2-4	IEC TR-62443-2-5
	Security Program Requirements for IACS Asset Owners	Implementation Guidance for an IACS Security Management System	Patch Management in the IACS Environment	Requirements for IACS Solution Suppliers	Implementation Guidance for IACS Asset Owners

3. System	IEC TR-62443-3-1	IEC TR-62443-3-2	IEC TR-62443-3-3
	Security Technologies for IACS	Security Risk Assessment and System Design	System Security Requirements and Security Levels

4. Component	IEC 62443-4-1	IEC 63443-4-2
	Secure Product Development Lifecycle Requirements	Technical Security Requirements for IACS Components

Tier 1 (General) is equally applicable to all the roles defined by the standard.

Tier 2 (Policies and Procedures) is most relevant to Asset Owners.

Tier 3 (System) focuses on technology-related aspects of security for systems.

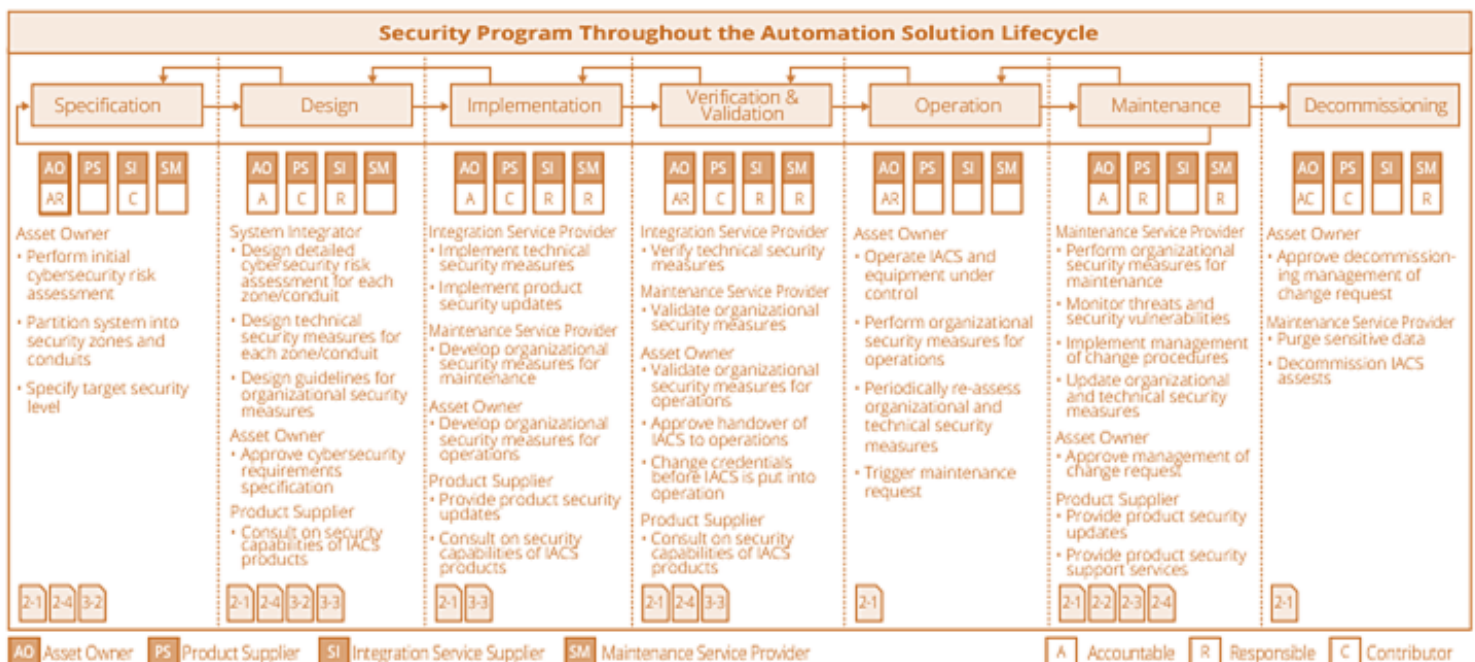
Tier 4 (Component) is most relevant to Product Suppliers.

- To serve the interests and concerns of the end user, the ISA/IEC 62443 conceptualized **“Security Levels”** (SL). Following are the five security levels of the standard:
 - a) SL 0 – No special requirement or protection provided.
 - b) SL 1 – Protection against unintentional or accidental misuse.

- c) SL 2 – Protection against intentional misuse by simple means with few resources, general skills, and low motivation.
- d) SL 3 – Protection against intentional misuse by sophisticated means with moderate resources, IACS-specific knowledge, and moderate motivation.
- e) SL 4 - Protection against intentional misuse using sophisticated with extensive resources, IACS-specific knowledge, and high motivation.

• **Maturity Levels** in ISA/IEC 62433:

- a) Maturity Level 1 – Initial level: Ad hoc and not fully documented.
- b) Maturity Level 2 – Managed: Development managed using documented, repeatable processes. Personnel are sufficiently expert, trained, and/or adhere to prescribed procedures.
- c) Maturity Level 3 – Defined/Practiced: The process is repeatable throughout the supplier's organization. Personnel are demonstrably well practiced.
- d) Maturity Level 4 – Improving: Appropriate process metrics to monitor the effectiveness and performance of the process and demonstrate continuous improvement in these areas.



Source: ISAGCA-Security-Lifecycles-whitepaper

IEC 62443 is still extensively used in the industry and serves as a foundation for certifications like the Embedded Device Security Assurance (EDSA) despite some of its components still being under development.

All the assets cannot be secured in the same way. Hence, ISA/IEC 62443 adopts a risk-based approach to cyber security, enabling users to identify their most important and vulnerable assets.

8. CYBERSECURITY FOR MEDICAL DEVICES

Connected medical devices enable the real-time flow of critical diagnostic data to information technology systems, where artificial intelligence and machine learning may be utilized to uncover unique patient health patterns and abnormalities. Furthermore, networked devices enable the monitoring of device performance, providing healthcare practitioners with early warning of a potential device failure or malfunction. Over time, linked devices and the data they create give critical information on the efficacy of various treatment methods, contributing significantly to continuous attempts to improve patient outcomes.

At the same time, the growing use of linked technology in healthcare delivery raises a variety of potentially serious cybersecurity vulnerabilities. According to some estimates, the healthcare business alone generates nearly 30% of the world's data volume, which is more than the volumes of data created by the industrial sector, financial services, or media and entertainment firms. Between now and 2025, healthcare data is predicted to rise at a compound annual growth rate (CAGR) of 36%.

There have been numerous events in which hackers discovered cybersecurity flaws in linked medical devices or device software, possibly allowing them to obtain remote access and control of the equipment.

In the last 12 months, more than 82% of medical device makers reported at least one cyberattack on one or more of their devices. And, as the distribution and use of linked medical devices grow, so will the number of cyberattacks.

8.1. Current State of Cybersecurity Requirements for Medical Devices:

In the midst of this expanding threat landscape for connected medical devices, regulators in major jurisdictions are becoming increasingly aware of the need to provide the industry with clearer and direct guidelines and supervision on emerging associated medical devices that can help secure them from the most likely cyber threats.

One such regulation is the MDCG 2019-16: The EU's Medical Device Coordination Group (MDCG) launched its "Guidance on Cybersecurity for Medical Devices" in

December 2019 to assist device makers in better understanding how to handle the relevant fundamental MDR standards related to cybersecurity. The MDCG's Guidance, also known as MDCG 2019-16, is 46 pages long and contains thorough definitions of core cybersecurity ideas, secure design and manufacturing techniques, documentation and instructions for usage, and post-market surveillance and vigilance.

This guideline covers a wide variety of subjects that are relevant to all stakeholders in the medical device supply chain, as well as end users. It connects regulatory requirements to cybersecurity processes and artefacts. It also includes all the subjects related to cybersecurity. The list is quite helpful in determining where cybersecurity standards should be applied in your QMS procedures. For example, design controls and post-market surveillance. It also recovers ideas such as defense in depth, excellent security hygiene (basic security hygiene according to FDA guidelines), and the link between security threats and safety issues. Another notion is provided that is not readily found in other guidance: the relationship between usability engineering and cybersecurity, as well as the concept of shared accountability. All stakeholders in the supply chain, including medical device integrators, operators, and consumers, must do their share. Manufacturers don't be deceived by this joint duty: in the event of an unfavorable incident, your obligation will be invoked as normal. You must have protocols in place to guarantee the secure installation, deployment, setup, and exploitation of your devices. Simply put, manufacturers are not exempt from common accountability. On the contrary, it involves the duty of other stakeholders.

8.2. Role of IEC 81001-5-1 in Strengthening Cybersecurity:

While there are a variety of industry-accepted standards that apply to cybersecurity concerns in general, medical device makers have lacked a life-cycle standard that explicitly tackles cybersecurity as it affects connected medical devices. The lack of a specific standard has stymied efforts to implement standardized measures to safeguard modern connected medical systems from existing and future cybersecurity threats. To address this significant gap, the International Electrotechnical Commission (IEC) has created a new standard that focuses solely on

cybersecurity risks affecting software used in linked health technology, such as medical devices and consumer-oriented health goods and services.

IEC 81001-5-1, which was published in December 2021 after more than three years of talks and consideration, is a major addendum to IEC 62304. IEC 81001-5-1 covers security problems for all sorts of "health software," which is described in the standard as: "Software intended to be used specifically for managing, maintaining, or improving the health of individual persons, or the delivery of care, or which has been developed for the purposes of being incorporated into a medical device."

IEC 81001-5-1 addresses the whole product life cycle of health software, from product development through post-market usage and monitoring. As a result, the standard emphasizes the need for bilateral contact between device makers and software developers, as well as those responsible for the actual usage of connected devices, in maintaining appropriate cybersecurity policies.

Specific clauses of the standard to help ensure protection against cyber threats are:

- **General Requirements:** Incorporates the installation and use of a quality management system that includes product security concerns, as well as the use of a risk management system that handles security in information technology devices and software.
- **Software Development Process:** Conducting a health software requirements analysis with a focus on software-specific security threats, software design and integration testing, including threat mitigation, vulnerability, and penetration testing are all covered.
- **Software Maintenance Process:** Establishing a software maintenance strategy that involves the timely distribution of software updates to guard against new and existing cyber threats, as well as modification implementation, is addressed.
- **Security Risk Management Process:** Identifies possible vulnerabilities, threats, and the related negative consequences, estimates and evaluates those risks, takes actions to mitigate those risks and monitors the efficacy of risk controls on an ongoing basis.
- **Software Configuration Management Process:** Manufacturers must provide comprehensive product development, maintenance, and support

strategy that includes configuration management with change controls and change history, as well as information on external components that are or might be vulnerable to security flaws.

- **Software Problem Resolution Process:** Establishing a mechanism for receiving information about possible security vulnerabilities, reviewing and analyzing such vulnerabilities, and taking measures to remedy security-related concerns are all part of the process.

The IEC 81001-5-1 standard is also anticipated to be accepted by the United States FCC as a "consensus standard" that may be utilized in support of 510(k) and PMA applications.

Because of the evolving cyber threat landscape for linked medical devices, device makers and software developers must be proactive in designing their products to reduce the risk of possible cybersecurity vulnerabilities. The IEC 81001-5-1 standard provides a thorough roadmap that manufacturers and developers may follow to assist assure the safety and security of their devices throughout their full lifespan, and the MDCG 2019-16 standard includes both premarket and post-market FDA cybersecurity guidance.

8.3. MDCG 2019-16 Guidance on Cybersecurity for medical devices

New texts establish specific new critical safety criteria for all medical devices that include electronic programmable systems and software that are themselves medical devices. Medical Device Regulations require medical device makers to consider the state of the art when designing, producing, and updating medical equipment throughout their life cycle. Manufacturers should exhibit state-of-the-art decision-making (based on relevant standards, guidelines, their own private knowledge, and publicly accessible scientific / technological information) while also demonstrating suitability to manage security risk correspondingly.

8.3.1. Cybersecurity activities across the life cycle of medical devices according to the Medical Devices Regulations:

Pre-Market Activities: Secure Design; Risk Management; Establish Risk Control Measures; Validation, Verification, Risk Assessment, Benefit Risk Analysis; Technical

documentation; Conformity Assessment; Establish a post-market surveillance plan and post-market surveillance system; Clinical Evaluation process.

Post-Market Activities: Risk Management; Modify Risk Control Measures; Validation, Verification, Risk Assessment, Benefit Risk Analysis; Maintain and update a post-market surveillance plan and system; Trend Reporting; Analysis of serious incidents; post-market surveillance report; Periodic Safety update report; Update Technical documentation; Inform the electronic system on Vigilance.

8.3.2. IT Security:

Key concepts involved in IT security specifically for medical devices are the following:

- Confidentiality of information at rest and in transit
- integrity, which is necessary to ensure information authenticity and accuracy
- Availability of processes, devices, data, and connected systems

8.3.3. Safety, Security and Effectiveness:

According to the Medical Devices Regulations, all risks connected with the use of medical devices must be acceptable in order to provide a high degree of health and safety protection. This can only be accomplished by establishing a sufficient balance between benefit and risk during all potential operation modes of a medical device. To that aim, there is a need to evaluate the link between "safety and security" as they relate to risk.

Security problems can be classified as either weak or restrictive:

a) weak security: For example, a lack of access control may allow malicious alteration of an implanted cardiac device's operation.

b) Restrictive security: Using too restrictive security measures that give a high level of protection may have a negative impact on safety, particularly if the security capabilities are poorly designed. For example, during an emergency, medical workers must have unrestricted access to an implanted cardiac device, yet rigorous security measures must be in place under regular working conditions.

8.3.4. Intended use and intended operational environment of use:

Manufacturers must separate two critical areas throughout the product security risk management process:

1. safety risk management, which is generally included in the overall product risk management, and
2. security risk, which is not linked with safety.

Operational Environment:

Healthcare providers should have a risk management approach that adheres to basic cybersecurity best practices in order to preserve the healthcare provider's overall security status, including the following:

- Good physical security to prevent unauthorized physical access to medical devices or network access points;
- Access control measures (e.g., role based) to ensure only authenticated and authorized personnel are allowed access to network elements, stored information, services and applications;
- Network access controls, such as segmentation, to limit medical device communication;
- General patch management practices that ensure timely security patch updates;
- Malware protection to prevent unauthorized code execution;
- Security awareness training.
- Auditability that supports non-repudiation, i.e., the ability to reliability determines who made what changes to the system and when to assist with forensics

8.3.5. Secure Design and Manufacture:

The general approach to security management for medical devices and software is like that of other cyber-physical systems. The eight common practices listed below outline the majority of the processes that need to be in place to develop a "Defense-in-Depth strategy" for the organization during the product lifecycle:

Practice 1 - Security management: The security management practice's goal is to guarantee that security-related actions are properly planned, documented, and implemented throughout the product's lifespan.

Practice 2 - Security requirements specification: The techniques outlined by this practice are used to determine the security capabilities that are necessary for proper protection of data confidentiality, integrity, and availability, as well as the stated product security context. Authentication, authorization, encryption, auditing, and other security capabilities that a product must have been examples of security capabilities. The product security context may contain elements such as physical security level, firewall protection of external interfaces, and so on.

Practice 3 - Secure by design: This practice's techniques are utilized to guarantee that the product is secure by design, including defense in depth.

Practice 4 - Secure implementation: The techniques outlined in this practice are used to guarantee that product features are safely implemented. With the exception of externally provided components, requirements in this practice apply to all hardware and software components in the product. Practice 1 (Security Management) requirements apply instead to externally sourced components.

Practice 5 - Security verification and validation testing: The methods provided by this practice are used to record the security testing necessary to guarantee that all of the product's security criteria have been satisfied and that the product's security is maintained when used as intended. Security testing should be coordinated with other product test activities and can be conducted at various times by various employees across the overall security lifecycle, depending on the kind of testing and the vendor's development strategy.

Practice 6 - Security-related issue management: The processes outlined by this practice are used to handle product security problems.

Practice 7 - Security update management: This practice specifies mechanisms for ensuring that security updates and security patches connected with the product are tested for regressions and made accessible to product users in a timely manner.

Practice 8 - Security guidelines: This practice's processes are used to generate and maintain user documentation that defines how to integrate, configure, and maintain the product's defense-in-depth strategy in compliance with its product security context.

8.4. US FDA 510(k) Pre-Market Guidelines for Device Security – 2022

The frequency of threats for medical devices is increasing manifold, in turn causing a problem for the hospital and patient security. A cybersecurity threat can affect the safety and efficacy of a device by compromising the operation of any asset in the system if proper cybersecurity considerations are not applied across all parts of these systems.

The FDA introduces terms such as “device lifecycle” and “SBOM (Software Bill of Materials)” implying that device OEMs must consider not only authentication and authorization but also decommissioning and recommissioning of devices in the market, as well as continuous checking, validating, and updating of SBOMs.

The original draft guidance document issued on April 8, 2022, states that “This guidance applies to all types of devices within the meaning of section 201(h) of the Federal Food, Drug, and Cosmetic Act (FD&C Act) whether or not they require a premarket submission. Therefore, the information in this guidance should also be considered for understanding FDA’s recommendations for devices for which a premarket submission is not required (e.g., for 510(k)-exempt devices)”.

This guidance also emphasises openness by requesting that manufacturers disclose technical material like as manuals that healthcare practitioners may use to easily patch devices. It states, “A lack of cybersecurity information, such as information necessary to integrate the device into the use environment, as well as information needed by users to maintain the device’s cybersecurity over the device lifecycle, has the potential to affect the safety and effectiveness of a device.”

Medical Device OEMs require a segmented yet synchronous approach to device and data security (Greenfield vs. Brownfield strategy) as well as the ability to manage all of their devices from a single platform. It is necessary to create and implement cybersecurity policies based on device groupings and automate device certificate lifecycles. To comply with the Executive Order on SBOMs, OEMs and their HDO, clients must additionally consider allowing continuous verification of device SBOMs and automating device quarantining and blacklisting according on these evaluations.

8.4.1. General Principles

The following is an overview of the general principles for device cybersecurity relevant to device manufacturers.

- a. Cybersecurity is Part of Device Safety and the Quality System Regulations
- b. Designing for Security
- c. Transparency
- d. Submission Documentation
- e. Using an SPDF to Manage Cybersecurity Risks
 - i. Security Risk Management
 - 1) Threat Modelling
 - 2) Third-Party Software Components
 - a) SBOM
 - b) Documentation supporting SBOM
 - 3) Security Assessment of Unresolved Anomalies
 - 4) Security Risk Management Documentation
 - 5) TPLC Security Risk Management
 - ii. Security Architecture
 - 1) Implementation of Security Controls
 - 2) Security Architecture Views
 - Global System View
 - Multi-Patient Harm View
 - Updateability/Patchability View
 - Security Use Case View(s)
 - iii. Cybersecurity Testing
- f. Cybersecurity Transparency
 - i. Labeling Recommendations for Devices with Cybersecurity Risks
 - ii. Vulnerability Management Plans

9. IMDRF

9.1. Principles and Practices for Medical Device Cybersecurity –2020

With the increased usage of wireless, Internet, and network-connected devices, the necessity for solid cybersecurity to assure medical device operation and safety has grown. Cybersecurity events have left medical devices and hospital networks unworkable, causing disruptions in patient care delivery throughout healthcare institutions. Such occurrences may cause patient damage due to delays and/or inaccuracies in diagnosis and/or therapeutic procedures, among other things. Stakeholders in the healthcare industry share responsibilities for medical device cybersecurity. This guideline is intended to help all stakeholders better understand their role in supporting proactive cybersecurity that protects and secures medical equipment in advance of potential attacks, problems, or incidents. This IMDRF guideline document's goal is to give general principles and best practices to aid worldwide regulatory convergence on medical device cybersecurity.

9.1.1. General guiding principles for medical device cybersecurity, relevant for all stakeholders to consider when developing, regulating, using, and monitoring medical devices, are:

- Global Harmonization - Convergence of global healthcare cybersecurity efforts is required to protect patient safety while stimulating innovation and providing patients with timely access to safe and effective medical products. All stakeholders are urged to coordinate their approaches to cybersecurity over the medical device's entire life cycle. This comprises product design harmonization, risk management efforts throughout the device's life cycle, device labelling, regulatory submission requirements, information exchange, and post-market activities.
- Total Product Life Cycle - To effectively manage the dynamic nature of cybersecurity risk, risk management should be applied throughout the total product life cycle (TPLC), where cybersecurity risk is evaluated and mitigated in the various phases of the TPLC including but not limited to design, manufacturing, testing, and post-market monitoring activities.
- Shared Responsibility - Shared Responsibility Medical device cybersecurity is a shared responsibility between stakeholders including the manufacturer,

healthcare provider, users, regulator, and vulnerability finder (Chip-OEM-GSI-ODM-Owner -SBOM provider).

- **Information Sharing** - The availability of timely information improves the capacity of all responsible parties to recognize hazards, analyze related risks, and respond appropriately. To foster collaboration and communication of cybersecurity incidents, threats, and vulnerabilities that may affect the safety, performance, integrity, and security of medical devices and the connected healthcare infrastructure, all responsible stakeholders are encouraged to actively participate in Information Sharing Analysis Organizations (ISAOs). These initiatives enhance transparency. Another information-sharing approach promoted as a best practice is coordinated vulnerability disclosure.

9.1.2. Pre-Market Considerations for Medical Device Cybersecurity:

It is important for companies to approach cybersecurity both before and after their products hit the market. IMDRF urges enterprises to consider design concepts like secure communications and data confidentiality in the development process before going to market. The idea is to reduce the likelihood of post-market difficulties by thinking about how a gadget will interact with other technologies and retain data.

Secure development principles are integral to secure device design.

- **Secure Communications** – Protocol agnostic, KeyScaler as RA, robust authentication, end to end encryption, new session new key, anti-clone
- **Data Protection** - End to End encryption - chip to application - at rest, in motion, owner policy driven with elements of access control, crypto key management, secure storage.
- **Device Integrity** – audit logging function, code signing, Anti clone.
- **Software Maintenance** – Code Signing & Secure Update, SBOM

IMDRF advocates a total product life cycle (TPLC) approach to medical device cybersecurity and has defined a security risk management strategy meant to detect, analyse, and control risks at each stage of development, from initial idea through end of support. As efforts to address the TPLC of medical device cybersecurity starting from the earliest device design and development stage continue to advance, availability of devices that maintain the capability of reasonable protection against cybersecurity threats through its use lifetime will become more and more the norm.

TPLC Cybersecurity Management Plan:

- TPLC Vigilance: Proactive monitoring and detection of newly identified cybersecurity vulnerabilities, risk assessment, and suitable remedies.
- Vulnerability Disclosure: A systematic procedure for gathering information from vulnerability finders, devising mitigation and remediation plans, and informing stakeholders about the presence of vulnerabilities and mitigation or remediation approaches.
- Updates and Remedial: A strategy explaining how software will be updated or other remediation steps will be implemented to preserve the device's continuous safety and performance, either on a regular basis or in reaction to a recognised vulnerability.
- Recovery: A strategy for either the manufacturer, the user, or both to return the equipment to normal operation after a cybersecurity event.
- Information Sharing: Participation in Information Sharing Analysis Organizations (ISAOs) or Information Sharing and Analysis Centers (ISACs) that facilitate communication and sharing of current information on security risks and vulnerabilities.

9.1.3 Post-Market Considerations for Medical Device Cybersecurity:

Because vulnerabilities evolve over time, pre-market controls established and implemented may be insufficient to maintain an acceptable risk profile; hence, a post-market strategy involving numerous stakeholders is required. Therefore, the IMDRF's post-market guidance is addressed separately to healthcare practitioners and manufacturers. According to the proposal, healthcare providers bear joint responsibility for cybersecurity and should consider implementing a risk-management procedure for devices linked to their IT infrastructure. And manufacturers are encouraged to share information and be transparent.

9.2. IMDRF - Principles and Practices for Medical Device Cybersecurity of Legacy Devices 2022

Even with medical devices improving at par with the advancing technology, there exist numerous outdated devices in the market today, often called “legacy devices,” that do not comply with the considerations of the newer devices. Such devices are prone to risks and could significantly threaten patient safety.

This document aims to “provide concrete recommendations on how to apply the TPLC to 111 legacy devices to aid in the implementation of the framework put forward in the preceding IMDRF 112 N60 guidance.” It addresses cybersecurity in the context of medical devices that incorporate software, including firmware and programmable logic controllers (for example, pacemakers) or exist solely as software (e.g., Software as a Medical device (SaMD)).

In prior IMDRF N60 recommendations, legacy devices were described as medical equipment that cannot be properly secured against contemporary cybersecurity risks. As a result, this document solely discusses legacy devices in the context of cybersecurity, rather than all other instances in which a device may be called "vintage" (e.g., an older model of a medical device).

This document intends to:

- Explain legacy medical device cybersecurity in the context of the TPLC Framework (Development, Support, Limited Support, and End of Support), with clear obligations for MDMs and HCPs at each step.
- Make recommendations for MDMs and HCPs on communication (including vulnerability management), risk management, and the transfer of responsibility to the HCP;
- Make recommendations on compensating controls after End of Support; and
- Make recommendations for MDMs and HCPs on communication (including vulnerability management), risk management, and the transfer of responsibility to the HCP;
- Make recommendations on compensating controls after End of Support; and
- Provide MDMs and HCPs with implementation considerations for existing legacy devices that were built prior to the TPLC Framework for medical device cybersecurity and are still in use.

9.2.1. General Principles

The following principles for legacy devices act as guidance to the stakeholders when developing, using, regulating, and monitoring medical devices:

a. TPLC

- The problems associated with cybersecurity threats and vulnerabilities must be evaluated at all stages of a medical device's life cycle, from initial conceptualization to end of support (EOS) and decommissioning.
 - Medical devices should have a cybersecurity life cycle that includes the stages of development, support, limited support, and EOS.
- b. Shared Risk Management
- Medical device cybersecurity is a shared responsibility.
 - MDMs should design and maintain their devices in a way that maximises cybersecurity throughout the maintenance phase and lowers security risk after EOS in the future to effectively manage risk for older devices.
 - Users should work actively with MDMs to secure an SBOM, ensuring that the device is operating in the proper environment, and prepare for the device's EOS date.
- c. Communication
- Transparent communication between stakeholders enables effective protection against threats.
 - MDMs are required to not only design and create medical devices with planned EOL and EOS stages, but also to explicitly convey such stages as soon as feasible, preferably during device acquisition and installation.
 - Users can thus plan for EOL and EOS by getting information from the MDM to inform subsequent device maintenance activities.

9.2.2. The Stages of IMRDF/N60 TPLC Framework for Medical Device Cybersecurity

Risk management should be applied throughout the TPLC where cybersecurity risk is evaluated and mitigated in the various phases of the TPLC including but not limited to design, manufacturing, testing, and post-market monitoring activities to effectively manage the dynamic nature of cybersecurity risk.

Legacy Medical Device Cybersecurity according to the IMDRF N60 goes through the following stages with each of the stages having its own set of expectations and responsibilities:

- a. Development (Stage 1)
- b. Support (Stage 2)
- c. Limited Support (Stage 3)
- d. EOS (Stage 4)

10. FIDO Device Onboarding (FDO)

A new generation of secure IoT protocol called FIDO Device Onboarding (FDO) aims to address the problems of supply chain security and passwords. The FIDO Alliance created the FDO based on the same guiding principles for FIDO Authentication: ease, security, and privacy.

To configure an IoT device now, the owner must either enter credentials in the factory, even though the product is still a few weeks or months away from hitting the market, or make customers go through a time-consuming enrollment process that is unsecure. In these situations, it is very challenging to maintain supply chain security since hostile devices may impersonate real, authentic IoT devices. In addition, poor user experiences result in manufacturers and end users using weak passwords, keeping default passwords the same, and reusing passwords.

Asymmetric public key cryptography is used by FDO, an automated onboarding protocol for IoT devices, to give the industrial IoT sector a quick and secure way to add any device to any device management system.

The following are some business benefits of the FIDO Device Onboard standard:

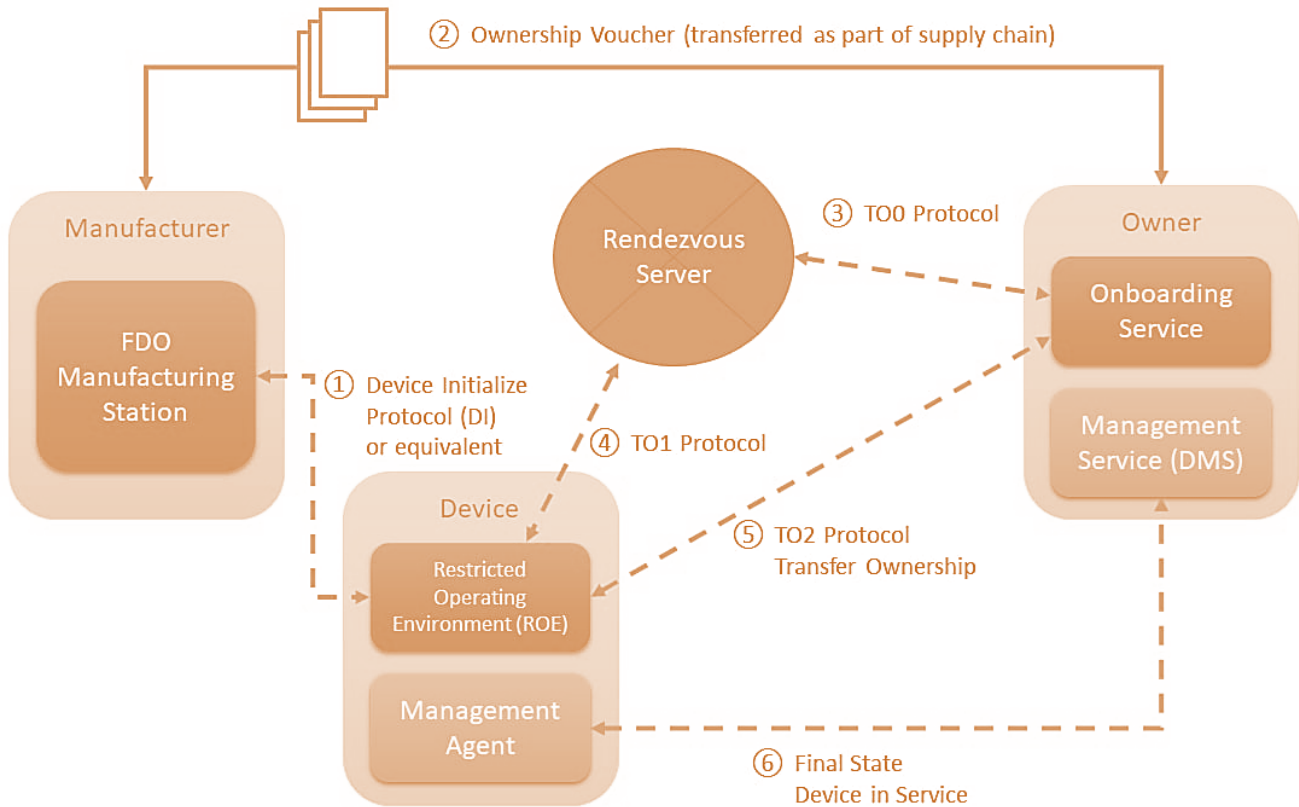
1. **Simplicity:** Companies no longer pay more for the devices themselves than they do for the protracted, highly complex installation process. People with any degree of experience can complete the fully automated FDO procedure swiftly and effectively.
2. **Flexibility:** Companies can choose which cloud platforms to onboard devices to at the time of installation (as opposed to manufacture). The device supply can be considerably simplified by onboarding a single device SKU to any platform.
3. **Security:** FDO uses an "untrusted installer" strategy, which implies that to connect a device to a network, the installer is no longer required to have access to or knowledge of any sensitive infrastructure or access control information.

The FIDO Alliance is the organization behind FIDO authentication. Reducing the need for passwords and enhancing authentication standards for desktops and mobile devices are the objectives of the FIDO authentication standards. Private keys and fingerprints, if utilized, never leave a person's device thanks to FIDO, which is made to protect people's security and privacy. You can avoid having to remember a long password by using a one-time PIN or swiping your fingerprint. Major operating systems and online browsers, including Windows 10 and Android, Mozilla Firefox, Microsoft Edge, and Apple Safari, also support FIDO.

The FIDO Alliance creates technical specifications that outline open standards for several interoperable authentication systems. Additionally, they have certification processes that enable businesses to confirm the interoperability of certified goods, which is important for widespread adoption.

Because FIDO is an open standard, it is available to the public and is free to adopt, implement, and upgrade. This indicates that it is designed for general use. Additionally, open standards are widely regarded in the developer community since they are controlled by a foundation of stakeholders that guarantee the standards' quality and interoperability.

Because FIDO prevents a person's information from being traced across various internet services they use, the FIDO authentication requirements are made to preserve user privacy. FIDO was created primarily to enhance user privacy.



Three sets of specifications, all of which are based on public key cryptography, have been released by the FIDO Alliance:

- Framework for Universal Authentication (UAF)
- FIDO2
- Universal Second Factor (U2F)

Universal Authentication Framework (UAF)

The FIDO UAF protocol allows online service providers to give password-less sign-on options to their users thanks to the FIDO UAF protocol. If more protection is needed, multi-factor sign-on experiences are also available.

Users need a personal device, like a computer or smartphone, that they register with an internet service to utilize UAF. Users are prompted to select their preferred method of future service authentication throughout the registration process.

Service providers decide what kinds of authentication procedures are necessary and offer a list of options, which may include reading a user's fingerprints, using facial or voice recognition, or inputting a PIN. Users can authenticate using more than one of these choices if a multi-factor sign-on experience is necessary.

Universal Second Factor (U2F)

Instead of completely replacing traditional password-based security, the FIDO U2F protocol enhances it. Users of U2F are required to submit two forms of identification verification:

Something they are familiar with, such as their login information.

something in their possession, such as a USB gadget or registered fob. These security tools, also known as U2F authentication tokens or security keys, can carry out authentication procedures using USB, NFC (near-field communication), or Bluetooth technology.

The computer browser interacts with the security device directly when it is activated, granting access to the online service.

FIDO2

The newest set of specifications from the FIDO Alliance is called FIDO2, and it was developed in collaboration with the World Wide Web Consortium (W3C).

The W3C standard WebAuthn and the FIDO Client To Authenticator Protocol (CTAP) are the two open standards upon which FIDO2 is based. When more security is required, the two collaborate to offer users password less login or two-factor and multi-factor authentication (2FA and MFA) experiences. These interactions could involve embedded authenticators like biometrics or PINs or roaming authenticators like USB devices or fobs.

The following requirements are part of FIDO2:

Platforms and browsers that accept FIDO authentication include a standard web API called WebAuthn. It can interact with both CTAP1 and CTAP2 authenticators and offers an interface for generating and managing public key credentials.

The new name for the FIDO U2F protocol is CTAP1. It offers customers a second-factor authentication experience, requiring them to tap their devices close to an NFC reader or plug security devices into their computers to access an online service.

Users can choose between password-free authentication and 2FA and MFA experiences with CTAP2, which enables the authenticator to be used as both the first and second factors of authentication.

Regulations requiring more reliable user authentication are compatible with the FIDO standards. Due to the necessity that customer authentication, be based on two or more elements, such as passwords or PINs, tokens or mobile devices, or biometrics, FIDO is made to comply with the PSD2 Regulatory Technical Specifications (RTS) of the European Union.

The FIDO standards are also intended to be followed to:

1. **The General Data Protection Regulation (GDPR)** applies to all businesses that operate, store, or otherwise process the personal data of EU individuals. PIN or biometrics are two examples of the multi-factor authentication that the GDPR mandates be used to confirm that a person is, in fact, who they claim to be.
2. **FATF, or the Financial Action Task Force:** The risk-based approach suggested by this Advise depends on a number of open sources, consensus-driven assurance frameworks, and technical standards for digital ID systems, according to FATF guidance on digital identity.

3. **New York Department of Financial Services (NYDFS) cybersecurity laws:**

The NYDFS is the main state regulator for the State of New York. To prevent unwanted access to non-public information or information systems, which is the person's private information, the NYDFS introduced Cybersecurity Requirements for Financial Services Companies, which mandate the implementation of MFA.

4. **NIST, the National Institute for Standards and Technology:** Because FIDO authentication complies with NIST recommendations for strong authentication, it is intended to be used for authenticating users to networks.

11. Software Bill of Materials (SBOM)

A Software Bill of Materials (SBOM) is formal and machine-readable metadata that uniquely identifies a software component, its dependencies, and license data. SBOM data formats are evolving and are likely to soon provide information to verify component authenticity and provide a link to known vulnerabilities. SBOMs are designed to be shared across organizations and are particularly helpful at providing transparency of components delivered by participants in a software supply chain. Organizations concerned about software security are making SBOMs a cornerstone of their cybersecurity strategy.

The basic components for a software bill of materials were recently issued by the NTIA (National Telecommunications and Information Administration) (more commonly known as SBOM)

These three groups comprise the minimal components that NTIA lists.

1. Automation Support for SBOM
2. Data Fields
3. Practices and Processes

Automation Support for SBOM

Making SBOMs machine-readable is what this component is all about, making them genuinely usable at scale and across enterprises. The following acceptable formats have been established by NTIA:

NTIA has defined the following approved formats:

1. **SPDX (Software Package Data eXchange)** — available now in FACT

Software bill of material data, such as provenance, license, security, and other relevant data, can be communicated via the open standard SPDX. By offering common formats for enterprises and communities to share crucial data, SPDX saves repetitive effort, streamlining and enhancing compliance, security, and dependability. As of ISO/IEC 5962:2021, the SPDX specification is acknowledged as the global open standard for security, licensing compliance, and other software supply chain artifacts.

The Linux Foundation serves as the home for the open-source project SPDX. Representatives from a wide range of businesses, including software, systems, and tool suppliers, foundations, and systems integrators, are involved in the grassroots initiative. The IT team, the legal team, and the outreach team all contribute to the work. Additionally, there is a monthly general call that offers a summary of the entire project's progress. Visit the Participate page for more details on how to participate.

The components of the SPDX project are:

- a. The actual SPDX Specification
- b. A list of SPDX licenses (including exceptions, matching guidelines, license IDs, and license expression syntax)
- c. Working with the SPDX documents and SPDX License List requires the use of SPDX tools and libraries.

Guiding Principles

- a. Data is represented using SPDX in ways that are readable by machines and people.
- b. A framework for making claims about such facts is provided by SPDX, which focuses on gathering and disseminating facts.
- c. No legal interpretations are made by SPDX (of licenses or license compliance).
- d. SPDX facilitates the efficient exchange of metadata in the supply chain.

2. **CycloneDX** — available by request

A simple Software Bill of Materials (SBOM) standard called OWASP CycloneDX is intended for usage in supply chain component analysis and application security scenarios.

The CycloneDX Core working group, which has its roots in the OWASP community, is responsible for the strategic development and upkeep of the specification.

For risk identification, a thorough and accurate inventory of all first-party and third-party components is necessary. All direct and transitive components, as well

as the dependence connections between them, should preferably be included in BOMs.

In response to U.S. Executive Order 14028, the National Telecommunications, and Information Administration (NTIA) established the Minimum Elements for Software Bill of Materials. CycloneDX considerably surpasses these requirements.

By implementing CycloneDX, companies can quickly satisfy these minimal needs and develop over time to use more complex use cases. All SBOM requirements outlined in the OWASP Software Component Verification Standard can be met by CycloneDX (SCVS)

Any sort of software component and the supporting services can be represented by CycloneDX. For more information on the numerous options for basic, moderate, and advanced SBOM use cases, see Use Cases.

3. **SWID (Software Identification)** — available now in FACT

In order to improve the precision and dependability of software asset management operations, the SWID tag standard was created to assist in overcoming the technical difficulties related to software discovery, identification, and contextualization. SWID tags provide a standardized signal of a software product's presence on a device, assisting in discovery. Incorporating a consistent label for a product into its tag, tags help with identification. Finally, tags facilitate contextualization by enabling the provision of a variety of associated product details, such as the complete name and version of the product.

SWID tags are advantageous to both people who make and distribute software as well as those who buy and use it. These stakeholders are named in the SWID specification as:

- Tag producers: Businesses and other entities that produce SWID tags for usage by consumers. The companies (or their authorised agents) in charge of designing, licencing, packaging, and/or distributing software products are examples of tag-producing entities. These companies are best able to guarantee that tags contain accurate, comprehensive

- Tag consumers: Organizations and entities that use information contained in SWID tags to support higher-level, software-related business and cybersecurity functions. Categories of tag consumers include software consumers, inventory/discovery tools, inventory-based cybersecurity tool providers (e.g., providers of software vulnerability management products, which rely on accurate inventory information to support accurate vulnerability assessment), and organizations that use these tools.

The data format for SWID tags discussed in this paper is specified by the international standard ISO/IEC 19770-2:2015.

- SWID tags were created to assist businesses in meeting the demand for precise and comprehensive software inventories to enable more advanced business and cybersecurity tasks.
- Organizations that produce and use SWID tags gain advantages.
- The objectives of four audiences in relation to SWID tags and tagging procedures are interrelated:
 - a. Software vendors frequently seek to make their clients' use of their products more manageable. They require consumers to convey unmistakable signals that they value product manageability as highly as features, functionalities, and usability to justify investing the resources necessary to become tag suppliers. SWID tags are frequently supported by vendors of software creation, packaging, and installation tools. Software developers that use their tools can benefit from this functionality by having it easier to generate tags during the product production and release processes.

The administration of installed tags on devices can also be supported by these tools during software installation, update, patch, and removal procedures. To guarantee that they provide SWID tags that are helpful to software customers, providers need explicit instructions on what data must be included.

- b. Companies that offer inventory-based goods and services frequently prefer to use SWID tags as their main strategy for classifying

software. For their specialised tools to be more generally used, these suppliers require tags to be more freely available.

- c. Software users frequently ask vendors to provide tags with their products as a standard procedure. In order to manage the difficulties of maintaining an accurate software inventory, as well as to solve software-related management and cybersecurity issues, consumers require tags to be routinely delivered.

Data Fields

The baseline information about each component that must be recorded and kept up to date in order to trace it across the software supply chain is known as a data field. With this knowledge in hand, a component can be mapped to other sources of data that are readily available, such as vulnerability databases or license databases. These fields are (at a minimum) necessary:

- a. Provider Name
- b. Subsystem Name
- c. Component's Version
- d. Additional Unique Identifiers
- e. Relationship of Dependence
- f. Writer of the SBOM Data
- g. Timestamp

By the way, gathering this data is very difficult. For instance, it can be quite challenging to get a product name right because of mergers and acquisitions, rebranding, and simple mistakes.

Procedures and Methods

These components speak to the usage of SBOMs' actual mechanisms. This section covers the SBOM-related provisions that must be made clear in any policy, agreement, or another arrangement. Additionally, it covers the sharing and distribution of SBOMs. The "Accommodation of Mistakes" was an intriguing

component that NTIA added. This is a recognition that in the short term, the industry should give up on expecting perfection to move quickly. The main goal is to move swiftly while securing the software supply chain and putting a constant improvement emphasis on it.

So, by this point, you undoubtedly want to know what an SBOM looks like in practise. Here is a real-world, SPDX-formatted SBOM for ICS software. It was produced by FACT, and as you can see, it is entirely compliant* and has all the NTIA-required data fields. (FACT also offers enhanced SBOMs that let you dive down and around all the components; we also offer risk scores and other useful data so you can determine which components are troublesome.)

CONCLUSION

The rapid growth and maturity of various technologies and the difficulty in keeping up with them and enabling stronger protection makes users and systems vulnerable to multiple threats. Establishing security standards improves the security of IT systems, networks, devices, and critical infrastructure. Manufacturers are also striving to become compliant with all the required standards and frameworks so that they do not have to face unnecessary actions. This document aims to highlight the security standards specific to IoT across various verticals like vehicles, control systems, medical devices, and IoT devices in general and provide a broad overview of each of those standards. However, it must be noted that this is not an exhaustive list of IoT security standards as IoT is still a niche technology and keeps improving and upgrading regularly. A few of the above-listed standards are also under development and set to release in the future.

ABBREVIATIONS

API – Application Programming Interface

BSI – British Standards Institution

CAGR – Compound Annual Growth Rate

CSMS – Cyber Security Management System

CVSS – Common Vulnerability Scoring System

DIS – Draft International Standard

ETSI – European Telecommunications Standards Institute

ECU – Electronic Control Unit

EU – European Union

FDA – Food and Drug Administration (see USFDA)

FCC – Federal Communications Commission

GDPR – General Data Protection Regulation

GSM – Global System for Mobile communication

IACS – Industrial Automation and Control Systems

IDD - IoT Device Developer

IEC – International Electrotechnical Commission

IoT – Internet of Things

ISA – International Society of Automation

ISD – IoT Service Developer

ISP – IoT Service Provider



ABBREVIATIONS

ISO – International Organization for Standardization

IT – Information Technology

IU – IoT User

MDCG – Medical Device Coordination Group

MDR – Medical Device Reporting

OT – Operational Technology

PAS – Publicly Available Specification

PMA – Pre-Market Approval

QMS – Quality Management System

SAE – Society of Automotive Engineers

STRIDE – Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege

TR – Technical Report

TS – Technical Specification

UMTS – Universal Mobile Telecommunications Service

UNECE – United Nations Economic Commission for Europe

USFDA – Food and Drug Administration of the United States

REFERENCES

- 1) <https://www.iso.org/standard/65695.html>
- 2) [Brief Overview of ISO/IEC 27400: Comprehensive standard on IoT Security and Privacy | All About Testing](#)
- 3) <https://www.iso27001security.com/html/27402.html>
- 4) [\[ISO27402\] ISO/IEC JTC1 SC27 WG4 \(2021\). ISO/IEC 27402: Cybersecurity – IoT Security and Privacy – Device Baseline Requirements \(2nd committee draft\)](#)
- 5) <https://www.isa.org/intech-home/2018/september-october/departments/new-standard-specifies-security-capabilities-for-c>
- 6) <https://www.iec.ch/blog/understanding-iec-62443>
- 7) <https://www.microchip.com/en-us/about/media-center/blog/2021/understanding-the-isa-iec-62443-standard-and-secure-elements-0>
- 8) <https://www.iso.org/en/contents/data/standard/07/09/70918.html>
- 9) <https://www.iso.org/obp/ui/#iso:std:iso-sae:21434:ed-1:v1:en>
- 10) <https://unece.org/sites/default/files/2021-03/R155e.pdf>
- 11) https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf
- 12) <https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards>
- 13) <https://blog.cm-dm.com/post/2020/05/03/MDCG-2019-16-Guidance-on-cybersecurity-for-medical-devices>
- 14) [IMDRF Document Template](#)

- 15) [Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions - Draft Guidance for Industry and Food and Drug Administration Staff \(fda.gov\)](#)
- 16) <https://www.deviceauthority.com/blog/iomt-fda-cybersecurity-guidelines/>
- 17) <https://www.surgicalroboticstechnology.com/articles/when-it-comes-to-protecting-iomt-medical-devices-is-good-enough-really-good-enough/>

