

Appendix E: Glossary

(1) **Actuator**

<Internet of Things> IoT device that changes one or more properties of a physical entity in response to a valid input. [ISO/IEC 20924:2024:202418]

(2) **Anti-tampering devices**

Device with an anti-tamper property. When used with devices, “anti-tamper” is used to describe that it is difficult to read or falsify the internal structure or stored data of the device.

(3) **Audit**

Systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled. [ISO/IEC 27000:202618]

(4) **Authentication**

Provision of assurance that a claimed characteristic of an entity is correct. [ISO/IEC 270029:202218]

(5) **Authenticity**

Property that an entity is what it claims to be. [ISO/IEC 270029:202218]

(6) **Availability**

Property of being accessible and usable on demand by an authorized entity. [ISO/IEC 27000:202618]

(7) **Basis of trustworthiness**

Point of view to ensure trustworthiness.

(8) **Biometric authentication**

Authentication method which identifies person by physical characteristics such as finger patterns, hand vein patterns, iris patterns or voiceprints.

(9) **CC (Common Criteria)**

Framework to evaluate if products and systems related to information technology are appropriately designed and properly implemented in terms of security. These criteria are defined as the international standard ISO/IEC 15408.

(10) **Chief Security Officer**

Person who has the highest responsibility in the operation and control of the security management systems in an organization.

(11) **Confidentiality**

Property that information is not made available or disclosed to unauthorized individuals, entities, or processes. [ISO/IEC 27000:202618]

(12) **CSA (Component Security Assurance) certification**

A third-party certification scheme for the security assurance of IACS (Industrial Automation and Control System) components, developed and operated by the U.S.-based ISCI (ISA Security Compliance Institute) based on IEC 62443-4-1 and IEC 62443-4-2. Target components are evaluated from three perspectives: development artifacts produced through a secure development lifecycle, technical security capabilities, and the detection of known vulnerabilities.

(12)(13) **CSIRT (Computer Security Incident Response Team)**

A capability set up for the purpose of assisting in responding to computer security-related incidents; also called a Computer Incident Response Team (CIRT) or a CIRC (Computer Incident Response Center, Computer Incident Response Capability). [NIST SP 800-61 Rev.2]An organizational unit (which may be virtual) or a capability that provides services and support to a defined constituency for preventing, detecting, handling, and responding to computer security incidents, in accordance with its mission. [FIRST Computer Security Incident Response Team (CSIRT) Services Framework Version 2.1]

~~(13)~~ (14) _____ CSMS (Cyber Security Management System)

Management system of the cyber security designed for industrial automation and its control systems. The requirements are defined in the international standard IEC62443-2-1.

~~(14)~~ (15) _____ Cyberattack

~~Attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset. A successful or unsuccessful unauthorized attempt to destroy, alter, disable, gain access to, expose, steal, or make unauthorized use of an asset.~~ [ISO/IEC 27002:2022+8]

~~(15)~~ (16) _____ Cybersecurity

To prevent the leak or falsification of electronic data as well as the malfunction of IT or control systems against expected behavior.

~~(16)~~ (17) _____ Cyberspace

Virtual space in computer systems or networks. It uses digital data to create value.

~~(17)~~ (18) _____ Digital certificate

Data which certifies that the public key for digital signature analysis is authentic, and issued by a certification authority (CA).

~~(18)~~ _____ ~~EDSA (Embedded Device Security Assurance) certification~~

~~Certification program related to security assurance for control devices. EDSA is developed and operated by the ISA Security Compliance Institute (ISCI) based on IEC 62443-4-2. The program evaluates the security on three aspects, namely, security at each phase of software development, implemented security features, and communication robustness test.~~

(19) _____ Entity

Thing (physical or non-physical) having a distinct existence. [ISO/IEC 15459-3:2014]

(20) **Firewall**

Software, devices or systems installed at the border between a certain computer/network and external network in order to protect the internal network from external attack by relaying and monitoring the internal/external communication.

(21) **Functional safety**

Part of the overall safety of EUC (controlled devices) and EUC control systems that depend on the normal functions of E/E/PE (electric/electronic/programmable electronic) safety systems and other risk mitigation measures. [IEC 61508-4 Ed.2]

(22) **Harm**

Injury or damage to the health of people, or damage to property or the environment. [ISO/IEC Guide 51:2014]

(23) **Hazard**

Potential source of harm. [IEC 61508-4:2010]

(24) **Hash function**

Function which maps strings of bits of variable (but usually upper bounded) length to fixed-length strings of bits, satisfying the following two properties:

- for a given output, it is computationally infeasible to find an input which maps to this output;
- for a given input, it is computationally infeasible to find a second input which maps to the same output. [ISO/IEC 10118-1:2016]

(25) **Hash value**

String of bits which is the output of a hash-function. [ISO/IEC 27037:2012]

(26) **Identifier**

Information that unambiguously distinguishes one entity from other entities in a given identity context. [ISO/IEC 20924:2024~~18~~]

(27) **IDS (Intrusion Detection System)**

System which monitors the external communication conducted by a server or network and alerts its controllers via e-mail when detecting unauthorized access (such as attack or intrusion attempt).

(28) **Industrial control system**

General term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as programmable logic controllers (PLC) found in the industrial sectors and critical infrastructures.~~An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition (SCADA) systems used to control geographically dispersed assets, as well as distributed control systems (DCSs) and smaller control systems using programmable logic controllers to control localized processes.~~ [NIST SP 800-53 Rev. 54]

(29) **Integrity**

Property of accuracy and completeness. [ISO/IEC 27000:202618]

(30) **IoT (Internet of Things)**

Infrastructure of interconnected entities, people, systems and information resources together with services which processes and reacts to information from the physical space and cyberspace. [partly changes the definition in ISO/IEC 20924:202418]

(31) **IoT device**

Entity of an IoT system that interacts and communicates with the physical space through sensing or actuating.

NOTE: An IoT device can be a sensor or an actuator. [partly changes the definition in ISO/IEC 20924:202418]

(32) **IPS (Intrusion Prevention System)**

System which monitors the external communication conducted by a server or network and prevents attack by detecting unauthorized access (such as attack or intrusion attempt).

(33) **ISMS (Information Security Management System)**

Framework to operate a system by determining the required security level, establishing a plan and distributing resources through its own risk assessment in order to manage an organization. The requirements are defined in the international standard ISO/IEC 27001.

(34) **ITSMS (IT Service Management System)**

Framework designed for IT service providers to maintain or improve their service quality by managing their services based on the PDCA cycle. The requirements are defined in international standard ISO/IEC 20000-1.

(35) **Malware**

Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code. [NIST SP 800-53 Rev.54]

(36) **Multifactor authentication**

Authentication using two or more different factors to achieve authentication. Factors include: (i) something you know (e.g., password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). See Authenticator. [NIST SP 800-53 Rev.54]

(37) **Multi-stakeholder process**

Process in which three or more stakeholders have meetings to have discussions on an equal footing, thereby understanding each other for consensus building in order to solve a problem that could not be solved by one or two stakeholder(s). [Cabinet Office of Japan]

(38) **Mutual authentication**

One of the authentication methods, in which two parties authenticate with each other.

(39) **Objective**

Result to be achieved. [ISO/IEC 900027000:202618]

(40) **Physical Space**

The real world. Expression to distinguish between cyberspace and world composed of substances.

(41) **Private key**

Secret key in the public-private key cryptosystem, a pair of different keys is used for the encryption and decryption. The private key is the one not released to the public.

(42) **Process**

Set of interrelated or interacting logical or physical activities which transforms inputs into outputs.

(43) **Protocol**

Predetermined mass of rules and steps for parties, so that more than one party can smoothly transmit signals, data and information with one another.

(44) **Public key**

Cryptographic kKey of an entity's asymmetric key pair, which can be made public.

NOTE: In the case of an asymmetric signature system the public key defines the verification transformation. In the case of an asymmetric encipherment system the public key defines the encipherment transformation. A key that is 'publicly known' is not necessarily globally available. The key can only be available to all members of a pre-specified group. [ISO/IEC 19790:202512]

(45) **Redundancy**

Existence of a means in addition to the means which would be sufficient for a functional unit to perform a required function or for data to represent information. [ISO/IEC 2382:2015]

(46) **Resilience**

The ability of an information system to operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities, and to recover to an effective operational posture in a time frame consistent with mission needs.~~The ability of an information system to continue to: (i) operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (ii) recover to an effective operational posture in a time frame consistent with mission needs.~~ [NIST SP 800-53 Rev. 54]

(47) **Risk**

Effect of uncertainty on objectives. [ISO/IEC 27000:202618]

(48) **Risk management**

Coordinated activities to direct and control an organization with regard to risk. [ISO 31000:2018]

(49) **Risk source**

Element which alone or in combination has the potential to give rise to risk. [ISO 31000:2018]

(50) **Safety**

State of being protected from recognized hazards that are likely to cause harm. [ISO/IEC Guide 51:2014]

(51) **Security-by-design**

To introduce the measures (e.g. threat analysis, security architecture, external specification analysis and privacy impact assessment) to ensure security at the planning and designing stages for a device or system.

(52) **Security event**

Identified occurrence of a system, service or network state indicating a possible breach of security policy or failure of controls, or a previously unknown situation that can be security relevant.

(53) **Security incident**

Single or a series of unwanted or unexpected security events that have a significant probability of compromising business operations and threatening information security.

(54) **Security measure organization (SOC/CSIRT)**

An entity that provides security services for managing cybersecurity risks in the business activities of an organization.~~Structure which continuously collects and analyzes the vulnerability information in or out of an organization in order to determine the appropriate scope and priority of measures against a security incident to be monitored. Security measure organization includes organizations and functions such as SOC and CSIRT. [ITU-T Recommendation X.1060Six Ws on cybersecurity information sharing for enhancing SOC/CSIRT Version 1.0 (ISOG-J, 2018)]~~

(55) **Security operation process**

Document which specifies the prompt preventive measures beforehand against the security incidents to be detected.

(56) **Security policy**

Top management's intentions and direction formally expressed regarding security of the organization, and rules to take security measures based on such intentions and direction.

(57) **Security risk**

Possibility of some effects on the objectives of the organization, relevant parties such as partners, or the whole society caused by the malfunctions related to security.

(58) **Security rule**

What defines the details on the measures against possible security risks clarifying each scope and priority.

(59) **Sensor**

<Internet of Things> An IoT device capable of observing one or more properties of a physical entity and converting those properties into information.~~IoT device that measures one or more properties of one or more physical entities and outputs digital data that can be transmitted over a network.~~ [ISO/IEC 20924:2024~~18~~]

(60) **Service**

Output of an organization with at least one activity necessarily performed between the organization and the customer. [ISO 9000:2026~~15~~]

(61) **Service Provider**

A provider of basic services or value-added services for operation of a network - generally refers to public carriers and other commercial enterprises. [NIST IR 4734]

(62) **SOC (Security Operation Center)**

A team composed primarily of security analysts organized to detect, analyze, respond to, report on, and prevent cybersecurity incidents. [RFC 2350, CNSS Instruction No. 4009]

(63) **Stakeholder**

Person or organization that can affect, be affected by, or perceive itself to be affected by a decision or activity. [ISO/~~IEC~~ 900027000:2026~~18~~]

(64) **Supplier**

Organization or an individual that enters into agreement with the acquirer for the supply of a product or service. [ISO/IEC 27036-1:2021~~14~~]

(65) **Supply chain**

Linked set of resources and processes between and among multiple tiers of organizations, each of which is an acquirer, that begins with the sourcing of products and services and extends through their life cycle.~~Linked set of resources and processes between multiple tiers of developers that begins with the sourcing of products and services and extends through the design, development, manufacturing, processing, handling, and delivery of products and services to the acquirer.~~ [ISO 28001:2007, NIST SP 800-53 Rev. ~~5~~⁴]

(66) **Threat**

Potential cause of an unwanted incident, which can result in harm to a system or organization. [ISO/IEC 2700~~20~~²²:20~~18~~¹⁸]

(67) **Threat hunting**

An active means of cyber defense that involves proactively searching organizational systems, networks, and infrastructure for advanced threats. The objective is to track and disrupt cyber adversaries as early as possible in the attack sequence and to measurably improve the speed and accuracy of organizational responses. [NIST SP 800-53 Rev.5]

(68) **Threat intelligence**

Threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision making processes. [NIST SP 800-150]

~~(67)~~(69) **Time-stamp**

Time variant parameter which denotes a point in time with respect to a common time reference. [ISO/IEC 18014-1:2008]

~~(68)~~(70) **Trust**

Degree to which a user or other stakeholder has confidence that a product or system will behave as intended. [ISO/IEC ~~TR 24028:2020~~^{25010:2011}]

~~(69)~~ (71) Trustworthiness

~~Ability to meet stakeholders' expectations in a verifiable way. Property of deserving trust or confidence. In the context of IoT, property of deserving trust or confidence within the entire lifecycle of an Internet of Things implementation to ensure security, privacy, safety, reliability and resiliency. [ISO/IEC TS 5723:202220924:2018]~~

~~(70)~~ (72) Vulnerability

Weakness of an asset or control ~~(3.14)~~ that can be exploited by one or more threats. [ISO/IEC 2700~~20~~:20~~22~~18]

~~(71)~~ (73) Vulnerability remediation plan

A plan to perform the remediation of one or more threats or vulnerabilities facing an organization's systems. The plan typically includes options to remove threats and vulnerabilities and priorities for performing the remediation. ~~[NIST SP 800-40 Ver.2.0]~~