MCMC MTSFB TC G031:2021

TECHNICAL CODE

INTERNET OF THINGS - APPLICATION SECURITY REQUIREMENTS

Developed by

Malaysian Technical Standards Forum Bhd

Registered by

MCMC

Registered date : 24 August 2021

MCMC MTSFB TC G031:2021

Development of technical codes

The Communications and Multimedia Act 1998 (‘the Act’) provides for Technical Standards Forum designated under section 184 of the Act or the Malaysian Communications and Multimedia Commission (‘the Commission’) to prepare a technical code. The technical code prepared pursuant to section 185 of the Act shall consist of, at least, the requirement for network interoperability and the promotion of safety of network facilities.

Section 96 of the Act also provides for the Commission to determine a technical code in accordance with section 55 of the Act if the technical code is not developed under an applicable provision of the Act and it is unlikely to be developed by the Technical Standards Forum within a reasonable time.

In exercise of the power conferred by section 184 of the Act, the Commission has designated the Malaysian Technical Standards Forum Bhd (‘MTSFB’) as a Technical Standards Forum which is obligated, among others, to prepare the technical code under section 185 of the Act.

A technical code prepared in accordance with section 185 shall not be effective until it is registered by the Commission pursuant to section 95 of the Act.

For further information on the technical code, please contact:

Malaysian Communications and Multimedia Commission (MCMC)
MCMC Tower 1
Jalan Impact
Cyber 6
63000 Cyberjaya
Selangor Darul Ehsan
MALAYSIA

Tel: +60 3 8688 8000
Fax: +60 3 8688 1000
http://www.mcmc.gov.my

OR

Malaysian Technical Standards Forum Bhd (MTSFB)
MCMC Centre of Excellence (CoE)
Off Persiaran Multimedia
Jalan Impact
Cyber 6
63000 Cyberjaya
Selangor Darul Ehsan
MALAYSIA

Tel: +60 3 8320 0300
Fax: +60 3 8322 0115
http://www.mtsfb.org.my

Contents

Committee representation

This technical code was developed by Internet of Things Security Sub Working Group under the Security, Trust and Privacy Working Group of the Malaysian Technical Standards Forum Bhd (MTSFB) which consists of representatives from the following organisations:

American Malaysian Chamber of Commerce

Celcom Axiata Berhad

Digi Telecommunications Sdn Bhd

Favoriot Sdn Bhd

Maxis Broadband Sdn Bhd

Telekom Malaysia Berhad

U Mobile Sdn Bhd

Universiti Kuala Lumpur

Foreword

This technical code for Internet of Things - Application Security Requirements ('this Technical Code') was developed pursuant to section 185 of the Act 588 by the Malaysian Technical Standards Forum Bhd (MTSFB) via its Internet of Things Security Sub Working Group under the Security, Trust and Privacy Working Group.

This Technical Code is the extension of MCMC MTSFB TC G013, *Internet of Things (IoT) - Security Management.*

This Technical Code shall continue to be valid and effective from the date of its registration until it is replaced or revoked.

INTERNET OF THINGS - APPLICATION SECURITY REQUIREMENTS

0. Introduction

The Internet of Things (IoT) has evolved exponentially at the global scale. Gartner reported that there were 8.4 billion connected IoT devices in 2017, up 31 % from 2016, and it is envisioned that this number will reach 20 billion by 2020. Another agency, Statista Research Department predicted that by 2025 there will be 75.44 billion connected IoT devices in the world.

Industry Revolution 4.0 also uses the IoT in order to perform digital manufacturing where some of the use cases of Industry Revolution 4.0 are as follows:

a) smart manufacturing (e.g., data driven quality control and augmented operations);

b) smart refinery (e.g., predictive maintenance and information-driven performance);

c) remote monitoring assistance for control and diagnostic of plant operations (e.g., energy and environment); and

d) smart city (e.g., waste management, traffic management and crowd sensing).

This rapid evolution brings its own challenges to the immature IoT ecosystem that includes a fragmentation of standards and security concerns in a non-homogeneous IoT market. Currently there are different solutions available in the market which use proprietary cloud services, protocols and operating systems.

The threats and risks related to the IoT devices, systems and services are manifold and evolve rapidly. This may impact citizens' safety, security and privacy. The threat landscape concerning the IoT is extremely wide, hence, it is important to understand what needs to be secured. In consequence, there is the necessity to develop specific security measures to protect the IoT ecosystem from cyber threats.

1. Scope

This Technical Code specifies requirements for IoT application security. It covers the definition, threat landscapes, security measures and security best practices for IoT applications. This Technical Code will benefit from the IoT device manufacturers up until the IoT software developers. It concerns from end to end, from the devices to the applications.

2. Normative references

The following normative references are indispensable for the application of this Technical Code. For dated references, only the edition cited applies. For undated references, the latest edition of the normative references (including amendments) applies.

MCMC MTSFB TC G013, *Internet of Things (IoT) - Security Management*

MCMC MTSFB TC G021, *Information and Network Security - Monitoring and Measurement of Security Control Objectives*

Act 709, *Personal Data Protection Act 2010*

3. Abbreviations

For the purposes of this Technical Code, the following abbreviations apply.

See Annex A.

4. Terms and definitions

For the purposes of this Technical Code, the following terms and definitions apply.

4.1 Communication

The IoT communication systems rely on the ability to both transmit and receive information in a structured manner, using interoperable communication infrastructure.

The communication medium within the IoT ecosystems can be either wired or wireless. The following are the example of the wireless communication protocols.

a) ZigBee;

b) Bluetooth or Bluetooth Low Energy (BLE);

c) Wireless Fidelity (WiFi);

d) WiFi HaLow;

e) Near Field Communication (NFC);

f) Radio Frequency Identification (RFID).

g) Low-Power Wide Area Network (LoRaWAN);

h) SigFox;

i) Narrow Band-IoT (NB-IoT); or

j) Long Term Evolution for Machines (LTE-M).

4.2 Embedded systems

The IoT devices can also be found as embedded systems, which include sensors and/or actuators, as well as network capabilities to connect directly to a network infrastructure. Additionally, the IoT embedded systems include internal memory and a processing unit that may have the capability to process data.

4.3 Internet of Things (IoT) application

A cyber-physical ecosystem that may be able to react based on gathered information from sensors

4.4 Internet of Things (IoT) high level reference model

The IoT high level reference model defined in MCMC MTSFB TC G013, *Internet of Things (IoT) - Security Management* includes the following 4 main layers (see Figure 1).

a) Device layer represents an object that has a specific identifier, with sensors and/or actuators.

b) Network layer represents the communication capabilities.

c) Service and application support layer represent the cloud platform, backend and services.

d) Application layer represents use cases.

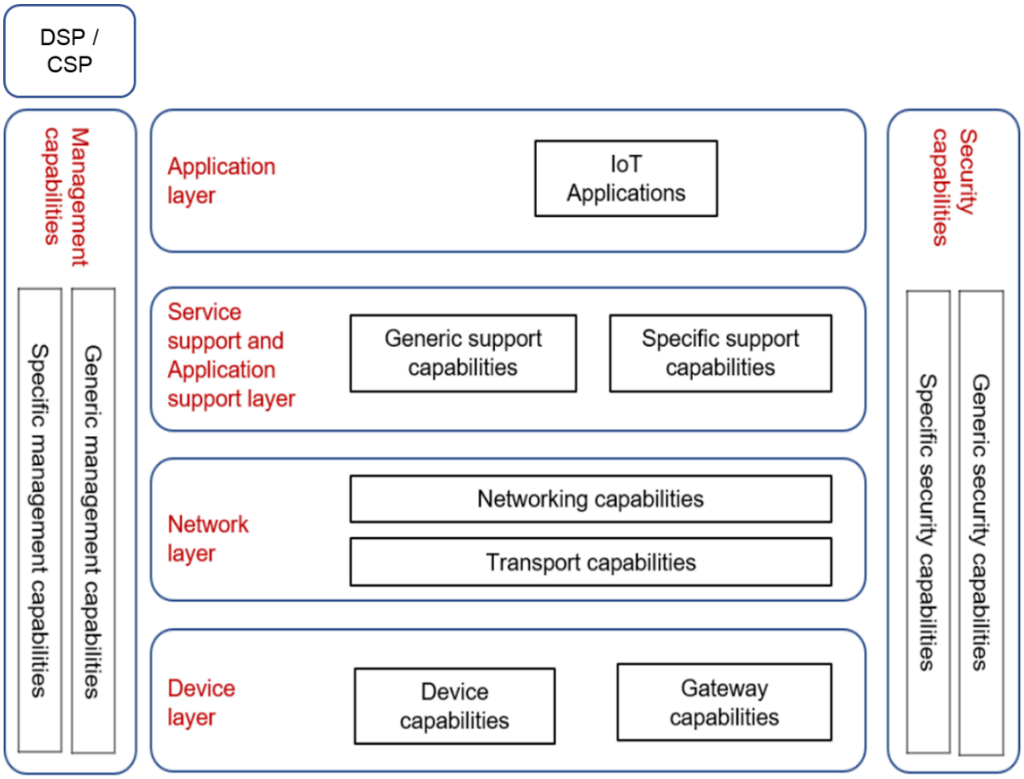


Figure 1. IoT high level reference model

4.5 Internet of Things (IoT) stakeholder

IoT stakeholders are all parties involved in the IoT application ecosystem.

4.6 Objects in the Internet of Things (IoT)

The physical devices or virtual objects capable of being identified and integrated into communication networks. It is imperative for objects to have the capability of communication such as exchanging data over a network between them and/or with the data processing systems and/or the cloud backend services.

An IoT ecosystem comprises of sets of objects that can be autonomously monitored and controlled by an intelligent system. This system can retrieve data from an object or a set of objects and process that data, obtaining useful information in order to make decisions.

4.7 Sensors and actuators

Sensor functions as an input device that gathers information about the environment and its context, which will be subsequently processed. In contrast, the actuator serves as an output device, which executes decisions based on processed information.

5. Internet of Things (IoT) application threat and risk

This clause describes common security incidents, assets classification, threats classification, and attack scenarios that affect IoT applications, devices and networks.

5.1 Security incidents

IoT security incidents have been discovered and/or taken place since 2005. Annex B shows attacks such as hacking, Distributed Denial-of-Service (DDoS) and botnet on IoT have increased over the years. This has raised concerns on the level of security offered by the IoT ecosystem.

5.2 Assets classification

The key asset groups and assets that shall be protected by the IoT application/solution providers in Figure 2 is based on TP-02-19-880-EN-N, *Good Practices for Security of IoT - Secure Software Development Lifecycle* by European Network and Information Security Agency (ENISA). It is divided into the following groups as described in Annex C.

a) Data (see Table C.1).

b) Human factor (see Table C.2).

c) Maintenance (see Table C.3).

d) Software design (see Table C.4).

e) Software deployment (see Table C.5).

f) Software development (see Table C.6).

g) Software components (see Table C.7).

h) Software Development Lifecycle (SDLC) infrastructure (see Table C.8).

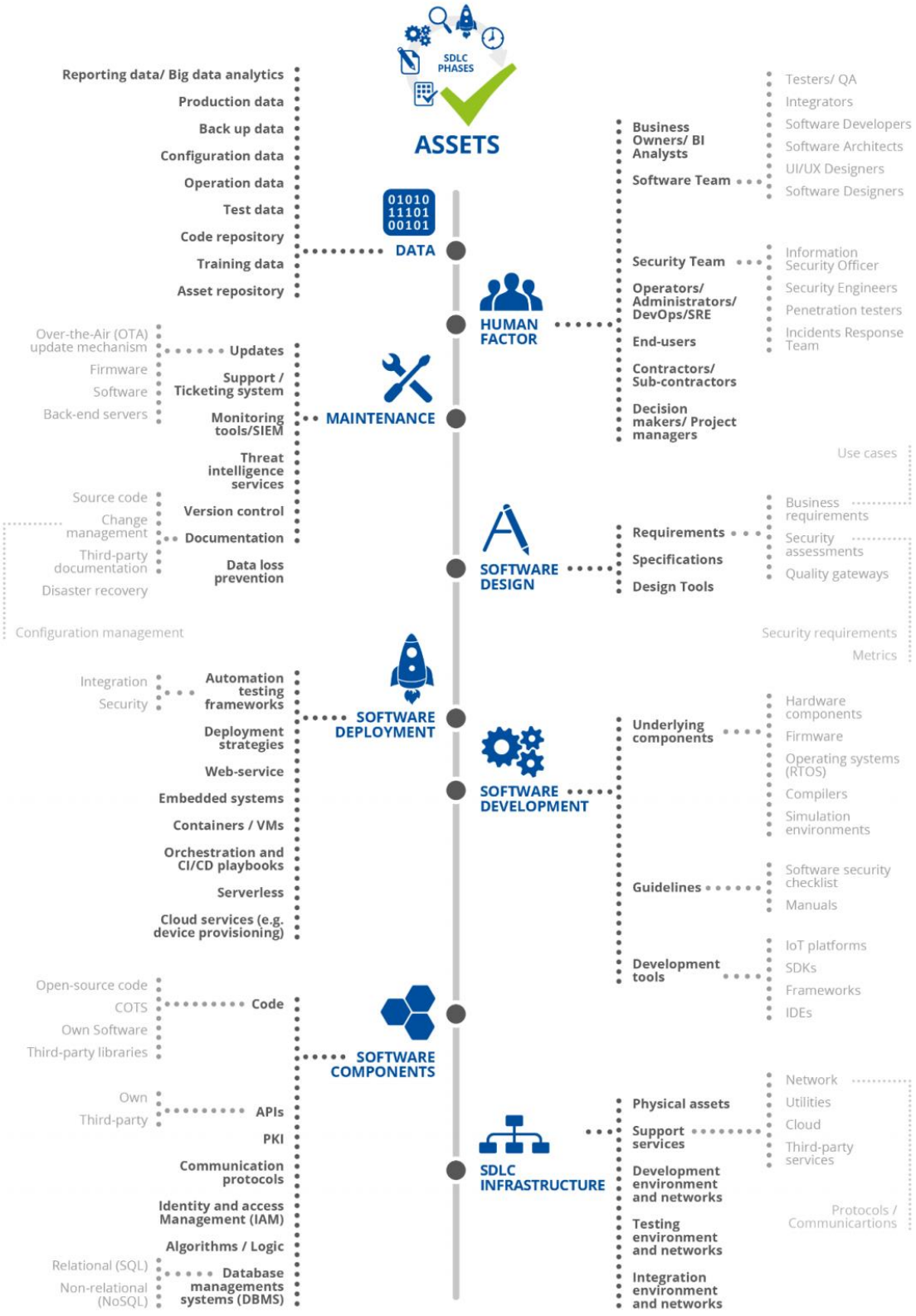


Figure 2. IoT assets classification

5.3 Threats classification

The Figure 3 is based on the TP-02-19-880-EN-N, *Good Practices for Security of IoT - Secure Software Development Lifecycle* by ENISA shows the IoT threat classification with some examples of attacks. It is divided into the following categories as described in Annex D.

a) Personnel (see Annex D.1).

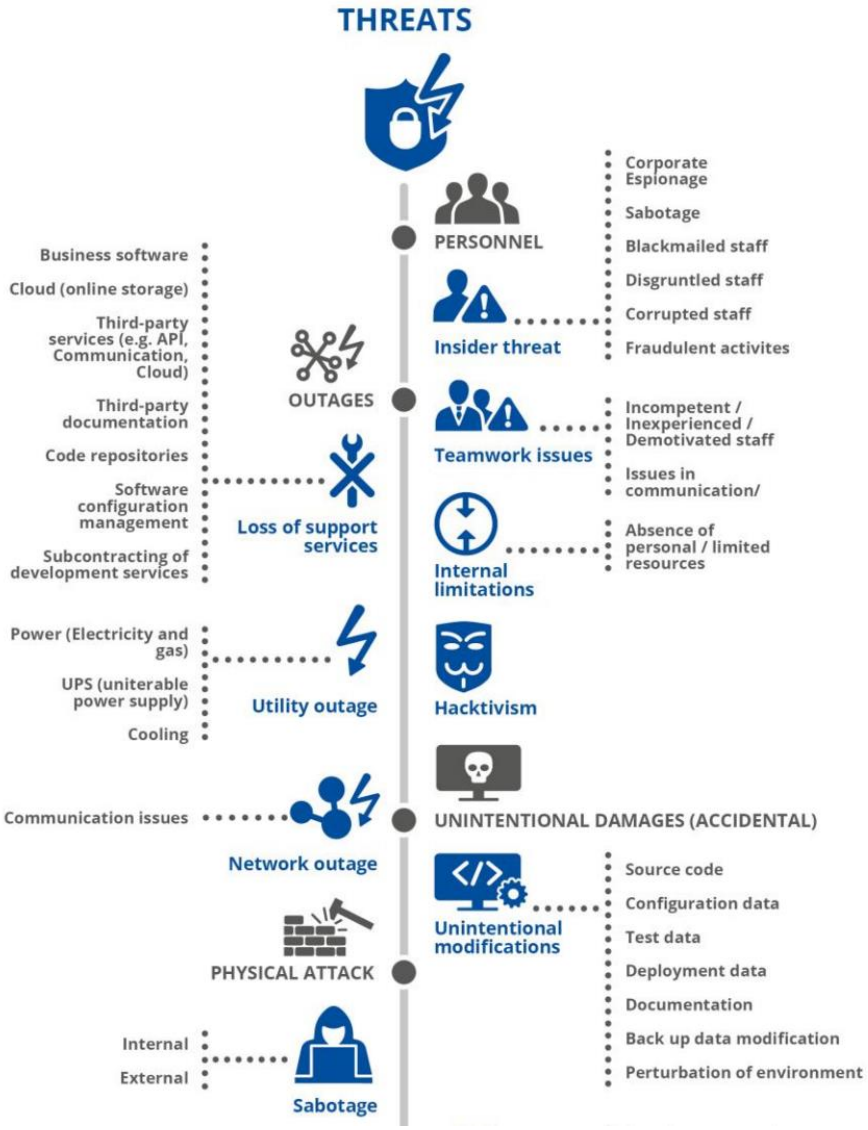
b) Outages (see Annex D.2).

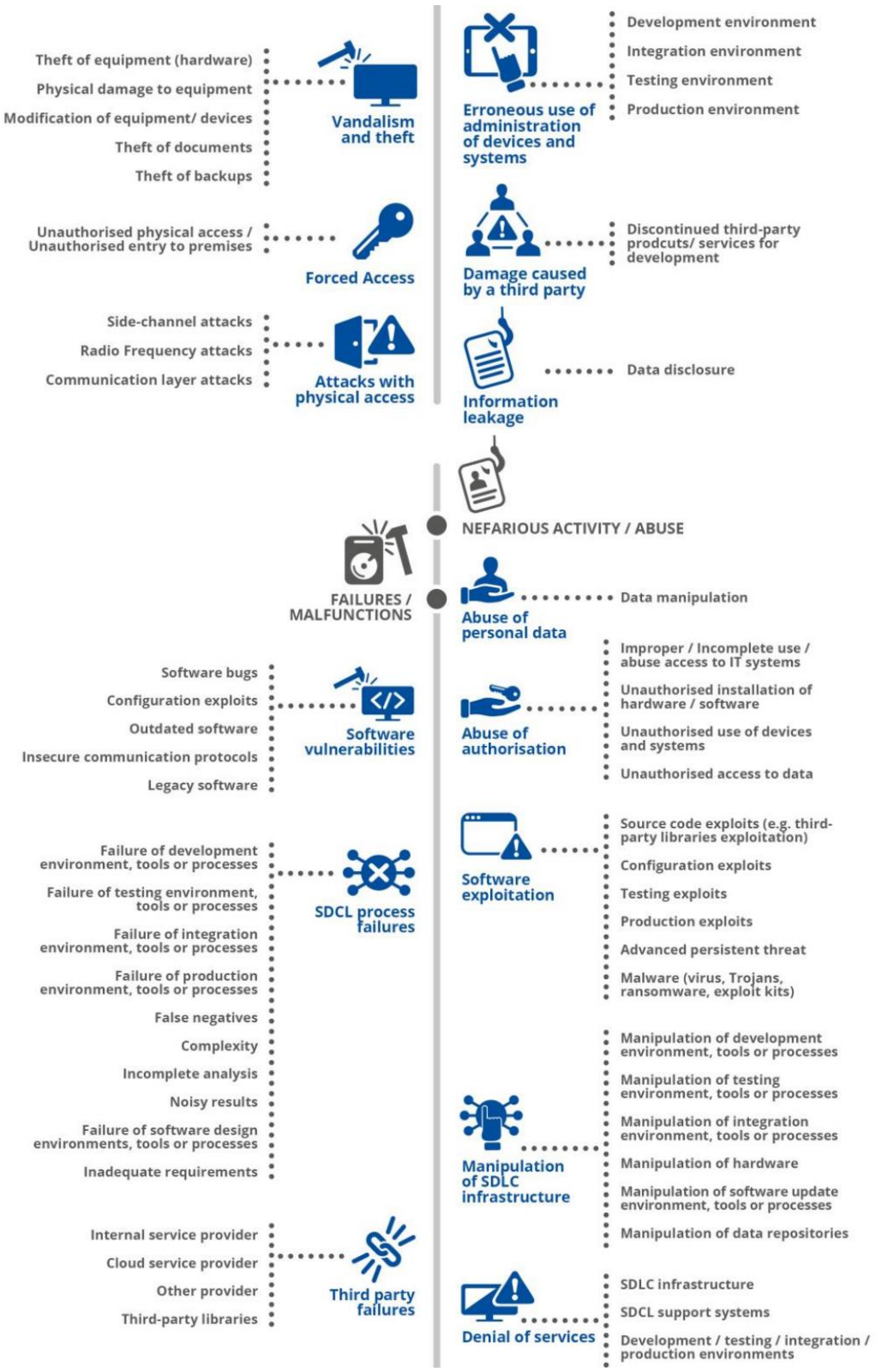
c) Unintentional damages (accidental) (see Annex D.3).

d) Physical attack (see Annex D.4).

e) Nefarious activity/abuse (see Annex D.5).

f) Failures/malfunctions (see Annex D.6).




Theft of equipment (hardware)
Physical damage to equipment
Modification of equipment/ devices
Theft of documents
Theft of backups
Vandalism and theft
Unauthorised physical access / Unauthorised entry to premises
Forced Access
Side-channel attacks
Radio Frequency attacks
Communication layer attacks
Attacks with physical access
FAILURES / MALFUNCTIONS
Software bugs
Configuration exploits
Outdated software
Insecure communication protocols
Legacy software
Software vulnerabilities
Failure of development environment, tools or processes
Failure of testing environment, tools or processes
Failure of integration environment, tools or processes
Failure of production environment, tools or processes
False negatives
Complexity
Incomplete analysis
Noisy results
Failure of software design environments, tools or processes
Inadequate requirements
SDCL process failures
Internal service provider
Cloud service provider
Other provider
Third-party libraries
Third party failures
Development environment
Integration environment
Testing environment
Production environment
Erroneous use of administration of devices and systems
Discontinued third-party prodcuts/ services for development
Damage caused by a third party
Data disclosure
Information leakage
NEFARIOUS ACTIVITY / ABUSE
Data manipulation
Abuse of personal data
Improper / Incomplete use / abuse access to IT systems
Unauthorised installation of hardware / software
Unauthorised use of devices and systems
Unauthorised access to data
Abuse of authorisation
Source code exploits (e.g. third-party libraries exploitation)
Configuration exploits
Testing exploits
Production exploits
Advanced persistent threat
Malware (virus, Trojans, ransomware, exploit kits)
Software exploitation
Manipulation of development environment, tools or processes
Manipulation of testing environment, tools or processes
Manipulation of integration environment, tools or processes
Manipulation of hardware
Manipulation of software update environment, tools or processes
Manipulation of data repositories
Manipulation of SDLC infrastructure
SDLC infrastructure
SDCL support systems
Development / testing / integration / production environments
Denial of services

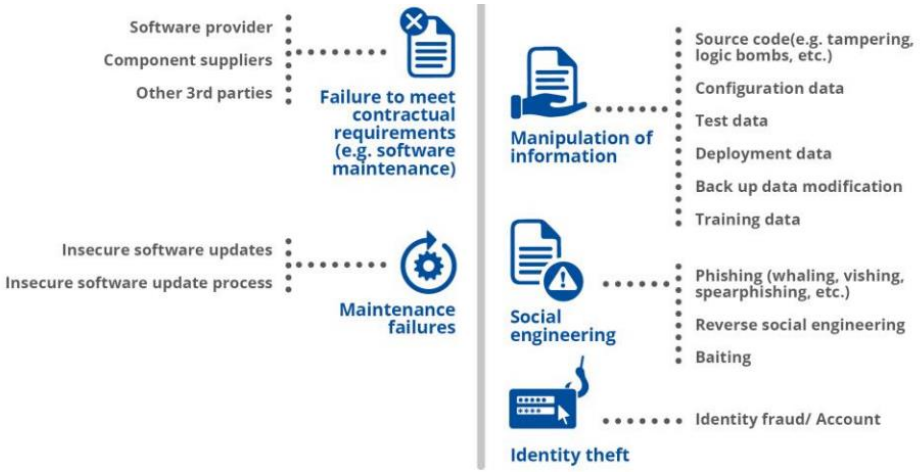


Figure 3. IoT threats classification

5.4 IoT security attack scenarios

The different attack scenarios and the level of importance of each attack have been gathered from experts. The importance level provided for the attack scenario ranges from low, medium, high and critical, representing the negative impact level of these attacks, which is described as follows:

a) **Low** - an attack that has no impact on the IoT system.

b) **Medium** - the attack can be detected by system monitoring and rectification can be done by the system administration.

c) **High** - the attack cannot be easily detected and rectified. It also has the potential to compromise the whole IoT system and other devices.

d) **Critical** - the attack has potential to compromise the whole IoT system and/or can cause severe damage physically and financially.

The attack scenarios and its importance level are defined in Table 1.

Table 1. Importance level of IoT attack scenarios

No.	Attack scenarios	Importance level
1.	Against the network link between controller(s) and actuators	High to critical
2.	Against sensors, modifying the values read by them or their threshold values and settings	High to critical
3.	Against actuators, modifying or sabotaging their normal settings	High to critical
4.	Against the administration systems of IoT	High to critical
5.	Exploiting protocol vulnerabilities	High
6.	Against devices, injecting commands into the system console	High to critical
7.	Stepping stones attack	Medium to high
8.	DDoS using the IoT botnet	Critical
9.	Power source manipulation and exploitation of vulnerabilities in data readings	Medium to high
10.	Ransomware	Medium to critical

6. Internet of Things (IoT) application security measures and best practices

This clause provides security measures and best practices, which aim to mitigate the threats, vulnerabilities and risks that affect the IoT ecosystem.

These security measures and best practices have been defined with the aim to apply to various IoT solutions which fall into several security domains. The security domains and its security measures are organised in Table 2.

Table 2. Security domains and measures

No.	Security domain	Security measure *(include but not limited to)*
1.	Information system security governance and risk management	a) Business impact analysis b) Risk analysis c) Policy d) Accreditation e) Indicators and audits f) Human resource security
2.	Ecosystem management	a) Ecosystem mapping b) Ecosystem relations
3.	Information Technology (IT) security architecture	a) Systems configuration b) Asset management c) System segregation d) Traffic filtering e) Cryptography f) Vulnerability management
4.	IT security administration	a) Administration account b) Administration information systems
5.	Identity and access management	a) Authentication b) Identification c) Access rights
6.	IT security maintenance	a) IT security maintenance procedures b) Remote access
7.	Physical and environmental security	Site security
8.	Detection	a) Detection b) Logging c) Log correlation and analysis
9.	Computer security incident management	a) Information system security incident analysis and response b) Incident report
10.	Continuity of operations	a) Business continuity management b) Disaster recovery management
11.	Crisis management	Crisis management organisation and process

The identified IoT application security measures, denoted henceforth as best practices, are organised into these 3 categories:

a) Organisational, People and Process measures (OP);

b) Policies (PS); and

c) Technical Measures (TM).

The monitoring and measurement requirements for each security measure defined in Table 2, Annex E, Annex F and Annex G shall comply with the MCMC MTSFB TC G021, *Information and Network Security - Monitoring and Measurement of Security Control Objectives.*

6.1 Organisational, People and Process measures (OP)

All businesses shall have organisational criteria to ensure information security. Their personnel practices need to foster outstanding security awareness, establish a reliable management of processes and implement a safe manoeuvre of the information in the organisation practices.

Organisations should ensure that contractors and suppliers are responsible and accountable for the functions considered.

In the event of an incident that may compromise the safety of the organisation, the organisation shall be prepared (responsibilities, evaluation and response) as per security measures defined in Annex E.

6.2 Policies (PS)

The policies generally target information security and aim at making it more concrete and robust. These should be adequate for the organisation's activity and shall contain well documented information. The security measures should reflect the particularities and the context in which the IoT device or system will be deployed.

In this context, the best practices per security measures have been defined in Annex F.

6.3 Technical Measures (TM)

The security measures and best practices shall consider and cover the technical elements in order to minimise the vulnerabilities of IoT. Applying these technical measures should take into account the particularities of the IoT ecosystem such as criticality and scalability, namely given the huge number of involved devices, certain measures might need to be carried out at the level of specialised architectural components, e.g., gateways.

The necessary technical measures to preserve and protect the security of information in IoT are defined in Annex G.

Annex A
(informative)

Abbreviations

2FA	Two-Factor Authentication
AI/ML	Artificial Intelligence/Machine Learning
API	Application Programming Interface
APT	Advanced Persistent Threat
BI	Business Intelligence
BLE	Bluetooth Low Energy
BP	Best Practices
CASE	Computer Aided Software Engineering
CI/CD	Continuous Integration/Continuous Delivery
CISO	Chief Information Security Officer
COTS	Commercial-Off-The-Shelf
CSRF	Cross-Site Request Forgery
DDoS	Distributed Denial-of-Service
DevOps	Software Development and IT Operations
DevSecOps	Software Development, Security, and IT Operations
DLP	Data Loss Prevention
ENISA	European Network and Information Security Agency
IDE	Integrated Development Environment
IoT	Internet of Things
IT	Information Technology
LoRaWAN	Low-Power Wide Area Network
LTE-M	Long Term Evolution for Machines
MFA	Multi-Factor Authentication
NB-IoT	Narrow Band-Internet of Things
NFC	Near Field Communication
NoSQL	Non-Relational Database
OP	Organisational, People and Process measures
OS	Operating Systems
OTA	Over-The-Air
PIN	Personal Identification Number
PKI	Public Key Infrastructure
POLP	Principle of Least Privilege
PS	Policies

QA	Quality Assurance
RF	Radio Frequency
RFID	Radio Frequency Identification
SDK	Software Development Kits
SDLC	Software Development Lifecycle
SIEM	Security Information and Event Management
SQL	Structured Query Language
SRE	Site Reliability Engineering
TLS	Transport Layer Security
TM	Technical Measures
UI/UIX	User Interface/User Interface Experience
UPS	Uninterruptible Power Supply
USB	Universal Serial Bus
VM	Virtual Machine
WiFi	Wireless Fidelity
XSS	Cross-Site Scripting

Annex B
(informative)

Security incidents

The study on *Evolution of IoT Attacks* by Sectigo illustrated Figure B.1 shows the security incidences such as hacking, DDoS and botnet on IoT have increased over the years.

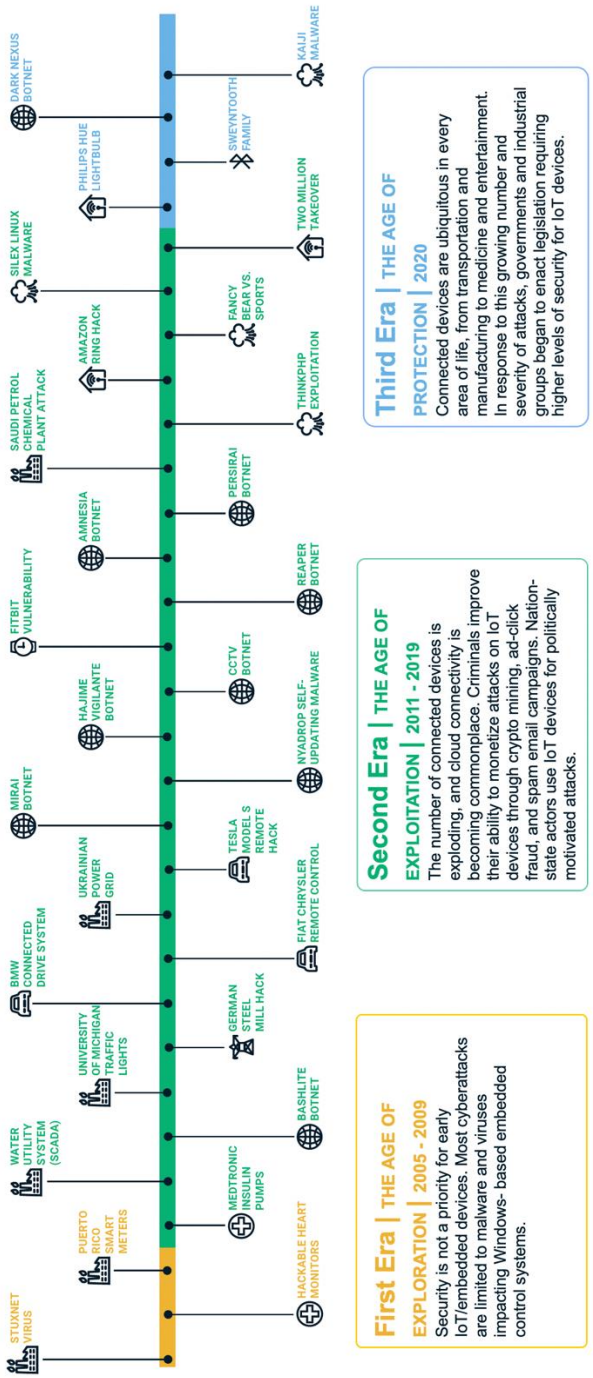


Figure B.1. IoT security incidents from 2005 to 2020

Annex C
(normative)

Assets classification

C.1 Asset group - Data

Table C.1 indicates the asset group and its indicative asset (data).

Table C.1. Asset group and its indicative asset - Data

Subgroup	Indicative assets	Description
Reporting data or big data analytics	N/A	This data informs of critical elements concerning an organisation's performance to improve different aspects.
Production data	N/A	Without this data, it would not be possible to complete daily business tasks and processes.
Backup data	N/A	Security copy of data files and folders to enable recovery in the event of data loss.
Configuration data	N/A	Data needed to set up the system correctly.
Operation data	N/A	Real data with which the software works.
Code repository	N/A	a) Platform that stores and centralises all the developed source code. b) Allows the development team to keep track of versions.
Test data	N/A	Data used to perform the different tests concerning software, e.g., penetration testing, black box testing, etc.
Asset repository	N/A	Provides a single, centralised database to store and track organisational assets.
Training data	N/A	Data used to train Artificial Intelligence/Machine Learning (AI/ML) algorithms. Training involves the learning phase where algorithms can make predictions based on the training data that has been fed to them.

C.2 Asset group - Human factor

Table C.2 indicates the asset group and its indicative asset (human factor).

Table C.2. Asset group and its indicative asset - Human factor

Subgroup	Indicative assets	Description
Business owners/ Business Intelligence (BI) analysts	N/A	Individual or team responsible for analysing data that are used by a business or organisation or a specific business function.
Software team	Testers Quality Assurance (QA)	People in charge of the quality of the software (QA staff), by means of checking it.
	Integrators	Specialised people in putting different IT components together, working as a whole system.
	Software developers	People that develop software applications.
	Software architects	Expert who makes high-level design choices and dictates technical standards, including software coding standards, tools, and platforms.
	User Interface/ User Interface Experience (UI/UIX) designers	Designers responsible for the user interface of an IoT application that need to work closely together.
	Software designers	Software designers that use principles of science and mathematics to develop IoT applications.
Security team	Chief Information Security Officer (CISO)	International standards and best practices applicable in the work process management.
	Security engineers	Security engineers are responsible for the security aspects in the design of systems that need to be able to deal robustly with possible sources of disruption, ranging from natural disasters to malicious acts.
	Penetration testers	Professional specialised in security that attempt to crack into a system for the purposes of security testing.
	Incident response team	A group of people who prepare for and respond to any emergency incident, such as a natural disaster or an interruption of business operations.
Operators/ Administrators/ Software Development and IT Operations (DevOps)/ Site Reliability Engineering (SRE) (Operations team)	N/A	People with this role undertake ongoing activities that are required for the provision of IoT software or services.
End users	N/A	People that use the software applications.
Contractors or sub-contractors	N/A	Entities or companies that provide services or products relevant to the processes of IoT software development.
Decision makers or project managers	N/A	Project managers are accountable for the success of a project, and their responsibilities include the planning and the execution of a project, building its comprehensive work plan, and managing the budget.

C.3 Asset group - Maintenance

Table C.3 indicates the asset group and its indicative asset (maintenance).

Table C.3. Asset group and its indicative asset - Maintenance

Subgroup	Indicative assets	Description
Updates	OTA update mechanism	Mechanism to update hardware remotely with new settings, software or firmware.
	Firmware	Software that sets the lowest-level logic to control a device's electronic circuits.
	Software	Minor software modifications deployed that provide security or functionality error fix.
	Back-end servers	Software component that provides functionality for other programs such as sharing data or resources.
Support/ Ticketing system	N/A	Software designed to organise and distribute incoming customer service requests.
Monitoring tools/ Security Information and Event Management (SIEM)	N/A	Monitoring tools used to continuously keep track of the status of the system in use, in order to ensure earliest warning of failures, defects or problems, and to improve them. Monitoring tools spans from servers, networks, and databases, to security, performance, end-devices and applications.
Threat intelligence services	N/A	Threat intelligence services generate, aggregate and distribute real-time feeds of intelligence data generated and derived from the use of the IoT.
Documentation	Source code	Written text or illustration that accompanies software and explain how to operate or how to use it. Different types of documentation exist such as source code, change management, etc.
	Change management	
	Disaster recovery	
	Third-party documentation	
Data Loss Prevention (DLP)	N/A	The practice used by organisations to detect and prevent breaches, leakages, or the undesired destruction of sensitive data. Also used for regulatory compliance. An example would a ransomware attack. DLP focuses on preventing illicit transfers of data outside of the organisation.
Version control	N/A	Management of the different changes made to the elements of a product or its configuration.

C.4 Asset group - Software design

Table C.4 indicates the asset group and its indicative asset (software design).

Table C.4. Asset group and its indicative asset - Software design

Subgroup	Indicative assets		Description
Requirements	Business requirements		High-level description of what the intended product or services should do based on the business and/or stakeholders needs.
	Security assessments	Metrics	Quantifiable measures that are used to track and assess the status of a specific business process.
		Quality gateways	Methodology for the quality assurance of a SDLC process.
		Use cases	Methodology used to identify and analyse the behaviour of a system when responding to an event.
Specifications	N/A		Detailed and technical documents that describe the technical functionalities of the end product or service.
Design tools	N/A		Tools to aid in the design of software or systems, also known as Computer Aided Software Engineering (CASE) tools.

C.5 Asset group - Software deployment

Table C.5 indicates the asset group and its indicative asset (software deployment).

Table C.5. Asset group and its indicative asset - Software deployment

Subgroup	Indicative assets	Description
Automation testing frameworks	Integration	A set of guidelines for creating and designing test cases. It is a conceptual part of automated testing that helps testers to use resources more efficiently.
	Security	
Deployment strategies	N/A	Deployment strategies provide a way to change or upgrade an application without downtime in a way that the user barely notices the improvements.
Web-services	N/A	A solution that uses different protocols and standards with the objective of exchanging data between applications.
Embedded systems	N/A	System designed to perform some dedicated functions, typically with low resources, and sometimes located remotely. Embedded systems with updatable software or firmware include a bootloader which is responsible for verifying the integrity of the software or firmware image on the device before loading it.
Containers/ Virtual Machines (VMs)	N/A	Software package that contains everything the software needs to run. This includes the executable program as well as system tools, libraries, and settings.
Orchestration and Continuous Integration and Delivery (CI/CD) playbooks	N/A	a) Continuous Integration is the engineering practice of frequently committing code in a shared repository. b) Continuous Delivery is the practice to build the software in a way that is always ready to run in their target environment.
Serverless	N/A	Applications where the management and allocation of servers and resources are completely managed by the cloud provider
Cloud services (e.g. device provisioning)	N/A	Cloud computing: the on-demand availability of computer system resources, especially data storage and computing power, without direct active management by the user.
Integrity verification software	N/A	Software that protects against unexpected or unauthorised changes in data once it was created by an authorised source.

C.6 Asset group - Software development

Table C.6 indicates the asset group and its indicative asset (software development).

Table C.6. Asset group and its indicative asset - Software development

Subgroup	Indicative assets	Description
Underlying components	Hardware components	Components on which the intended software relies or is built on.
	Firmware	
	Operating Systems (OS)	
	Compilers	
	Simulation environments	
Guidelines	Software security checklist	A set routines or practices that streamline a particular process.
	Manuals	
Development tools	IoT platforms	A multi-layer technology that enables management tasks and data visualisation.
	Software Development Kits (SDKs)	A set of functionalities and tools to allow developing software in a programming language.
	Frameworks	A set of functionalities and libraries to ease and speed up the software development, being the foundation of software applications.
	Integrated Development Environments (IDEs)	Software application that provides a set of tools to aid in software development.
	Algorithm training tools	a) Algorithms to perform a task without instructions, resorting to patterns and inference. b) A subset of artificial intelligence, the algorithms that make a mathematical model from 'training data' depend on the kind of problem, the computing resources available, and the nature of the data (supervised, unsupervised, classification, regression, etc.).

C.7 Asset group - Software components

Table C.7 indicates the asset group and its indicative asset (software components).

Table C.7. Asset group and its indicative asset - Software components

Subgroup	Indicative assets	Description
Code	Open-source code	Software is readily available for users to build and distribute new solutions.
	Commercial-Off-The-Shelf (COTS)	a) Software and services built and delivered usually from a third-party vendor. b) COTS can be purchased, leased or even licensed to the general public.
	Own software	Software developed and maintained by the own company.
	Third-party libraries	Software not developed or maintained by the company, but they are part of an application or system of the company.
Advanced Persistent Threat (APT) interfaces	Own	A set of subroutine definitions, communication protocols, and tools offered for one library to be used by other software
	Third-party	
Public Key Infrastructure (PKI)	N/A	Technology that is used for authenticating users and devices in the IoT ecosystem.
Communication protocols	N/A	Formal descriptions of digital message formats and rules that allow two or more entities of a communications system to transmit information.
Identity and access management	N/A	A framework of business processes, policies and technologies that facilitate management access control.
Algorithms/Logic	N/A	A set of unambiguous specifications for performing calculation, data processing, automated reasoning, and other tasks.
Database management systems	Relational: SQL	Software packages designed to define, manipulate, retrieve and manage data in a database.
	Non-relational: Non-relational database (NoSQL)	

C.8 Asset group - SDLC infrastructure

Table C.8 indicates the asset group and its indicative asset (SDL infrastructure).

Table C.8. Asset group and its indicative asset - SDLC infrastructure

Subgroup	Indicative assets	Description
Physical assets	N/A	Any type of tangible asset that is used to support the SDLC process (e.g., computers, wires, etc).
Support servicers	Network	Intangible assets in the form of internal or external services that support the operation of the SDLC infrastructure.
	Utilities	
	Cloud	
	Third-party services	
Development environment and networks	N/A	Environment and networks used for the development of the IoT applications.
Testing environment and networks	N/A	Environment and networks used for testing purposes of the IoT applications.
Integration environment and networks	N/A	Environment and networks used for the integration of the IoT applications.

Annex D
(informative)

Threats classification and assets affected

D.1 Threat category - Personnel

Table D.1 indicates the threat classification and assets affected (personnel).

Table D.1. Threat classification and assets affected - Personnel

Sub-Category	Threat	Description	Assets affected
Insider threat	Corporate espionage	Theft of data to gather critical and valuable information, by an employee or by some other company (competitors), throughout the development lifecycle process, affecting the final product, intellectual property, time to market, etc.	a) Data b) Human factor c) Software development d) Software components e) SDLC infrastructure
	Sabotage	Intentional unauthorised actions (non-fulfilment or defective fulfilment of personal duties) aimed at causing a disruption or damage during the software development, to obstruct the process, to affect the integrity of the software or to ultimately compromise the objective of the software.	a) Data b) Human factor c) Maintenance d) Software design e) Software deployment f) Software development g) Software components h) SDLC infrastructure
	Fraudulent activities	A team member or an attacker may use confidential information or exploit system vulnerabilities to carry out fraudulent activities (theft of sensitive information, industrial espionage, or extortion) that may affect the integrity of the software or cause damages to third parties.	a) Data b) Human factor c) Maintenance d) Software design e) Software deployment f) Software development g) Software components h) SDLC infrastructure
	Blackmailed staff	A member of the team is under duress from a malicious third party to carry out certain actions that could compromise the security of software in exchange for not revealing embarrassing, disgraceful or otherwise damaging information about the employee. It is a form of extortion.	Human factor
	Disgruntled staff	A disgruntled employee may deliberately use his or her privileges in order to seek revenge by leaking sensitive information to competitors or other companies that offer some kind of incentive to the employee to compensate for this dissatisfaction.	Human factor

Table D.1. Threat classification and assets affected - Personnel *(continued)*

Sub-Category	Threat	Description	Assets affected
Insider threat	Corrupted staff	A corrupt employee may deliberately seek to exploit his or her privileges in relation to corporate resources to his or her own benefit, leveraging the said resources for personal gain despite not being dissatisfied with the situation at the organisation.	Human factor
Teamwork issues	Incompetent/ inexperienced/ demotivated staff	An incompetent or inexperience or demotivated may pose a threat to the organisation due to absentmindedness or to a lack of knowledge and awareness of security, resulting in accidental risks.	Human factor
	Issues in communication/ coordination	Lack of a proper communication between project members, either internals or communications with service providers, may lead to errors such as misunderstandings, duplication of tasks, undefined scope, lack of systems integration, use of obsolete versions, etc.	Human factor
Internal limitations	Absence of personnel/ limited resources	A lack or unavailability of necessary personnel (strike, unexpected events, disasters, or staff turnover) may lead to an inability to ensure the level of security required due to the excessive workloads burdening other staff members and preventing them from paying the necessary attention to security throughout the process.	Human factor
Hacktivism	The use of illegal logical tools	A way of activism that uses and/or abuses technology to spread ideas or to punish organisations or people based on their beliefs. This threat can be posed either by isolated individuals or by organised professionals taking advantage of an organisation's security flaws.	a) Data b) Human factor c) Maintenance d) Software design e) Software deployment f) Software development g) Software components h) SDLC infrastructure

D.2 Threat category - Outages

Table D.2 indicates the threat classification and assets affected (outrages).

Table D.2. Threat classification and assets affected - Outages

Sub-Category	Threat	Description	Assets affected
Loss of support services	Business software	Unavailability of business software required for development of the software, failure of business software, failure of the support services, or loss of the license.	a) Data b) Human factor c) Maintenance d) Software development e) Software components f) SDLC infrastructure
	Cloud (online storage)	Unavailability, interruption or failure of online storage on the cloud. Depending on the communication, and on the time required to recover, the importance of this threat ranges from high to critical.	a) Software deployment b) SDLC infrastructure
	Third-party services (e.g., Application Programming Interface (API), communication brokers, cloud)	The failure or malfunction of a service or support that has been assigned to a third party (supplier), thus creating a dependency, can affect the whole product lifecycle, from the development process (e.g. drawing the project out) to the release of the product in the market (e.g. unavailability of the service).	a) Data b) Human factor c) Maintenance d) Software deployment e) Software components f) SDLC infrastructure
	Third party documentation	Threat of unavailability documents of private company archives, often a failure of document management control affects the specifications of the software, information leakage/sharing caused by inadequate security measures of the third-party.	a) Data b) Human factor c) Maintenance d) Software design e) SDLC infrastructure
	Code repositories	Unavailability of the code repositories, due to a lack of support of the repository, failure of the third parties, failure of communications, etc.	a) Data b) Maintenance c) Software development d) Software components e) SDLC infrastructure
	Software configuration management	Unavailability of proper software configuration management, unawareness of the correct version of the code or modification of the code.	a) Data b) Maintenance c) Software deployment d) Software components
	Subcontracting of development services	Unavailability of subcontracting of development services required for development process. Unavailability of key personnel and their competences, unavailability of the business development, etc.	a) Data b) Human factor c) Maintenance d) Software development e) Software deployment f) Software components g) SDLC infrastructure

Table D.2. Threat classification and assets affected - Outages *(continued)*

Sub-Category	Threat	Description	Assets affected
Utility outage	Power (Electricity and Gas)	Interruption or failure in the supply of power (electricity or gas), either intentional or accidental, and the time required to recover. The importance of this threat ranges from high to critical.	a) Data b) Human factor c) Maintenance d) SDLC infrastructure
	Uninterruptible Power Supply (UPS)	Interruption or failure in the UPS, either intentional or accidental, and the time required to recover. The importance of this threat ranges from high to critical.	a) Data b) Human factor c) Maintenance d) SDLC infrastructure
	Cooling	An interruption or failure in the cooling services (air-conditioning in the server room), either intentional or accidental, may affect hardware support and prevent access to project information (loss of information, file deletion, etc.)	a) Data b) Human factor c) Maintenance d) SDLC infrastructure
Network outage	Communication issues	A lack of communication links (wireless, mobile, fixed network, internet) prevents information flows due to problems with networks' blocking file update, repository access, teamwork communications, information exchanges, etc.	a) Data b) Human factor c) Maintenance d) SDLC infrastructure

D.3 Threat category - Unintentional damages accidental

Table D.3 indicates the threat classification and assets affected (unintentional damages (accidental)).

Table D.3. Threat classification and assets affected - Unintentional damages (accidental)

Sub-Category	Threat	Description	Assets affected
Unintentional modifications	Source code	A member of the team unconsciously makes a mistake in any of the tasks, causing an unwanted modification of the source code (and probably damaging it).	a) Data b) Maintenance c) Software components
	Configuration data	A member of the team unconsciously makes a mistake in any of the tasks, causing an unwanted modification of configuration files (and probably damaging them).	a) Data b) Maintenance
	Test data	A member of the team unconsciously makes a mistake in any of the tasks, causing an unwanted modification of test reports (and probably damaging them).	a) Data b) Maintenance
	Deployment data	The information about how to put the software into production, or about how to launch the system (start scripts) is quite sensitive. Errors concerning this data could leave the software in a vulnerable state (security measures not activated, etc.)	a) Data b) Software deployment c) Software development d) Software components

Table D.3. Threat classification and assets affected - Unintentional damages (accidental)
(continued)

Sub-Category	Threat	Description	Assets affected
Unintentional modifications	Documentation	A member of the team unconsciously makes a mistake in any of the tasks, causing an unwanted modification of project documentation (and probably damaging it).	a) Data b) Human factor a) Maintenance
	Backup data modification	An unexpected modification that affects the backups could put at risk the system's operation or even bring about a loss of the application in case of a system failure.	b) Data c) Maintenance
	Perturbation of environment	A change of the environmental work conditions can cause the failure of results in the SDLC process (testing results, maintenance and operation environment, etc.)	a) Data b) Maintenance c) Software design d) Software deployment e) Software development f) Software components g) SDLC infrastructure
Erroneous use or administration of devices and systems	Development environment	Information leakage / sharing / damage or system management misuse that could affect the programming process and tools during the development phase.	a) Data b) Maintenance c) Software development d) Software components e) SDLC infrastructure
	Integration environment	Information leakage / sharing / damage or system management misuse that could affect the process and tools when all software components are put together and tested as a whole.	a) Data b) Software design c) Software deployment d) Software development e) Software components f) SDLC infrastructure
	Testing environment	Information leakage / sharing / damage or system management misuse that could affect the validation process and tools (automated checks or non-automated techniques) causing failed tests or false test results.	a) Data b) Software deployment c) Software development d) Software components e) SDLC infrastructure
	Production environment	Information leakage / sharing / damage or system management misuse that could modify the current conditions of the software (such as configuration) during its production phase.	a) Data b) Maintenance c) Software deployment d) Software development e) Software components f) SDLC infrastructure
Damage caused by a third-party	Discontinued third-party products/ services for development	A failure on the part of a service provider on which the project depends puts at risk the proper operation of the software development process because the corresponding dependency (service or product) will no longer be provided.	a) Maintenance b) Software components c) SDLC infrastructure

Table D.3. Threat classification and assets affected - Unintentional damages (accidental)
(concluded)

Sub-Category	Threat	Description	Assets affected
Information leakage	Data disclosure	A sensitive information exposure occurs when, due to an accidental event, an application or program does not adequately protect information such as passwords, payment info, or health data. With this information, cybercriminals can make fraudulent purchases, access a victim's personal accounts, or even blackmail someone.	a) Data b) Software components

D.4 Threat category - Physical attack

Table D.4 indicates the threat classification and assets affected (physical attack).

Table D.4. Threat classification and assets affected - Physical attack

Sub-Category	Threat	Description	Assets affected
Sabotage	Internal	Intentional actions by internal people aimed at causing false feedback, disruption or damage of the physical components or facilities.	a) Data b) Human factor c) Maintenance d) Software design e) Software deployment f) Software development g) Software components h) SDLC infrastructure
	External	Intentional actions by external people aimed at causing false feedback, disruption or damage of the physical components or facilities.	a) Data b) Human factor c) Maintenance d) Software design e) Software deployment f) Software development g) Software components h) SDLC infrastructure
Vandalism and theft	Theft of equipment (hardware)	Theft of information or IT assets that support the development process	a) Data b) Software components c) SDLC infrastructure
	Physical damage to equipment	Incidents such as device thefts, bomb attacks, vandalism or sabotage could damage the equipment.	a) Maintenance b) Software deployment c) SDLC infrastructure
	Modification of equipment/ devices	Intentional attacks on development process support (servers, laptops, mobile) of development software, dependencies thereof, and on IoT devices that are closer to the physical process.	a) Maintenance b) Software deployment c) Software development d) SDLC infrastructure
	Theft of documents	Theft of documents from private company archives, often for the purpose of re-sale or to obtain personal benefits.	a) Data b) Maintenance
	Theft of backups	Stealing media devices on which copies of essential information are kept.	a) Data b) Maintenance

Table D.4. Threat classification and assets affected - Physical attack *(continued)*

Sub-Category	Threat	Description	Assets affected
Attacks with physical access	Side-channel attacks	Attack based on the collection of information about what the system does when performing cryptographic operations to reverse-engineer it instead of on cryptographic weaknesses.	a) Data b) Maintenance c) Software deployment d) Software components e) SDLC infrastructure
	Radio Frequency (RF) attacks	Theft or data tampering by an attacker leveraging the vulnerabilities of RF communications in order to access facilities or physical components.	a) Data b) Maintenance c) Software deployment d) Software components e) SDLC infrastructure
Attacks with physical access	Communication layer attacks	Attacks that could involve the modification of messages, identity theft, repudiation, data analysis, etc. when a communication among different entities is performed with the aim of accessing facilities or physical components.	a) Data b) Maintenance c) Software deployment d) Software components f) SDLC infrastructure
Forced access	Unauthorised physical access or unauthorised entry to premises	Unapproved access to facilities that could be leveraged for malicious actions.	a) Data b) Maintenance c) Software deployment d) Software components e) SDLC infrastructure

D.5 Threat category - Nefarious activity/abuse

Table D.5 indicates the threat classification and assets affected (nefarious activity/abuse).

Table D.5. Threat classification and assets affected - Nefarious activity/abuse

Sub-Category	Threat	Description	Assets affected
Abuse of personal data	Data manipulation	In this case, the objective is to manipulate the data in order to modify data, cause the failure of the software, or acquire monetary gains. By accessing the operation data of the system, an attacker may modify them to alter the operation of the application for malicious purposes.	Data
Abuse of authorisation	Improper or incomplete use or abuse access to IT systems	Abuse of authorised access systems that support the infrastructure, making it possible to modify the version of the software and the tools during the process of software.	a) Data b) Maintenance c) Software deployment d) Software development e) SDLC infrastructure
	Unauthorised installation of software/ hardware	Threat of unauthorised manipulation of hardware and software that can be used to modify source code for malicious purposes, posing threats such as bomb injections, backdoor generation, or the destruction of source code.	a) Maintenance b) Software deployment c) Software development d) Software components e) SDLC infrastructure
	Unauthorised use of devices and systems	An unauthorised modification of configuration data could cause the system to work incorrectly or the security measures implemented may not act correctly, allowing attacks against the system.	a) Data b) Maintenance c) Software deployment d) Software development e) Software components f) SDLC infrastructure
	Unauthorised access to data	Unauthorised modification of code or data, attacking its integrity. In this case, it can result in the manipulation of information, unauthorised access to confidential information, and access to source code.	a) Data b) Software development c) Software components
Software exploitation	Source code exploits (e.g. third-party libraries exploitation)	Unauthorised modification of source code for malicious purposes such as bomb injections, backdoor generation, or the destruction of source code.	a) Data b) Maintenance c) Software development Software components
	Configuration exploits	The default configuration is vulnerable, containing weak/default passwords, software bugs, and configuration errors. This threat is usually connected to others, like exploit kits.	a) Data b) Maintenance c) Software deployment d) Software components
	Testing exploits	Threat leveraging the use of default configuration of the testing environment, with default passwords, software bugs, and configuration errors.	a) Software deployment b) Software components SDLC infrastructure

Table D.5. Threat classification and assets affected - Nefarious activity/abuse *(continued)*

Sub-Category	Threat	Description	Assets affected
Software exploitation	Production exploits	Threats leveraging the use of outdated software versions, bugs, improper configurations, zero-day vulnerabilities or specific software components, such as weak cryptographic algorithms or vulnerable opensource libraries.	a) Maintenance b) Software deployment c) Software components d) SDLC infrastructure
	APT	In APT attacks, eavesdropping and information gathering comprise one of the first stages carried out in order to identify weak spots and potential entry/attack points.	a) Data b) Human factor c) Maintenance d) Software design e) Software deployment f) Software development g) Software components h) SDLC infrastructure
	Malware (virus, Trojans, ransomware, exploit kits)	Exploit kit code designed to take advantage of a vulnerability in order to gain access to a system. This threat is difficult to detect and during the software development process its impact ranges from high to crucial, depending on the assets affected.	a) Maintenance b) Software deployment c) Software components d) SDLC infrastructure
Manipulation of SDLC infrastructure	Manipulation of development environment, tools or processes	Threat of unauthorised manipulation of development environment, tools or processes to intentionally manipulate the information systems or review process of the development to cover other nefarious activities (false results, modification of the information, information integrity loss, no testing updates), or to obtain information about the software under development (intellectual property, etc.).	a) Maintenance b) Software development c) SDLC infrastructure
	Manipulation of testing environment, tools or processes	Unauthorised modification of testing elements (environment, processes, tools) with malicious intentions (modifying test results, obtaining intellectual property or other sensitive information, etc.). For instance, an attacker could modify the test data in order to allow a system that has not passed the security tests to be accepted and continue to the production phase with security flaws.	a) Maintenance b) Software deployment c) Software development d) SDLC infrastructure
	Manipulation of integration environment, tools or processes	Threats that aim to modify the integration environment to obtain intellectual property (the whole solution), or modify the results of the tests when all software components are put together.	a) Maintenance b) Software deployment c) Software development e) SDLC infrastructure

Table D.5. Threat classification and assets affected - Nefarious activity/abuse *(continued)*

Sub-Category	Threat	Description	Assets affected
Manipulation of SDLC infrastructure	Manipulation of production environment, tools or processes	Production environment is critical because it is the real scenario to work with. Malicious modifications can affect the availability of the IoT solution, as well as the way to measure or control how software behaves (try to cover other malicious activities). It may also have severe effects, for instance. providing access to sensitive information (personal data, code, configuration data, operation data, etc.), or modifying it.	a) Maintenance b) Software deployment c) Software development a) SDLC infrastructure
	Manipulation of hardware	Unauthorised manipulation of hardware elements of the solution, affecting the integrity of hardware elements (which are the basis of the rest of technologies: infrastructure technologies, support systems, etc.)	a) Maintenance b) Software deployment c) SDLC infrastructure
	Manipulation of software update environment, tools or processes	Threat of unauthorised manipulation of software update environment Patched the lack of a formal update management procedure entails that the urgency of fixing an application or system may bring about errors that cause vulnerabilities in the system.	a) Maintenance b) Software deployment c) SDLC infrastructure
	Manipulation of data repositories	Threat of manipulation of data repositories with the objective of manipulating source code for malicious purposes such as bomb injections, backdoor generation, or the destruction of source code.	a) Data b) Maintenance c) Software components
Denial of service	SDLC infrastructure	Understanding IT infrastructure as the set of technologies that provide the needed environment (networks, operating systems, etc.) for the systems and applications, these threats aim to make them unavailable, affecting all technologies that need them. It can have severe consequences.	a) Maintenance b) Software development a) SDLC infrastructure
	SDLC support systems	Threats that aim to compromise the availability of all types of systems and middleware that sustain the software development process, stopping or delaying the development process.	a) Maintenance b) Software deployment c) Software components b) SDLC infrastructure
	Development/ testing/ integration/ production environments	When an environment is not available due to malicious activities, the development process may be stopped or delayed (tests cannot be performed, etc.). In the case of the production environment, the availability of the IoT solution may be partially or completely impacted.	a) Maintenance b) Software deployment c) Software development c) SDLC infrastructure

Table D.5. Threat classification and assets affected - Nefarious activity/abuse *(concluded)*

Sub-Category	Threat	Description	Assets affected
Manipulation of information	Source code (e.g., tampering, logic bombs, etc.)	Unauthorised modification of source code for malicious purposes such as bomb injections, backdoor generation, or the destruction of source code.	d) Data e) Maintenance f) Software components
	Configuration data	The unauthorised modification of this type of data may result in an alteration of software parameters, which can affect the security of the solution (disabling security measures, etc.).	a) Data b) Software deployment c) Maintenance
	Test data	Threat of intentional manipulation of test data with the objective to modify the test data in order to allow a system that has not passed the security tests to be accepted and continue to the production phase with security flaws.	a) Data b) Maintenance
	Deployment data	Threat of intentional manipulation of deployment data. A lack of an adequate testing environment affects the validity of the security tests since the environment should be as similar to production as possible.	a) Data b) Software deployment
	Backup data modification	Not adequately protecting backups could allow an attacker to access and modify or destroy data, compromising the system's operation in the event of a failure if access to the backups is required.	a) Data b) Maintenance c) Software deployment
	Poisoning training/testing data	Training data tampering could cause a diversion from expected data, highly impacting the final results of the SDLC process.	a) Data b) Maintenance c) Software deployment d) Software development
Social engineering	Phishing (whaling, vishing, spear phishing, etc.)	Threat of an e-mail fraud method in which the perpetrator sends out a legitimate-looking email in an attempt to gather personal and financial information from recipients. Typically, the messages appear to come from well-known and trustworthy Web sites. The main object in this case is to obtain information of the member of the team development and get identify, passwords and could be modification of the source code.	Human factor
	Reverse social engineering	A reverse social engineering attack is a person-to-person attack in which an attacker convinces the victim that he/she has or will have a problem, and the attacker is the key to solve it.	Human factor
	Baiting	It is a technique to drive the victim into a trap by resorting to his/her curiosity and interest (like putting rouge Universal Serial Bus (USBs) on the floor of a parking area).	Human factor
Identity theft	Identity fraud or account	This threat aims to steal the identity of a legitimate user of the system to perform actions on behalf of the original user, or to access information that the user can access.	Human factor

D.6 Threat category - Failures/malfunctions

Table D.6 indicates the threat classification and assets affected (failures/malfunctions).

Table D.6. Threat classification and assets affected - Failures/malfunctions

Sub-Category	Threat	Description	Assets affected
Software vulnerabilities	Software bugs	Flaws or errors in the software programming or system that produce an incorrect or unexpected operation or result.	a) Maintenance b) Software deployment c) Software development d) Software components e) SDLC infrastructure
	Configuration exploits	Due to a failure in the configuration system, an attacker can leverage the vulnerability to launch an attack on the system.	a) Data b) Maintenance c) Software deployment d) Software development e) Software components f) SDLC infrastructure
	Outdated software	Software that is not up to date may trigger severe risks for a software solution. Potential issues may arise from vulnerabilities that are present in the software dependencies legacy systems.	a) Maintenance b) Software deployment c) Software development d) Software components e) SDLC infrastructure
Software vulnerabilities	Insecure communication protocols	Use of insecure communication protocols that an attacker could leverage in order to cause a malfunction of the system or capture sensitive information.	a) Data b) Maintenance c) Software deployment d) Software components a) SDLC infrastructure
	Legacy software	Software that is obsolete and presents a vulnerability due to a lack of support, updates or patches.	a) Maintenance b) Software deployment c) Software development d) Software components b) SDLC infrastructure
SDLC process failures	Failure of secure development environment, tools or processes	These kinds of failures can stop the secure development process, or delay it, or bring about a loss of control over it.	c) Human Factor d) Maintenance e) Software design f) Software deployment Software development
	Failure of testing environment, tools or processes	Issues in the testing environment could affect the veracity of testing results (not tested correctly, not tested uniformly, etc.), or may make it impossible to carry out some tests, stopping or delaying the development process.	a) Data b) Software deployment c) Software development d) Software components SDLC infrastructure
	Failure of integration environment, tools or processes	The integration phase is critical since all software pieces are put together to ensure they work as expected. If potential issues arise, they may result in software integration issues or bad results in integration testing.	a) Data b) Software deployment c) Software development d) Software components SDLC infrastructure

Table D.6. Threat classification and assets affected - Failures/malfunctions *(continued)*

Sub-Category	Threat	Description	Assets affected
SDLC process failures	Failure of production environment, tools or processes	The production environment is critical because it is the real scenario to work with. Failures can affect the availability of the whole solution, as well as the way to measure or control how software behaves. It may also result in a leakage of sensitive information due to errors.	a) Data b) Software deployment c) Software development d) Software components e) SDLC infrastructure
	False negatives	The ratio of false negatives in the security tools is too high to rely on the results.	a) Data b) Software deployment c) Software development f) SDLC infrastructure
	Complexity	The security tools are too complex, leading to their incorrect use and results that are difficult to interpret.	a) Software design b) Software deployment c) Software development g) SDLC infrastructure
	Incomplete analysis	The tool does not analyse the full project or the tool is used when the software is not finished, leaving parts of the software unanalysed from the point of view of security.	a) Data b) Software deployment c) Software development h) SDLC infrastructure
	Noisy results	Either the means by which the results are presented or the high volume of false positives make the results hard to process, causing vulnerabilities that may go unnoticed.	a) Data b) Software deployment c) Software development SDLC infrastructure
	Failure of software design environments, tools or processes	In the design phase, secure software requirements are included in the solution as design features. Potential failures at this point can lead many vulnerabilities to go unnoticed during the following stages of development.	a) Data b) Maintenance c) Software design d) Software deployment e) Software development f) Software components SDLC infrastructure
	Inadequate requirements	Establishing security requirements that are not appropriate for the solution or for the development process can lead to the emergence of vulnerabilities.	a) Data b) Software design c) Software deployment d) Software development Software components

Table D.6. Threat classification and assets affected - Failures/malfunctions *(continued)*

Sub-Category	Threat	Description	Assets affected
Third party failures	Internal service provider	A failure of a service such as the programming of a code part or component design that has been developed by IT departments/service providers within an organisation.	a) Maintenance b) Software design c) Software components d) Software deployment e) SDLC infrastructure
	Cloud service provider	A failure of a service that is supported by a cloud provider, such as an application through the Internet or SaaS.	a) Maintenance b) Software deployment c) Software components d) SDLC infrastructure
	Other providers	A failure or unexpected result of any part that has been outsourced and whose operation has an impact on software development.	a) Maintenance b) Software deployment c) Software components d) SDLC infrastructure
	Third-party libraries	It is necessary to adopt risk management for these assets. These risks must be mitigated to prevent various types of threats from being executed.	a) Maintenance b) Software deployment c) Software components d) SDLC infrastructure
Failure to meet contractual requirements e.g. software maintenance	Software providers	Contractual requirements for software providers can manage many different aspects, such as how software is developed, when it has to be delivered, security in workstations of developers, how to deliver the software, security maturity of the software, maintenance of the software, etc. In case of failure, it may have severe consequences, such as intellectual property loss, inability to provide software when needed, immature security for the software delivered, etc.	a) Human factor b) Maintenance c) Software design d) Software components e) SDLC infrastructure
	Component suppliers	Many different aspects can be included in the contract, and they depend on the component that they provide. SDLC may be impacted if components are not needed, stopping or delaying the process, or not providing the functionalities that they need, or lacking maintenance when it is required (SLAs).	a) Human factor b) Maintenance c) Software deployment d) Software components SDLC infrastructure
	Other third-parties	Security is an aspect to consider globally in an organisation, and any organisation provider may result in security issues such as an information leakage or damage to information integrity, if security clauses of the contract are not correctly followed (for instance, third party software developer or cleaning service staff may expose sensitive information when they manage an organisation's maintenance, integration or residues).	a) Human factor b) Maintenance c) Software deployment d) Software components SDLC infrastructure

Table D.6. Threat classification and assets affected - Failures/malfunctions *(concluded)*

Sub-Category	Threat	Description	Assets affected
Maintenance failures	Insecure software updates	New updates (new software versions) need to be tested thoroughly to ensure that they do not impact the properties of the software. Insecure updates can make software that was safe in the previous version vulnerable.	a) Maintenance b) Software deployment c) Software components
	Insecure software update process	The process to update software is not secure enough (hardcoded credentials for maintenance, backdoors, integrity is not checked), allowing potential attackers to compromise the software by abusing the updating process.	a) Maintenance b) Software deployment

Annex E
(normative)

Security measures for Organisation, People and Process (OP)

Table E.1 indicates the security measures and best practices for OP.

Table E.1. Security measure and best practices for OP

Security measure	Best practices	Description
End-of-life support	BP-OP-01	Develop an end-of-life strategy for IoT products.
	BP-OP-02	Disclose the duration and end-of-life security and patch support (beyond product warranty).
	BP-OP-03	Monitor the performance and patch known vulnerabilities up until the end-of-support period of a product's lifecycle.
Proven solutions	BP-OP-04	a) Use proven solutions, i.e., well-known communications protocols and cryptographic algorithms, recognised by the scientific community, etc. b) Certain proprietary solutions, such as custom cryptographic algorithms, should be avoided.
Management of security vulnerabilities and/or incidents	BP-OP-05	Establish procedures for analysing and handling security incidents.
	BP-OP-06	Coordinated disclosure of vulnerabilities.
	BP-OP-07	Participate in information-sharing platforms for the following objectives: a) to report vulnerabilities and receive them timely; and b) to report critical information about current cyber threats and vulnerabilities from public and private partners.
	BP-OP-08	Create a publicly disclosed mechanism for vulnerability reports, e.g. Bug Bounty programs.
Human resources security training and awareness	BP-OP-09	Ensure the personnel practices promote privacy and security and train employees in good privacy and security practices.
	BP-OP-10	Document and monitor the privacy and security training activities.
	BP-OP-11	Ensure that cybersecurity roles and responsibilities for all workforce are established and introduce personnel assignments in accordance with the specifics of the projects and security engineering needs.
Third-party relationships	BP-OP-12	Data processed by a third-party shall comply the Act 709, *Personal Data Protection Act 2010.*
	BP-OP-13	Any personal data sharing with third parties shall comply the Act 709, *Personal Data Protection Act 2010.*
	BP-OP-14	For IoT hardware manufacturers and IoT software developers, the following necessary applies. a) To adopt cyber supply chain risk management policies. b) To communicate cyber security requirements to its suppliers and partners.

Table E.1. Security measure and best practices for OP *(continued)*

Security measure	Best practices	Description
NOTES: For the purposes of this table, the following abbreviations apply. 1) BP is Best Practices. 2) OP is Organisational, People and Process measures.		

Annex F
(normative)

Security measures for Policies (PS)

Table F.1 indicates the security measures and best practices for PS.

Table F.1. Security measures and best practices for PS

Security measure	Best practices	Description
Security by design	BP-PS-01	Shall consider the security of the whole IoT system from a consistent and holistic approach during its whole lifecycle across all levels of the following: a) device/application design and development; b) integrating security throughout the development; c) manufacture; and d) deployment.
	BP-PS-02	Shall ensure the ability to integrate different security policies and techniques.
	BP-PS-03	Security shall consider the risk posed to human safety.
	BP-PS-04	Designing for power conservation shall not compromise security.
	BP-PS-05	Shall design architecture by compartments to encapsulate elements in case of attacks.
	BP-PS-06	IoT hardware manufacturers and IoT software developers shall a) implement Software Development, Security, and IT Operations (DevSecOps) and test plans to verify whether the product performs as it is expected; and b) perform penetration tests to identify malformed input handling, authentication bypass attempts and overall security posture.
	BP-PS-07	IoT software developers shall conduct code review during implementation as it helps to reduce bugs in a final version of a product.
Privacy by design	BP-PS-08	Make privacy an integral part of the system.
	BP-PS-09	Perform privacy impact assessments before any new applications are launched.
Asset management	BP-PS-10	Establish and maintain asset management procedures and configuration controls for key network and information systems.
Risk and threat identification and assessment	BP-PS-11	Identify significant risks using a defence-in-depth approach.
	BP-PS-12	Identify the intended use and environment of a given IoT device.

NOTES:

For the purposes of this table, the following abbreviations apply.

1) BP is Best Practices.

2) PS is Policies.

Annex G
(normative)

Security measures for Technical Measures (TM)

Table G.1 indicates the security measures and best practices for TM.

Table G.1. Security measures and best practices for TM

Security measure	Best practices	Description
Hardware security	BP-TM-01	Employ a hardware-based immutable root of trust.
	BP-TM-02	a) Use hardware that incorporates security features to strengthen the protection and integrity of the device, for example, specialised security chips or coprocessors that integrate security at the transistor level, embedded in the processor, providing, among other things, a trusted storage of device identity and authentication means, protection of keys at rest and in use, and preventing unprivileged from accessing to security sensitive code. b) Protection against local and physical attacks can be covered via functional security.
Trust and integrity management	BP-TM-03	Trust shall be established in the boot environment before any trust in any other software or executable program can be claimed.
	BP-TM-04	Sign code cryptographically to ensure it has not been tampered with after signing it as safe for the device, and implement run-time protection and secure execution monitoring to make sure malicious attacks do not overwrite code after it is loaded.
	BP-TM-05	Control the installation of software in operating systems to prevent unauthenticated software and files from being loaded onto it.
	BP-TM-06	Enable a system to return to a state that was known to be secure, after a security breach has occurred or if an upgrade has not been successful.
	BP-TM-07	Use protocols and mechanisms able to represent and manage trust and trust relationships.
Strong default security and privacy	BP-TM-08	Any applicable security features should be enabled by default, and any unused or insecure functionalities should be disabled by default.
	BP-TM-09	Establish hard to crack, device-individual default passwords.
Data protection and compliance	BP-TM-10	Personal data shall be collected and processed lawfully as per Act 709, *Personal Data Protection Act 2010.*
	BP-TM-11	Make sure that personal data is used for the specified purposes for which they were collected, and that further processing of personal data is compatible and comply the Act 709, *Personal Data Protection Act 2010.*
	BP-TM-12	Minimise the data collected and retained.
	BP-TM-13	IoT stakeholders shall be compliant with the Act 709, *Personal Data Protection Act 2010.*

Table G.1. Security measures and best practices for TM *(continued)*

Security measure	Best practices	Description
Data protection and compliance	BP-TM-14	Users of IoT products and services shall be able to exercise their rights on the following: a) information; b) access; c) erasure; d) rectification; e) data portability; f) restriction of processing; and g) objection to processing.
System safety and reliability	BP-TM-15	Design with the system and operational disruption in mind, preventing the system from causing an unacceptable risk of injury or physical damage.
	BP-TM-16	Mechanisms for self-diagnosis and self-repair/healing to recover from failure, malfunction or a compromised state.
	BP-TM-17	Ensure a standalone operation which essential features should continue to work with a loss of communications and chronicle negative impacts from compromised devices or cloud-based systems.
Secure software or firmware updates	BP-TM-18	Ensure that the device software or firmware shall be able to provide the following items: a) its configuration and its applications have the ability to update Over-The-Air (OTA); b) the update server is secure; c) the update file is transmitted via a secure connection; d) it does not contain sensitive data (e.g., hardcoded credentials); e) it is signed by an authorised trust entity and encrypted using accepted encryption methods; and f) the update package has its digital signature, signing certificate and signing certificate chain, verified by the device before the update process begins.
	BP-TM-19	Offer automatic firmware update mechanism. Any automated measure comes with its own risks. The operator should be able to test and accept the updated version before clearing it for usage.
	BP-TM-20	a) Backward compatibility of firmware updates. b) Automatic firmware updates should not modify user-configured preferences, security, and/or privacy settings without user notification.
Authentication	BP-TM-21	Design the authentication and authorisation schemes (unique per device) based on the system-level threat models.
	BP-TM-22	a) Shall ensure that default passwords and even default usernames are changed during the initial setup. b) Shall ensure that weak, null or blank passwords are not allowed.
	BP-TM-23	a) Authentication mechanisms shall use strong passwords or Personal Identification Numbers (PINs). An AAA based authentication system should be the minimum standard. b) Should consider using Two-Factor Authentication (2FA) or Multi-Factor Authentication (MFA) like smartphones, biometrics, etc., on top of certificates.
	BP-TM-24	Authentication credentials shall be salted, hashed and/or encrypted.

Table G.1. Security measures and best practices for TM *(continued)*

Security measure	Best practices	Description
Authentication	BP-TM-25	Protect against brute force and/or other abusive login attempts. This protection should also consider keys stored in devices or certificate-based authentication backed by certificate Lifecycle management.
	BP-TM-26	Ensure password recovery or reset mechanism is robust and does not supply an attacker with information indicating a valid account. The same applies to key update and recovery mechanisms.
Authorisation	BP-TM-27	Limit the actions allowed for a given system by implementing fine-grained authorisation mechanisms and using the Principle of Least Privilege (POLP) where applications shall operate at the lowest privilege level possible.
	BP-TM-28	a) Device firmware should be designed to isolate privileged code, processes and data from portions of the firmware that do not need access to them. b) Device hardware should provide isolation concepts to prevent unprivileged from accessing security sensitive code.
Access control - Physical and environmental security	BP-TM-29	Data integrity and confidentiality shall be enforced by access controls. When the subject requesting access has been authorised to access particular processes, it is necessary to enforce the defined security policy.
	BP-TM-30	Ensure context-based security and privacy that reflects different levels of importance.
	BP-TM-31	a) Measures for tampering protection and detection. b) Detection and reaction to hardware tampering should not rely on network connectivity.
	BP-TM-32	a) Ensure that the device cannot be easily disassembled. b) Ensure that the data storage medium is encrypted at rest and cannot be easily removed.
	BP-TM-33	Ensure that devices only feature the essential physical external ports (such as USB) necessary for them to function and that the test/debug modes are secure, so they cannot be used to maliciously access the devices. In general, lock down physical ports to only trusted connections.
Cryptography	BP-TM-34	a) Ensure a proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of data and information (including control messages), in transit and in rest. b) Ensure the proper selection of standard and strong encryption algorithms and strong keys, and disable insecure protocols. Verify the robustness of the implementation.
	BP-TM-35	Cryptographic keys shall be securely managed.
	BP-TM-36	Build devices to be compatible with lightweight encryption and security techniques.
	BP-TM-37	Support scalable key management schemes
Secure and trusted communications	BP-TM-38	Guarantee the following different security aspects of the information in transit on the networks or stored in the IoT application or in the cloud. a) Confidentiality (privacy). b) Integrity. c) Availability and authenticity.

Table G.1. Security measures and best practices for TM *(continued)*

Security measure	Best practices	Description
Secure and trusted communications	BP-TM-39	Shall ensure that communication security is provided using state-of-the-art, standardised security protocols, such as Transport Layer Security (TLS) for encryption.
	BP-TM-40	Shall ensure credentials are not exposed in internal or external network traffic.
	BP-TM-41	a) Shall guarantee data authenticity to enable reliable exchanges from data emission to data reception. b) Data shall always be signed whenever and wherever it is captured and stored.
	BP-TM-42	a) Shall not trust the data received and always verify any interconnections. b) Discover, identify and verify/authenticate the devices connected to the network before trust shall be established, and preserve their integrity for reliable solutions and services.
	BP-TM-43	IoT devices shall be restrictive rather than permissive in communicating.
	BP-TM-44	a) Shall make intentional connections. b) Shall prevent unauthorised connections to it or other devices the product is connected to, at all levels of the protocols.
	BP-TM-45	Shall disable specific ports and/or network connections for selective connectivity.
	BP-TM-46	a) Shall perform rate limiting. b) Shall control the traffic sent or received by a network to reduce the risk of automated attacks.
Secure interfaces and network services	BP-TM-47	a) Risk segmentation. b) Splitting network elements into separate components to help isolate security breaches and minimise the overall risk.
	BP-TM-48	Protocols should be designed to ensure that, if a single device is compromised, it does not affect the whole set.
	BP-TM-49	Avoid provisioning the same secret key in an entire product family since compromising a single device would be enough to expose the rest of the product family. Use of baseline key/password management system is recommended.
	BP-TM-50	Ensure only necessary ports are exposed and available.
	BP-TM-51	Implement a DDoS-resistant and load-balancing infrastructure.
	BP-TM-52	Ensure web interfaces fully encrypt the user session, from the device to the backend services, and that they are not susceptible to Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), Structured Query Language (SQL) injection, etc.
	BP-TM-53	Avoid security issues when designing error messages.
Secure input and output handling	BP-TM-54	Data input validation (ensuring that data is safe prior to use) and output filtering.

Table G.1. Security measures and best practices for TM *(concluded)*

Security measure	Best practices	Description
Logging	BP-TM-55	a) Implement a logging system that records events relating to the following: i) user authentication; ii) management of accounts and access rights; iii) modifications to security rules; and iv) the functioning of the system. Logs shall be preserved on durable storage and retrievable via authenticated connections.
Monitoring and auditing	BP-TM-56	Implement continuous monitoring to verify the device behaviour, to detect malware and to discover integrity errors.
	BP-TM-57	a) Conduct periodic audits and reviews of security controls to ensure that the controls are effective. b) Perform penetration tests at least biannually.
NOTES: For the purposes of this table, the following abbreviations apply. 1) BP is Best Practices. 2) TM is Technical Measures.		

Bibliography

[1] MCMC MTSFB TC G009, *Information and Network Security - Requirements*

[2] MCMC MTSFB TC G022, *Internet of Things (IoT) - High-Level Functional Architecture*

[3] ITU-T Y.4806 (11/2017), *Security capabilities supporting safety of the Internet of things*

[4] TP-02-19-880-EN-N, *Good Practices for Security of IoT - Secure Software Development Lifecycle*

[5] TP-05-17-148-EN-N, *Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures*

[6] TP-07-18-076-EN-N, *IoT Security Standards Gap Analysis, Mapping of existing standards against requirements on security and privacy in the area of IoT*

[7] “Evolution of IoT Attacks” Study Exposes the Arms Race Between Cybercriminals and Cybersecurity
https://sectigo.com/resource-library/evolution-of-iot-attacks-study-exposes-the-arms-race-between-cybercriminals-and-cybersecurity

[8] Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016
http://www.gartner.com/newsroom/id/3598917

[9] Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions)
https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

Acknowledgements

Members of Internet of Things Security Sub Working Group

Prof Dr Shahrulniza Musa (Chairman)	Universiti Kuala Lumpur
Dr Ahmad Shahrafidz Khalid (Draft lead)	Universiti Kuala Lumpur
Ms Norkhadhra Nawawi (Secretariat)	Malaysian Technical Standards Forum Bhd
Ms Nuramirah Abd Ajib	American Malaysian Chamber of Commerce
Mr Haris Tahir	Celcom Axiata Berhad
Mr Yuwanthiran Sukalingam	Digi Telecommunications Sdn Bhd
Dr Gopinath Rao Sinniah	Favoriot Sdn Bhd
Mr Wong Chup Woh/ Mr Yasdy Md Yasin	Maxis Broadband Sdn Bhd
Mr Muhamad Hasyimi Shaharuddin/ Mr Najib Fadil Mohd Bisri Aka Bisri	Telekom Malaysia Berhad
Ms Lisa Lim Kher Chuen	U Mobile Sdn Bhd
Ts Herny Ramadhani Mohd Husny Hamid/ Ts Norhaiza Ya Abdullah/ Dr Shafiza Mohd Shariff	Universiti Kuala Lumpur

By invitation:

Ms Intan Harnila Abdullah	CyberSecurity Malaysia
Ms Azleyna Ariffin/ Mr Harme Mohamed/ Ms Siti Hajar Roslan	National Cyber Security Agency