

Technical Report

[TR-e-IoT-SCS-Part-2]

Generic Protection Profile

Beta — v1.0

RELEASE

Editor: Roland Atoui – Red Alert Labs

Contributors & Reviewers: François Guerin – Thales, Alban Feraud – Idemia, Rachel Shabat – Winbond, Sebastian Colle – Infineon, Steffen Heinkel – Infineon, Jonas Andersson – Fingerprint, Eric Vetillard – NXP, Sylvie Wuidart – STM, Jan Eichholz – G&D, Christine Crippa-Martinez – Thales, Isaac Dangana – Red Alert Labs, Ayman Khalil – Red Alert Labs

Approved by: Martin Schaffer – SGS, Philippe Proust – Thales, Gisela Meister – G&D, John Boggie – NXP, Stefane Mouille – Cabinet Louis Reynaud

Date	Version	Description of changes
25/10/18	V0.1	Initial version created
29/10/18	V0.2	Chapter 1 and 2 covering TOE definition
02/11/18	V0.3	Chapters 3, 4, 6, 7 covering TOE life-cycle and Operational Environment
04/11/18	V0.4	Chapters 8-12 covering assets, threats, vulnerabilities, security goals and requirements.
09/11/18	V0.5	Definition of the general concept of a Security Profile and updates to the Security Requirements
16/11/18	V0.6	Risk-based security analysis methodology completed – Section 13.3, 14 and 15
22/11/18	V0.7	Updates to Chapters 8, 11,12 and 13 to cover the latest ENISA release security baseline on IIoT,
30/11/18	V0.8	Added a full description of the Security Requirements.
13/12/18	V0.9	Added the Allowed Cryptography List in Annex IV
22/03/19	V0.9.1	Updated the requirements related to the Operational Environment
29/03/19	V0.9.2	Included TOEx, which is the TOE that incorporates a mobile application
8/04/19	V1.0	General updates
27/05/2019	V1.0_B	BETA RELEASE

Table of Contents

1	INTRODUCTION.....	7
1.1	Scope.....	7
1.1.1	IoT Definition.....	7
1.1.2	IoT Device - Typical Infrastructure.....	7
1.1.3	IoT Device Definition.....	8
1.1.4	IoT Product/Solution Definition.....	8
1.1.5	IoT Device Typical Components.....	9
1.1.6	IoT Device Features.....	9
1.1	Disclaimer.....	10
1.2	Normative References.....	10
1.7.1	General References.....	10
1.7.2	Requirements & Evaluation.....	12
1.7.3	CABs Accreditation.....	13
1.7.4	Certification Secure Life-Cycle Management.....	13
1.7.5	Supporting Documents.....	13
1.3	Terms and Definitions.....	13
1.4	Abbreviations and Notations.....	14
1.5	Audience of this Document.....	14
1.6	Support.....	14
1.7	README.....	14
2	Security Profile.....	14
3	ToE(x).....	15
3.1	IoT Application.....	16
3.2	Mobile Application.....	16
3.3	IoT Core.....	16
3.4	IoT ROE (Restricted Operating Environment).....	16
3.5	IoT HW.....	17
3.6	IoT Device Data Flow.....	17
4	Stakeholders & Risk-Owners.....	17
4.1	IoT Device Owner.....	17
4.2	IoT Service Provider.....	18
4.3	IoT Device Vendor.....	18
4.4	IoT Security Operator/Administrator.....	18
4.5	Other Parties.....	18
5	IoT Device Life-Cycle.....	19
6	Operational Environment.....	19

7	Generic Assets.....	20
7.1	Primary Assets.....	20
7.2	Secondary Assets	20
7.2.1	Non-ToE related – Secondary assets.....	22
8	Common Threats.....	25
9	Common Vulnerabilities.....	26
9.1	Software/Product Vulnerabilities	26
9.1.1	Improper Input validation.....	26
9.1.2	Poor Code Quality	27
9.1.3	Improper Permissions, Privileges, and Access Controls.....	27
9.1.4	Improper Authentication	28
9.1.5	Insufficient Verification of Data Authenticity	28
9.1.6	Cryptographic Issues	29
9.1.7	Weak Credentials Management	29
9.2	Network vulnerabilities.....	29
9.2.1	Network Design Weaknesses.....	29
9.2.2	Weak Firewall Rules	30
9.2.3	Network Component Configuration (Implementation) Vulnerabilities.....	30
9.2.4	Improper Audit and Accountability.....	30
9.3	Configuration vulnerabilities.....	31
9.3.1	Permissions, Privileges, and Access Controls.....	31
9.3.2	Improper Authentication	31
9.3.3	Poor Credentials Management	31
9.3.4	Poor Security Configuration and Maintenance.....	31
9.3.5	Weak Planning/Policy/Procedures.....	32
9.3.6	Audit and Accountability issues	32
10	Assumptions & Organizational Security Policies.....	32
10.1	Policies	32
10.1.1	Security by design	32
10.1.2	Privacy by design.....	33
10.1.3	Asset management	33
10.1.4	Risk and Threat Identification and Assessment	34
10.2	Organisational, People and Process measures	34
10.2.1	Endpoints lifecycle Support	34
10.2.2	Security Architecture	35
10.2.3	Management of security vulnerabilities and/or incidents	35
10.2.4	Human Resources Security Training and Awareness.....	35
10.2.5	Third-Party relationships.....	36

10.2.6	Implementation Considerations	36
11	Security Goals & Security Requirements	36
12	How To Create a Security Profile	42
12.1	Security Profile Properties	42
12.1.1	Owner.....	42
12.1.2	Timeline.....	42
12.1.3	Validity	42
12.2	A 3 steps approach (1 COLLECT → 2 DEFINE → 3 DECIDE)	43
12.3	Risk-Based Methodology	43
12.3.1	A Simplified Process	44
12.3.2	STEP 1 - COLLECT.....	44
12.3.3	STEP 2 - DEFINE	46
12.3.4	STEP 3 - DECIDE.....	52
13	Vendor Questionnaire.....	56
14	Integration to the IoT device Development Life-Cycle	57
15	About us	59
16	Our members	59
	ANNEX I – Sample of Risk Calculation	60
	ANNEX II – SECURITY REQUIREMENTS (93)	67
	ANNEX III – SECURITY ASSURANCE ACTIVITIES MAPPING WITH IMPACTS/LIKELIHOOD.....	109
	ANNEX IV – ALLOWED CRYPTOGRAPHY LIST	110
	ANNEX V- THREATS CATALOGUE	122

TABLE OF TABLES

Table 1: Common list of Security Goals & Requirements	42
Table 2: Likelihood Calculation in 3 steps.....	47
Table 3: Likelihood Table of Calculation	47
Table 4: Probability of Success Calculation.....	48
Table 5: Technical Difficulty Calculation	49
Table 6: Global Likelihood Calculation.....	49
Table 7: Impact Calculation - Reference Table	51
Table 8: Risk Calculation Table (Impact vs Likelihood)	51
Table 9: Risk Calculation Grid - Granular representation	53
Table 10: Risk Treatment Options.....	54
Table 11: Risk Decision Table	54
Table 12: Security Profile - Sample Template	56
Table 13: Vendor Questionnaire Template (Sample)	57
Table 14: Threat Model Representation - Attacks Scenarios	63

TABLE OF FIGURES

Figure 1: IoT Device - Typical Infrastructure	7
Figure 2: IoT Products/Solution - Different Market Applications	8
Figure 3: IoT Device Reference Architecture	9
Figure 4: Target of Evaluation	15
Figure 5: IoT Threat Taxonomy	26
Figure 6: IoT Threats Impacts.....	26
Figure 7: From GPP to a Security Profile	43
Figure 8: IoT Risk-Based Assessment Methodology	44
Figure 9: High-Level representation of the IoT Security Risk Analysis.....	46
Figure 10: Impacts & Operational Environments	50
Figure 11: Potential Security Assurance Activities (pSAA) mapping with impacts/likelihood	52
Figure 12: Mapping between applicable security assurance requirements and security requirements	55
Figure 13: RAL IoT Device Security Assurance Development Life-Cycle	58

I INTRODUCTION

This document is a generic representation of common security requirements on IoT devices. It is based on a security risk analysis approach of an IoT Device operating in a typical infrastructure without considering a specific type of data or a context for risk calculation.

The main output of this document is a list of security goals and requirements qualifying the need to counter security threats identified on a typical IoT device.

I.1 Scope

I.1.1 IoT Definition

For ENISA, IoT is an emerging concept comprising a wide ecosystem of interconnected services and devices, such as sensors, consumer products and everyday smart home objects, cars, and industrial and health components. The “Things” collect, exchange and process data to dynamically adapt to a specific context, transforming the business world and the way we live. IoT is tightly bound to cyber-physical system and, in this respect, safety implications are pertinent.

I.1.2 IoT Device - Typical Infrastructure

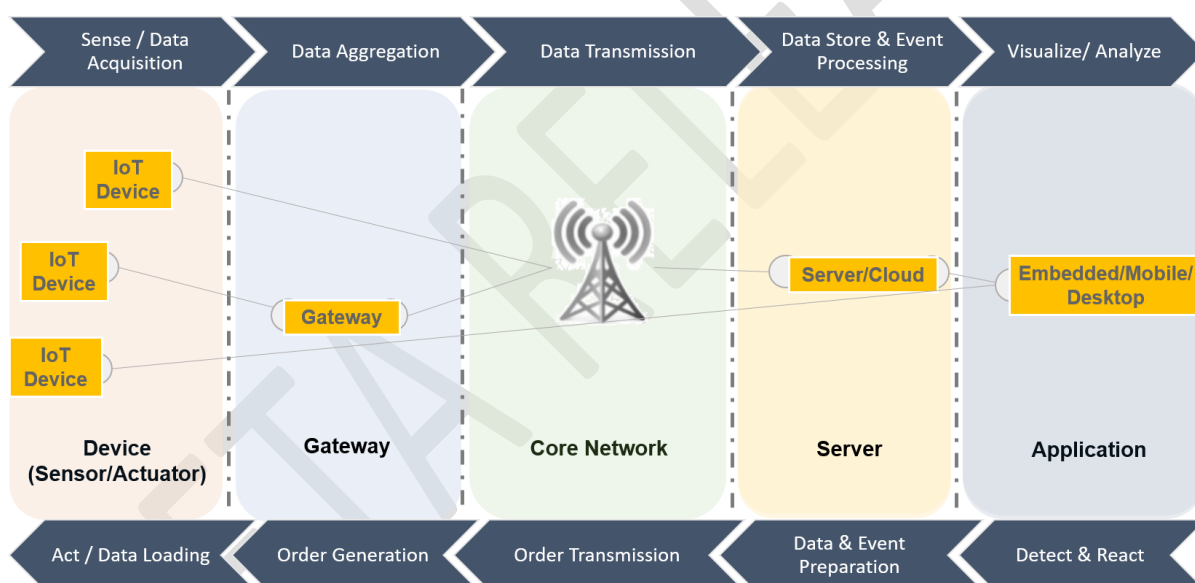


Figure 1: IoT Device - Typical Infrastructure

The overall IoT system is broken into the following five domains:

- **Device:** This includes both simple and complex IoT devices such as sensors, actuators, industrial machines, etc.
- **Gateway:** IoT gateways are IoT devices performing several functions such as connectivity, protocol translation, data filtering and processing, security, updating, management and more. Newer IoT gateways also operate as platforms for application code that processes data and becomes an intelligent part of a device-enabled system. IoT gateways sit at the intersection of edge systems and the cloud.
- **Server:** All the data from the devices are sent through the gateway to the cloud/server. All the control signals are sent back to the devices from the server. Through the cloud/server, all the administrative functions are done and also the functions like data visualisation, predictive maintenance, etc.

- **Application:** It includes business and management applications (Embedded, Mobile or Desktop) used to monitor, analyse, manage and administer the IoT devices and gateways.
- **Core Network:** It includes all the communication in the system and the components that facilitate the communication. For better visibility, the network is divided into the following.
 - **Device-Gateway:** The network between the devices and the gateway
 - **Device-Cloud/server:** The network between the devices and gateway
 - **Gateway-Cloud/server:** The network between the gateway and the cloud/server

1.1.3 IoT Device Definition

An IoT Device is a “Thing” as per the IoT definition above or an ICT device as defined by the Cybersecurity Act that is mainly composed of:

- Hardware including microcontrollers, microprocessors, mother board, ICs, physical ports.
- Software including an embedded OS, its firmware, programs and applications
- Sensors which detect and/or measure events in its operational environment and send the information to other components
- Actuators which are output units that execute decisions based on previously processed information

The internet of things, or IoT, is a system of interrelated computing devices, mechanical and digital machines, with the ability to monitor and transfer data over a network without requiring human-to-human or human-to-computer interaction.

1.1.4 IoT Product/Solution Definition

An IoT Product/Solution such as a Connected Camera, Smart TV, Smart Thermostat along with a Mobile Application, a Smart lock, an RTU or a Gateway. It could be composed of one or more IoT devices and could be part of different market applications as shown in the figure below.

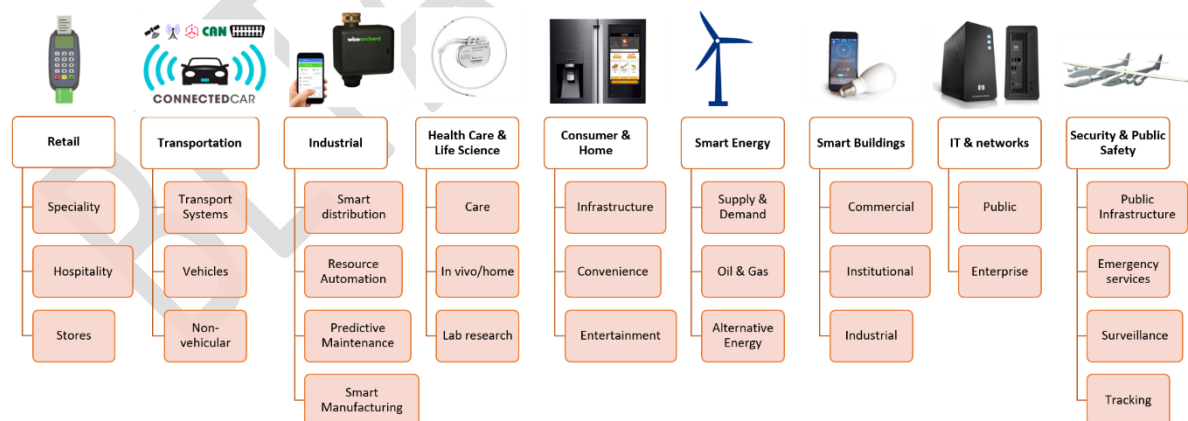


Figure 2: IoT Products/Solution - Different Market Applications

1.1.5 IoT Device Typical Components

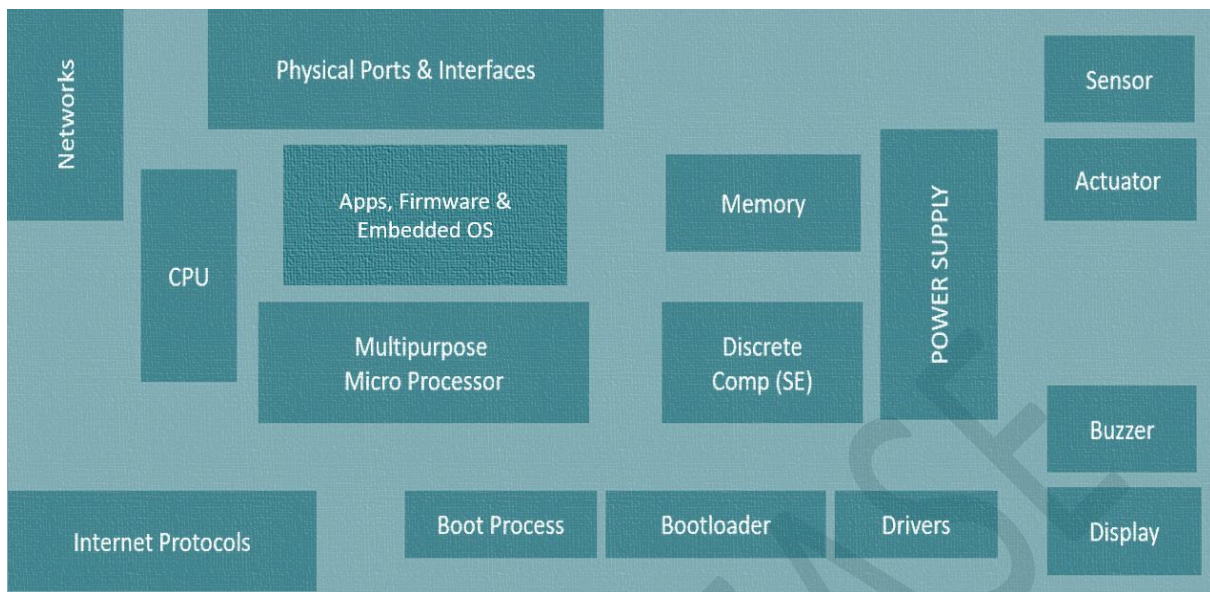


Figure 3: IoT Device Reference Architecture

1.1.6 IoT Device Features

Each IoT device provides one or more features or functions it can use on its own or in conjunction with other IoT and non-IoT devices to achieve one or more goals. A part of these capabilities could be affected by cybersecurity attacks such as:

- **Transducer features (sensors & actuators):** Every IoT device has at least one transducer feature. The two types of transducer features are:
 - o Sensors: feature allowing to observe an aspect of the operational environment in the form of measurement data. Examples include temperature measures, computerized tomography scans (radiographic images), optical sensors, and audio sensors.
 - o Actuators: feature impacting the operational environment. Examples of actuators include heating coils, cardiac electric shock delivery, electronic door locks, unmanned aerial vehicle operation, servo motors, and robotic arms.
- **Data Features (storing & processing)** are typical digital computing functions involving data.
- **Interface Features** allows to interact with the IoT Device through an interface (e.g., device-to-device communications, human-to-device communications). The types of interface features are:
 - o Application interface: such as an API (Application Programming Interface) or a HUI (Human User Interface). Examples of HUIs include keyboards, mice, microphones, cameras, scanners, monitors, touch screens, touchpads, speakers, and haptic devices.
 - o Network interface (communication network). Such as Ethernet, Wi-Fi, Bluetooth, Long-Term Evolution (LTE), and ZigBee. Every IoT device has at least one enabled network interface feature and may have more than one.
- **Supporting Features** provide functionality that supports the other IoT features. Examples are device management, cryptographic features, etc.

1.1 Disclaimer

EUROSMART and all related entities, provide all materials, work products and, information (“TECHNICAL REPORTS”) AS IS, WITHOUT WARRANTY AND WITH ALL FAULTS, and hereby disclaim all warranties and conditions, whether express, implied or statutory, including, but not limited to, any (if any) implied warranties, duties or conditions of merchantability, of fitness for a particular purpose, of reliability or availability, of accuracy or completeness of responses, of results, of workman like effort, of lack of viruses, and of lack of negligence, all with regard to the TECHNICAL REPORTS, and the provision of or failure to provide support or other services, information, software, and related content through the TECHNICAL REPORTS or otherwise arising out of the use of the TECHNICAL REPORTS.

ALSO, THERE IS NO WARRANTY OR CONDITION OF TITLE, QUIET ENJOYMENT, QUIET POSSESSION, CORRESPONDENCE TO DESCRIPTION, OR NON-INFRINGEMENT WITH REGARD TO THE TECHNICAL REPORTS.

WITHOUT LIMITING THE FOREGOING, EUROSMART DISCLAIMS ALL LIABILITY FOR HARM TO PERSONS OR PROPERTY, AND USERS OF THESE TECHNICAL REPORTS ASSUME ALL RISKS OF SUCH HARM.

IN ISSUING AND MAKING THE TECHNICAL REPORTS AVAILABLE, EUROSMART IS NOT UNDERTAKING TO RENDER PROFESSIONAL OR OTHER SERVICES FOR OR ON BEHALF OF ANY PERSON OR ENTITY, NOR IS EUROSMART UNDERTAKING TO PERFORM ANY DUTY OWED BY ANY PERSON OR ENTITY TO SOMEONE ELSE.

ANYONE USING THIS TECHNICAL REPORT SHOULD RELY ON HIS OR HER OWN INDEPENDENT JUDGMENT OR, AS APPROPRIATE, SEEK THE ADVICE OF A COMPETENT PROFESSIONAL IN DETERMINING THE EXERCISE OF REASONABLE CARE IN ANY GIVEN CIRCUMSTANCES.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL EUROSMART OR ITS SUPPLIERS BE LIABLE FOR ANY SPECIAL, INCIDENTAL, PUNITIVE, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF PROFITS OR CONFIDENTIAL OR OTHER INFORMATION, FOR BUSINESS INTERRUPTION, FOR PERSONAL INJURY, FOR LOSS OF PRIVACY, FOR FAILURE TO MEET ANY DUTY INCLUDING OF GOOD FAITH OR OF REASONABLE CARE, FOR NEGLIGENCE, AND FOR ANY OTHER PECUNIARY OR OTHER LOSS WHATSOEVER) ARISING OUT OF OR IN ANY WAY RELATED TO THE USE OF OR INABILITY TO USE THE TECHNICAL REPORTS, THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT OR OTHER SERVICES, INFORMATION, SOFTWARE, AND RELATED CONTENT THROUGH THE TECHNICAL REPORTS OR OTHERWISE ARISING OUT OF THE USE OF THE TECHNICAL REPORTS, OR OTHERWISE UNDER OR IN CONNECTION WITH ANY PROVISION OF THESE TECHNICAL REPORTS, EVEN IN THE EVENT OF THE FAULT, TORT (INCLUDING NEGLIGENCE), MISREPRESENTATION, STRICT LIABILITY, BREACH OF CONTRACT OF EUROSMART OR ANY SUPPLIER, AND EVEN IF EUROSMART OR ANY SUPPLIER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

1.2 Normative References

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

1.7.1 General References

Reference	Name/Description
-----------	------------------

[BSI-St2003]	BSI-Standard 200-3: Risk Analysis based on IT-Grundschutz
[EBIOS-RM]	ANSSI – EBIOS Risk Manager - version 1.0
[ECISO-META]	European Cyber Security Certification – A Meta-Scheme Approach v1.1 – Oct 2018
[ENISA-Baseline-CII]	Baseline Security Recommendations for IoT in the context of CII
[ENISA-Glossary]	Glossary of risk management terminology – Published under Risk Management - https://www.enisa.europa.eu/...
[ENISA-Threats]	ENISA Threat Taxonomy – Version 1.0 Jan 2016
[EU Cybersecurity Act]	European Parliament legislative resolution of 12 March 2019 on the proposal for a regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act") (COM(2017)0477 – C8-0310/2017 – 2017/0225(COD))
[FIPS 199]	Standards for Security Categorization of Federal Information and Information Systems https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf
[GDPR-Art9]	Processing of General Categories of Personal Data as defined by GDPR Article 9 http://data.europa.eu/eli/reg/2016/679/oj
[GDPR-Risk]	Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf
[ISO/IEC 15408]	Common Criteria for Information Technology Security Evaluation (Part 1-3)
[ISO/IEC 17000:2004]	Conformity assessment — Vocabulary and general principles
[ISO/IEC 17025]	General requirements for the competence of testing and calibration laboratories
[ISO/IEC 17065:2012]	Conformity assessment — Requirements for bodies certifying products, processes and services
[ISO/IEC 17067:2013]	Conformity assessment — Fundamentals of product certification and guidelines for product certification schemes

[ISO/IEC 18045]	Information technology -- Security techniques -- Methodology for IT security evaluation
[ISO/IEC 27005:2018]	Information technology — Security techniques — Information security risk management
[ISO31000:2018]	Risk Management – Principles and Guidelines
[ISO-SAECD21434]	ISO/SAE 21434 – Road Vehicles – Cybersecurity Engineering
[NIST-SP800-82]	Guide to Industrial Control Systems (ICS) Security – NIST Publication https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf
[OCTAVE-Allegro]	OCTAVE Allegro risk assessment methodology https://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14885.pdf
[Privacy-RAM]	Privacy Risk Assessment Metrics – OIC Australia https://www.oic.qld.gov.au/__data/assets/pdf_file/0015/16242/guideline-dataset-publication-and-risk-assessment-appendix-1.pdf
[RAL-IIoTSA]	Industrial Internet of Things Security Analysis - Red Alert Labs – Sept 2018
[RAL-IoTSA]	Internet of Things Security Analysis - Red Alert Labs – Dec 2017

1.7.2 Requirements & Evaluation

<i>Reference</i>	<i>Name/Description</i>
[TR-e-IoT-SCS-Part-1]	E-IoT-SCS Certification Scheme Process & Policy - This document defines the policies and processes that govern the IoT device certification scheme.
[TR-e-IoT-SCS-Part-2]	<p>E-IoT-SCS Generic Protection Profile - This document is a generic representation of common security requirements on IoT devices. It is based on a security risk analysis approach of an IoT Device operating in a typical infrastructure without considering a specific type of data or a context for risk calculation.</p> <p>The main output of this document is a list of security goals and requirements qualifying the need to counter security threats identified on a typical IoT device.</p>
[TR-e-IoT-SCS-Part-3]	E-IoT-SCS Evaluation Methodology - Document defining the evaluation activities to be performed by an evaluator and links between them in order to conduct properly an evaluation. It lists evaluation evidences required to perform actions as defined in the security assurance requirements. It

	defines way to report evaluation results in Evaluation technical report and observation report. It also provides rules to define verdict and criteria of failure.
--	---

1.7.3 CABs Accreditation

The following documents describe how to become an Accredited CAB

<i>Reference</i>	<i>Name/Description</i>
[TR-e-IoT-SCS-Part-4]	CABs Agreement - Guidelines listing the rules for setting up agreement between CABs and Certification Scheme stakeholders (e.g. other CABs – CAB reviewer, CAB evaluator, NABs, etc.)
[TR-e-IoT-SCS-Part-5]	CABs Accreditation Policy - Guidelines describing policy for CABs accreditation

1.7.4 Certification Secure Life-Cycle Management

<i>Reference</i>	<i>Name/Description</i>
[TR-e-IoT-SCS-Part-6]	Vulnerability Management, Maintenance & Continuous Assurance Policy: Document describing vulnerability management procedures and the life-cycle management of the Certificate after issuance
[TR-e-IoT-SCS-Part-7]	Mark & Certificate Usage Policy for e-IoT Certification Scheme: Document describing the procedure and conditions which govern the use of the e-IoT SUBSTANTIAL mark and certificate by IoT device vendors, CABs and end-users
[TR-e-IoT-SCS-Part-8]	The Metadata Certification Policy for e-IoT Certification Scheme: Document describing the Metadata Certification Concept and Requirements guaranteeing the relevancy and Authenticity of the Certificates.

1.7.5 Supporting Documents

<i>Reference</i>	<i>Name/Description</i>
[TR-e-IoT-SCS-Part-9]	Templates (Vendor Questionnaire, Impact Analysis Report, Security Profile, Evaluation Report, Mapping Table Concept)
[Informative Annexes]	A set of informative annexes complementing the e-IoT Security Certification Scheme deliverables such as the “e-IoT-SCS Candidate Certification Scheme Pre-Study – v1.0 RELEASE”, or “Risk Assessment Methodologies”.

1.3 Terms and Definitions

Refer to **[TR-E-IOT-SCS-PART-1]**, SECTION 1.4

1.4 Abbreviations and Notations

Refer to [TR-E-IOT-SCS-PART-1], SECTION 1.5

1.5 Audience of this Document

The primary audience of this documents are technical working groups composed mainly of vendors¹ developing IoT devices, IoT security experts and CABs undergoing the E-IoT-SCS Certification process.

It is intended to help them mainly generate Security Profiles and Vendor Questionnaires tailored for a class of IoT Devices (e.g. Smart TV, Connected Cam, etc.)

1.6 Support

For help and support, contact e-IoT-SCS@eurosmart.com

1.7 README

More than 50 billion IoT devices will be made available across all industries including automotive, education, home appliances, consumer electronics, banking, medical, manufacturing, and more.

It is not realistic to evaluate the entire implementation of an IoT device since there are too many different IoT device applications and frequent updates of IoT device applications.

The Target of Evaluation (ToE) presented below will focus on:

- the parts including the security functionality
- a modular approach allowing to adapt to different IoT applications through Security Profiles
- a context-based approach allowing to identify different threat models and risks for four different Operational Environments (Consumer, Enterprise, Industrial and Critical)

This Scheme could cover an Extended ToE as described below. The Security Profile will be specifying the scope of coverage.

Finally, the catalogue of Security Requirements provided in this version of the document is relevant to the ToE scope.

2 Security Profile

A Security Profile (SP) defines the security requirements and security assurance activities specific security problem definition of a type of an IoT Product/Solution (thermostat, smart cam, etc.) while considering the sensitivity of assets, the context of the operational environment and the risk factor.

Its definition is a step towards an economic way of dealing with security risk analysis and security targets. It helps to scale security controls and security-related process activities in accordance to the identified risks, i.e. to spend most effort where the highest risks are.

Finally, this Certification Scheme defines a methodology allowing a harmonized and quick creation of Security Profile covering the full attack surface threat model from Chip to Cloud including the Applications (Business and Mobile), Gateways, the Connectivity and the Cloud.

FAQ 2.1

Q2.1: When and How to create a Security Profile?

¹ A vendor could be an integrator¹ of different components purchased from other vendors.

R2.1: A Security Profile is a pre-requisite for every certification process. Once a Vendor applies for a Certification, the Vendor could either use an existing “Standard” Security Profile² covering fully or partially the ToE Scope or create a new Security Profile tailored to its IoT Product/Solution.

Refer to [Section 12](#) for a clear description of how to create a Security Profile in 3 steps.

FAQ 2.2

Q2.2: What products could be covered by a Security Profile?

R2.2: A Security Profile could be created for a full/part of an IoT Product/Solution such as a Connected Camera, Smart TV, Smart Lock + Dedicated Mobile Application, an RTU or a Gateway. The scope of a Security Profile must include at least the IoT Device as defined in [Section 1.1.3](#) above.

3 ToE(x)

The image below provides a high-level logical layer for an IoT Device which, excluding the IoT Application, constitutes the Target of Evaluation (ToE). On the other hands, it shows an IoT Device including the IoT Application and the Mobile Application layers forming the Extended Target of Evaluation (ToEx).

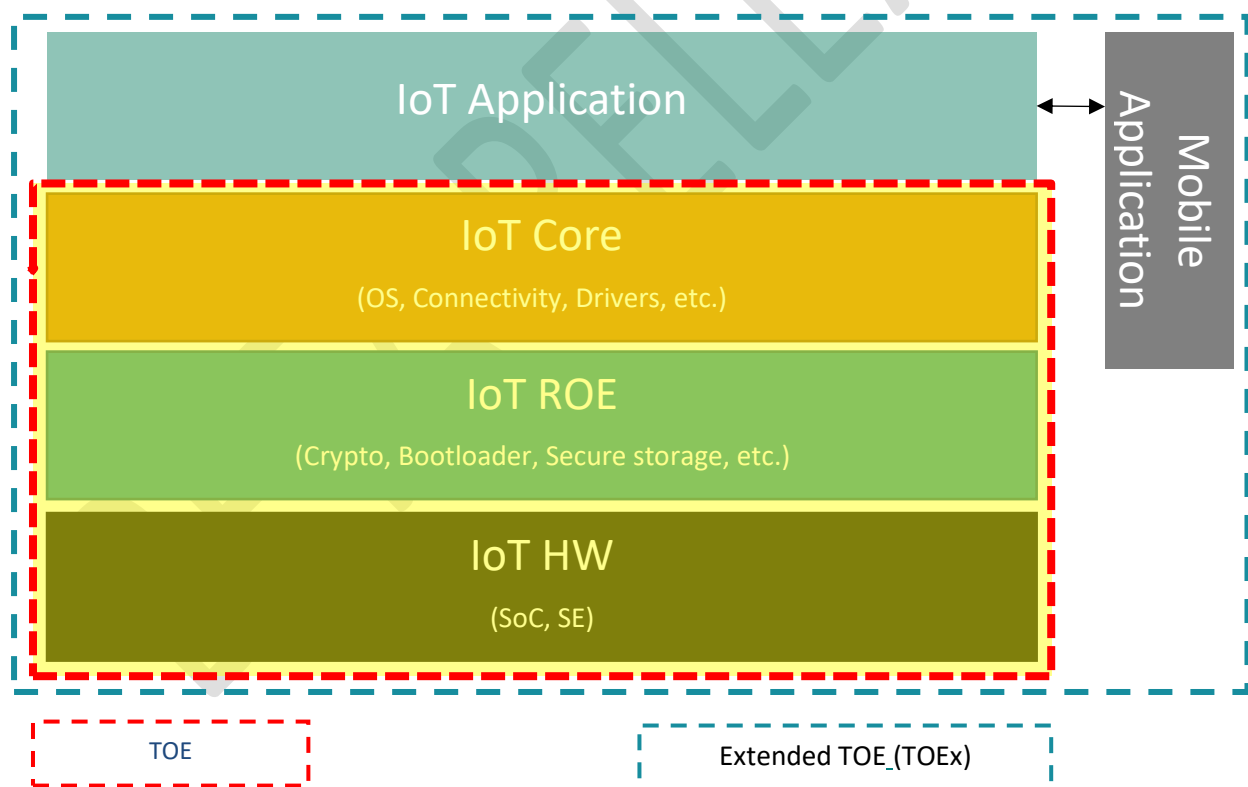


Figure 4: Target of Evaluation

The Extended ToE (ToEx) is composed of the following components:

² A “Standard” Security Profile must have been recognized by Eurosmart or an associate industrial consortium or task force.

3.1 IoT Application

An IoT application is an implementation of the end user functionality of an IoT Device allowing the final IoT product to be fulfilling its intended use in the operational environment.

Application Note

<i>Incorporating the IoT application to the original TOE constitutes the “Extended TOE (TOEx)”. It is assumed that IoT Application shall have no possibility to communicate with external network devices without going through the IoT Core described below.</i>

3.2 Mobile Application

A mobile application is a software application designed to run on a mobile device such as a phone/tablet or watch. It is intended to provide Interface features for the end-user or the administrator to interact with the IoT device.

Application Note

<i>Incorporating the mobile application to the original TOE constitutes the “Extended TOE (TOEx)”. Mobile applications are increasingly becoming a necessary feature in the remote manipulation of IoT devices. The adoption of mobile applications varies across domains, with the consumer domain accounting for the highest and much less so in other domains, hence the importance of proactively including the assessment of mobile applications in the evaluation process. In the TOEx approach, the security assurance of mobile applications shall be evaluated according to existing acceptable standards of mobile application security (e.g. OWASP Mobile)</i>

3.3 IoT Core

The IoT Core main purpose is to provide trusted channel/path to external network device and shall allow connections to configured devices only.

It shall include all OSI layers except the IoT Application layer which is essential to cover all the communication part in the scope of the evaluation.

The IoT Core is mainly (but not strictly) responsible of the following functionality:

- Secure implementations of communication protocols used
- Secure network connection control functionality
- Secure firmware update functionality
- Resistance to logical/network-based attacks

3.4 IoT ROE (Restricted Operating Environment)

The IoT ROE shall provide an environment mainly to establish the root of trust, for secure storage and usage of IoT device keys used by the IoT Core to be finally provided to the IoT Application. It provides a level of protection against physical attacks.

The IoT Restricted Operating Environment is responsible of the following functionality

- Secure storage/usage
- Secure Boot
- Access Control policy, Isolation of Applications

- Resistance to physical/local attacks
- Resistance to all types of side-channel leakage analysis

3.5 IoT HW

No restricted form factor composed typically of a SoC with an MCU, Memory, Ports and maybe an SE with no specific restrictions.

IoT Devices could have the following characteristics (but not restricted to):

- Embedded Devices
- Linux Based Devices
- Resource Constraint Devices
- Microcontroller based devices with flash/firmware
- Microprocessor based devices
- Devices with Medium Memory Capacity (1MB and above)
- Can be used with or without a TPM or a Secure Element (SE)

3.6 IoT Device Data Flow

Data is pervasive throughout the IoT system. Each set of data has a different lifecycle, time of relevancy and potential risk associated with its compromise. The threat may result from its modification, interception or duplication. The effects of attacks on data vary from immediate change in system behaviour to subtler negative behaviour in the future.

The data protection strategies for each type of data fall into three categories:

- **Data-at-Rest (DAR)** is data in persistent storage, for example, in a solid-state disk (SSD) on an edge device.
- **Data-in-Use (DIU)** is data placed in non-persistent storage such as random-access memory (RAM) and CPU caches and registers.
- **Data-in-Motion (DIM)** is data moving between two or multiple IoT devices

4 Stakeholders & Risk-Owners

4.1 IoT Device Owner

The IoT Device Owner³ is the OEM of the IoT device. IoT Device Owners takes part of the risks related to cybersecurity threats, but their top protection priorities are the following:

- Resistance of the device against remote attacks/scalable attacks
- Preserving the privacy and the integrity of the data transferred to a Service Provider
- No data flow to unauthorized network entities
- Availability of the Service

³ Note that the IoT Product/Solution's owner is the end-user or the end-consumer mainly but in some cases it could be the IoT Service Provider who owns the product.

4.2 IoT Service Provider

IoT Service Provider (IoTSP) could be the IoT device vendor itself or a third-party service provider such as IoT Cloud Platforms (private, public or hybrid). An IoTSP top priorities to reduce cybersecurity risks are the following:

- Prevention of identity-theft / identity-cloning of devices
- Protection of the business case (e.g., in a pay-per-use model)

4.3 IoT Device Vendor

The IoT Device Vendor would be mainly interested in the following goals:

- Providing assurance to the different stakeholders in an IoT Solution
- Cost-effectiveness/reusability of evaluation/certification, possibility of post-certification changes
- Meeting the objectives of the IoT device owner

4.4 IoT Security Operator/Administrator

An IoT Security Operator/Administrator is responsible to monitor, manage and administer the security of the IoT device. His main concerns could be the following:

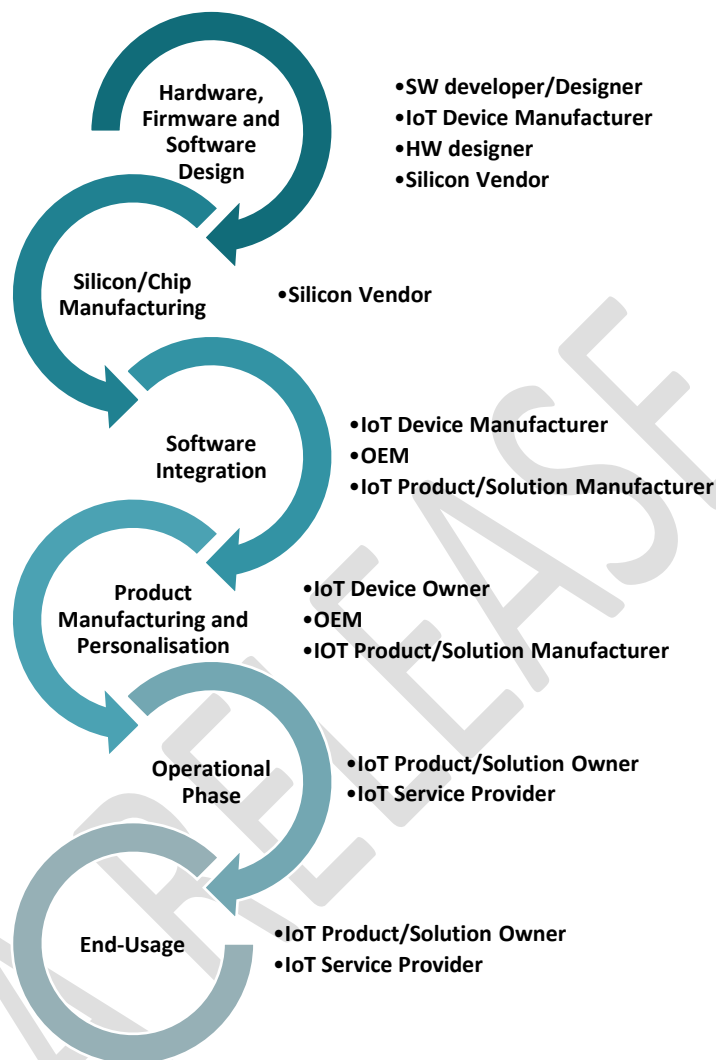
- Preventing of attacks on IoT device compromising escalation of privileges
- Prevention of attacks on communication protocols
- Insuring the Software Integrity
- Guaranteeing a secure configuration

4.5 Other Parties

Other parties could be involved in the IoT device operational environment such as Owners of Other IoT devices, Insurance companies, Businesses, Industries and Governments in general.

- Prevention of creation of botnets or similar attacks
- Prevention of attacks on critical infrastructures (e.g., electricity grid)
- Etc.

5 IoT Device Life-Cycle



6 Operational Environment

The Operational Environment is where the IoT device is intended to work. Adding assumptions on the application area of the product is essential to set its security objectives and subsequently the corresponding security functions.

Example: Ensuring secure communication in connected equipment that handles financial transactions is obviously not achieved in the same way as for a smart calendar that connects to the user's smartphone to remind them of their appointments. Same goes for a connected camera that could be installed at home (indoor environment) and the one that is installed on the side of the road (outdoor environment) the security requirements would vary depending on the operational environment.

Therefore, this GPP will cover 4 generic types of Operational Environments in order to estimate the risks and therefore provide an adequate Substantial security assurance.

- Consumer (Basic to Substantial)
- Enterprise (Substantial)
- Industrial (Substantial to High)

- Critical (High)

What follows are only an example of IoT devices that could fit in different operational environments.

Operational Environment	Types of IoT DEVICES (Sample)
<ul style="list-style-type: none"> • Consumer 	Connected Light bulbs, Connected TVs, eReaders, Power Systems, Dishwashers, lighting, Washers/Dryers, Alarm systems, Humidity sensors, etc.
<ul style="list-style-type: none"> • Enterprise 	Storage, Routers, Thermostat, Switches, PBXs, CCTV, Alarm systems, etc.
<ul style="list-style-type: none"> • Industrial 	Connected Pumps, Valves, Vats, Conveyors, Pipelines, Motors Drives, Converting, Fabrication, Vessels/Tanks, etc.
<ul style="list-style-type: none"> • Critical 	MRI, PDAs, Implants, Pumps, Monitors Telemedicine, Connected Turbines, Windmills, UPS, Batteries, Generators, Meters, Drills, Fuel Cells, road traffic sensors,

7 Generic Assets

7.1 Primary Assets

Here we mainly address the primary assets which are the Data.

Data can be of different types and for different purposes. Here it is classified into three types depending on its functions.

Device Data: This includes all the data that is generated by the different devices and sent to the server along with the control signals that is sent back to the devices from the cloud server.

Security Data: This includes all the data that is generated and used for implementing different security mechanisms in the system

Configuration and Monitoring Data: This includes all the data that is required for the configuration, management and monitoring of the different components of the system.

The secondary assets could be representing the physical components of the IoT device or those part of its operational environment.

7.2 Secondary Assets

ASSET GROUP	ASSETS	DESCRIPTION
IoT End Devices	Sensors	These devices detect and/or measure events in their environment and transmit information to other electronic systems to be processed. There are sensors for many purposes, such as to measure temperature, motion, vibration etc.

	Actuators	These devices interact with the environment by moving or controlling a mechanism or system. In order to do so, they convert energy (e.g. electrical, hydraulic or pneumatic) into motion.
Communication networks & components	Routers	These networking devices forward data packets between different networks in industrial environments and IoT ecosystems
	Gateways	These network nodes are used to interface with another network from an IoT environment using different protocols. Gateways may provide protocol translators, fault isolators, etc., to provide system interoperability
	Switches	These network components filter and forward packets within the local area network
	Wireless Access Points	These components enable wireless devices to connect to a wired network using Wi-Fi, or related standards
	Firewall	These network security devices or systems control network traffic between networks or between a host and a network based on predetermined rules
	Networks	They allow the different nodes of an IoT ecosystem to exchange data and information with one another, via a data link. There are different kinds of networks related to their spatial coverage, including e.g. (W)LANs, (W)PANs, PANs and (W)WANs, among others
	Protocols	They define the set of rules on how two or more IoT devices communicate over a given channel. There are many communication protocols, which can be either wired or wireless

	Power Supply	It supplies electric power to an IoT device and its internal components. The power source can be external and wired or a battery integrated in the device itself
Software and Licenses	Operating System	This term refers to a system that manages computer hardware resources and provides common services for other computer programs to run
	Mobile application	These programs run on mobile devices, such as tablets and smartphones, which are used for remote supervision and control of a process (e.g. mobile SCADA client applications), equipment maintenance and other tasks (e.g. warehouse inventory).
	Firmware	This term refers to a class of software stored on a device's read-only memory and provides instructions on how the device should operate. During execution, it cannot be dynamically written or modified

7.2.1 Non-ToE related – Secondary assets

Decision Making Algorithms	Artificial Intelligence and Machine Learning	These terms describe the ability of a machine (e.g. computer, robot, etc.) to perform tasks typical for intelligent beings, where enormous amounts of data is collected, various ML and AI algorithms can be utilised for analysis
Cloud Computing Services		These services enable swift universal network access to a shared set of resources such as networks, servers and applications with minimal requirement of management

		effort and service provider interaction
Big Data Analytics		This term describes the process of examining vast amounts of various data sets generated in real time by smart sensors, devices, log files, video and audio, etc. Big Data is analysed to uncover hidden patterns, unknown correlations, trends and other useful information that can help make more-informed and deliberate decisions
Real time monitoring and security tools	SIEM	These applications are utilised to collect and aggregate security data from various system components and render them in the form of meaningful information via a single interface
	IDS/IPS	These systems enable automatic monitoring of the events that occur in a computer system or network and their analysis for signs of possible incidents. In addition, IPS may execute actions in an attempt to stop detected incidents
Software and Licenses		
	Antivirus	This term refers to a software that monitors a computer or network to identify malware, prevent it from infecting devices and clean infected devices.

Servers and Systems	Application Servers	These computers host applications, e.g. user workstations' applications
	Database Servers	These servers are used as repositories for event information provided by sensors, agents, and management servers
Mobile devices	Tablets, smartphones	These portable devices can be operated by hand. They run mobile applications enabling operators to perform various tasks.
Personnel	Operators, maintenance staff, third parties	This asset group refers to all the individuals who have physical or remote access to the system. All the people with access to an environment can introduce malware to the system (intentionally or unintentionally), become targets of phishing or cause damage to the system and compromise its security in a variety of ways. On the other hand, people require protection, as their privacy and physical safety may be endangered in the event of security incident.

8 Common Threats

ENISA defined a Baseline Security Recommendations for IoT⁴ which we primarily rely on (but adapted) to consider all the threats relevant to the ToE in an IoT Typical Infrastructure.

This re-adaptation became necessary in order to align the granularity in the analytical resolution of ENISA Threat Taxonomy⁵ with our threat analysis methodology. In Figure 5, we depict the new threat taxonomy focused on IoT with some examples of attacks listed (non-exhaustive listing). Full documentation of the threats can be found in the “ANNEX V-THREATS CATALOGUE”.

Threat ID	Threat Description
T01.	Replay of data
T02.	Disclosure of data (stored, processed, transported)
T03.	Manipulation or injection of data (stored, processed, transported)
T04.	Deletion of data (stored, processed, transported)
T05.	Vandalism or Theft of device, storage media, etc.
T06.	Loss of device, storage media, etc.
T07.	Compromise of personal data/sensitive info/ confidential info etc.
T08.	Unauthorized use or administration of devices & systems
T09.	Physical access to operation workstation/devices by malicious external actor
T010.	Lack of organizational policies & Procedures
T011.	Substandard, malicious or fake device components
T012.	Regulatory Sanctions
T013.	Malicious access to device/system assets.
T014.	Failure or malfunction of the power supply
T015.	Unavailability of communication systems
T016.	Failure or disruption of service providers
T017.	Failure of Internal information systems
T018.	Environmental disasters
T019.	Natural disasters
T020.	Interfering radiation
T021.	Network Denial of service
T022.	Intercepting compromising emissions

⁴ ENISA Baseline Security Recommendations for IoT with an interactive tool. Another version of the Baseline is defined for the context of Critical Information Infrastructure

⁵ See <https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/etl2015/enisa-threat-taxonomy-a-tool-for-structuring-threat-information>

Figure 5: IoT Threat Taxonomy

Nevertheless, the different threats have different potential impacts, since they vary according to the use case scenarios. ENISA provided insight into the varying impact of the threats. The most relevant ones are shown in Figure 6.

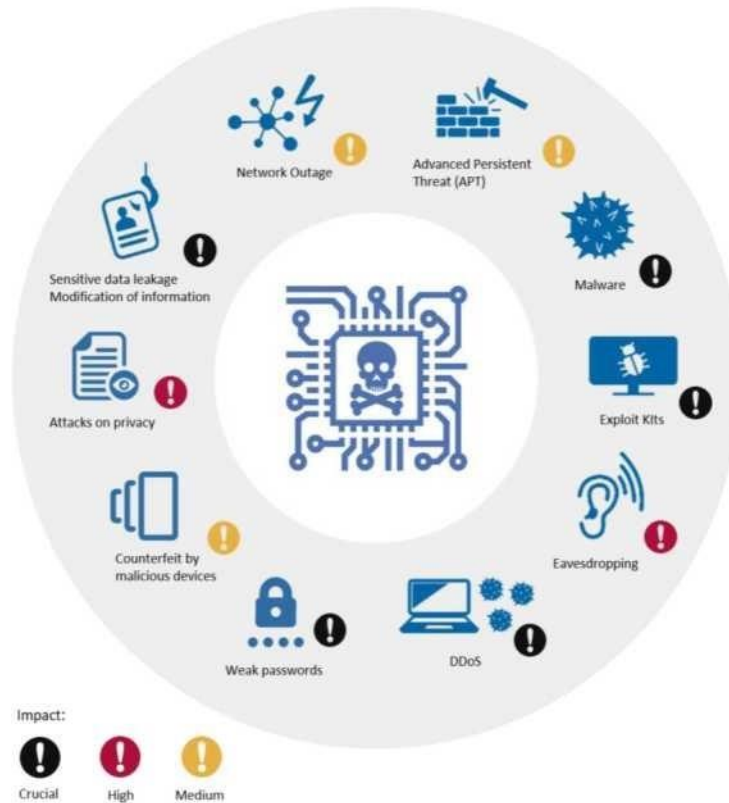


Figure 6: IoT Threats Impacts

9 Common Vulnerabilities

After all the potential threats are identified, the vulnerabilities that can lead to the threats are identified hereafter.

9.1 Software/Product Vulnerabilities

9.1.1 Improper Input validation

Input validation is used to ensure that the content provided to an application does not grant an attacker access to unintended functionality or privilege escalation. Some of the common input validation vulnerabilities are:

Buffer overflow

Buffer overflows result when a program tries to write more data into a buffer than the space allocated in memory. The “extra” data then overwrite adjacent memory and ultimately result in abnormal operation of the program. A careful and successful memory overwrite can cause the program to begin execution of actual code submitted by the attacker. Most exploit code allows the attacker to create an interactive session and send commands with the privileges of the program with the buffer

overflow. When network protocols have been implemented without validating the input values, these protocols can be vulnerable to buffer overflow attacks

Lack of Bounds Checking

The lack of input validation for values that are expected to be in a certain range, such as array index values, can cause unexpected behaviour. For instance, unvalidated input, negative, or too large numbers can be input for array access and cause essential services to crash

Command Injection

Command injection allows for the execution of arbitrary commands and code by the attacker. If a malicious user injects a character (such as a semi-colon) that delimits the end of one command and the beginning of another, it may be possible to then insert an entirely new and unrelated command that was not intended to be executed. Two types of command injection commonly found are OS command injection and Structured Query Language (SQL) injection

Cross-Site Scripting

Cross-site scripting vulnerabilities allow attackers to inject code into the web pages generated by the vulnerable web application. Attack code is executed on the client with the privileges of the web server. An attacker is able to inject malicious script into a link and have a website return it to the victim as though it is legitimate. The victim's web browser will then run the malicious script, because it came from the server, potentially compromising the victim's computer by using one of many browser exploits

Improper Limitation of a Pathname to a Restricted Directory (Path Traversal)

Directory traversal vulnerabilities occur when file paths are not validated. Directory traversals are commonly associated with web applications, but all types of applications can have this class of vulnerability. Directory traversals occur when the software uses external input to construct a pathname that is intended to identify a file or directory that is located underneath a restricted parent directory. However, the software does not properly neutralize special elements within the pathname that can cause the pathname to resolve to a location that is outside of the restricted directory

9.1.2 Poor Code Quality

Poor code quality refers to code issues that are not necessarily vulnerabilities but indicate that it was not carefully developed or maintained. These products are more likely to contain vulnerabilities than those that were developed using secure development concepts and other good programming practices.

Use of Potentially Dangerous Functions

Otherwise known as unsafe function calls, the application calls a potentially dangerous function that could introduce vulnerability if used incorrectly

NULL Pointer Dereference

A NULL pointer dereference occurs when the application dereferences a pointer that it expects to be valid, but is NULL, typically causing a crash or exit. NULL pointer dereference issues can occur through a number of flaws, including race conditions, and simple programming omissions

9.1.3 Improper Permissions, Privileges, and Access Controls

Permissions, privileges, and other security features are used to perform access controls on computer systems. Missing or weak access controls can be exploited by attackers to gain unauthorized access.

Improper Access Control (Authorization)

If the software does not perform or incorrectly performs access control checks across all potential execution paths, users are able to access data or perform actions that they should not be allowed to perform.

Execution with Unnecessary Privileges

Services are restricted to the user rights granted through the user account associated with them. Exploitation of any service could allow an attacker a foothold on the network with the exploited service's permissions. Privilege escalation can be accomplished by exploiting a vulnerable service running with more privileges than the attacker has currently obtained. If successfully exploited, services running as a privileged user would allow full access to the exploited host.

9.1.4 Improper Authentication

Many vulnerabilities identified in IoT products are due to the software failing to sufficiently verify a claim to have a given identity.

Authentication Bypass Issues

The software does not properly perform authentication, allowing it to be bypassed through various methods

Missing Authentication for Critical Function

The software does not perform any authentication for functionality that requires a provable user identity or consumes a significant amount of resources. Many critical IoT functions do not require authentication.

Client-Side Enforcement of Server-Side Security

Applications that authenticate users locally trust the client that is connecting to a server to perform the authentication. Because the information needed to authenticate is stored on the client side, a moderately skilled hacker may easily extract that information or modify the client to not require authentication.

Channel Accessible by Non-endpoint (Man-In-The-Middle)

Commands from the HMI cause actions in the IoT system. Alarms are sent to the HMI that notify operators of triggered events. The integrity and timely delivery of alarms and commands are critical in an IoT. MitM is possible if the system does not adequately verify the identity of actors at both ends of a communication channel or does not adequately ensure the integrity of the channel, in a way that allows the channel to be accessed or influenced by an actor that is not an endpoint.

9.1.5 Insufficient Verification of Data Authenticity

If IoT protocols and software do not sufficiently verify the origin or authenticity of data, it may accept invalid data. This is a serious risk for systems that rely on data integrity.

Cross-Site Request Forgery

When a web server is designed to receive a request from a client without any mechanism for verifying that it was intentionally sent, then it might be possible for an attacker to trick a client into making an unintentional request to the web server that will be treated as an authentic request.

Missing Support for Integrity Check

Many IoT transmission protocols do not include a mechanism for verifying the integrity of the data during transmission. If integrity check values or "checksums" are omitted from a protocol, there is no way of determining if data have been corrupted in transmission. The lack of checksum functionality in a protocol removes the first application-level check of data that can be used.

Download of Code without Integrity Check

If a component downloads source code or an executable from the network and executes the code without sufficiently verifying the origin and integrity of the code, an attacker may be able to execute malicious code by compromising the host server, spoofing an authorized server, or modifying the code in transit

9.1.6 Cryptographic Issues

Missing Encryption of Sensitive Data

Credentials sent across the network in clear text leave the system at risk to the unauthorized use of a legitimate user's credentials. If attackers are able to capture usernames and passwords, they will be able to log onto the system with that user's privileges

Use of a Broken or Risky Cryptographic Algorithm

Some standard IT encryption protocols used in systems were exploited due to encryption weaknesses. Use of such protocols will result in loss of sensitive data.

9.1.7 Weak Credentials Management

Insufficiently Protected Credentials

Credentials sent across the network in clear text leave the system at risk to the unauthorized use of a legitimate user's credentials. Network sniffing tools, many of which are freely downloadable, can be used to view this type of network traffic. If attackers are able to capture usernames and passwords, they will be able to log onto the system with that user's privileges

Use of Hard-Coded Credentials

Hard-coded credentials found in code and configuration scripts for authentication between components can prove to be a major vulnerability

9.2 Network vulnerabilities

The network architecture needs to be securely designed and implemented to allow remote control and monitoring of a process and provide process data for business functions while preventing any other traffic from entering or leaving the control network.

9.2.1 Network Design Weaknesses

The network infrastructure environment within the IoT has often been developed and modified based on business and operational requirements, with little consideration for the potential security impacts of the changes. Over time, security gaps may have been inadvertently introduced within particular portions of the infrastructure. Without remediation, these gaps may represent backdoors into the system

No Security Perimeter Defined

If the control network does not have a security perimeter clearly defined, then it is not possible to ensure that the necessary security controls are deployed and configured properly. This can lead to unauthorized access to systems and data as well as other problem

Lack of Network Segmentation

Minimal or no security zones allow vulnerabilities and exploitations to gain immediate full control of the systems, which could cause high-level consequences

Lack of Functional DMZs

The use of several DMZs provides the added capability to separate functionalities and access privileges and has proved to be very effective in protecting large architectures composed of networks with different operational mandates

Firewalls Non-existent or Improperly Configured

A lack of properly configured firewalls could permit unnecessary data to pass between networks such as control and corporate networks. This could cause several problems, including allowing attacks and malware to spread between networks, making sensitive data susceptible to monitoring/eavesdropping on the other network, and providing individuals with unauthorized access to systems.

9.2.2 Weak Firewall Rules

Firewall rules are the implementation of the network design. Enforcement of network access permissions and allowed message types and content is executed by firewall rules.

Access to Specific Ports on Host Not Restricted to Required IP Addresses

Detailed findings under this common vulnerability involve firewall rules restricting access to specific ports, but not IP addresses. A common finding was that network device access control lists did not restrict management access to the required IP addresses.

Firewall Rules Are Not Tailored to the Traffic

IoT network administrators should restrict communications to only that necessary for system functionality. System traffic should be monitored, and rules should be developed that allow only necessary access. Any exceptions created in the firewall rule set should be as specific as possible, including host, protocol, and port information

9.2.3 Network Component Configuration (Implementation) Vulnerabilities

Network Devices Not Securely Configured

A common finding was that network device access control lists did not restrict management access to the required IP addresses. Network devices were also found that were configured to allow remote management over clear-text authentication protocols. Without these restrictions, an attacker can gain control by changing the network device configurations

Port Security Not Implemented on Network Equipment

A malicious user who has physical access to an unsecured port on a network switch could plug into the network behind the firewall to defeat its incoming filtering protection

9.2.4 Improper Audit and Accountability

Network Architecture Not Well Understood

The implemented network architecture is not well understood by the different actors involved

Weak Enforcement of Remote Login Policies

Any connection into the IOT LAN is considered part of the perimeter. Often these perimeters are not well documented, and some connections are neglected.

Weak Control of Incoming and Outgoing Media

Media protections for IoT lack written and approved policies and procedures, lack control of incoming and outgoing media, and lack verification scans of all allowed media into the environment

9.3 Configuration vulnerabilities

9.3.1 Permissions, Privileges, and Access Controls

Poor System Access Controls

Within access controls, the following common vulnerabilities have been identified.

Lack of separation of duties through assigned access authorization.

Lack of lockout system enforcement for failed login attempts.

Terminated remote access sessions after a defined time period.

Open Network Shares on IoT Hosts

The storage of artefacts, such as source code and system configuration on a shared file system, provides significant potential for information mining by an attacker.

9.3.2 Improper Authentication

Poor System Identification/Authentication Controls

Some organizations have not developed policies or procedures to facilitate the implementation of identification and authentication controls, and do not uniquely identify and authenticate users and specific devices before establishing connections.

9.3.3 Poor Credentials Management

Insufficiently Protected Credentials

User credentials should be vigorously protected and made inaccessible to an attacker. Whenever credentials are passed in clear text, they are susceptible to being captured and then cracked if necessary, by the attacker.

Weak Passwords

Some applications are configured without passwords or weak ones, which means that anyone able to access these applications are guaranteed to be able to authenticate and interact with them.

9.3.4 Poor Security Configuration and Maintenance

Weak Testing Environments

Backup or test environments are necessary for testing patches before applying them on critical systems.

Limited Patch Management Abilities

Many organizations have no test facilities, so security changes must be implemented using the live operational systems.

Weak Backup and Restore Abilities

Backups, restores, and testing environments have been identified as a common issue within the industry for continuity of operations in the event of an incident. Backups are usually made, but usually not stored offsite and rarely exercised and tested.

9.3.5 Weak Planning/Policy/Procedures

Insufficient Security Documentation

A common security gap can be that the organization has not developed a formal business case for IoT security.

Poor Security Documentation Maintenance

Another common is that the organization does not develop, implement, disseminate, and periodically review/update policy and procedures to facilitate implementation of security planning controls.

9.3.6 Audit and Accountability issues

Lack of Security Audits/Assessments

Security audits are not regularly performed to determine the adequacy of security controls within their systems.

Lack of Logging or Poor Logging Practices

Event logging (applications, events, login activities, security attributes, etc.) is not turned on or monitored for identification of security issues. Where logs and other security sensors are installed, they may not be monitored on a Realtime basis, and therefore, security incidents may not be rapidly detected and countered.

10 Assumptions & Organizational Security Policies

10.1 Policies

The first set of assumptions refers to policies that generally target information security and aim at making it more concrete and robust. These should be adequate for the organisation's activity and must contain well documented information. In this context, the following security assumptions have been defined.

It is worth mentioning that when referring to security and privacy by design, the security measures should reflect the particularities and the context in which the IoT device or system will be deployed (for example, security by design will refer to different specifications when an IoT device at a home environment is considered, compared to the case of an IoT device in a critical infrastructure). As discussed, when it comes to IoT the cyber risk is context-dependent (i.e. based on the application scenario) and in this respect the security measures should be applied with this consideration in mind.

10.1.1 Security by design

- Consider the security of the whole IoT system from a consistent and holistic approach during its whole lifecycle across all levels of device/application design and development, integrating security throughout the development, manufacture, and deployment.
- Ensure the ability to integrate different security policies and techniques.
- Security must consider the risk posed to human safety.
- Designing for power conservation should not compromise security.
- Design architecture by compartments to encapsulate elements in case of attacks.

- For IoT hardware manufacturers and IoT software developers it is necessary to implement test plans to verify whether the product performs as it is expected. Penetration tests help to identify malformed input handling, authentication bypass attempts and overall security posture.
- For IoT software developers it is important to conduct code review during implementation as it helps to reduce bugs in a final version of a product.
- Equip, as deemed appropriate after a security and safety assessment, even the most basic connected devices holding very limited processing capabilities (e.g. actuators, converters) with identification and authentication features and ensure compatibility with IAM class solutions.
- Perform risk and threat analysis involving cybersecurity experts from the very early stages of the design process of the device to find out which security features will be necessary

10.1.2 Privacy by design

- Make privacy an integral part of the system.
- Perform privacy impact assessments before any new applications are launched. Conduct a Privacy Impact Analysis (PIA) for the data that will be processed by the device.
- Address privacy related issues based on applicable local and international regulations, such as the General Data Protection Regulation (GDPR)
- Define the scope of the data that will be processed by the device as well as the objective of this processing during the design phase, avoiding collecting or unnecessarily providing sensitive data.
- Establish a physical location of data storage and define between which organisations data will be transferred restricting access to collected personal data only to authorised individuals.
- Separate data that can be used to identify an individual from other information and ensure its security, e.g. through encryption of any personal data transferred within the IoT environment.
-

10.1.3 Asset management

- Establish and maintain asset management procedures and configuration controls for key network and information systems.
- Utilise tools supporting asset management that are able dynamically to discover, identify and enumerate assets specific to the organisation and industrial environment.
- Ensure that your company has a consistent and up-to-date asset inventory.
- In complex industrial environments with legacy systems, use passive monitoring devices wherever feasible or precede the implementation with a testing phase if you consider active monitoring tools.
- Consider secure administration of assets with management of the infrastructure and security devices via a dedicated management network.
- Introduce a new device into the system only according to an established, accepted and communicated change management process.
- Avoid the usage of removable devices disabling the USB ports if there is no accepted business requirement.

10.1.4 Risk and Threat Identification and Assessment

- Identify significant risks using a defence-in-depth approach.
- Identify the intended use and environment of a given IoT device.
- Establish risk and threat management process according to the individual needs and security requirements of your company.
- For critical infrastructures, establish a number of risk management areas completely aligned with corporate, safety and environmental sides. Assess and characterise threats, vulnerabilities and protection measures against those risk management areas.
- Perform risk analysis which includes cybersecurity aspects at least annually. Also, integrate it with other processes, such as change management, incident handling and vulnerability management. The risk assessment should cover technical and procedural testing of effectiveness of the security policies and process.
- Consider incorporating threat intelligence process within the threat management approach of your company relying on various sources of information and sharing information with trusted industry partners, ISACs and CERTs.
- From an organisational perspective, monitor selected threats and determine their impact on systems by performing a risk analysis.
- Regarding the Risk Management process, adopt two different approaches at the same time: top-down, addressing cybersecurity from the organisation-wide perspective, and bottom-up, providing a very granular and detailed view on the company's situation.
-

10.2 Organisational, People and Process measures

All businesses must have organisational criteria for information security. Their personnel practices need to promote good security, ensure the management of processes and safely operate 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 in the safety of the organisation, the organisation must be prepared (responsibilities, evaluation and response).

10.2.1 Endpoints lifecycle Support

- Focus on the security of software and hardware during every stage of the endpoint lifecycle.
- Take into account security considerations throughout the supply chain.
- Consider security aspects during the overall procurement process defining security measures and requirements tailored to particular devices/solutions.
- Conduct cybersecurity acceptance tests against technical specification during different validation activities or stages of the product lifecycle.
- During the handover phase of the project implementation process, properly build and transfer all cybersecurity documentation, processes and procedures.
- Develop an end-of-life strategy for IoT products.
- Disclose the duration and end-of-life security and patch support (beyond product warranty).
- Monitor the performance and patch known vulnerabilities up until the “end-of-support|” period of a product's lifecycle.

10.2.2 Security Architecture

- To ensure security in a computerised ecosystem, adopt a holistic architectural-based approach and develop a risk-aligned security architecture based on business requirements.
- While defining security architecture, ensure that it comprises all relevant security aspects – from organisational to physical implementation issues.
- Within the security architecture, allocate clear roles and responsibilities for security. Clearly define and communicate roles for both systems and security processes.
- Integrate compliance enforcement controls to the established Security Architecture and ensure that all products meet the requirements defined within it.
- Use proven solutions, i.e. well-known communications protocols and cryptographic algorithms, recognized by the scientific community, etc. Certain proprietary solutions, such as custom cryptographic algorithms, should be avoided.

10.2.3 Management of security vulnerabilities and/or incidents

- Establish procedures for analysing and handling security incidents.
- Define a comprehensive vulnerability management process within the organisation that covers utilisation of automatic and manual tools resulting from risk analysis.
- Define cyber incidents relevant for your area and range of operation and classify them according to applicable standards.
- Consider creation of a Cybersecurity Operations Centre (SOC) with cybersecurity specialists to support cybersecurity incidents dividing them into specific lines of support with appropriate roles and responsibilities.
- Establish a process for incidents handling that consists of identification of affected assets, identification and classification of vulnerabilities, escalation and notification.
- Detect and investigate promptly every unusual security related event.
- Coordinated disclosure of vulnerabilities.
- While eliminating vulnerabilities, begin from the most critical ones taking into account criticality of assets and systems.
- Conduct penetration tests of new IoT solutions in a controlled environment or before / during commissioning phase, and also regularly and after an important update of the system.
- Participate in information-sharing platforms to report vulnerabilities and receive timely and critical information about current cyber threats and vulnerabilities from public and private partners.

10.2.4 Human Resources Security Training and Awareness

- Ensure the personnel practices promote privacy and security – train employees in good privacy and security practices.
- Document and monitor the privacy and security training activities.
- 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.
- Ensure that security training is continuous, regular and frequently updated.

10.2.5 Third-Party relationships

1. Data processed by a third-party must be protected by a data processing agreement.
2. Only share consumers' personal data with third parties with express consent of the consumers, unless otherwise required and limited for the use of product features or service operations.
3. Strictly control access of third parties to a control or production layer only granting access on demand, in a specified time window, for a specific purpose, and in a least privileged way.
4. Do not provide a direct connection for the vendor to a system in a control or production layer. Allow access only to the necessary selected functions and parts of the network.
5. Prompt suppliers for information on security of their processes and commitments to their product and develop dedicated security requirements for vendors and service providers
6. Clearly define all relevant aspects of the partnership with third parties, including security, within the appropriate agreements and contracts.
7. For IoT hardware manufacturers and IoT software developers it is necessary to adopt cyber supply chain risk management policies and to communicate cyber security requirements to its suppliers and partners.

10.2.6 Implementation Considerations

Vendors must include a solution for generating cryptographic quality random numbers in their products. Randomness is an important component in security protocols and without such randomness many of today's security protocols offer weak or no security protection. Hardware random-number generators, when feasible, should be utilized, but may be combined with other sources of randomness.

11 Security Goals & Security Requirements

Refer to ANNEX II for a full description of the security requirements.

The following is a list of Security Goals covering the common threats identified above.

Since these are horizontal security goals across vertical sectors, given the particularities of each vertical, more concrete security goals can be introduced for each vertical on the Security Profile level.

Applying these Security Goals should consider the particularities of the IoT ecosystem such as 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.

Security Goals	Description	Security Requirements	Ref
Integrity of data (DIU)	Ensure that the data being processed does not undergo malicious changes.	Use protocols and mechanisms able to represent and manage trust and trust relationships	EIA_SF.1
		Control the installation & update of software in operating systems.	EIA_SF.2
		Secure Boot	EIA_SF.3

		Roll-back to a secure state (Ensure that the system can return to a secure state after any malicious update or modification)	EIA_SF.4
		Sign code cryptographically to ensure it has not been tampered with after signing it as safe for the device	EIA_SF.5
		implement run-time protection & secure execution	EIA_SF.6
Confidentiality of data (DIU)	Ensure that data is not read when in motion	Data encryption during processing.	EIA_SF.7
		Code obfuscation	EIA_SF.8
		Generic Error messages	EIA_SF.9
Identification and Authentication	Ensure the legitimacy of the applicant for access to the product (user and / or machine)	Authenticate all users before performing any sensitive actions.	EIA_SF.10
		Enforce strong passwords (length, complexity (uppercase, numbers, symbols), etc.	EIA_SF.11
		Multi-factor authentication (knowledge factor, possession factor, location factor, time factor, inheritance factor)	EIA_SF.12
		Management of authentication failure	EIA_SF.13
		Robust password recovery and reset mechanism.	EIA_SF.14
		Limiting the number of authentication attempts	EIA_SF.15
		Mandatory change of default password & username at first-login	EIA_SF.16
		Authenticate All Devices	EIA_SF.17
		Uniqueness of the identifier	EIA_SF.18
		Secure pairing	EIA_SF.19
Access Control	Ensure that information is accessible only to those whose appropriate access is permitted.	Enforce Disconnection of inactive connection/user session.	EIA_SF.20
		Access Control Policy is enforced	EIA_SF.21
		Ensure a context-based security	EIA_SF.22

		Tamper Detection	EIA_SF.23
		Tamper Protection	EIA_SF.24
		Tamper detection and reaction should not rely on network connectivity	EIA_SF.25
		Ensure device cannot be easily disassembled	EIA_SF.26
		Data storage medium is encrypted	EIA_SF.27
		Device only feature essential physical external ports (such as USB) necessary for it to function	EIA_SF.28
		Test/Debug modes are secure	EIA_SF.29
Authorization	Ensure that only authorized processes can process data	Limit allowed actions by implementing authorization mechanism	EIA_SF.30
		Use principle of least privilege (POLP)	EIA_SF.31
		Isolate privileged code, processes and data from portions of the firmware that do not need access to them.	EIA_SF.32
		Authorize all devices before establishing connection	EIA_SF.33
Availability of data	Ensure that data continues to be available at the required level of performance in situations ranging from normal to "disastrous".	Resistance to Perturbation	EIA_SF.34
		Presence of an alarm system	EIA_SF.35
		Enforce Network Throttling/Rate Limiting	EIA_SF.36
		Reliable Communication protocols (Example: TCP: guarantee the non-loss of data, UDP: possibility of data loss)	EIA_SF.37
Confidentiality of stored data (DAR)	Ensure that stored data cannot be read	Data Encryption during storage	EIA_SF.38
integrity stored data (DAR)	Ensure that stored data cannot be modified	Hash of the stored data and its verification	EIA_SF.39
		Integrity controller (check the integrity of the data and detect any malicious changes)	EIA_SF.40
	Ensure key management and the check	Encryption or Verification of data	EIA_SF.41
		Signing & Verification of digital signature	EIA_SF.42

Strong cryptography	cryptography (quality) resistance.	Generation of Cryptographic message integrity code	EIA_SF.43
		Secure Hashing	EIA_SF.44
		Encryption & Verification of Cryptographic Keys	EIA_SF.45
		Disable Insecure Algorithms	EIA_SF.46
		Support a strong RNG	EIA_SF.47
Privacy	Ensure that the user's personal information is protected and that he can use a resource or service without revealing his user identity.	Anonymity (Ensures that a user can use a resource or service without revealing their identity.)	EIA_SF.48
		Nickname anonymity	EIA_SF.49
		Unlikability (ensures that a user can use resources or services multiple times without others being able to link these uses)	EIA_SF.50
		Non-observability (ensures that a user can use a resource or service without others, particularly third parties, being able to see that the resource or service is in use.)	EIA_SF.51
		Deleting temporary data (ensuring that destroyed information will no longer be accessible and newly created objects do not contain information that should not be accessible.)	EIA_SF.52
Physical security	Protect the assets against physical attacks	Protection of external and internal interfaces against disturbances.	EIA_SF.53
		Debug port protection	EIA_SF.54
		HW-based immutable root of trust	EIA_SF.55
		Use a Restricted Operating Environment (Use hardware that incorporates security features to strengthen the protection and integrity of the device – for example, specialised security chips / coprocessors that integrate security at the transistor level, embedded in the processor,	EIA_SF.56

		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. Protection against local and physical attacks can be covered via functional security)	
Secure & Trusted communication	Ensure that the object sends the data to protect it from reading, modification (cryptography) or loss (secure protocols).	Encryption of the data to be transmitted	EIA_SF.57
		Ensure that communication security is provided using state-of-the-art, standardised transport layer security protocols like IPsec, TLS, etc.	EIA_SF.58
		Communications access control (firewall, access list, etc.)	EIA_SF.59
	→ integrity, confidentiality and reliability of transmitted data)	Ensure credentials are not exposed in internal or external network traffic	EIA_SF.60
		Adopt Restrictive approach rather than permissive in communicating	EIA_SF.61
		Prevent unauthorized connections at all levels of the protocols	EIA_SF.62
Security audit & Monitoring	Diagnose or check the security status of the object or to determine whether there has been a breach of security and possibly what resources are being compromised. It is also intended to detect and examine events that may pose a threat to the safety of the environment.	Detection intrusion	EIA_SF.63
		Detection of replay	EIA_SF.64
		Logging sensitive events (user authentication, management of accounts and access rights, modifications to security rules, and the functioning of the system.	EIA_SF.65
		Review of the audit log. Logs must retrievable only via authenticated connections.	EIA_SF.66
		Storage of the audit log	EIA_SF.67
	Provide data management and	Integrity and confidentiality of security data	EIA_SF.68

Secure Data Management	security functions (administration and protection of security data)	Administration of security features and data	EIA_SF.69
Non-repudiation	Make sure the product cannot deny having sent or received data.	Digital signature	EIA_SF.70
		Logging	EIA_SF.71
Safety	Ensure the safety of human in the operational environment	System and Operational disruption	EIA_SF.72
		Self-diagnosis and Self-repair/healing to recover from failure, malfunction or a compromised stated	EIA_SF.73
		Standalone Operation Enforced – essential features should continue to work with a loss of communications and chronicle negative impacts from compromised devices or cloud-based systems.	EIA_SF.74
Secure Software / Firmware updates	Ensure that the device software/firmware, its configuration and its applications have the ability to update Over-The-Air (OTA) securely	Update file is transmitted via a secure connection	EIA_SF.75
		Update file shall not contain sensitive data (e.g. hardcoded credentials)	EIA_SF.76
		Update file is signed by an authorised trust entity	EIA_SF.77
		Update file encrypted using accepted encryption methods	EIA_SF.78
		Signature and Certificate verified by the device before the update process begins	EIA_SF.79
		Updates Firmware Automatically	EIA_SF.80
		Non-disruptive updates	EIA_SF.81
		Avoid provisioning the same secret key in an entire product family	EIA_SF.82
Secure Interfaces and Network Services		Ensure only necessary ports are exposed and available	EIA_SF.83
		Ensure Web Interfaces fully encrypt the user session, from the device to the backend services, and that they are not susceptible to XSS, CSRF, SQL Injection, etc.	EIA_SF.84
		Secure input and output handling	EIA_SF.85

		Data input validation (prior to use) and output filtering	EIA_SF.86
Strong default security and privacy		Any applicable security features should be enabled by default	EIA_SF.87
		Any unused or insecure functionalities should be disabled by default	EIA_SF.88
Data protection and compliance		Personal data must be collected and processed fairly and lawfully	EIA_SF.89
		Make sure that personal data is used for the specified purposes for which they were collected	EIA_SF.90
		Minimise the data collected and retained	EIA_SF.91
		IoT stakeholders must be compliant with the EU General Data Protection Regulation (GDPR)	EIA_SF.92
		Users of IoT products and services must be able to exercise their rights to information, access, erasure, rectification, data portability, restriction of processing, objection to processing, and their right not to be evaluated based on automated processing	EIA_SF.93

Table 1: Common list of Security Goals & Requirements

12 How To Create a Security Profile

12.1 Security Profile Properties

12.1.1 Owner

Security Experts⁶ in the relevant technical field and the proposed risk-based methodology are intended to create Security Profiles which must be validated first by Technical Working Groups⁷ composed of Vendors developing a type of IoT device for one or more IoT market vertical. Finally, the Certification Scheme Owner must endorse the newly created Security Profile.

12.1.2 Timeline

The estimated effort and time required to follow the 3 steps described below is of 5 to 10 working days including the validation period. Note that automated tools could be used to accelerate the process and guarantee the most objective results.

12.1.3 Validity

Once a Security Profile has been created and validated by this Scheme, it will become the “only” Security Profile that is used by Vendors for certifying a claimed type of ToE.

⁶ Security Experts/Companies/CABs capable of generating compliant Security Profiles must receive a dedicated training from Eurosmart and successfully pass a knowledge test.

⁷ Note that Technical Working Groups may not be involved during the creation for the Security Profile.

A Security Profile must be reviewed every year or exceptionally when the Certification Scheme Owner decides to update it for various reasons (e.g. new vulnerability, update of the GPP, etc.)

12.2 A 3 steps approach (1 COLLECT → 2 DEFINE → 3 DECIDE)

The main input of this 3 steps approach is the GPP (this document) which contains the list of common assets, security threats, security vulnerabilities, generic assumptions and Organizational Security Policies and the common set of security goals and security requirements.

- **Step 1 (COLLECT)** will identify the list of threats (e.g. subpart of the common threats) relevant to the ToE
- **Step 2 (DEFINE)** will measure the severity of impacts and the likelihood of the identified threats on the IoT device in order to measure the security risks. Will define the list of potential security assurance activities that are mapped to impacts and likelihoods.
- **Step 3 (DECIDE)** will extract and decide the relevant list of security requirements and security assurance activities to the ToE based on the security risks qualification (accept, avoid, reduce or transfer).

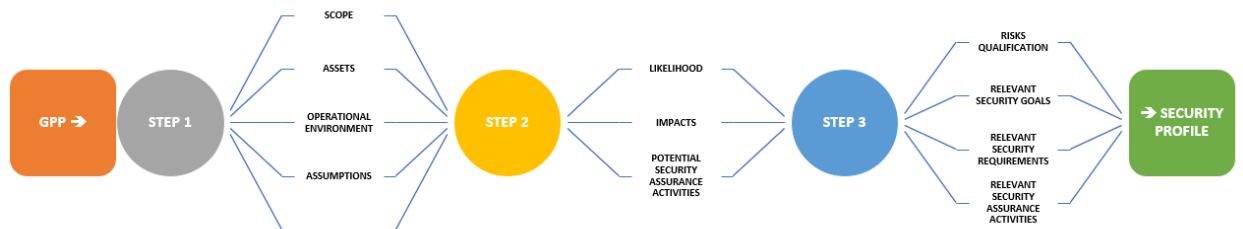


Figure 7: From GPP to a Security Profile

12.3 Risk-Based Methodology

The goal of the following security risk analysis methodology is to simplify the process of identifying risk. We look at threats adapted to the IoT typical infrastructure presented in Section 1.1.2 on a high-level of abstraction and from different perspectives, in order to maximize the number of potential threats on the IoT Device.

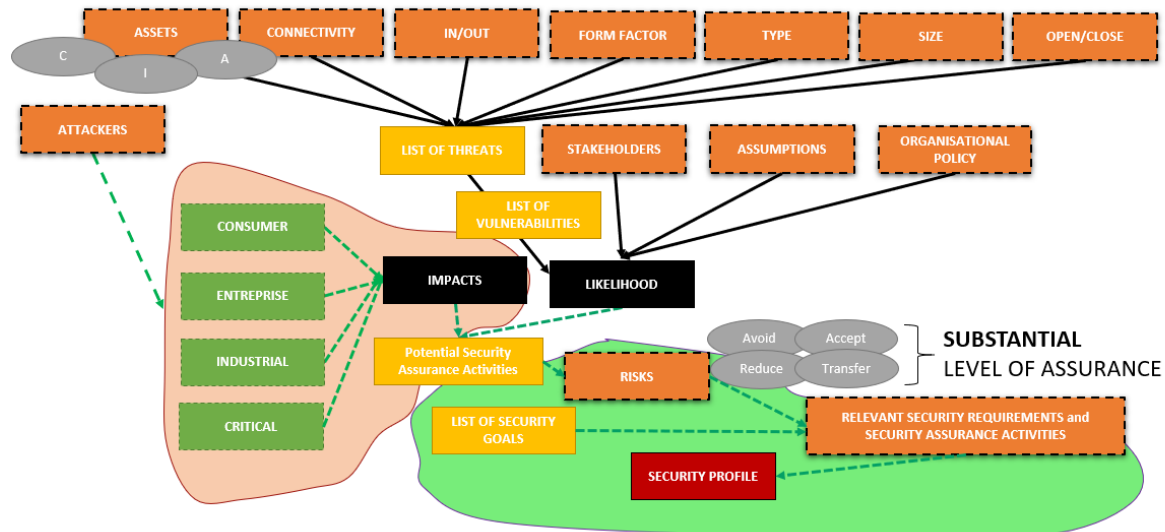


Figure 8: IoT Risk-Based Assessment Methodology

The chosen method is a hybrid risk analysis approach covering both quantitative and qualitative techniques. Indeed, quantitative evaluation is used for tangible assets when applicable (e.g. monetary data, human, ...) and qualitative evaluation is used for intangible assets when applicable (e.g. cryptographic keys where we do not assign numbers and monetary values to assets but instead assign properties to protect each asset against).

12.3.1 A Simplified Process

An experienced technical working group and security experts walk through different scenarios of possible risks and rank their likelihood and impact severity in addition to the validity of each security requirement based on opinions. This includes judgment, best practices, intuition, and experience.

This scheme strongly recommends the use of adapted questionnaires with workshops or meetings involving both the risk-owners and technical/security experts.

At the end of these 3 steps, the Security Profile is compiled into a standard format⁸ and presented to the Scheme owner.

Only by reassessing the risks on a periodic basis (e.g. every 2 years) can a Security Profile be trusted. If the risk has not changed, and the security requirements are still efficient, then the risk is being properly mitigated.

Vulnerability analysis and continued asset identification and valuation are also important tasks of risk management monitoring and performance.

12.3.2 STEP 1 - COLLECT

It all starts with an identification of the ToE, the assets to protect in Confidentiality, Integrity and Availability, with the specifics of the data flows between the various devices/Things and Mobile Application for instance and between the devices and the IoT Server.

⁸ Most likely into a Excel Spreadsheet

12.3.2.1 Assets

Definition of the primary and secondary assets relevant to the ToE. The primary assets could be a refinement of the type of assets defined in Section 7.

The protection properties (C,I,A) of these depends on the type of data that the ToE is processing (Move/Impact, Location, Luminosity, Temperature, Weight, Depth, Pressure, Button, Humidity, etc.), and its sensitivity within the operational environment.

12.3.2.2 Connectivity

The network protocol supported (Sigfox, Lte-M, Lora, Nb-IoT, Wifi, BLE, Zigbee, GSM, 433Mhz, etc.)

The type of connectivity to internet (e.g. through Gateway/box/router, a Smartphone, Autonomous).

12.3.2.3 In/out

The ToE is located indoor or outdoor or could be flexible/mobile (indoor and outdoor).

12.3.2.4 Form Factor

A physical description of the IoT device. It might provide some tamper-proof or resistance or maybe none.

12.3.2.5 Type

This is a refinement of the ToE parts as defined in Section 3.

12.3.2.6 Size

The size of the ToE (lines of code, interfaces, etc.)

12.3.2.7 Open/Close

The ToE could allow to update its firmware after issuance or not. This includes the maintenance requirements.

12.3.2.8 Costs

This must provide a summary of the generic costs of the product, design/planning, Implementation, testing, repair, replacement update, operating and support, subscription, monitoring and responding to alerts, etc.

12.3.2.9 List of Threats

A threat is any potential danger that is associated with the exploitation of a vulnerability. Attackers take advantage of a vulnerability to compromise assets.

Based on the inputs listed above, the methodology continues with an analysis of potential security threats on the ToE by considering the list of common threats defined in Section 8.

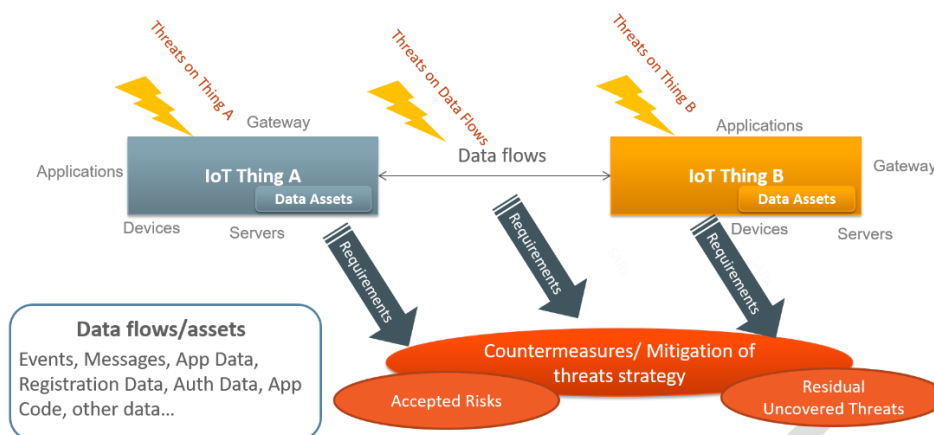


Figure 9: High-Level representation of the IoT Security Risk Analysis

12.3.2.10 Stakeholders

The different stakeholders involved in the ToE life-cycle (Users, Service Providers, Network Operator, Administrator, etc.)

12.3.2.11 Assumptions

The assumptions that are made on the operational environment in order to be able to provide security functionality. If the ToE is placed in an operational environment that does not meet these assumptions, the ToE may not be able to provide all of its security functionality anymore. Assumptions can be on physical, personnel and connectivity of the operational environment.

12.3.2.12 Organisational Security Policy

This is a set of security rules, procedures, or guidelines for an organisation. A policy may pertain to a specific operational environment.

12.3.2.13 List of Vulnerabilities

These are suspected common weaknesses in the ToE that can be used to conduct a security threat.

It can be a software, hardware, procedural, or human weakness that can be exploited. It may be a unpatched application or OS, an unrestricted wireless access point, an open port, a lax physical security that allows anyone to enter a secure area, or unenforced password management on an IoT device.

The common vulnerabilities are defined in Section 9.

12.3.3 STEP 2 - DEFINE

12.3.3.1 Likelihood

This is an estimate of the feasibility or probability that a security threat will occur, according to the scale defined hereafter.

4 - Almost Certain
3 - Very Likely
2 - Likely

1 - Unlikely

Evaluating the overall likelihood of the scenario, based on general considerations relative to the source of risk (motivations, resources, determination and capacity/competence) and the security of supporting assets targeted in the scenario (exposure, vulnerabilities).



Table 2: Likelihood Calculation in 3 steps

In this approach (based on [ISO/IEC 27005:2018], [BSI-St2003], [NIST-SP800-82], [EBIOS-RM]⁹), the security expert can estimate the likelihood level of the attack while scoring its probability of success and its technical difficulty and deduce by crossing the likelihood of the scenario according to the standard matrix presented hereafter:

3 → LIKELIHOOD		3 → Technical Difficulty			
		1 – Low	2 - Moderate	3 - High	4 - Very High
2 → Probability of Success	4 - Almost Certain	4	3	2	1
	3 – Very High	3	3	2	1
	2 - Significant	2	2	2	1
	1 - Low	1	1	1	1

Table 3: Likelihood Table of Calculation

- A. First, we prepare an attacker's threat model graph. This consist of drawing the attack path scenarios through the following four steps:
1. Identify (e.g. Social engineering, Remote Access, etc.),
 2. Access (e.g. Intrusion via Wi-Fi, LAN port, etc.),
 3. Discover (e.g. Sniffing the communication, etc).

⁹ According to EBIOS, there are three approaches to choose the threat operational scenario. They are Express method, Standard method and Advanced method. You can find more details on these methods and other methods in [INFORMATIVE ANNEXES].

4. Exploit (e.g. Injecting incorrect data, read of secure cryptographic keys, etc.)
- B. Then we proceed to the evaluation of the threat's likelihood. These all depends upon the chances of the threat agent to attain its objective (i.e. to attack).

You will first rate each step of the operational attack scenario according to an index of probability of success seen from the attacker's perspective. The following scale is adopted, the percentages are mentioned as an indication to facilitate the listing.

Probability of Success (for each step of the attack scenario)	%
4 - Almost Certain	> 90%
3 - Very High	> 60%
2 - Significant	> 20%
1 - Low	< 20%

Table 4: Probability of Success Calculation

For instance, if an IoT device have several ports open, there is a higher likelihood that an attacker will use one to access the network in an unauthorised way. If the IoT device does not have a secure firmware update feature, there is a higher likelihood an attack will exploit the vulnerable firmware and compromise assets.

- C. Once you score in the previous step each action according to a probability index of success, you can evaluate the overall index of probability of success scenario by applying the following rule:

$$\text{Index_Pr (AEn)} = \text{Min} \{ \text{Index_Pr(AEn)}, \text{Max}(\text{Index_Pr(AEn-1)}_{\text{cumulative intermediate}}) \}$$

The principle is to progress in a procedure by evaluating step by step each step action "AEn" of a node "n", an intermediate cumulative probability index from a step index of "AEn". And intermediate cumulative indexes of the previous node "n-1".

- D. Then you will rate the technical difficulty of achieving each step of the attack, from the point of view of the attacker. It allows to estimate the resources that the attacker will have to engage to carry out his action and increase his chances of successfully exploiting a vulnerability. It may occur that several types of expertise are required. Also taking in to account the security of the ToE. In fact, this method allows to consider the return on investment for the attacker and therefore to build a strategy of risk management driven by a logic of discouragement.

The following scale of difficulties depends on the resources (time, expertise, knowledge and equipment) required to conduct an attack.

Technical Difficulty (for each step of the attack scenario)	Description
4 - Very High	Attacker use very important resources to achieve a successful attack (e.g. Expert knowledge or specialized equipment), >= one week)
3 - High	Attacker use important resources to achieve a successful attack (e.g. Specific knowledge or equipment is required, <= one week)

2 - Moderate	Attacker use moderate resources to achieve a successful attack (e.g. Generic knowledge or equipment is required, <= one day)
1 - Low	Attacker use low resources to achieve a successful attack (e.g. No specific knowledge or equipment is required, <= one hour)

Table 5: Technical Difficulty Calculation

- E. The rating criteria "technical difficulty and probability of success" are not rigorously independent. However, the "technical difficulty" is more particularly related to the level of protection of the ToE (its exposure and its vulnerabilities), while "probability of success is more influenced by its level of defence and Resilience (Supervisory, Incident Response and Continuity capabilities of activity).

$$\text{Index_Diff (AEn)} = \text{Max} \{ \text{Index_Diff(AEn)}, \text{Min}(\text{Index_Diff(AEn-1)}_{\text{cumulative intermediate}}) \}$$

- F. Finally, the global likelihood is calculated as the Maximum of all attack scenarios likelihood. Hereafter is a sample of calculation:

	Probability of success	Technical Difficulty	Likelihood
Scenario1	1	3	1
Scenario2	0	2	1
Scenario3	2	3	2
Global Likelihood			2 Likely

Table 6: Global Likelihood Calculation

12.3.3.2 Impacts

This is the magnitude of harm expected to result from a security threat. The severity of an impact could be expressed as follows:

- Level of impact for various threats on the evaluated item's attributes (Privacy, Confidentiality, Integrity, Availability, Authenticity)
- Level of impact on other factors, external to the evaluated item (such as impact on persons, environment, as well as financial and reputational impact for the organization)
- Scale of impact, depending on, a. o. number of people affected, time to recovery, cascading effects, etc.

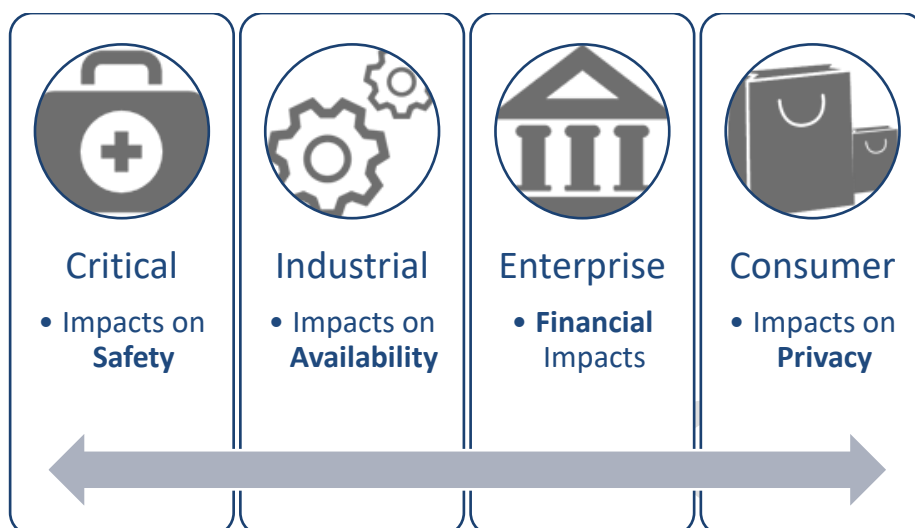


Figure 10: Impacts & Operational Environments

. Hereafter we present a comprehensive representation of the impact levels.

IMPACT LEVEL	PRIVACY	CONFIDENTIALITY	INTEGRITY	AVAILABILITY	AUTHENTICITY	SAFETY	REPUTATION & FINANCIAL LOSS	SCALE
Severe	Disclosure of sensitive personal data (GDPR special category ¹⁰).	Disclosure of high value information, trade secrets, IP, mission critical data, master-keys etc.	Complete change in normal System functioning	Prolonged interruption of operations. (Estimated days/Weeks)	Impersonation or cheating the verification	Serious injury to an individual(s); & real danger to life. Major pollution/damage with long-term environmental consequences	The financial loss is significant (Greater than _____% annual revenue loss). Threat to business existence Reputation is irrevocably destroyed or damaged.	International-Wide Scale
Moderate	Disclosure of personal data (according to GDPR ¹¹) which CAN be processed or aggregated to uniquely identify consumers.	Disclosure of privileged information Access credentials/ configuration data etc.	Alteration of some system functionality and features/output	Short-term Interruption in operations. (Estimated hours/Days)	Impossible to verify authenticity	Temporary recoverable impairment of health. Significant pollution/damage to environment	The financial loss is considerable, (Between _____to_____% annual revenue loss) Reputation is damaged, time, effort & resources required to recover.	Automated & Repeatable but not scalable

¹⁰Special data category in GDPR: data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation

¹¹ 'personal data' in GDPR means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Minor	Disclosure of personal data which, with aggregation or processing, is unlikely to reveal unique consumer's identity.	Disclosure of information for internal use. No specific impact on its disclosure	Minor/Unnoticeable effect on system behavior/output	Brief Interruption in operations. (Estimated in secs/mins/hours)	Difficult to verify authenticity	No loss or significant threat to health/life Limited/temporary pollution	The financial loss is acceptable (Less than _____% yearly revenue loss) Reputation is minimally affected; little or no effort or expense is required to recover	Local to the system but not scalable
Low	No impact on possible disclosure of data	No impact on possible disclosure of information	No effect on system behavior/output	Availability is possibly not impacted	Authenticity is possibly not impacted	People or environment are possibly not harmed	Reputation and financial loss not possibly impacted	Local to one device but not scalable

Table 7: Impact Calculation - Reference Table

Depending on the Operational Environment (Consumer, Enterprise, Industrial, Critical), the severity of impacts varies in priority. In addition, the quantified parameters must be adapted by the Risk-Owner according to the use case under evaluation.

Each threat could have a low, minor, moderate or high impact on each of the properties shown above and the overall impact is equal to the Maximum of the impact property that is more important in the Operational Environment (Privacy in CONSUMER, Financial in ENTREPRISE, Availability in INDUSTRIAL and Safety in CRITICAL).

This step of the process helps in taking the right decision when deciding on what risks to mitigate or accept in the next step.

IMPACT VS LIKELIHOOD	UNLIKELY (1)	LIKELY (2)	VERY LIKELY (3)	ALMOST CERTAIN (4)
SEVERE (4)				
MODERATE (3)				
MINOR (2)				
LOW (1)				

Table 8: Risk Calculation Table (Impact vs Likelihood)

12.3.3.3 Potential Security Assurance Activities (pSAA)

The security assurance activities will determine according to the impact and the likelihood of a specific identified threat, how the device should be tested against. This approach is based on a list of testing methods such as "Source code review" and "Vulnerability Scanning" that are part of two global activities: Conformity and Vulnerability analysis.

This list is determined by referring to the mapping table between the impacts/likelihoods and the security assurance activities of the Figure below.

IMPACT VS LIKELIHOOD	UNLIKELY (1)	LIKELY (2)	VERY LIKELY (3)	ALMOST CERTAIN (4)
SEVERE (4)	CA.DocumentationReview CA.SourceCodeReview CA.CompositionAnalysis (if applicable) VA.VulnerabilityScanning	CA.DocumentationReview CA.SourceCodeReview CA.FunctionalSecurityTesting CA.CompositionAnalysis (if applicable) VA.VulnerabilityScanning VA.BasicRobustnessTesting	CA.DocumentationReview CA.SourceCodeReview CA.FunctionalSecurityTesting CA.CompositionAnalysis (if applicable) VA.VulnerabilityScanning VA.BasicRobustnessTesting VA.AdvancedRobustnessTesting VA.NonIntrusivePentesting	CA.DocumentationReview CA.SourceCodeReview CA.FunctionalSecurityTesting CA.CompositionAnalysis (if applicable) VA.VulnerabilityScanning VA.BasicRobustnessTesting VA.AdvancedRobustnessTesting VA.NonIntrusivePentesting VA.IntrusivePentesting
MODERATE (3)	CA.DocumentationReview CA.CompositionAnalysis (if applicable) VA.VulnerabilityScanning	CA.DocumentationReview CA.SourceCodeReview CA.CompositionAnalysis (if applicable) VA.VulnerabilityScanning VA.BasicRobustnessTesting	CA.DocumentationReview CA.SourceCodeReview CA.FunctionalSecurityTesting CA.CompositionAnalysis (if applicable) VA.VulnerabilityScanning VA.BasicRobustnessTesting VA.NonIntrusivePentesting	CA.DocumentationReview CA.SourceCodeReview CA.FunctionalSecurityTesting CA.CompositionAnalysis (if applicable) VA.VulnerabilityScanning VA.BasicRobustnessTesting VA.AdvancedRobustnessTesting VA.NonIntrusivePentesting
MINOR (2)	CA.DocumentationReview CA.CompositionAnalysis (if applicable)	CA.DocumentationReview CA.SourceCodeReview CA.CompositionAnalysis (if applicable)	CA.DocumentationReview CA.SourceCodeReview CA.CompositionAnalysis (if applicable) VA.VulnerabilityScanning VA.BasicRobustnessTesting	CA.DocumentationReview CA.SourceCodeReview CA.FunctionalSecurityTesting CA.CompositionAnalysis (if applicable) VA.VulnerabilityScanning VA.BasicRobustnessTesting
LOW (1)	CA.DocumentationReview CA.CompositionAnalysis (if applicable)	CA.DocumentationReview CA.CompositionAnalysis (if applicable)	CA.DocumentationReview CA.CompositionAnalysis (if applicable) VA.VulnerabilityScanning	CA.DocumentationReview CA.SourceCodeReview CA.CompositionAnalysis (if applicable) VA.VulnerabilityScanning

Figure 11: Potential Security Assurance Activities (pSAA) mapping with impacts/likelihood

Example: if a security threat (called **Threat1**) is determined with a **moderate impact** and an **unlikely likelihood**, the potential security assurance activities will be:

- Potential Security Assurance Activity 1 = **CA.DocumentationReview**,
- Potential Security Assurance Activity 2 = **CA.CompositionAnalysis**,
- Potential Security Assurance Activity 3 = **VA.VulnerabilityScanning**.

For more information about the definitions of each security assurance activity please refer to the **Error! Reference source not found.** document.

12.3.4 STEP 3 - DECIDE

The goal at this step is to perform a quick assessment of the threats, their impact and likelihood as described above, and to assign a security profile to mitigate the risks that the risk-owner would like to address.

12.3.4.1 Risks

A risk is the likelihood of an Attacker exploiting a vulnerability and the corresponding impact.

Depending on the selected list of threats agent involved, the attack that will be used, the vulnerability involved, and the impact of a successful exploit on the IoT device business application, security risk rating is qualified.

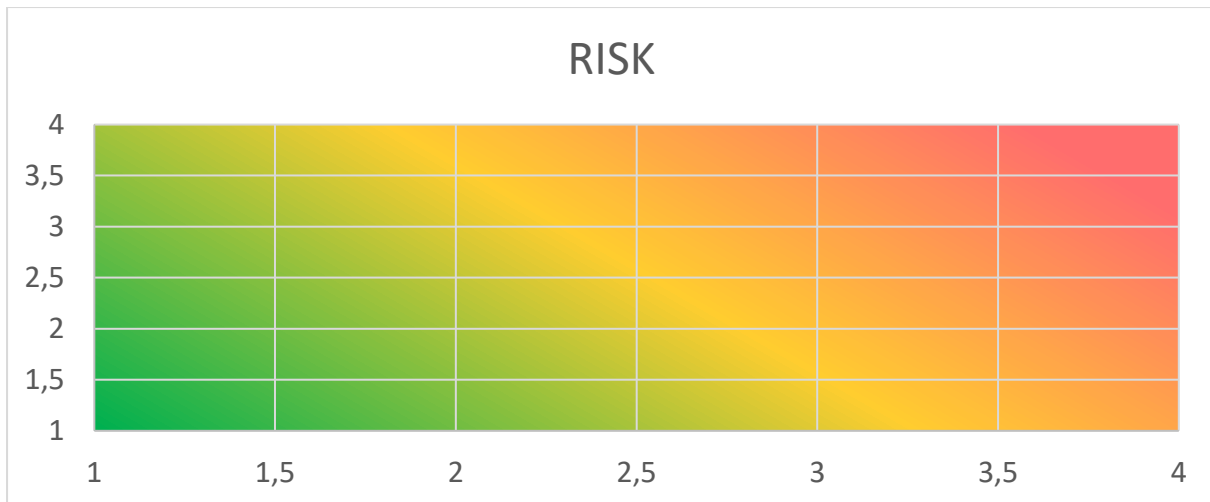


Table 9: Risk Calculation Grid - Granular representation

So, risk ties the vulnerability, threat, the assets value and likelihood of exploitation to the resulting impact. At this step, the resulted risk level will be identified which is the result of the equation (Impacts x Likelihood).

12.3.4.1.1 Handling Risk

Once we know the total risk the IoT device is faced with, the risk-owner must decide how to handle it.

Risk can be dealt with in four basic ways: Avoid it, Reduce it, Accept it or Transfer it (described in **Error! Reference source not found.**) and finally chooses the ones relevant to the level of assurance (High, Substantial and Basic) depending on the level of trust required.

NOTE: By default, the option “Reduce”, is chosen for handling the risk except when otherwise chosen by the risk-owner.

Avoid (Av)	<p>Terminate the feature that is introducing the risk. Assumptions, security organisational policies are implemented that prevents the risk of happening, but without specifically addressing it.</p> <p>For instance, a Vendor could decide to remove a User Interface feature in its IoT device therefore avoiding the risk of disclosing confidential information through that interface.</p>
Reduce (R)	<p>Reduce threat impact or likelihood (or both) through intermediate steps;</p> <p>For instance, a threat with a high likelihood of occurring, but the financial impact is small. The best response is to implement a countermeasure to reduce the risk of potential loss.</p>
Accept (Ac)	<p>Accept or Assume the chance of the negative impact of a risk. The risk is accepted without the need to enforce any security requirement.</p> <p>For instance, if the cost-benefit analysis determines that the cost to mitigate risk is higher than cost to bear the risk, then the best response is to accept and continually monitor the risk.</p>
Transfer (T)	<p>The threat is transferred to another actor, typically because it affects a component that is out of the scope.</p>

	Typically, threats with low probability of occurring, but with a large financial impact could be transferred to a third-party party that can manage the outcome such as the insurance.
--	--

Table 10: Risk Treatment Options

The following table of decision could be used to treat each risk.

Threat	Risk Level	Risk treatment option
Threat ID	Low, Moderate, High, Very High	Av, R, Ac, T

Table 11: Risk Decision Table

12.3.4.2 List of Security Goals

At this step, we list the Security Goals covering the risks that we decided to reduce. The goal is to reduce the overall risk to an acceptable level. Indeed, no system or environment is 100 percent secure, which means there is always some risk left over to deal with.

For instance, the following security goals could be generated the same IoT device (e.g. Connected Cam) according to each Operational Environment.

CONSUMER	<ul style="list-style-type: none"> Secure external interfaces, Data Confidentiality, IP Protection, ...
ENTREPRISE	<ul style="list-style-type: none"> Secure Firmware updates/Reprogramming and Remote Access Authentication, ...
INDUSTRIAL	<ul style="list-style-type: none"> Local Internal Interface Access Enforced Authentication, Assets Availability, Communication Integrity, ...
CRITICAL	<ul style="list-style-type: none"> Firmware Integrity, Secure Booting and Physical Access Authentication, ...

12.3.4.3 List of Security Requirements

For each selected security goal, one or more security requirements relevant to the Substantial level of assurance are listed to achieve the goal.

The chosen Security Requirement must make a good business sense, meaning it must be cost-efficient (its benefit outweighs its cost) for the IoT market.

FAQ 2.3

Q2.3: What happens if the risk owner changes his decision about handling a risk after the security requirements are generated?

R2.3: The steps from "Handling Risk" to "List of Security Requirements" is executed in an iterative process. The process can be re-done multiple times until the risk owner is satisfied with his decision on each risk item on the list.

12.3.4.4 List of Security Assurance Activities

For each selected security requirement, one or more security assurance activities relevant to the Substantial level of assurance are listed to achieve the goal.

The chosen Security Assurance Activity must follow the method below:

1. Map the common items between the potential security assurance activities (Potential-SAA list) that was defined in STEP2 and the mapped list between applicable security activities (Applicable-SAA list) and security requirements (extract example in the figure below); These

common items list for each requirement is called the “Base-SAA list” in the context of the evaluation methodology.

2. Applying the rules explained in Section 5.3 of the evaluation methodology document on the Base-SAA list, CAB-E is then able to generate the Final-SAA list for each security requirement.

Ref	Security Requirement	Security Goal	Applicable Security Assurance Activity
EIA_SF.1	The device SHALL Use protocols and mechanisms able to represent and manage trust and trust relationships.	DIU INTEGRITY	CA.DocumentationReview CA.SourceCodeReview CA.FunctionalSecurityTesting VA.VulnerabilityScanning VA.NonIntrusivePentesting VA.IntrusivePentesting
EIA_SF.2	The device SHALL verify 3rd party software's authenticity and integrity during initialization. If the software authenticity and integrity cannot be ensured, it shall not be installed.	DIU INTEGRITY	CA.DocumentationReview CA.SourceCodeReview CA.FunctionalSecurityTesting CA.CompositionAnalysis VA.AdvancedRobustnessTesting VA.NonIntrusivePentesting VA.IntrusivePentesting

Figure 12: Mapping between applicable security assurance requirements and security requirements

The formula to generate the Final-SAA list is simply:

Potential-SAA list x Applicable-SAA list = Base-SAA list

Base-SAA list + Rules in Evaluation Methodology (Section 5.3) = Final-SAA list

Example:

If we continue with the same example of [section 12.3.3.3](#), where **Threat 1** had the following 3 potential security assurance activities considering the identified impacts and likelihoods:

- **Potential Security Assurance Activity 1 = CA.DocumentationReview,**
- **Potential Security Assurance Activity 2 = CA.CompositionAnalysis,**
- **Potential Security Assurance Activity 3 = VA.VulnerabilityScanning.**

And the **EIA_SF.1** is one of the security requirements that was identified as relevant to cover the risk that is linked to **Threat1**.

If we follow the described method:

1. The common list between the potential security assurance activities that was defined in STEP2 for **Threat1** and existing mapping list between applicable security activities and security requirements for **EIA_SF.1** would be:
 - a. **CA.DocumentationReview,**
 - b. **VA.VulnerabilityAnalysis**
2. Choosing the specific tests to be performed i.e either a or b in 1 above, is done according to some rules explained in the evaluation methodology document (refer to “Eurosmart_IoTSCS-Evaluation” document for complete details)

12.3.4.5 Security Profile

Finally, the Security Profile which will address a specific Type of ToE usage such as Smart Thermostat, Connected Cam, Connected Pumps, Alarm Systems, etc. While considering the Operational Environment context (Consumer, Enterprise, Industrial or Critical).

The main output of a Security Profile is a list of standard security requirements and assurance activities that the IoT device must be tested against.

Threat ID	Threat	Asset	Asset Value	Vulnerability	Impact	Likelihood	Total Risk	Security Goals	Security Requirements	Security Assurance Activities
THT_06	Alteration of data in use	Transaction Data	Authenticity, Integrity, Availability	IMPROPER ACCESS CONTROL	Moderate	Likely	Substantial	Integrity	EIA_SF.1; EIA_SF.10; EIA_SF.17; EIA_SF.22	CA.SCR VA.BRT VA.NIP
								Identification & Authentication		

Table 12: Security Profile - Sample Template

As can be seen in the Security Profile sample template Table 12 above, contents of the security requirements column contain codes. Due to space constraints, full texts of each security requirement cannot appear in the security profile. This constraint informs the use of the identification codes as a reference to specific texts of security requirements in the backend. The same (as above) is the case for Security assurance activities. Among other things, the security requirements text and SAA are put into a table, which also includes a space provided for comments/response of both the vendor and evaluator. This information forms the primary content of the vendor questionnaire which will be discussed in the next topic.

13 Vendor Questionnaire

A Vendor Questionnaire¹² provides a list of generic questions covering all the domains (e.g. Scope, Assumptions, Organisational Policies, Requirements, Security Assurance Activities) on each part of the ToE. The goal is to allow the Vendor to reformulate and refine the security requirements of a Security Profile thus helping both the Vendor's and the CABs to communicate. It will draw a list of questions and actions for both the Vendor and the CAB.

- (VA) Actions addressed for Vendors could be to provide for instance coverage rationale, documentation/evidence, testing materials etc.
- (CA) Actions addressed for CABs which could be to do a review, vulnerability scanning, penetration testing, etc.

These VA and CA will be tailored to the Security Profile that is selected to constitute the basis of evidence requests and evaluation procedures required for to complete a certification.

Besides, Vendor Questionnaires associated with mapping tables allow reuse of existing certification scheme results or evidence.

Ref	Security Requirement Questionnaire	Security Goal	Security Assurance Activity	Vendor Instructions	Vendor Responses	Evaluator Feedback
-----	------------------------------------	---------------	-----------------------------	---------------------	------------------	--------------------

¹² Vendor Questionnaire concept is intended to replace the Security Target and the Security Assurance Requirements concept as introduced by the Common Criteria. The main benefits are gain of time up to 80% for both Vendors and CABs.

EIA_SF.10	The device SHALL enforce verification/authentication before performing any sensitive actions on behalf of that user.	Secure Updates	CA.DR CA.FST	Provide a response of how the requirement is fulfilled.		
-----------	--	----------------	-----------------	---	--	--

Table 13: Vendor Questionnaire Template (Sample)

13.1.1.1 How is a vendor questionnaire generated?

The Security Requirement Questionnaire and the corresponding Security Assurance Activity are fetched using their unique codes (shown previously in the security profile). The vendor instructions column further refines the security requirement thereby assisting the vendor to make correct responses as to how the requirement is met by the TOE (in the vendor responses column).

The evaluator feedback column is used in cases where the evaluator needs to exchange correspondence or provide feedback to the vendor about a specific requirement.

Kinds of Requirements:

There are Basically 2 kinds of requirements (separated according to their applicability).

- There are generic requirements which apply to every TOE and so will always feature in every vendor questionnaire and must be answered by every vendor (an example is the requirement group concerning “device lifecycle”)
- The second group of requirements are those that are filtered according to the specificities of the TOE in order to give the vendor a well-tailored vendor questionnaire in addition to the generic requirements to be responded for his/her device category (an example is the Security functionality Requirements).

14 Integration to the IoT device Development Life-Cycle

This scheme encourages making deliberate, explicit choices about security requirements at design time rather than leaving security as an afterthought. The GPP, Security Profile is also useful later in the life cycle of an IoT device if other features have been added or when the security strategy has changed; for instance, it can help identify whether the original design choices fulfilled their intended function or failed to do so, or whether a newly discovered threat was not anticipated in the original design.

Since this Scheme is thought to address and smartly assess the security of IoT devices while reducing the time that usually Vendors spend thinking security and going through the evaluation process, a dedicated IoT Security Assurance Development Life-Cycle process is strongly recommended by this scheme to insure a cost-efficient security by design.

A typical approach is presented below in Figure 13 but remains optional for Vendors to implement.

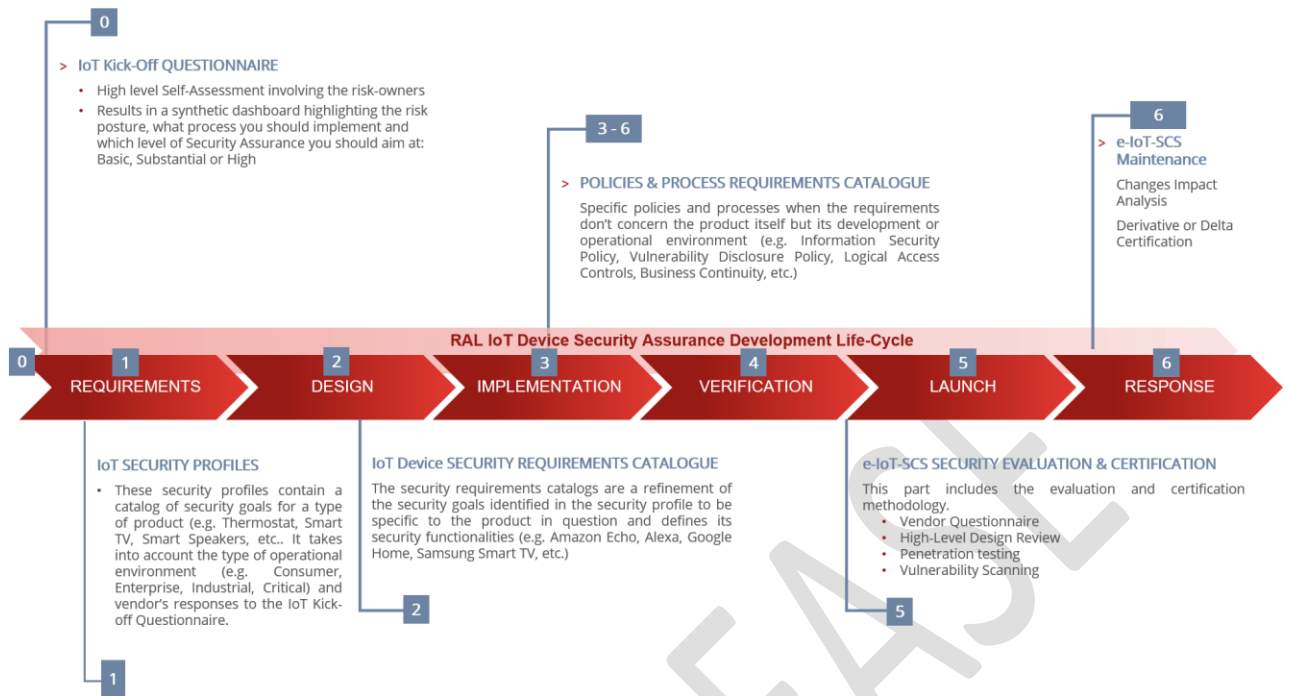


Figure 13: RAL IoT Device Security Assurance Development Life-Cycle¹³

This new concept adds the “Assurance” factor to the standard Security Development Life-Cycle (SDLC) methodology deployed widely in software development. The main benefit is to allow to incorporate security in a risk-based approach and verify the robustness of the security features based on a structured and objective approach.

¹³ This new approach has been first introduced, developed and tested efficiently by Red Alert Labs

15 About us

Eurosmart, the Voice of the Digital Security Industry, is an **international non-profit association located in Brussels**, representing the **Digital Security Industry** for multisector applications. **Founded in 1995**, the association is committed to expanding the world's Digital secure devices market, developing smart security standards and continuously improving the quality of security applications.

16 Our members

Members are manufacturers of secure element, semiconductors, smart cards, secure software, High Security Hardware and terminals, biometric technology providers, system integrators, application developers and issuers.

EUROSMART members are companies (**BCA, Fingerprint Cards, Gemalto, Giesecke+Devrient, GS TAG, IDEMIA, IN GROUPE, Infineon Technologies, Inside Secure, Internet of Trust, Linxens, Nedcard, NXP Semiconductors, +ID, Prove & Run, Qualcomm, Real Casa de la Moneda, Samsung, Sanoia, Sarapis, SGS, STMicroelectronics, Tiempo Secure, Toshiba, Trusted Objects, Trust CB, WISEkey, Winbond**), laboratories (**Keolabs, Serma, Brightsight, Red Alert Labs, Cabinet Louis Renaud**), research organisations (**Fraunhofer AISEC, Institut Mines-Telecom - IMT, ISEN - Institut Supérieur de l'Électronique et du Numérique Toulon**), associations (**SCS Innovation cluster, Smart Payment Association, SPAC, Mobismart, Danish Biometrics**).

EUROSMART and its members are also active in many other security initiatives and umbrella organisations on EU-level, like CEN, ECIL, ETSI, ECSO, ESIA, ETSI, GP, ISO, SIA, TCG and others.

ANNEX I — Sample of Risk Calculation

Scenario

An industrial SCADA system with an Admin Monitoring console, Sensors, Actuators and heavy machinery.

Operational Environment:

Industrial

Devices:

Admin Monitoring console (AMC), Temperature Sensor (TS), Connected Valve (CV), and heavy fabrication machinery (HFM).

Assets:

TS data, AMC Configuration data, CV control signal, router configuration data, AMC monitoring data

TOE

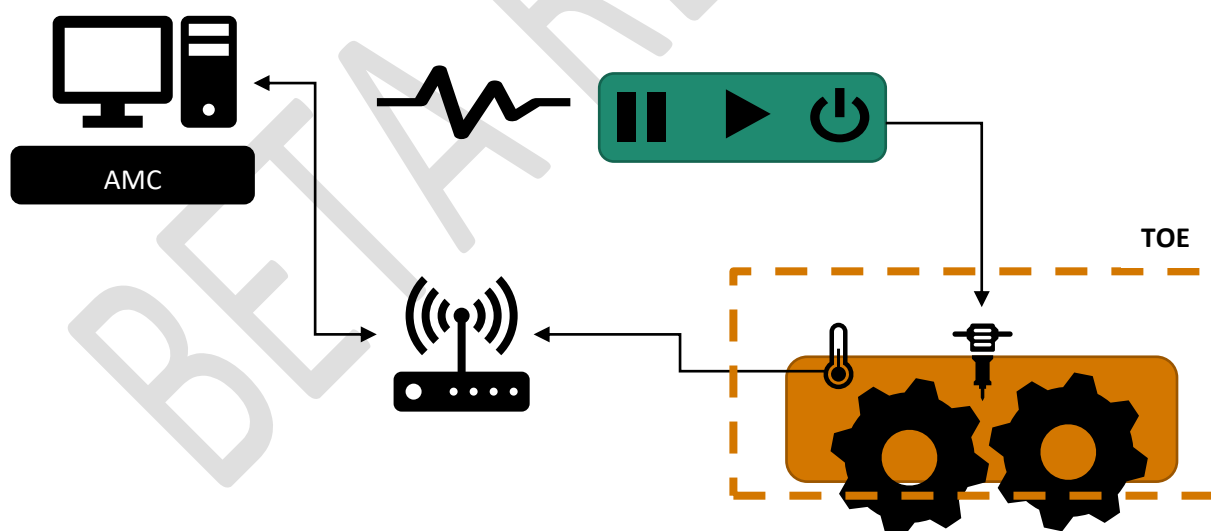
HFM: which contains a Wi-Fi enabled sensor and a connected valve which can receive instructions to start, stop or pause operations based on instructions from the AMC.

It's hardware components are shown in the picture below.

Form Factor:

Linux Based sensors in a Heavy factory machine

Data Flow:



Threats	Vulnerabilities
Network outage	Network Devices Not Securely Configured
Device modification	Network Devices Not Securely Configured Download of Code without Integrity Check Client-Side Enforcement of Server-Side Security
Software attacks	Buffer overflow Command Injection Lack of Bounds Checking Use of Potentially Dangerous Functions NULL Pointer Dereference
MITM	Channel Accessible by Non-endpoint Network Devices Not Securely Configured Use of Potentially Dangerous Functions Poor System Identification/Authentication Controls
Malware	Download of Code without Integrity Check
DDOS	No Security Perimeter Defined Lack of Network Segmentation Lack of Functional DMZs Lack of lockout system enforcement for failed login attempts
Modification of information	Insufficiently Protected Credentials Command Injection Use of Hard-Coded Credentials Missing Authentication for Critical Function

IMPACT CALCULATION

Threats	Privacy	Confidentiality	Integrity	Availability	Authenticity	Safety	Reputation & Financial Loss	Scale
Network outage	Low	Minor	Moderate	Severe	Minor	Severe	Severe	
Device modification	Low	Moderate	Severe	Severe	Moderate	Severe	Moderate	Moderate
Software Attacks	Low	Minor	Moderate	Severe	Moderate	Moderate	Minor	
MITM	Low	Minor	Moderate	Moderate	Severe	Moderate	Moderate	
Malware	Low	Minor	Severe	Severe	Moderate	Moderate	Moderate	
DDOS	Low	Minor	Moderate	Severe	Minor	Severe	Severe	
Modification of information	Low	Minor	Severe	Moderate	Moderate	Severe	Severe	Moderate
Overall Impact (INDUSTRIAL)				Severe		Severe		

EUROSMART
The Voice of the Digital Security Industry



www.eurosmart.com



@Eurosmart_EU



@Eurosmart

Rue de la Science 14b | B-1040 Brussels | Belgium
Tel +32 2 880 36 00 | mail eurosmart@eurosmart.com

Likelihood:

To estimate the likelihood, we first plot an operational scenario of a security threat “Device Modification” or “Modification of Information” resulting in a “Valve Malfunction”.

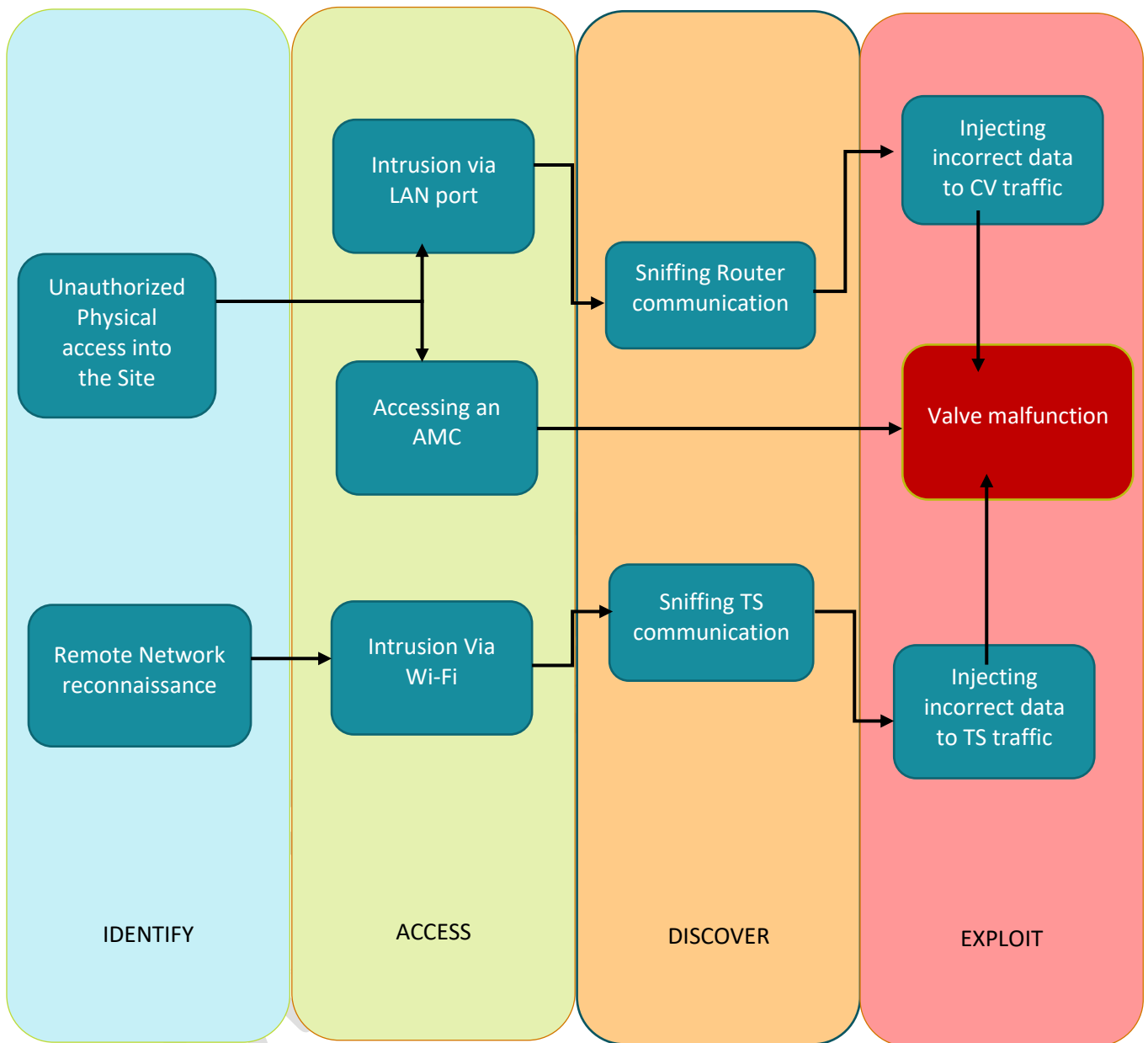


Table 14: Threat Model Representation - Attacks Scenarios

Step 1:

Calculate probability of each individual step of an attack scenario:

- Unauthorized Physical access into the Site: 1 (<20%)
- Remote network reconnaissance: 3 (>60%)
- Intrusion via Lan: 1 (<20%)
- Accessing AMC: 0 (<3%)
- Intrusion via WIFI: 2 (>20%)
- Sniffing Router: 2 (>20%)

- Sniffing TS communication: 3 (>60%)
- Injecting incorrect data to CV: 4 (>90%)
- Injecting incorrect data to TS: 4 (>90%)

Step 2:

Calculate probability for each scenario using the formula:

$$\text{Indice_Pr}_{\text{cumulé intermédiaire}}(AE_n) = \text{Min} \left\{ \text{Indice_Pr}(AE_n), \text{Max}_{\text{cumulés intermédiaires}}(\text{Indices_Pr}(AE_{n-1})) \right\}$$

Scenario 1:

Unauthorized Physical access:1

Intrusion via Lan: 1

Sniffing Router: 2

Injecting incorrect data to CV: 4

Answer for scenario1 = 1

Scenario 2:

Physical Visit:1

Accessing AMC:0 (<3%)

Answer for scenario2 = 0

Scenario 3:

Remote network reconnaissance: 3 (>60%)

Intrusion via WIFI:2 (>20%)

Sniffing TS communication: 3 (>60%)

Injecting incorrect data to TS:4 (>90%)

Answer for scenario 3 = 2

Step 3:

Select the max value as overall likelihood

Overall Likelihood = 2

TECHNICAL DIFFICULTY

Step 1:

Calculate technical difficulty of each individual elementary action

- Unauthorized Physical access into the Site: 1
- Remote network reconnaissance: 2
- Intrusion via Lan: 2
- Accessing AMC: 2
- Intrusion via WIFI: 2
- Sniffing Router: 1
- Sniffing TS communication: 2
- Injecting incorrect data to CV: 3
- Injecting incorrect data to TS: 3

Step 2:

Calculate the technical difficulty for each scenario using the formula:

$$\text{Indice_Diff}_{\text{cumulé intermédiaire}}(AE_n) = \text{Max} \left\{ \text{Indice_Diff}(AE_n), \text{Min}(\text{Indices_Diff}_{\text{cumulés intermédiaires}}(AE_{n-1})) \right\}$$

Scenario1:

Unauthorized Physical access: 1

Intrusion via Lan: 2

Sniffing Router: 1

Injecting incorrect data to CV: 3

Difficulty = 3

Scenario2

Unauthorized Physical Visit: 1

Accessing AMC: 2

Difficulty = 2

Scenario3:

Remote network reconnaissance: 2

Intrusion via WIFI: 2

Sniffing TS communication: 2

Injecting incorrect data to TS: 3

















Difficulty = 3

Overall technical Difficulty level is 2

GLOBAL LIKELIHOOD

	Probability of success	Technical Difficulty	Likelihood
Scenario1	1	3	1
Scenario2	0	2	1
Scenario3	2	3	2
Global Likelihood			2

RISK CALCULATION

IMPACT VS LIKELIHOOD	UNLIKELY (1)	LIKELY (2)	VERY LIKELY (3)	ALMOST CERTAIN (4)
SEVERE (4)				
MODERATE (3)				
MINOR (2)				
LOW (1)				

So, based on the risk grid above, the Likelihood of 2 and Impact level of “SEVERE” puts us at a “YELLOW” risk level based on the matrix above.

ANNEX II — SECURITY REQUIREMENTS (93)

1. INTEGRITY OF DATA IN USE

EIA_SF 1 Use of trust-managing protocols

Description

This requirement addresses the use of protocols and mechanisms that can represent and manage trust and trust relationships.

The use of these protocols enhances the trust over the communication in which the IoT device is a part, thus ensuring integrity of data we receive.

Application Note

Before implementing this, one must take in to account the architectural design and how to implement these protocols without modification.

EIA_SF 2 Controlled installation/updates

Description

The control over the installation or updates of software in operating systems helps to ensure the integrity of the software i.e. it has not been tampered or modified and it will work exactly as it has been designed to function.

Application Note

Implement run-time protection and secure execution monitoring to ensure malicious attacks do not overwrite code after it is loaded. This requirement is enhanced by the security goal “secure software/firmware updates”.

EIA_SF 3 Secure Boot

Description

The device should include a secure boot process, which verifies that the device bootloader has not been modified. The device should perform integrity checks and refuse to boot on non-original system software.

Application Note

This is related to “cryptographically signed code”, “Root of trust”, “authentication” and “encryption”, in which cryptographic assets need to be protected.

EIA_SF 4 Roll-back to Secure state

Description

This ensures that the device can return to a state that is known to be secure, after a security breach occurs or if an upgrade is not successful.

Application Note

While implementing roll-back mechanism, one must include protections for it, in order to prevent roll-back attacks. These protections include using non-volatile memory

element in order to store the state, storing integrity information separately inside a trusted server, use of TPMs, etc.

EIA_SF 5 Cryptographically signed code

Description

This assures platforms that a genuine code has not been tampered with and it is therefore safe for the device to execute.

Application Note

This requirement gives more sense to “EIA_SF 2 Controlled installation/updates” such that when a signed code is going to be installed, its genuine-ness can be easily verified.

EIA_SF 6 Implement run-time protection and secure execution

Description

This ensures that the device doesn't execute malicious code. An example could be the DES functionality of windows.

Application Note

Think about Sandboxing execution of untrusted programs.

CONFIDENTIALITY OF DATA IN USE

EIA_SF 7 Encryption of data during processing

Description

This ensures that the data while being processed, is not exposed to or accessed by an unauthorised party.

Application Note

Sensitive data should always be encrypted in device memory, until when it is absolutely required to be in plain text. Also consider Homomorphic encryption.

EIA_SF 8 Code obfuscation

Description

The purpose of this is to protect the confidentiality of source codes from reverse engineering and IP theft.

Application Note

One should always keep in mind that when a code is obfuscated, it should never affect code's functionality.

EIA_SF 9 Generic Error messages

Description

Secure error handling mechanism ensures that the error messages doesn't reveal any sensitive information to an attacker, with which he might be able to get an insight of the inside functioning of the application/software.

Application Note

Best & secure coding practices must be followed.

IDENTIFICATION & AUTHENTICATION

EIA_SF 10 Authenticate all users

Description

Every device user **MUST** be authenticated before access is granted to manipulate any sensitive operation.

Application Note

This requirement is enhanced by ensuring that all user activity on sensitive device functions are logged.

EIA_SF 11 Enforce strong password use

Description

The use of a strong password substantially reduces the risk of password guessing. This also protects from password attacks using dictionary, rainbow tables and brute forcing thus enhancing strong authentication.

Application Note

The password should be difficult to be guessed by any person and it should strictly not contain any personal information of the user (date of birth, name, etc). Consider usage of best practice guidelines on password generation from a standards organization.

EIA_SF 12 Multi-factor Authentication

Description

Where possible, it is recommended to use multiple authentication factors to increase the difficulty of an attack, especially for privileged users such as maintenance staff to enhance strong authentication by implementing other mechanisms such as face recognition, biometric fingerprint authentication, etc.

Application Note

The storage of these user verification reference data must be done securely. (see "SECURITY DATA MANAGEMENT").

EIA_SF 13 Authentication failure Management

<i>Description</i>
This ensures that a defined action occurs after multiple failed authentication attempts. i.e should the device be blocked and demand for an admin authentication to unblock? Should the device be blocked and force an account reset? Should the device be blocked and force a device reset?
<i>Application Note</i>
To implement authentication failure management, one must develop clear policies based on the device threat model to define the device behaviour in the event of multiple failed authentication attempts.

EIA_SF 14 Robust password recovery & reset mechanism

<i>Description</i>
In the event of an authentication failure, there must be a robust method for managing account recovery or reset whereby users can safely and securely reset or recover lost & forgotten passwords. The same applies to key update and recovery mechanisms.
<i>Application Note</i>
A rate-limit shall be implemented in answering the security questions asked and a random number shall be generated as a one-time-password.

EIA_SF 15 Limit Authentication attempts

<i>Description</i>
This functionality ensures the protection against ‘brute force’ and/or other abusive login attempts by rate-limiting. The waiting time should also progressively increase with the number of failed attempts.
<i>Application Note</i>
This protection should also consider keys stored in devices.

EIA_SF 16 Mandatory change of password & username at first-login

<i>Description</i>
This ensures that default passwords and even default usernames are changed during the initial setup, and that weak, null or blank passwords are not allowed. Thus, enhancing protection against guessing attacks & brute forcing.
<i>Application Note</i>
The new password must not contain any personal data and it must be changed at regular intervals. This requirement is enhanced by “Enforce strong password use”.

EIA_SF 17 Authenticate all devices

<i>Description</i>

Discover, identify and authenticate the devices connected to the network before trust can be established (mutual authentication). This helps to confirm that the communication is taking place with authenticated device, making it secure.

<i>Application Note</i>

The verification needs to take care of the validity of the identifiers or credentials, with which the verification is done. Consider the use of Digital certificates.

EIA_SF 18 Identifier uniqueness

<i>Description</i>

Identifier uniqueness ensures the unique identification of each devices and the correct composition & operation of the system. Examples of identifiers can be serial numbers assigned during manufacturing, User Identifier, etc.

<i>Application Note</i>

The cryptographic algorithms used for the unique identifier generation must be strong, valid and must produce unique values. Proper identification standard must be followed.

EIA_SF 19 Secure Pairing

<i>Description</i>

This ensures the establishment of a secure communication channel among IoT devices, enabling authentication and privacy.
--

<i>Application Note</i>

This must be secure, error-free, inexpensive and must ensure that the right devices are being paired. Hence secure protocols should be employed to achieve this. Consider “Use of Trust Managing Protocols”

ACCESS CONTROL

EIA_SF 20 Enforce Disconnection of inactive connection/user session

<i>Description</i>

This requirement ensures that a user session is not illegally accessible when the device is idle due to users’ absence.

<i>Application Note</i>

The preferred waiting time before a session timeout should be selected carefully, according to the device threat model.

EIA_SF 21 Enforce Access control policy

<i>Description</i>

Data integrity and confidentiality must be enforced by access controls. When the subject requesting access has been authorised to access a process, it is necessary to enforce the defined access control policy.

Application Note

The effectiveness and the strength of access control depend on the correctness of the access control decisions (e.g., how the security rules are configured) and the strength of access control enforcement (e.g., the design of software or hardware security).

EIA_SF 22 Ensure context-based security

Description

Ensures the security of the access credentials of the devices, based on the context. For example, it could be in a context where a device-to-device communication takes place continuously, where it takes the credentials only once and authenticates the communication with the fingerprints. Here if a third device comes in between with a similar fingerprint, it is not allowed to interact in between. It can also be a situation inside the software of the device, where the communication takes place between applications, without allowing a third application to come in between.

Application Note

Implement proper error-correcting codes in case the fingerprints of two devices matches or implement dedicated space for the applications which engages in such communications.

EIA_SF 23 Tamper Protection and Detection

Description

Ensures that the device is protected against tampering (implementation using Secure Element, TEE, etc) and proper tamper detection system, i.e., the ability to sense that an attempt is being made to disrupt the device's integrity or data (e.g. Sensors which detect high temperature exceeding the limits) is implemented.

Application Note

Implementation of device's hardware including SE, TEE, sensors, etc.

EIA_SF 24 Tamper detection and reaction should not rely on network connectivity

Description

Ensures that the tamper detection and reaction will continue to work even after the device loses network connectivity.

Application Note

The detection mechanism must be implemented inside the device and must not rely on any network connectivity for its functioning.

EIA_SF 25 Device not easily disassembled

Description

Ensure that the device cannot be easily disassembled, and the processor should protect against extraction of device firmware.

<i>Application Note</i>

Proper screwing of the all the detachable components must be implemented.

EIA_SF 26 Data storage medium must be encrypted

<i>Description</i>

This ensures that the content of the device storage is unreadable in the event where the device gets stolen.
--

<i>Application Note</i>

Ensure that FULL disk encryption is implemented.
--

EIA_SF 27 Devices only feature the essential physical external ports (such as USB) necessary for them to function

<i>Description</i>

Ensures that all the unused external physical ports are disabled preventing an unauthorised access.

<i>Application Note</i>

Consider physically blocking the unused ports in addition to logical disabling of the ports

EIA_SF 28 Secure test/debug modes

<i>Description</i>

Ensure that the test/debug modes are secure, so they cannot be used to maliciously access the devices.
--

<i>Application Note</i>

Any other debug interface (for example, I/O ports such as JTAG) should only communicate with authorised and authenticated entities on the production devices.

AUTHORIZATION

EIA_SF 29 Implement authorization mechanism

<i>Description</i>

Ensure that only authorized processes can process data.

<i>Application Note</i>

Implement fine-grained authorisation mechanisms such as Attribute-Based Access Control (ABAC) or Role-Based Access Control (RBAC)- for executing privileged actions, access to files and directories, applications, etc.
--

EIA_SF 30 Use of least privilege principle

<i>Description</i>
Limit the permissions of actions allowed for a given system by Implementing fine-grained authorisation mechanisms and using the Principle of least privilege (POLP).
<i>Application Note</i>
Applications must operate at the lowest privilege level possible, so that it accesses only the information and resources that are necessary for its legitimate purpose.

EIA_SF 31 Isolate privilege code from portions of the firmware that do not need access to them

<i>Description</i>
Ensures that an unauthorised or malicious access to that firmware doesn't lead an access to the privilege code.
<i>Application Note</i>
Consider implementing hardware-based isolation such as SE, TEE, etc.

EIA_SF 32 Authorise all devices

<i>Description</i>
Authorizing all devices prevents exchange of sensitive information with an unauthorized entity, thereby leading to a loss of confidentiality & integrity of the whole communication.
<i>Application Note</i>
This requirement ensures that the device communicates with each entity according to authorization level that is applicable for such entity.

AVAILABILITY OF DATA

EIA_SF 33 Resistance to perturbation

<i>Description</i>
The ensures that the device is resistant to perturbation attacks such as a laser shot, fluctuation in temperature or voltage levels, value modification, etc, that could lead to the malfunctioning of the device.
<i>Application Note</i>
Resistance mechanisms such as a hardware protection shield must be implemented, or a detection system to detect the perturbations in an earlier stage and act accordingly (e.g., resetting the secret keys, etc).

EIA_SF 34 Implement alarm system

Description

Whenever the data becomes unavailable beyond a certain amount of time, the alarm system helps to notify about this scenario. This enforces the notion of data availability.

Application Note

A real-time alarm system must be implemented.

EIA_SF 35 Enforce throttling/Rate Limiting.

Description

Rate Limiting ensures controlling the traffic sent or received by a network to reduce the risk of automated attacks.

Application Note

The important aspect here lies in the choosing of protocol. For example, in the case of TCP, there is a guarantee of non-loss of data, whereas in the case of UDP, there is possibility of data loss.

EIA_SF 36 Use Reliable communication protocols

Description

The choice of communication protocols could affect the level of communication reliability. Stateful protocols help to prevent loss of data packets when the devices communicate with each other.

Application Note

The important aspect here lies in the choosing of protocol. For example, in the case of TCP, there is a guarantee of non-loss of data, whereas in the case of UDP, there is possibility of data loss.

CONFIDENTIALITY OF STORED DATA

EIA_SF 37 Encrypt stored data

Description

This ensures that the data which is stored cannot be read, which enhances the confidentiality.

Application Note

The encryptions algorithms which are used must be cryptographically strong and valid, and the storage should be secure. Encryption is only as robust as the ability for any encryption-based system to keep the encryption key hidden.

INTEGRITY OF STORED DATA

EIA_SF 38 Hashing of stored data

<i>Description</i>
In order to assure the integrity of stored data, it should be hashed before storage. The verification can be done by hashing the data again and comparing it with the stored hash value. This ensures that the data has not been modified thus enforcing integrity.
<i>Application Note</i>
The important aspect to be considered is the algorithm used behind. The hashing algorithm must be strong, collision-resistant and non-depreciated.

EIA_SF 39 Integrity controller

<i>Description</i>
There is another way to verify the integrity of the data stored. This is achieved by the implementation of Integrity controller, which checks the integrity of the data and detect any malicious changes.
<i>Application Note</i>
The difficulties can be in the implementation of the controllers where it needs to maintain the synchronization between processor, etc. The criteria of choosing which type of controller implementation is also important.

STRONG CRYPTOGRAPHY

EIA_SF 40 Encryption & Verification of data

<i>Description</i>
Ensures that appropriate cryptographic algorithms are chosen and used correctly; the chosen algorithms should be strong and lightweight enough to be used on constrained devices for encryption and decryption of data.
<i>Application Note</i>
These cryptographic activities must be performed securely and according the <i>allowed cryptography list</i> .

EIA_SF 41 Signing & Verification of digital signature

<i>Description</i>
Verification of digital signature helps to ensure that the source with whom the device is communicating is authentic. For complete assurance, mutual verification of signatures should be done
<i>Application Note</i>

The process of signing & verifying digital signatures must be secure and according to the *allowed cryptography list*.

EIA_SF 42 Generation of Message Integrity code

Description

Message Integrity Code (MAC) ensures that the confidentiality & integrity of a message is assured. The appropriate MAC should be selected taking into consideration the device capability.

Application Note

The algorithms must be secure, and the device must ensure proper verification according to *Allowed Cryptography List*.

EIA_SF 43 Secure Hashing

Description

The selection of algorithm must be appropriate i.e., the algorithms must be collision-resistant, strong and valid.

Application Note

The process of hashing must be secure and according to the *allowed cryptography list*.

EIA_SF 44 Encryption & verification of keys

Description

Key encryption that the keys are encrypted before storage (if stored outside SE or TEE), which prevents unauthorised apps from accessing it. Key verification ensures that the protocols (e.g. PGP) that use end-to-end encryption, verifies the end-point device is legitimate by verifying the public key.

Application Note

Standard encryption & verification algorithms must be used.

EIA_SF 45 Disable insecure algorithms

Description

Some of the algorithms that the device can use might be depreciated. Those algorithms must be disabled/replaced, in order to maintain the cryptographic standard of that device and to ensure security.

Application Note

The implementor needs to stay up to date about crypto algorithms used and the ones which has been declared as depreciated.

EIA_SF 46 Use Strong RNG

Description

Random number generator generates unique random numbers for several operations on the device such as key generation, unique identifier generation etc. Hence it is very important to use strong RNG, which produces outputs which are non-deterministic.

Application Note

The important aspect lies in the selection of RNG. For example, if a Hardware (True) RNG is used, the output it produces is completely non-deterministic, whereas if a Deterministic RNG is used, the level of assurance slightly decreases. In that case, one might need to monitor the strength of the algorithm used.

PRIVACY

EIA_SF 47 Ensure anonymity

Description

Ensures that a user can use a resource or service without revealing their identity.

Application Note

The implementation requires role-based allocation of the users accesses in order to access the resources or services.

EIA_SF 48 Nickname Anonymity

Description

Ensures that a user can use a resource or service using a pseudonym.

Application Note

Ensure non-duplication of nicknames to ensure that the holder can be identified (not the holder's true identity)

EIA_SF 49 Ensure Unlinkability

Description

This functionality ensures that a user can use resources or services multiple times without others being able to link these uses.

Application Note

The role-based allocation of access should be encrypted, having considered all legal requirements.

EIA_SF 50 Ensure non-observability

Description

This ensures that a user can use a resource or service without others, particularly third parties, being able to see that the resource or service is in use. This enhances privacy of usage.

Application Note

The resource allocation system should be implemented keeping in mind, the importance of encryption and avoiding non-availability of resources.

EIA_SF 51 Ensure deletion of temporary data

Description

Deleting temporary data ensures that temporary user-specific information will no longer be accessible and newly created objects do not contain information that should not be accessible.

Application Note

While implementing this mechanism, consider the caching mechanism, the storage of sensitive information (to avoid accidental deletion) etc.

PHYSICAL SECURITY

EIA_SF 52 Protect interfaces against disturbances

Description

This ensures the protection of internal and external interfaces against disturbances.

Application Note

This implementation requires restricted access control, allowing the right person to access the right interface.

EIA_SF 53 Debug port protection

Description

Ensures that the debug ports are protected against hardware-based attacks, which could access the PCB or motherboard inside the device.

Application Note

Secure passphrase/OTP mechanism for the debug port or secure key (e.g., JTAG key)

EIA_SF 54 Hardware based immutable root of trust

Description

A hardware-based root of trust assures integrity and security of the critical data that impacts the device's crypto security.

Application Note

The implementation needs to be done in a dedicated hardware module such as Trusted Platform Module, Secure Element, etc.

EIA_SF 55 Use ROE

<i>Description</i>
Use ROE to protect against side channel attacks, which emanates from the leakage of certain electric or heat signals from which the attacker can gain sensitive information.
<i>Application Note</i>
The implementation must be done using the components resistant to side-channel attacks. Use hardware that incorporates security features to strengthen the protection and integrity of the device – for example, specialised security chips / 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 access to security sensitive code.

SECURE/TRUSTED COMMUNICATION

EIA_SF 56 Data encryption

<i>Description</i>
Ensures that the device sends & receives data in a manner that is protected from reading and modification. This protects the data even in the event of an interception/failure of the transport layer security.
<i>Application Note</i>
The algorithms chosen for encryption must be cryptographically strong and valid.

EIA_SF 57 Ensure communication security

<i>Description</i>
Ensures that communication security is provided using state-of-the-art, standardized transport layer security protocols (latest version) like IPsec, TLS, etc.
<i>Application Note</i>
The selection of protocol is the important factor to be considered here. The protocols must be of latest secure version.

EIA_SF 58 Access-controlled communication

<i>Description</i>
This is achieved by implementing some rules for communication, such as configuring the Firewall rules, access control lists etc. This enforces trusted & secure communication.
<i>Application Note</i>
The implementation should be done carefully, in order not to block the required communication.

EIA_SF 59 Non-exposure of credentials

<i>Description</i>
Ensures that the credentials are not exposed to internal or external network traffic, which means that whenever the credentials are transmitted from one end to another, they are made secure by proper encryption.
<i>Application Note</i>
Credentials should be sent over encrypted channels only or a secure key exchange mechanism should be employed.

EIA_SF 60 Adopt Restrictive approach rather than permissive in communicating

<i>Description</i>
This ensures that the device denies all the communications by default, unless otherwise explicitly allowed. For example, adopting a white list approach, instead of Black list.
<i>Application Note</i>
Strong firewalling rules must be implemented.

EIA_SF 61 Prevention of unauthorised connections

<i>Description</i>
Ensures that unauthorised connections are prevented at all levels of the network protocol (internet layer, transport layer, etc).

SECURITY AUDIT & MONITORING

EIA_SF 62 Intrusion detection

<i>Description</i>
Diagnoses or checks the security status of the device or determines whether there has been a breach of security and possibly what resources are being compromised by some intruders.
<i>Application Note</i>
Select the appropriate tool (with proper monitoring system) which can detect the intrusion, by verifying the changes or modifications made.

EIA_SF 63 Detection of replay

<i>Description</i>
This ensures that pre-transmitted data will not be re-sent by an attacker to establish a connection with the device.
<i>Application Note</i>

Maintain sensitive data/information inside dedicated hardware space (SE, TEE, etc).
“Continuous Monitoring and Logging” must be implemented.

EIA_SF 64 Logging Sensitive events

<i>Description</i>
This logs the sensitive events such as user authentication, management of accounts and access rights, modifications to security rules, and the functioning of the system.
<i>Application Note</i>
A real-time logging system must be adopted, supported by the OS (syslog) or trusted tools and it must be non-modifiable.

EIA_SF 65 Review of Audit logs

<i>Description</i>
This ensures that the logs can be retrievable only via authenticated connections.
<i>Application Note</i>
Proper authentication/access control to logs must be implemented.

EIA_SF 66 Storage of audit logs

<i>Description</i>
The audit logs must be stored securely, preventing it from accidental/intentional modification/deletion.
<i>Application Note</i>
Audit Logs must be encrypted and back up should be stored offsite.

SECURE DATA MANAGEMENT

EIA_SF 67 Integrity & Confidentiality of security data

<i>Description</i>
Ensures the integrity and confidentiality of security data, by enforcing strong encryption and secure storage.
<i>Application Note</i>
Proper encryption/hashing must be implemented, and storage must be done inside SE, TEE, etc.

EIA_SF 68 Administration of security features/data

<i>Description</i>

This ensures that proper access controls and authorization are implemented for accessing the security features and manipulating security related data.
--

<i>Application Note</i>

Be careful to ensure that the device is properly configured

NON-REPUDIATION

EIA_SF 69 Digital signature

<i>Description</i>

This ensures that the device cannot deny having sent or received data.
--

<i>Application Note</i>

“Strong cryptography” must be implemented according to the <i>allowed cryptography list</i> .

EIA_SF 70 Logging

<i>Description</i>

The logging mechanism helps to keep track of the sender and timestamp of each message to make sure there is always traceability.
--

<i>Application Note</i>

“Real-time Monitoring” of activities of the device is a must.

SAFETY

EIA_SF 71 System and Operational disruption

<i>Description</i>

Ensures that the disruptions in the system and the operational environment are minimized/eliminated, which enhances the safety of humans’ present.
--

<i>Application Note</i>

Proper “Monitoring” system on functionality must be implemented in order to have early detection of any such disruption.
--

EIA_SF 72 Enable self-diagnosis

<i>Description</i>

Self-diagnosis and Self-repair/healing on a device help to pre-empt potentially hazardous scenarios which could be harmful to human safety by taking preventive actions.
--

<i>Application Note</i>

“Roll back to secure state” feature must be implemented.
--

EIA_SF 73 Enforce standalone operation

Description

This ensures that essential features should continue to work with a loss of connectivity or be able to log negative impacts from interaction with compromised devices or cloud-based systems.

SECURE SOFTWARE & FIRMWARE UPDATES

EIA_SF 74 Ensure Update-server security

Description

This ensures that the update server security is taken seriously because of the potential scale of impact of a compromise on this server.

Application Note

Implement proper information system security according to an accepted standard.

EIA_SF 75 Transmit update file securely

Description

Ensures that the update file is transmitted over a secure channel

Application Note

Consider “secure communication”

EIA_SF 76 Update file shall not contain sensitive data

Description

This ensures that the update file doesn't contain any hardcoded sensitive data that an attacker could retrieve for malicious usage.

Application Note

If possible, Sensitive information should never leave the secure space where it has been stored unencrypted.

EIA_SF 77 Signed update files

Description

Update files should be signed using an authorized trust entity before pushing it to devices, to prevent malicious actors from pushing compromised update files.

Application Note

Consider a robust PKI

EIA_SF 78 Encryption of update file

Description

Ensures that the update files are encrypted such that where an attacker compromises the communication channel, the security of the update file is maintained.

Application Note

Cryptographically strong algorithms should be used according to the *allowed cryptography list*.

EIA_SF 79 Verification of signature before use

Description

This ensures that the trust is maintained on devices by checking for authenticity & integrity of update file using its signature before the file is executed.

Application Note

Cryptographically strong & valid signature verification must be used.

EIA_SF 80 Automatic update of firmware

Description

Automatic or frequent updates of firmware removes the overheads (reduces human intervention) of running updates manually. It also ensures that security updates are verified and installed in consistent and timely manner at any time of the day, thereby keeping the device always up to date.

EIA_SF 81 Non-disruptive updates

Description

Ensures that updates do not cause disruptions by altering user settings.

Application Note

Updates should be done such that devices maintain their user configured settings. This will avoid unnecessary disruptions on the device operation and security posture.

SECURE INTERFACES & NETWORK SERVICES

EIA_SF 82 Avoid provisioning of same secret key

Description

This ensures that when the confidentiality of a device secret key is compromised, it is easily traceable and localized than when the same key is shared by multiple devices.

EIA_SF 83 Ensure only necessary ports are available

Description

Ensures that only the necessary OS ports are made available, disabling the unused ones. This prevents the misuse of unauthorised ports and ensures trusted communication.

Application Note

Available ports should only communicate with authorised and authenticated entities.

EIA_SF 84 Encrypted Web interfaces

Description

This ensures that it fully encrypt the user session, from the device to the backend services, and that they are not susceptible to XSS, CSRF, SQL Injection, etc.

Application Note

“Strong Cryptography”, “Encryption” & “Strong Protocols” must be implemented according to the *allowed cryptography list*.

EIA_SF 85 Secure input & output handling

Description

This ensures secure handling of input and output, i.e., the device should give a consistent and reliable behaviour such that it does not crash due to input or output errors.

Application Note

Adopt secure coding best practices.

EIA_SF 86 Data input validation

Description

This ensures that the input data is validated against malicious tampering, injection, etc.

Application Note

“Out of bound checks”, “Buffer/Stack overflow”, “input data length” must be implemented. (Fuzzing)

STRONG DEFAULT SECURITY & PRIVACY

EIA_SF 87 Enable Security features by default

Description

This ensures that any applicable security features are enabled by default.

Application Note

Features like “Secure Boot” and other security parameters must be part of the device default settings.

EIA_SF 88 Disable unused security features by default

Description

Any device feature that is not frequently used or requires careful expert knowledge to securely configure, should be disabled by default.

DATA PROTECTION& COMPLIANCE

EIA_SF 89 Fair collection & processing of personal data

Description

This ensures that the personal data is collected and processed in a manner transparent to the person whose data is collected.

Application Note

Strong “access policy”, “authorisation” and “encryption” of personal data must be implemented.

EIA_SF 90 Ensure proper usage of personal data

Description

This makes sure that personal data is used for the specified purposes for which they were collected.

Application Note

EIA_SF 91 Minimization of data collected

Description

This ensures the minimization of data collected and retained.

Application Note

Data collected should only be as much data as is required to successfully accomplish a given task.

EIA_SF 92 Ensure Compliance of IoT stakeholders with GDPR

Description

This ensures that IoT stakeholders are compliant with the EU General Data Protection Regulation (GDPR). Users of IoT products and services can exercise their rights to information, access, erasure, rectification, data portability, restriction of processing, objection to processing, and their right not to be evaluated based on automated processing.

Application Note

“GDPR” standard must be implemented/followed on all operations related to data.

	OPERATIONAL ENVIRONMENT	SECURITY GOAL
EIA_OE.1	There must be a person who is capable of taking the ownership and also the responsibility of the TOE, its service and to provide business level security.	RESPONSIBLE PERSONNEL
EIA_OE.2	Competent administrators, operators, officers, and auditors will be assigned to manage the target of evaluation and the security of the information it contains.	RESPONSIBLE PERSONNEL
EIA_OE.3	All internal servers deployed must be owned by an operational group that is responsible for system administration.	RESPONSIBLE PERSONNEL
EIA_OE.4	A competent person is assigned the role of maintaining & monitoring an up-to-date asset inventory to the system owner/administrator.	RESPONSIBLE PERSONNEL
EIA_OE.5	All administrators, operators, officers, and auditors are familiar with the certificate policy (CP) and certification practices statement (CPS) under which the target of evaluation is operated.	AWARENESS & TRAINING
EIA_OE.6	General users, administrators, operators, officers and auditors are trained in techniques to thwart social engineering attacks etc.	AWARENESS & TRAINING
EIA_OE.7	Security trainings are continuous and regular for all categories of users.	AWARENESS & TRAINING
EIA_OE.8	The users who require access to at least some of the information managed by the target of evaluation are expected to act in a cooperative manner.	ETHICAL BEHAVIOUR
EIA_OE.9	All authorized users perform functions essential to security correctly and without errors	ETHICAL BEHAVIOUR
EIA_OE.10	There is no abuse of granted authorization to collect or send sensitive or security data	ETHICAL BEHAVIOUR
EIA_OE.11	The TOE is adequately physically protected against loss of communications i.e., availability of communications.	PHYSICAL & ENVIRONMENTAL

EIA_OE.12	There is controlled physical access to buildings, areas, rooms and locations etc. where the TOE is located.	PHYSICAL & ENVIRONMENTAL
EIA_OE.13	The TOE hardware, software, and firmware critical to security policy enforcement will be protected from unauthorized physical modification.	PHYSICAL & ENVIRONMENTAL
EIA_OE.14	Servers are specifically prohibited from operating from uncontrolled cubicle areas.	PHYSICAL & ENVIRONMENTAL
EIA_OE.15	Servers should be physically located in an access-controlled environment.	PHYSICAL & ENVIRONMENTAL
EIA_OE.16	File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.	PHYSICAL & ENVIRONMENTAL
EIA_OE.17	Audit logs are required for security-relevant events and must be reviewed by the auditors.	MONITORING, REVIEW & LOGS
EIA_OE.18	Administrators, operators, officers, auditors, and other users notify proper authorities of any security issues that impact their systems to minimize the potential for the loss or compromise of data.	MONITORING, REVIEW & LOGS
EIA_OE.19	For security, compliance, and maintenance purposes, authorized personnel may monitor and audit equipment, systems, processes, and network traffic per the Audit Policy.	MONITORING, REVIEW & LOGS
EIA_OE.20	All security-related events on critical or sensitive systems must be logged and audit trails saved	MONITORING, REVIEW & LOGS
EIA_OE.21	Logs shall be created whenever defined activities are requested to be performed by the system.	MONITORING, REVIEW & LOGS
EIA_OE.22	Servers must be registered within the corporate enterprise management system.	MONITORING, REVIEW & LOGS
EIA_OE.23	Information in the corporate enterprise management system must be kept up-to-date.	MONITORING, REVIEW & LOGS
EIA_OE.24	Security-related events will be reported to InfoSec, who will review logs and report incidents to IT management.	MONITORING, REVIEW & LOGS

EIA_OE.25	An authentication data management policy is enforced to ensure that users change their authentication data at appropriate intervals and to appropriate values, such as proper lengths, histories, and variations. This assumption is not applicable to biometric authentication data.	ASSET & CREDENTIAL MANAGEMENT
EIA_OE.26	Proper storage of Server User Names, Passwords and other credentials shall be stored securely to preserve confidentiality & integrity.	ASSET & CREDENTIAL MANAGEMENT
EIA_OE.27	All hardware tokens, smartcards, USB tokens, etc., shall not be stored or left connected to any end user's computer when not in use.	ASSET & CREDENTIAL MANAGEMENT
EIA_OE.28	The loss, theft, or potential unauthorized disclosure of any encryption key or other system credential shall be reported immediately to The Infosec Team.	ASSET & CREDENTIAL MANAGEMENT
EIA_OE.29	System level and user level passwords must comply with the Password Policy. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.	ASSET & CREDENTIAL MANAGEMENT
EIA_OE.30	An accurate inventory of information systems (including hardware, software, and other data required by the company or regulations) shall be maintained in the official system inventory repository.	ASSET & CREDENTIAL MANAGEMENT
EIA_OE.31	All PINs, passwords or passphrases used to protect encryption keys must meet complexity and length requirements described in the organisation's Password Policy	ASSET & CREDENTIAL MANAGEMENT
EIA_OE.32	Proper disposal of authentication data and associated privileges is performed after access has been removed, such as for a job termination or a change in responsibility.	ASSET & CREDENTIAL DISPOSAL
EIA_OE.33	When Technology assets have reached the end of their useful life they should be securely disposed, erasing all content of storage mediums in accordance with current industry best practices.	ASSET & CREDENTIAL DISPOSAL
EIA_OE.34	Computer workstations must be shut completely down at the end of the work day.	USER WORKSTATION

EIA_OE.35	Workstations shall be auto-locked after a defined period of inactivity to protect from the possibility of unauthorised access.	USER WORKSTATION
EIA_OE.36	Securing laptops that contain sensitive information by using cable locks or locking laptops up in drawers or cabinets.	USER WORKSTATION
EIA_OE.37	Installing privacy screen filters or using other physical barriers to alleviate exposing data.	USER WORKSTATION
EIA_OE.38	Ensuring that all workstations use a surge protector or UPS	USER WORKSTATION
EIA_OE.39	Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.	USER WORKSTATION
EIA_OE.40	Upon disposal Restricted and/or Sensitive documents should be shredded in the official shredder bins or placed in the lock confidential disposal bins.	USER WORKSTATION
EIA_OE.41	Mass storage devices such as CDROM, DVD or USB drives SHALL be treated as sensitive and are secured in a locked drawer	USER WORKSTATION
EIA_OE.42	All sensitive/confidential information in hardcopy or electronic form shall be secure in the work area at the end of the day and when the user is expected to be gone for an extended period.	USER WORKSTATION
EIA_OE.43	File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.	USER WORKSTATION
EIA_OE.44	The workstations used by administrators to manage the TOE remotely shall be trusted.	
EIA_OE.45	Printouts containing Restricted or Sensitive information should be immediately removed from the printer.	USER WORKSTATION
EIA_OE.46	Roles and responsibilities for security between IT, Engineering/Automation and Operations departments are clearly defined, separate and communicated to both the OT & IT systems and security personnel.	ORGANIZATIONAL
EIA_OE.47	Security architecture shall comprise all relevant security aspects – from	ORGANIZATIONAL

	organizational to physical implementation issues.	
EIA_OE.48	Compliance enforcement controls SHALL be integrated to the established Security Architecture and ensure that all products meet the requirements defined within it.	ORGANIZATIONAL
EIA_OE.49	The organization SHALL verify compliance to its policies through various methods.	ORGANIZATIONAL
EIA_OE.50	There is a close collaboration between the OT and IT department. Ensuring that IT and OT departments share their knowledge about systems operations as well as about threats.	ORGANIZATIONAL
EIA_OE.51	While eliminating security gaps, the most critical vulnerabilities are addressed first, considering the criticality of assets and systems.	ORGANIZATIONAL
EIA_OE.52		ORGANIZATIONAL
EIA_OE.53	Establish the physical location of data stored by the organization and define between which organizations data will be transferred.	ORGANIZATIONAL
EIA_OE.54	The use of removable media such as USB is restricted according to business needs across the organisation.	ORGANIZATIONAL
EIA_OE.55	An employee found to have violated policy may be subject to disciplinary action, up to and including termination of employment.	ORGANIZATIONAL
EIA_OE.56	Least Privilege Principle is used across all processes and procedures within the organisation	ORGANIZATIONAL
EIA_OE.57	Keeping food and drink away from workstations in order to avoid accidental spills.	ORGANIZATIONAL
EIA_OE.58		ORGANIZATIONAL
EIA_OE.59	Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by InfoSec.	ORGANIZATIONAL
EIA_OE.60	Third party aspects are well covered in the business continuity & disaster recovery plan	BUSINESS CONTINUITY
EIA_OE.61	Create and apply a comprehensive backup plan, including provisions for periodic testing, tailored to different types of assets.	BUSINESS CONTINUITY

	Perform backups before updates and other important changes to the system.	
EIA_OE.62	There shall be a documentation, detailing which data is backed up, the media to which it is saved, where that media is stored, and how often the backup is done. It should also describe how that data could be recovered	BUSINESS CONTINUITY
EIA_OE.63	Third parties SHALL be involved in the organization's IT security communication plan, and your organization should be part of theirs, as data breaches on their end could affect your data.	BUSINESS CONTINUITY
EIA_OE.64	Updates shall be done by a physically present authorized user who verifies the authenticity of the updates (Not Automatic)	UPDATES
EIA_OE.65	Updates shall be managed automatically by an update server which verifies the authenticity of the updates (Automatic)	UPDATES
EIA_OE.66	The most recent security patches shall be installed on the system as soon as practically possible.	UPDATES
EIA_OE.67	There is an established process or plan for validating and executing updates on an on-going or remedial basis.	UPDATES
EIA_OE.68	There exists a well implemented network transport security.	NETWORK
EIA_OE.69	If wireless network access is used, ensure access is secure by following the Wireless Communication policy	NETWORK
EIA_OE.70	Broadcast of wireless access points identifiers (SSIDs) shall be disabled.	NETWORK
EIA_OE.71	All interconnections between the organisation and external entities including off-site contractors must be documented in an Interconnection Security Agreement (ISA) that is approved by the CISO. ISA's must, at a minimum, be reviewed annually.	NETWORK
EIA_OE.72	All PC based hosts will require the company's approved virus protection before the network connection.	ANTIVIRUS
EIA_OE.73	Remote access tools shall support strong, end-to-end encryption of the remote access communication channels as specified in the	REMOTE ACCESS

	company's network encryption protocols policy.	
EIA_OE.74	Authorized Users shall ensure the remote host is not connected to any other network at the same time, with the exception of personal networks that are under their complete control or under the complete control of an Authorized User or Third Party	REMOTE ACCESS
EIA_OE.75	Secure remote access must be strictly controlled with encryption (i.e., Virtual Private Networks (VPNs)) and strong pass-phrases.	REMOTE ACCESS
EIA_OE.76	All remote access tools or systems that allow communication to company's resources from the Internet or external partner systems must require multi-factor authentication.	REMOTE ACCESS
EIA_OE.77	The organisation shall be compliant to ISO27001 (Information Security Magement)	COMPLIANCE
EIA_OE.78	The organisation shall be compliant to NIST SP800-53 controls for information systems	COMPLIANCE
EIA_OE.79	The organisation shall be compliant to ISO 28000 controls (Supply chain security management)	COMPLIANCE
EIA_OE.80	The organisation shall be compliant to PCI-DSS (Payment Card Industry Data Security Standard)	COMPLIANCE
EIA_OE.81	The organisation shall be compliant to HIPAA (Healthcare Information Privacy)	COMPLIANCE
EIA_OE.82	The organisation shall be compliant to ISO 28000:2007	COMPLIANCE
EIA_OE.83	The organisation shall be compliant to ITAR (International traffic in arms regulations)	COMPLIANCE
EIA_OE.84	The organisation shall be compliant to CT-PAT standards for logistics (Customs Trade Partnership Against Terrorism)	COMPLIANCE
EIA_OE.85	Research or Test labs are managed & maintained as required by accepted industry-specific standards & regulations.	COMPLIANCE
EIA_OE.86	Configuration changes for production servers must follow the appropriate change management procedures.	COMPLIANCE

EIA_OE.87	All the security policies are compliant with cybersecurity recommendations, in line with the industry standards.	COMPLIANCE
EIA_OE.88	The organisation implements a PKI in accordance with the highest security standards.	COMPLIANCE
EIA_OE.89	Employees may not install software on Company's computing devices operated within or outside the Company network. All software shall be obtained through IT service desk	INSTALLATION & CONFIGURATION
EIA_OE.90	Information Technology Department will obtain and track the licenses, test new software for conflict and compatibility, and perform the installation.	INSTALLATION & CONFIGURATION
EIA_OE.91	All host servers, desktops, laptops shall be replaced or re-imaged with a company-hardened standard image or shall be required to be hardened using a standard recommended/approved InfoSec guideline	INSTALLATION & CONFIGURATION
EIA_OE.92	All the organization's antivirus, data loss prevention, and other security systems shall not be disabled, interfered with, or circumvented in any way.	INSTALLATION & CONFIGURATION
EIA_OE.93	All network devices shall be replaced or re-imaged with a company standard image or shall be hardened using a standard recommended/approved InfoSec guideline.	INSTALLATION & CONFIGURATION
EIA_OE.94	All mobile and computing devices that connect to the internal network must comply with the Minimum Access Policy.	BYOD
EIA_OE.95	Personal equipment used to connect to the company's networks must meet the requirements of company-owned equipment for remote access as stated in the Hardware and Software Configuration Standards for Remote Access to company's Networks.	BYOD
EIA_OE.96	Users shall promptly report the theft, loss or unauthorized disclosure of the organization's devices/proprietary information.	BYOD
EIA_OE.97	Devices must be kept up to date with manufacturer or network provided patches. As a minimum patch should be checked weekly and applied at least once a month.	BYOD

EIA_OE.98	Devices must not be jailbroken or rooted or have any software/firmware installed designed to gain access to prohibited applications.	BYOD
EIA_OE.99	Devices must be encrypted in line with Company's compliance standards.	BYOD
EIA_OE.100	Users shall not use third-party email systems and storage servers such as Google, Yahoo, and MSN Hotmail etc. to conduct Company business, to create or memorialize any binding transactions, or to store or retain email on behalf of the Company.	EMAIL
EIA_OE.101	Users shall have no expectation of privacy in anything they store, send or receive on the company's email system	EMAIL
EIA_OE.102	All company data contained within an email message or an attachment must be secured according to the Data Protection Standard.	EMAIL
EIA_OE.103	All use of email must be consistent with company policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.	EMAIL
EIA_OE.104	Lab equipment must be physically separated and secured from non-lab areas.	LABS
EIA_OE.105	The lab network must be separated from the corporate production network with a firewall between the two networks.	LABS
EIA_OE.106	All acquired labs must meet with LabSec lab policy, or be granted a waiver by LabSec.	LABS
EIA_OE.107	The organisation shall define reasonable levels of security and associated controls; requiring sub-contractors, vendors, and critical supply chain partners to meet or exceed those standards as terms and conditions of established business agreements	SUPPLY CHAIN
EIA_OE.108	The organisation SHALL ensure supply chain risk management is included in contracts where appropriate and acquirers must determine whether the acquisition risk is acceptable given their system's environment.	SUPPLY CHAIN
EIA_OE.109	Manufacturers SHALL have written and verifiable processes for the selection of business partners including, carriers, other	SUPPLY CHAIN

	Manufacturers, product suppliers and vendors	
EIA_OE.110	Products should be assessed and warranted to be free of known malicious code or other vulnerabilities at the time of delivery and/or implementation.	SUPPLY CHAIN
EIA_OE.111	All approved and authorized distribution channels SHALL be clearly documented	SUPPLY CHAIN
EIA_OE.112	Tamper proof seals shall be placed on all product units at the time of manufacture.	SUPPLY CHAIN

	FUNCTIONAL SPECIFICATION	SECURITY GOAL
EIA_FS.1	All the entry and exit points to and from the security function of the IoT device SHALL be documented as physical or logical access points, considering the implementation.	
EIA_FS.2	If the device possesses an 'Application Programming interface' that could communicate directly or indirectly with the security function of the IoT device, it SHALL be documented as a logical interface of the device.	
EIA_FS.3	If the IoT device possesses an external or internal power source, which could be an input to the security function of that IoT device, it SHALL be documented.	
EIA_FS.4	If the entry and exit points to and from the security function of the IoT device shares the same physical port, the logical separation details or the implementation details of it SHALL be documented.	
EIA_FS.5	All the inflow and outflow of the data and control signals to and from the security function of the IoT device SHALL be documented.	
EIA_FS.6	In the event of key generation and other crucial cryptographic operations, the information about whether the output data ports are logically disconnected SHALL be documented.	

EIA_FS.7	All the defined input and output data and control paths to the security function of the IoT device SHALL be documented.	
EIA_FS.8	All the purpose, method of use and parameters associated with each physical and logical ports SHALL be documented.	
EIA_FS.9	If the interface of the IoT device produces error messages, it SHALL be documented.	

	INSTALLATION GUIDANCE	SECURITY GOAL
EIA_IG.1	All the guidelines related to the use of the IoT devices SHALL be documented.	
EIA_IG.2	The guidelines SHALL include appropriate warnings regarding the proper usage of the IoT devices.	
EIA_IG.3	The guidelines SHALL describe the user privileges and access controls implementation regarding the IoT device.	
EIA_IG.4	The installation guidelines SHALL describe proper usage of interfaces present in the IoT device.	
EIA_IG.5	The installation guidelines SHALL describe the security parameters present and the method of usage of the same in the IoT device(for example, how it is invoked, the default values of the parameters, the response to the function, etc).	
EIA_IG.6	The installation guidelines SHALL include documentation on modification of security characteristics or functionalities of the IoT device.	
EIA_IG.7	The guidelines SHALL describe all possible modes of operation of the IoT device in order to maintain the security level of usage.	
EIA_IG.8	The guidelines SHALL include all possible security measures related to the operational environment where the IoT device is being used.	
EIA_IG.9	The documentation of the guidelines SHALL be clear and understandable.	

EIA_IG.10	The guidelines SHALL describe the basic requirements needed for the successful installation of the IoT device (for example: network connectivity).	
-----------	--	--

	FLAW REMEDIATION	SECURITY GOAL
EIA_FR.1	The developer shall document flaw remediation procedures addressed to IoT device developers. These flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the IoT device.	
EIA_FR.2	The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.	
EIA_FR.3	The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.	
EIA_FR.4	The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to IoT device users.	
EIA_FR.5	As part of flaw remediation policies a set of actions must be defined to fix the flaw securely in IoT devices supporting remote software update.	
EIA_FR.6	Establish a comprehensive and well-defined process for disclosure of vulnerabilities.	
EIA_FR.7	Information about Security flaws discovered should be confidential until the bug is fixed.	
EIA_FR.8	Implement a secure flaw tracking application.	
EIA_FR.9	Performance targets shall be set & followed, in the event of vulnerability disclosure.	

EIA_FR.10	The developer shall establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws.	
EIA_FR.11	The procedures for processing reported security flaws shall provide safeguards (such as analysis, testing, or a combination of the two) that any corrections to these security flaws do not introduce any new flaws.	
EIA_FR.12	The developer shall document flaw remediation guidance addressed to IoT device users. This guidance shall describe a means by which IoT device users report to the developer any suspected security flaws in the IoT device	
EIA_FR.13	The flaw remediation guidance shall describe a means by which IoT device users may register with the developer, to be eligible to receive security flaw reports and corrections.	

	DEVICE LIFECYCLE PROCESS	SECURITY GOAL
EIA_DLP.1	The security expert shall review and validate third party components to be used in the device.	
EIA_DLP.2	Policies and procedures related to secure practices in manufacturing process shall be adopted according to a recognized standard.	
EIA_DLP.3	Software code development is done securely, taking into account, standard secure coding practices recommendations like OWASP.	
EIA_DLP.4	There is a Logically separate development environment from business/ production environment.	
EIA_DLP.5	There are access controls between developer environments and critical systems.	
EIA_DLP.6	The developer systems are hardened using a standard recommended list to reduce the attack surface.	

EIA_DLP.7	Before releasing production software images, a thorough assessment is done in order to remove all the unnecessary debug and symbolic information.	
EIA_DLP.8	The build environment and the toolchain used to create the software is under configuration management and version control and its integrity is validated regularly.	
EIA_DLP.9	Software Is developed such that fails safely.	
EIA_DLP.10	Cryptographic keys that are generated during manufacturing are generated as required by the standard referenced in the "Allowed Cryptography List".	
EIA_DLP.11	There is Secure & Scalable key management scheme for managing and provisioning keys assigned to all devices under production.	
EIA_DLP.12	Long-term service-layer keys (other than public keys) are stored in a server-HSM residing in infrastructure equipment.	
EIA_DLP.13	The HSM containing the M2M long-term service keys should be bound to the M2M Device or M2M Gateway, using physical and/or logical means.	
EIA_DLP.14	The process for secure provisioning of keys which includes generation, distribution, revocation and destruction should be done in compliance with a known standard.	
EIA_DLP.15	The cryptographic key chain used for signing production software SHALL be different from that used for any other test, development or other software images, to prevent the installation of non-production software into production devices. (Often test or development images have fewer restrictions and/or more privileges.)	
EIA_DLP.16	All the product related cryptographic functions are sufficiently secure for the lifecycle of the product.	
EIA_DLP.17	The secure provisioning of cryptographic keys for updates during manufacturing	

	must be done in accordance with the industry standards.	
EIA_DLP.18	The key insertion must take place securely such that it protects the keys against copying.	
EIA_DLP.19	All asymmetric encryption private keys that are unique to each device must be secured in accordance with accepted standards and truly randomly generated internally or securely programmed in to each device.	
EIA_DLP.20	A securely controlled area and process SHALL be used for device provisioning where the production facility is untrusted.	
EIA_DLP.21	The functional and/or technical specification document at least includes information on security measures used (eg architecture, access control, interfaces and communication security, policy enforcement, mobile security, cloud security, backup/disaster recovery).	
EIA_DLP.22	In each design document a chapter addressing security of all information and control systems in environment where the device can be used, SHALL be included.	
EIA_DLP.23	The supplier or manufacturer of the TOE SHALL provide information about how the device is setup to maintain the end user's privacy & security.	
EIA_DLP.24	The supplier or manufacturer of the TOE SHALL provide information about how the TOE's removal and/or disposal shall be carried out to maintain the end user's privacy and security.	
EIA_DLP.25	The supplier or manufacturer of the TOE provides clear information about the end user's responsibilities to maintain the devices and/or services privacy and security.	
EIA_DLP.26	Manufacturer SHALL develop a process in order to ensure that any devices with duplicate serial numbers are not shipped and they are either reprogrammed or destroyed.	

EIA_DLP.27	Ensure that your company has a consistent and up-to-date asset inventory. This inventory SHALL include, among others, IP addresses, physical location, host, current firmware/OS version, used communication protocols, etc. The asset inventory should also include gathered known vulnerabilities related to specific assets.	
EIA_DLP.28	Utilize tools supporting asset management (i.e. automatic asset discovery). Asset management systems should be solid and robust.	
EIA_DLP.29	All devices SHALL be logged by the product vendor, so that cloned or duplicated devices can be identified and either disabled or prevented from being used.	
EIA_DLP.30	Use a centralized asset inventory for the overall computerized environment inside a manufacturing plant.	
EIA_DLP.31	Define the scope of the data that will be processed by the device as well as the objective of this processing during the design phase.	
EIA_DLP.32	The device manufacturer SHALL ensure that the identity of the device is independent of the end user in order to ensure anonymity and this must be compliant with relevant local data privacy laws.	
EIA_DLP.33	Address cybersecurity through embedded features of endpoints rather than only on the network level.	
EIA_DLP.34	Adopt a holistic architectural-based approach and develop a risk-aligned security architecture based on business requirements.	
EIA_DLP.35	Perform risk and threat analysis involving cybersecurity experts from the very early stages of the design process of the device to find out which security features will be necessary.	
EIA_DLP.36	Devices and services SHALL be designed in such a way that security usability is kept in mind, reducing where possible, security	

	friction and decision points that may have a detrimental impact on security.	
EIA_DLP.37	If possible, limit the number of protocols implemented within a given TOE.	
EIA_DLP.38	Equip, after a security and safety assessment, the TOE with identification and authentication features and ensure compatibility with IAM class solutions.	
EIA_DLP.39	The device SHALL have all the production test and calibration software used during manufacture, erased or removed or secured before the product is dispatched from the factory.	
EIA_DLP.40	Where an application's user interface password is used for login authentication, the initial password or factory reset password is unique to each device in the product family.	
EIA_DLP.41	Password entry follows the standard recommendations of the Password policy.	
EIA_DLP.42	The mobile application ensures that any related databases or files are either tamper resistant or restricted in their access. Upon detection of tampering of the databases or files they are re-initialized.	
EIA_DLP.43	Implement certificate pinning and communication via secure channels (TLS) Where the application communicates with a remote server(s).	
EIA_DLP.44	Obscure passwords when they are being entered on a user interface, to prevent the capture of passwords.	
EIA_DLP.45	Comply with security best practices of a secure mobile application development e.g. (OWASP)	
EIA_DLP.46	There SHALL be policies defined for dealing with both internal & third party security researchers who are involved in the TOE development.	
EIA_DLP.47	The developer shall identify & document the development tools (programming languages and compiler, CAD systems) being used for the IoT device. The documentation of the development tools	

	shall unambiguously define the meaning of all statements as well as all conventions and directives used in the implementation.	
EIA_DLP.48	The documentation of the development tools shall unambiguously define the meaning of all implementation-dependent options.	
EIA_DLP.49	The developer shall document the selected implementation-dependent options of the development tools.	
EIA_DLP.50	The documentation of software development tools should include definitions of implementation-dependent options that may affect the meaning of the executable code, and those that are different from the standard language as documented.	
EIA_DLP.51	Where source code is provided to the evaluator, information should also be provided on compilation and linking options used.	
EIA_DLP.52	The documentation for hardware design and development tools should describe the use of all options that affect the output from the tools (e.g. detailed hardware specifications, or actual hardware).	

	INTEGRATION	SECURITY GOAL
EIA_INT.1	Consider security aspects during whole procurement process defining security measures and requirements tailored to devices/solutions.	
EIA_INT.2	Take into account security considerations throughout the whole supply chain. Monitor software, hardware and its components throughout the supply chain to detect and prevent unauthorized changes, e.g.	

	introduction of malware to the software.	
EIA_INT.3	At the ordering/procurement stage, provide the vendor with defined security requirements, including the security capability level of individual components.	
EIA_INT.4	Prompt suppliers for information on the security of their processes and commitments to the product they deliver, e.g. by preparing a questionnaire for suppliers regarding their security contributions to the items they deliver and select partners taking into account its results.	
EIA_INT.5	Clearly define all relevant aspects of the partnership with Third Parties, including security, within the appropriate agreements and contracts (e.g. SLA - service level agreement, NDA - Non-Disclosure Agreements).	
EIA_INT.6	Allow Third Parties to perform patching only if they guarantee and are able to prove that the patch has been tested and will not have any negative consequences on the device or if the Third Party assumes the liability for the update according to an applicable agreement.	
EIA_INT.7	Before implementation of change in the system configuration, configuration or addition of a new asset/solution, perform an analysis to determine the criticality of the considered change.	
EIA_INT.8	There are policies defined for addressing any changes that could impact security and affect the organisation's technology, the TOE's components or services rendered.	
EIA_INT.9	TOE Monitoring Tools and Solutions are tested to verify its effect on the system before deployment	

EIA_INT.10	Establish baseline security configurations tailored to all types of IoT assets used. In addition, establish procedures for reviewing and creating new baselines, and include this in the change management policy.	
EIA_INT.11	The configuration of the device and any related web services should be made tamper resistant.	
EIA_INT.12	Devices are tested and analysed, their impact and likely threats are studied before deployment.	
EIA_INT.13	Methodology for secure decommissioning and recommissioning of TOE is documented and followed by all concerned parties.	
EIA_INT.14	Avoid the usage of removable devices/removable media, if there are no accepted business requirements.	
EIA_INT.15	In the event of a factory reset, the device SHALL warn that the secure operation may be compromised unless updated.	
EIA_INT.16	The supplier or manufacturer of the device SHALL provide information about how the device will function within the end user's network.	
EIA_INT.17	The supplier or manufacturer of any devices and/or services SHALL provide information about how the device removal and/or disposal is to be carried out to maintain the end user's privacy and security.	
EIA_INT.18	The manufacturer SHALL document the Physical and Logical Boundary of the device including all hardware and software dependencies that enables the smooth functioning of the IoT device.	
EIA_INT.19	There SHALL be procedures defined for determining how an update may be securely applied in accordance with other requirements.	

EIA_INT.20	Audit and verify device onboarding/pairing process to be secure, robust and ensure it does not compromise network security.	
EIA_INT.21	Develop policies & procedures guiding automated device onboarding.	
EIA_INT.22	Automated device onboarding should include such actions as immediately allow/deny internet access; segmenting the device to a separate network section, etc.	
EIA_INT.23	Management of the infrastructure assets and security devices should occur via a dedicated secure management network.	
EIA_INT.24	Monitor the availability of the IoT devices in real time, where technically feasible.	
EIA_INT.25	Implement a mechanism and supporting tools that allow for configuration management. This mechanism should enable tracking of changes and recreation of the state of the system from before the change.	
EIA_INT.26	In case of extensive and diversified networks with a large number of devices, adopt the Privilege Access Management (PAM) solution to manage elevated privileges (i.e. administrator privileges) in an orderly manner.	

ANNEX III — SECURITY ASSURANCE ACTIVITIES MAPPING WITH IMPACTS/LIKELIHOOD

IMPACT VS LIKELIHOOD	UNLIKELY (1)	LIKELY (2)	VERY LIKELY (3)	ALMOST CERTAIN (4)
SEVERE (4)	CA.DocumentationReview CA.SourceCodeReview CA.CompositionAnalysis (if applicable) VA.VulnerabilityScanning	CA.DocumentationReview CA.SourceCodeReview CA.FunctionalSecurityTesting CA.CompositionAnalysis (if applicable) VA.VulnerabilityScanning VA.BasicRobustnessTesting	CA.DocumentationReview CA.SourceCodeReview CA.FunctionalSecurityTesting CA.CompositionAnalysis (if applicable) VA.VulnerabilityScanning VA.BasicRobustnessTesting VA.AdvancedRobustnessTesting VA.NonIntrusivePentesting	CA.DocumentationReview CA.SourceCodeReview CA.FunctionalSecurityTesting CA.CompositionAnalysis (if applicable) VA.VulnerabilityScanning VA.BasicRobustnessTesting VA.AdvancedRobustnessTesting VA.NonIntrusivePentesting VA.IntrusivePentesting
MODERATE (3)	CA.DocumentationReview CA.CompositionAnalysis (if applicable) VA.VulnerabilityScanning	CA.DocumentationReview CA.SourceCodeReview CA.CompositionAnalysis (if applicable) VA.VulnerabilityScanning VA.BasicRobustnessTesting	CA.DocumentationReview CA.SourceCodeReview CA.FunctionalSecurityTesting CA.CompositionAnalysis (if applicable) VA.VulnerabilityScanning VA.BasicRobustnessTesting VA.NonIntrusivePentesting	CA.DocumentationReview CA.SourceCodeReview CA.FunctionalSecurityTesting CA.CompositionAnalysis (if applicable) VA.VulnerabilityScanning VA.BasicRobustnessTesting VA.AdvancedRobustnessTesting VA.NonIntrusivePentesting
MINOR (2)	CA.DocumentationReview CA.CompositionAnalysis (if applicable)	CA.DocumentationReview CA.SourceCodeReview CA.CompositionAnalysis (if applicable)	CA.DocumentationReview CA.SourceCodeReview CA.CompositionAnalysis (if applicable) VA.VulnerabilityScanning VA.BasicRobustnessTesting	CA.DocumentationReview CA.SourceCodeReview CA.FunctionalSecurityTesting CA.CompositionAnalysis (if applicable) VA.VulnerabilityScanning VA.BasicRobustnessTesting
LOW (1)	CA.DocumentationReview CA.CompositionAnalysis (if applicable)	CA.DocumentationReview CA.CompositionAnalysis (if applicable)	CA.DocumentationReview CA.CompositionAnalysis (if applicable) VA.VulnerabilityScanning	CA.DocumentationReview CA.SourceCodeReview CA.CompositionAnalysis (if applicable) VA.VulnerabilityScanning

ANNEX IV — ALLOWED CRYPTOGRAPHY LIST

The goal of this list is to support the security requirements listed in Annex II above allowing on one side the vendor to implement recognized standard algorithms and the evaluator to validate the conformity of the implementation while spending less time on assessing their robustness at a substantial level.

This Annex is based on [FIDO Allowed Cryptography List], [BSI-TR-02102-1] and [RGS_v-2-0_B1].

The writings in **BLACK** indicates the input from FIDO document, the **BROWN** indicates the ones from BSI. And the in **RED** recommendations from RGS/ANSSI.

All the references are listed in the end.

FUTURE WORK:

This draft must address the light-weight cryptographic algorithms defined in [ISO/IEC 29192-2:2012] and supported by most common implementation of IoT devices.

A dedicated technical working group must review, decide and update this list on a yearly basis.

Allowed Cryptographic Functions

The stated security level identifies the expected number of computations that a storage-constrained attacker (who has access to no more than 2^{80} bytes of storage) shall expend in order to compromise the security of the cryptographic security function, under the currently best-known attack that can be conducted under this storage constraint. This has been extracted from the currently best-known relevant attacks against each cryptographic primitive and is expected to shift over time as attacks improve. If the security level stated is n , then the expected number of computations is less than the expected number of computations required to guess an $(n+1)$ -bit random binary string, and not less than the number of computations required to guess an n bit random binary string (i.e., on average, the number of computations required is less than 2^n computations and greater than or equal to $2^{(n-1)}$ computations).

Recommended key lengths for different cryptographic mechanisms [10]

Block cipher	MAC	RSA	DH Fp	DH (elliptic curve)	ECDSA
128	128	2000 ^a	2000 ^a	250	250

^aFor the period of use beyond 2022, the present Technical Guideline [10] recommends using a key length of 3000 bits in order to achieve a similar security level for all asymmetric schemes. The suitability of RSA, DSA and DLIES key sizes below 3000 bits will not be extended further. A key length of ≥ 3000 bits will be binding for cryptographic implementations which are to conform to this Technical Guideline as from 2023. Any key size ≥ 2000 is, however, in conformity with this Technical guideline until the end of 2022. More detailed information can be found in the Remarks 4 and 5 in Chapter 3. (Refer [10])

Confidentiality Algorithms

NOTE: Provide confidentiality, up to the stated security level

Algorithm	Specified in	Security Level (bits)
Three-Key	Triple-DES [ANSI-X9-52]	112[1]
AES-128	[FIPS197]	128
AES-192	[FIPS197]	192
AES-256	[FIPS197]	256

[1] Based on the standard meet-in-the-middle attack.

Three-key triple-DES is not allowed for any certification issued after January 1, 2020. This is due to the increased applicability of a weaknesses shared by all block ciphers with a 64-bit block size, and similar deprecation plans by other certification programs

NOTE: Since it can take many months to complete a certification it is suggested that no authenticators using three-key triple-DES start the certification process after July 1, 2019 so they likely have enough time to complete the certification process before January 1, 2020.

Hashing Algorithms

NOTE Provide pre-image resistance, 2nd pre-image resistance, and collision resistance

Algorithm	Specified in	Security Level (bits)
SHA-256	[FIPS180-4]	128
SHA-384	[FIPS180-4]	192
SHA-512	[FIPS180-4]	256
SHA-512/t, $256 \leq t < 512$	[FIPS180-4]	t/2
SHA3-256	[FIPS202]	128
SHA3-384	[FIPS202]	192
SHA3-512	[FIPS202]	256

NOTE: The hash function SHA-224 is no longer among the recommended algorithms. The hash functions of both the SHA-2 family and SHA-3 family are cryptographically strong. With respect to classical attacks on collision resistance and one-way properties, there is no practically relevant difference between the two function families that is known today. In certain other scenarios, there are differences; the functions of the SHA-3 family, for example, are resistant to length extension attacks.

Data Authentication Algorithms

NOTE : Provide data authentication

Algorithm	Specified in	Security Level (bits)	Key length	Recommended tag length
HMAC	[FIPS1981]	Minimum of the length of the output of the hash used [2], one-half of the number of bits in the hash state [3], or the number of bits in the HMAC key.	≥ 128	≥ 96

CMAC	[SP80038B]	Equal to the minimum of the strength of the underlying cipher and the length of the output MAC.	≥ 128	≥ 96
GMAC	[SP80038D]	Equal to the minimum of the strength of the underlying cipher and the length of the output MAC.	≥ 128	≥ 96

[c2] Both due to the obvious guessing attack and covers the case where the supplied key is hashed for the HMAC.

[3] Based on a birthday attack; a collision of the final state can lead to an existential forgery of longer messages with the same prefix

For the application of these schemes, the following recommendations must be observed [10]:

1. As for the tag length, ≥ 96 bits are recommended for general cryptographic applications in all three schemes. As an absolute minimum for general applications, the recommendation is to use 64 bits. Shorter tag lengths should only be used after all circumstances affecting the respective application have been taken into consideration by experts. For GMAC tags, there are attacks in which forgeries of tags of the length t for messages of a length of n blocks are possible with a probability of $2^{-t+\log_2(n)}$ per attempt and where this probability increases further if successful forgeries are detected [12]. This means that, with the same tag length, GMAC (and thus also the authenticated encryption mode GCM) provides a weaker protection of integrity than it is expected for CMAC or HMAC with the block ciphers and/or hash functions recommended in this document. The practical relevance of these attacks grows significantly if short authentication tags (< 64 bits) are used. The use of short tags with GMAC/GCM is therefore strongly discouraged.
2. The authentication keys used must be protected just as well as other cryptographic secrets in the same context.

Key Protection Algorithms

NOTE: Provide confidentiality and data authentication.

Algorithm	Specified in	Security Level (bits)
Key Wrapping	[SP800-38F]	Equal to the strength of the underlying cipher.
GCM Mode, with length 96 bit or larger IVs. For any given key, the IV length must be fixed.	[SP800-38D]	Equal to the strength of the underlying cipher.
RSA OAEP	[RFC3447]. Key generation must be according to [FIPS186-4].	112
CCM Mode	[SP800-38C]	Equal to the strength of the underlying cipher.

Encrypt-then-HMAC[4]	Encryption specification depends on the cipher selected. HMAC specification [FIPS198-1]	The minimum of the strength of the cipher and the HMAC.
Encrypt-then-CMAC[5]	Encryption specification depends on the cipher selected. CMAC specification [SP800-38B]	The minimum of the strength of the cipher and the CMAC.

[4] The cipher and HMAC shall use independent keys, and the information HMACed shall include any IV / Nonce / Counter (if sent/stored), and, if the message size varies, the length of the message; when present, this message length shall reside prior to any variable length message components.

[5] The cipher and CMAC shall use independent keys, and the information CMACed shall include any IV / Nonce / Counter (if sent/stored).

Conditions of use in different Modes of operation [10]

1. For GCM:

- Initialisation vectors may not repeat themselves within a key change period. More precisely, two AES encryptions (i.e. applications of the underlying AES block cipher) with the same input values (key, message) must not be carried out in the entire mechanism.
- Moreover, GCM requires the generation of nonce for the integrated authentication mechanism.
- For general cryptographic applications, GCM with a length of the GCM tags of at least 96 bits should be used. For special applications, shorter tags can be used as well upon consultation with experts. In this case, the guidelines for the number of allowed calls of the authentication function with a shared key from [11] must be complied with strictly.

2. For CBC:

- Only unpredictable initialisation vectors are to be used.
- The CBC Mode requires an additional padding step: When partitioning a plaintext to be encrypted, it may occur that the last plaintext block is smaller than the block size of the cipher used. Formatting realised by filling this last block in order to achieve the size required is also referred to as padding.

Random Number Generator

Physical/True (TRNG)/Non-Deterministic Random Number/Bit Generator (NRBG) Requirements

The (physical) random number generator shall meet the requirements specified in:

1. AIS 20/31 PTG.2 or PTG.3 or in

NOTE

If PTG.2 is used, an application-specific post processing may additionally be required to prevent any bias in the output function.

For instance, these requirements are met if a certified hardware platform is used (e.g. according to Global Platform TEE Protection Profile or Eurosmart Security IC Platform

Protection Profile) and the Security Target contains Extended Component FCS_RNG.1 including at least one of the allowed classes PTG.2, or PTG.3.

2. NIST SP800-90C NRBG [\[SP800-90C\]](#) or in

Algorithm	Specified in	Security Level (bits)
Source RBG is DRBG with access to Live Entropy Source or it is an NRBG.	[SP800-90C] , SECTION 6	Any security strength.

3. NIST FIPS 140-2 [\[FIPS140-2\]](#) validation (issued on August 7th 2015 or after), with Entropy Source Health Tests. The related security level is as defined in the module's security policy.

We consider this a physical RNG if at least as much entropy is added into the RNG as is retrieved per request.

NOTE

It is uncommon for the DRBGs in FIPS modules to meet these requirements, unless their design anticipates one of the SP800-90C NRBG designs.

The security strength (in bits) of an allowed physical/true random number generator is equivalent to the size (in bits) of the random bytes retrieved from it.

If a physical random number generator is used, it is generally recommended to use a PTG.3 generator in accordance with AIS 31 [13]. This applies in particular to applications in which an adversary is at least in principle able to combine information about different random numbers. For certain specific applications, a class PTG.2 random number generator is sufficient. It is possible to construct a PTG.3 generator from of a PTG.2 generator by cryptographically post-processing the output of the PTG.2 generator in a suitable manner. This post-processing can usually be implemented in software.

Broadly speaking, PTG.2- and/or PTG.3-conformant random number generators must fulfil the following properties:

1. The statistical properties of the random numbers can be described sufficiently well by means of a stochastic model. Based on this stochastic model, the entropy of the random numbers can be reliably estimated.
2. The average increase in the entropy per random bit is above a given minimum limit (close to 1).
3. The digitised noise signals are subjected to statistical tests online, which are suitable to detect unacceptable statistical defects or deteriorations in the statistical properties within a reasonable period of time.
4. A total failure of the noise source is de facto identified immediately. Random numbers which were generated after a total failure of the noise source must not be output.
5. If a total failure of the noise source or unacceptable statistical defects of the random numbers are identified, this results in a noise alarm. A noise alarm is followed by a defined, appropriate response (e.g. shutting down the noise source).
6. (Only PTG.3-conformant random number generators) The (possibly supplementary) strong cryptographic post-processing ensures that the security level of a DRG.3-conformant deterministic random number generator is still assured even if a total failure of the noise source is not noticed.

Deterministic Random Number (DRNG)/Bit Generator (DRBG) Requirements

NOTE

Provide computational indistinguishability from an ideal random sequence, cycle resistance, non-destructive reseeding, insensitivity of a seeded generator to seed source failure or compromise, backtracking resistance. Ideally, the ability to provide additional input, and ability to recover from a compromised internal state.

The (deterministic) random number generator shall meet the requirements specified in:

1. AIS 20/31 DRG.3 or DRG.4 (having an entropy of the seed of at least N bits, where N is the targeted security level) or in
2. NIST SP800-90A DRBG [[SP800-90ar1](#)],

Algorithm	Specified in	Security Level (bits)
HMAC_DRBG	[SP800-90ar1] , Revision 1, SECTION 10.1.2	The instantiated security level, as defined in [SP800-90ar1] .
CTR_DRBG	[SP800-90ar1] , Revision 1, SECTION 10.2.1	The instantiated security level, as defined in [SP800-90ar1] .
HASH_DRBG	[SP800-90ar1] , Revision 1, SECTION 10.1.1	The instantiated security level, as defined in [SP800-90ar1] .

3. or in NIST FIPS 140-2 [[FIPS140-2](#)] validation (issued on August 7th 2015 or after).

NOTE

We consider this a deterministic RNG if less entropy is added into the RNG than is retrieved.

NOTE

The [\[SP800-90ar1\]](#) standard requires that the DRBG must be seeded using either another [\[SP800-90ar1\]](#) Approved DRBG, or an Approved [\[SP800-90b\]](#) entropy source. [\[FIPS140-2\]](#) further allows for testing as described in IG7.15.

The internal state of a deterministic random number generator must be protected reliably against readout and manipulation.

If a deterministic random number generator is used, it is recommended to use a DRG.3- or DRG.4-conformant random number generator against the potential of attack high in accordance with AIS 20 [13]

1. It is practically impossible for an adversary to calculate predecessors or successors for a known random number sequence or to guess them with a significantly higher probability than would be possible without knowing this subsequence.

2. It is practically impossible for an adversary to calculate previously outputted random numbers based on the knowledge of an internal state or to guess them with a significantly higher probability than would be possible without knowing the internal state.
3. (Only DRG.4-conformant random number generators) Even if an adversary knows the current internal state, it is practically impossible for them to calculate random numbers which are generated after the next reseed / seed update or to guess them with a significantly higher probability than would be possible without knowing the internal state. Also, with respect to implementation attacks, DRG.4 generators have certain advantages over DRG.3-conformant random number generators.

Non-physical non-deterministic random number generators [10]

For many cryptographic applications, such as in e-business or e-government, neither a physical nor a deterministic random number generator are available, since they generally run on computers without certified cryptographic hardware. Non-physical non-deterministic random number generators (NPTRNG) are usually used instead. For more information, refer [10].

Key Derivation Functions (KDFs)

Deriving keys.

Algorithm	Specified in	Security Level (bits)
KDF in counter mode	[SP800-108]	min(Bit length of key derivation key K_i used as input, Security level of PRF)
KDF in feedback mode	[SP800-108]	min(Bit length of key derivation key K_i used as input, Security level of PRF)
KDF in double pipeline iteration mode	[SP800-108]	min(Bit length of key derivation key K_i used as input, Security level of PRF)
HKDF	[SP800-56cr1], [RFC5869]	min(Bit length of key derivation key K_i used as input, Security level of HMAC)

Where PRF denotes an acceptable pseudorandom function as defined in [SP800-108].

NOTE: The following method is recommended for all applications of key derivation functions: “Key derivation through extraction-then-expansion according to [20]”.

Signature Algorithms

NOTE

Provide data authentication, and non-repudiation.

Algorithm	Specified in	Security Level (bits)
ECDSA on P-256	[ECDSA-ANSI], [FIPS186-4]	128
2048-bit RSA PSS	[FIPS186-4]	112
1024*n-bit RSA PKCS v1.5 (n=2,3,4)	[FIPS186-4]	112
ECDSA on secp256k1	[ECDSA-ANSI], [FIPS186-4], Certicom SEC 2	126[7]

SM2 digital signatures (SM2 part 2) using the SM3 hash on the SM2 curve specified by OSCCA.	SM2 [ISO.IEC.14888-3] SM3 [ISO.IEC.10118-3]	128
Ed25519	EDDSA [RFC8032]	128[8]
ECGDSA, ECKDSA	see [17, 15],	
RSA,	see [14],	
DSA,	see [15] and [16],	
Merkle signatures	see [18]	

[7] Based on an attack using Pollard rho on the equivalence classes defined by the curve's easily computable endomorphism.

[8] Based on the difficulty of performing discrete logs on the group defined by the recommended curve parameters.

a: Merkle signatures differ from the other signature algorithms recommended here in essential aspects. In contrast to the signature algorithms described so far, the security of the algorithm described in [18] is only based on the cryptographic strength of a hash function and a pseudo-random function family. In particular, no assumptions on the absence of efficient algorithms for problems from algorithmic number theory such as the RSA problem or the calculation of discrete logarithms are needed. It is therefore generally assumed that Merkle signatures would, unlike all other signature algorithms recommended in [10], also remain secure against attacks using quantum computers

BIS_document_Page 36: Usage of the older PKCS#1v1.5 paddings is not recommended, as in this context variations of the Bleichenbacher attack have repeatedly turned out to be a problem.

RGS_French_Page 21: The RSASSA asymmetric signature mechanism, implemented according to the PKCS # 1 v 1.5 document, does not conform to the repository when the public exponent e is small and for a poor choice of placement of verifications related to the padding. In effect, Bleichenbacher highlighted in 2006 an attack allowing to forge signatures in this case.[21]

Anonymous Attestation Algorithms

NOTE

Provide anonymous attestation.

The strength in this section is the minimum of three values:

1. The strength of the underlying hash.
2. The difficulty of conducting a discrete log within the Elliptic Curve.
3. The difficulty of conducting a discrete log within a finite field in which the Elliptic Curve can be embedded (we'll refer to this field as the embedding field).

In most cases, the limiting factor was the difficulty of performing the discrete log calculation within the embedding field.

The security level values here were taken from NIST guidance. This NIST guidance is based on conducting the discrete log calculation within prime ordered fields; the structure of the fields here is richer, and this structure could possibly allow for a more advanced discrete log approach that could be considerably faster. Currently, the best-known algorithms in both cases have the same asymptotic complexity ($L_q[1/3]$), but without extensive testing, it isn't clear how the number of computations compares.

In addition, the NIST guidance does not allow for security levels other than a few specific proscribed values: if the number of bits required to represent the order of the embedding field is between 3072 and 7679, the security level is reported as 128 bits. Similarly, if the number of bits required to represent the order of the embedding field is between 2048 and 3071, the security strength is reported as 112 bits.

Algorithm	Specified in	Security Level (bits)
ED256	[FIDOEcdaaAlgorithm], section Object Formats and Algorithm Details, [TPMv2-Part4]	128
ED256-2	[FIDOEcdaaAlgorithm], section Object Formats and Algorithm Details, [DevScoDah2007]	112
ED512	[FIDOEcdaaAlgorithm], section Object Formats and Algorithm Details, [ISO15946-5]	128
ED638	[FIDOEcdaaAlgorithm], section Object Formats and Algorithm Details, [TPMv2-Part4]	128

Recommended password length for the access to cryptographic hardware components [10]

The following constraints are recommended:

1. In general, it is recommended to use passwords with an entropy of at least $\log_2(106)$ bits. This can be achieved, for example, by means of an ideally random assignment of six-digit PINs (see also [19], Section 4.3.3).
2. The number of consecutive unsuccessful attempts to gain access must be limited tightly. In the case of a password entropy of $\log_2(106)$ bits, a restriction to three attempts is recommended.

ALLOWED CRYPTOGRAPHY LIST REFERENCES

FIDO Authenticator Allowed Cryptography List <https://fidoalliance.org/specs/fido-v1.0--20180629/fido-allowed-crypto-v1.0--20180629.html>

[ANSI-X9-52] Triple Data Encryption Algorithm Modes of Operation. July 29, 1998. Current. URL:

[DevScoDah2007] Augusto Jun Devegili; Michael Scott; Ricardo Dahab. Implementing Cryptographic Pairings over Barreto-Naehrig Curves. 2007. URL: <https://eprint.iacr.org/2007/390.pdf>

[ECDSA-ANSI] Public Key Cryptography for the Financial Services Industry - Key Agreement and Key Transport Using Elliptic Curve Cryptography ANSI X9.63-2011 (R2017). 2017. URL: [https://webstore.ansi.org/RecordDetail.aspx?sku=ANSI+X9.63-2011+\(R2017\)](https://webstore.ansi.org/RecordDetail.aspx?sku=ANSI+X9.63-2011+(R2017))

[FIDOEcdaaAlgorithm] R. Lindemann; J. Camenisch; M. Drijvers; A. Edgington; A. Lehmann; R. Urian. FIDO ECDAa Algorithm. Review Draft. URL: <https://fidoalliance.org/specs/fido-uaf-v1.2-rd-20171128/fido-ecdaaalgorithm-v1.2-rd-20171128.html>

[FIPS140-2] FIPS PUB 140-2: Security Requirements for Cryptographic Modules. May 2001. URL: <http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>

[FIPS180-4] FIPS PUB 180-4: Secure Hash Standard (SHS). March 2012. URL: <http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf>

[FIPS186-4] FIPS PUB 186-4: Digital Signature Standard (DSS). July 2013. URL: <http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf>

[FIPS197] FIPS PUB 197: Specification for the Advanced Encryption Standard (AES). November 2001. URL: <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>

[FIPS198-1] FIPS PUB 198-1: The Keyed-Hash Message Authentication Code (HMAC). July 2008. URL: http://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf

[FIPS202] FIPS PUB 202: SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions. August 2015. URL: <http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf>

[ISO15946-5] ISO/IEC 15946-5 Information Technology - Security Techniques - Cryptographic techniques based on elliptic curves - Part 5: Elliptic curve generation. URL: <https://webstore.iec.ch/publication/10468>

[RFC3447] J. Jonsson; B. Kaliski. Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1. February 2003. Informational. URL: <https://tools.ietf.org/html/rfc3447>

[RFC5869] H. Krawczyk; P. Eronen. HMAC-based Extract-and-Expand Key Derivation Function (HKDF). May 2010. Informational. URL: <https://tools.ietf.org/html/rfc5869>

[RFC8032] S. Josefsson; I. Liusvaara. Edwards-Curve Digital Signature Algorithm (EdDSA). January 2017. Informational. URL: <https://tools.ietf.org/html/rfc8032>

[SP800-108] Lily Chen. NIST Special Publication 800-107: Recommendation for Key Derivation Using Pseudorandom Functions. October 2009. URL: <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-108.pdf>

[SP800-38B] M. Dworkin. NIST Special Publication 800-38B: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication. May 2005. URL: <http://dx.doi.org/10.6028/NIST.SP.800-38B>

[SP800-38C] M. Dworkin. NIST Special Publication 800-38C: Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality. July 2007. URL: http://csrc.nist.gov/publications/nistpubs/800-38C/SP800-38C_updated-July20_2007.pdf

[SP800-38D] M. Dworkin. NIST Special Publication 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC. November 2007 URL: <https://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf>

[SP800-38F] M. Dworkin. NIST Special Publication 800-38F: Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping. December 2012. URL: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38F.pdf>

[SP800-56Cr1] Elaine Barker; Lily Chen; Rich Davis. NIST Special Publication 800-56C revision 1: Recommendation for Key Derivation Methods in Key Establishment Schemes. April 2018. URL: <https://doi.org/10.6028/NIST.SP.800-56Cr1>

[SP800-90C] Elaine Barker; John Kelsey. NIST Special Publication 800-90C: Recommendation for Random Bit Generator (RBG) Constructions. August 2012. URL: http://csrc.nist.gov/publications/drafts/80090/sp800_90c_second_draft.pdf

[SP800-90Ar1] Elaine Barker; John Kelsey. NIST Special Publication 800-90a: Recommendation for Random Number Generation Using Deterministic Random Bit Generators. August 2012. URL: <http://dx.doi.org/10.6028/NIST.SP.800-90Ar1>

[SP800-90b] Elaine Barker; John Kelsey. NIST Special Publication 800-90b: Recommendation for the Entropy Sources Used for Random Bit Generation. April 2016. URL: <http://csrc.nist.gov/publications/drafts/800-90/draft-sp800-90b.pdf>

[TPMv2-Part4] Trusted Platform Module Library, Part 4: Supporting Routines. URL: http://www.trustedcomputinggroup.org/files/static_page_files/8C6CABBC-1A4B-B294D0DA8CE1B452CAB4/TPM%20Rev%202.0%20Part%204%20%20Supporting%20Routines%2001.16-code.pdf

[10] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf?__blob=publicationFile&v=8

[11] NIST. Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) for Confidentiality and Authentication, Special Publication SP800-38D, National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, November 2007.

[12] N. Ferguson, Authentication Weaknesses in GCM, 2005. Available at <http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/comments/CWC-GCM/Ferguson2.pdf>.

[13] W. Killmann, W. Schindler: Functionality classes for random number generators. Federal Office of Information Security (BSI), Version 2.0, 18.09.2011, mathematical-technical annex to [2] and [3]. Available at https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_31_Functionality_classes_for_random_number_generators_e.pdf.

[14] ISO/IEC 14888-2-2008 Information technology – Security techniques – Digital signatures with appendix – Part 2: Integer factorization-based mechanisms, 2008.

[15] ISO/IEC 14888-3-2006. Information technology – Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm-based mechanisms, 2006.

[16] Federal Information Processing Standards Publication 186-4 (FIPS PUB 186-4), Digital Signature Standard (DSS), 2013.

[17] BSI, Elliptic Curve Cryptography, BSI Technical Guideline TR-03111, Version 2.0, 2012, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03111/BSI-TR-03111_pdf.html.

[18] J. Buchmann, E. Dahmen, A. Hülsing XMSS—A Practical Forward Secure Signature Scheme Based on Minimal Security Assumptions, Fourth International Conference in Post-Quantum Cryptography, LNCS 7071/2011, 117-129.

[19] Federal Information Processing Standards Publication 140-2 (FIPS PUB 140-2), Security Requirements for Cryptographic Modules, 2002

[20] NIST Recommendation for Key Derivation through Extraction-then-Expansion, Special Publication SP800-56C, National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, 11/2011.

[21] RGS https://www.ssi.gouv.fr/uploads/2015/01/RGS_v-2-0_B1.pdf

BETA RELEASE

ANNEX V- THREATS CATALOGUE

T01. Replay of data

In a "replay attack" (replay of data) attackers record valid messages and play this information later almost unchanged. Also, only part of a message may suffice, such as a password, to enter into an IT system without authorisation.

T02. Disclosure of data (stored, processed, transported)

The threat of valuable data about a device or system being revealed such that this data can be used by an attacker to gain understanding of possible attack paths, device commands, installed security controls, etc.

T03. Manipulation or injection of data (stored, processed, transported)

The threat of unwanted and unauthorized data modification by an attacker. This may apply to compromising IT, OT or production supporting systems, such as SCADA, MES, Historian and manipulation of process data. In the slightly different injection, attackers send specially prepared messages to individuals or devices within the system with the aim of gaining an advantage for themselves or to cause damage or change output. To construct the messages in a proper way, attackers use interface descriptions, protocol specifications, or records logging of the communication behavior from the past.

T04. Deletion of data (stored, processed, transported)

The threat of losing all data in its storage, in transport or while being processed. This generally results in a denial of service which could, in some cases lead to a system collapse, like in cases of high availability systems.

T05. Vandalism or Theft of device, storage media, etc.

The threat of causing physical damage to the device by a saboteur who gains physical access to the OT environment - either an outsider who has managed to bypass insufficient physical security measures or an insider, e.g. a disgruntled employee who, for some reasons, wants to harm the organization. This threat also includes theft.

T06. Loss of device, storage media, etc.

Data loss may also occur due to damage, loss or theft of devices or data storage media. This risk is extremely high in case of mobile terminals and removable data storage media.

T07. Compromise of personal data/sensitive info/ confidential info etc.

The threat of compromising personal / sensitive information stored on devices or in the cloud. The attacker's goal is to gain unauthorized access to this kind of data and use it in an illicit manner. In manufacturing companies this may apply to names and roles of system users. Production data is not considered to be subject to privacy, but it may also pose problems if it can be linked to the performance of individual employees. When the target is a manufacturing company, the attacker may, for instance, attempt to steal formulas or recipes and sell them to the competition.

T08. Unauthorized use or administration of devices & systems

The Use of an IT system includes not only the possibility to legally use particular services of this IT system pertaining to this interface, but also the risk of unauthorized access to the IT system via this interface.

T09. Physical access to user workstation/devices by malicious external actor

Threat of unauthorized manipulation of devices, software or applications within an OT system by an attacker.

T010. Lack of organizational policies & Procedures

The threat of attacks happening due to:

1. absence/incoherent/non-exhaustive security policies,
2. non-adherence to existing security policies,
3. Lack of/insufficient skilled human resources
4. Failure to use devices in accordance with the manuals and guidelines
5. Lack of maintenance of devices, sensors control systems,
6. Unintentional data (or configuration) change by an insufficiently trained employee, etc.

T011. Substandard, malicious or fake device components

The threat of being supplied a device with substandard or malicious component. This generally leads to advanced persistent threats (APTs) where the attacker lies deep within the system for prolonged periods, usually very difficult to detect.

T012. Regulatory Sanctions.

A typical case of this is the abuse of personal data law, for example, which takes place if an institution collects, too much personal data, collects it without legal basis or consent, uses it for purposes different from the objective stated at the time of collecting, deletes personal data too late or discloses such data in an unauthorized manner, etc.

This also includes the threat of violating contractual requirements by 3rd party components manufacturers and software providers in case of failure to ensure the required security measures.

T013. Malicious access to device/system assets.

The threat of gaining unauthorized access to an organization's resources (i.e. data, systems, devices, etc.) by exploiting:

1. weak/ default credentials,
2. software bugs,
3. lack of updates
4. insecure ports etc.

T014. Failure or malfunction of the power supply

The threat of failure or malfunction of the power supply. If no emergency power supply exists for critical systems, any power supply disruption may result in serious consequences due to a sudden shutdown of production processes.

T015. Unavailability of communication systems

The threat of unavailability of communication links related to problems with cable, wireless or mobile network.

T016. Failure or disruption of service providers

The threat of disruption of processes that rely on third party services in case of failure or malfunction of these services.

T017. Failure of Internal information systems

The threat of failure, malfunction or crash of operating systems, firmware or other complex programs supporting production or logistics, i.e. MES, ERP and CRM.

T018. Environmental disasters

The threat of incidents and unfavorable conditions such as fires, pollution, dust, corrosion, explosions, which may cause physical damage to OT environment components.

T019. Natural disasters

The threat of natural disasters such as floods, lightning strikes, heavy winds, rain and snowfall, which may cause physical damage to the OT environment components.

T020. Interfering radiation

Due to electromagnetic interference having an effect on electronic components in devices, electronic devices can be impaired in their function or even damaged. As a consequence, disruptions, wrong processing results or communication errors/disruptions can occur, among other failures/threats.

T021. Network Denial of service

An IoT system can be targeted, resulting in system unavailability and production disruption caused by a massive number of requests sent to the system.

T022. Intercepting compromising emissions

Electrical devices emit electromagnetic waves. In cases of equipment which process information (e.g. computers, displays, network coupling elements, printers) this radiation can also carry the information currently being processed with it. Such information-bearing radiation is called expositional or compromising emissions.