ETSI TR 103 946 V1.1.1 (2023-10)

Methods for Testing & Specification (MTS);
Security validation of IoT architecture application and conformity;
Case Study Experiences

Reference
DTR/MTS-TST11Sec_IoTconf

Keywords
conformity, IoT, security, testing

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

BLUETOOTH® is a trademark registered and owned by Bluetooth SIG, Inc.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Methods for Testing and Specification (MTS).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The goal of the present document is to compile case study experiences related to the security validation and assurance for the integration and conformity of IoT applications with an existing IoT architecture in order to have a common understanding in MTS and related committees and to support trustworthiness. Industrial experiences may cover but are not restricted to the following domains: smart home, smart grid, unmanned air systems, automated driving.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] IEC 60730-1: "Automatic electrical controls - Part 1: General requirements".

[i.2] IEC 61508: "Functional safety of electrical/electronic/programmable electronic safety-related systems".

[i.3] IEC 61850: "Communication networks and systems for power utility automation".

[i.4] STANAG 4586: "Standard Interfaces of UAV Control System (UCS) for NATO UAV Interoperability - AEP-84 Edition A".

[i.5] UL 991: "Tests for Safety-Related Controls Employing Solid-State Devices".

[i.6] UL 1998: "UL Standard for Safety Software in Programmable Components".

[i.7] ETSI TS 103 942: "Testing (MTS); Security Testing; IoT Security Functional Modules".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

MODBUS: network protocol used in the industrial manufacturing sector

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

4G	4th Generation (mobile networks) also known as LTE
5G	5th Generation (mobile networks)
AD	Attack Detection
AI	Artificial Intelligence
API	Application Programming Interface
AUDRIC	AUtomated DRIving Core
C2	Command and Control
C4I	Command, Control and Coordination Centre Infrastructure
CAM	Cooperative Awareness Message
CAN	Controller Area Network
CAV	Connected and Automated Vehicle
CERTH	CEntre for Research & Technology Hellas
DARIUS	Integrated Deployable SAR chain with Unmanned Systems
DENM	Decentralized Environmental Notification Message
DER	Distributed Energy Resources
DFD	Dataflow Diagram
DSRC	Dedicated Short Range Communication
ECU	Electronic Control Unit
EO/IR	Electro-Optical/Infra-Red
FEAM	Front-End Access Management
GCS	Ground Control Station
GGCS	Generic Ground Control Station
GGS	Generic Ground Station
GPS	Global Positioning System
GPU	Graphics Processing Unit
GSM	Global System for Mobile communication
ICT	Information and Communication Technology
ID	Identity
IEC	International Electrotechnical Commission
IMU	Inertial Measurement Unit
IoT	Internet of Things
IoTAC	Security by design IoT development and certificate framework with front-end Access Control
IR	Infrared
IT	Information Technology
ITI	Informatics and Telematics Institute
ITS	Intelligent Transportation Systems
JSON	JavaScript Object Notation
MODBUSRTU	MODBUS Remote Terminal Unit
MODBUSTCP	TCP-based MODBUS protocol
MQTT	Message Queueing Telemetry Transport
MTS	Methods for Testing & Specification
nZEB	near-Zero-Emission Building
OBU	On-Board Unit
PC	Personal Computer
PLC	Programmable Logic Controller
PMR	Personal Mobile Radio
PV	PhotoVoltaic
SAE	Society of Automotive Engineers
SEGOVYA-RT	SafE Generator of Vehicle trajectory using lAne information on Real-Time
SITL	Software-In-The-Loop
SME	Small and Medium Enterprise
STANAG	NATO Standardization Agreement
STRIDE	Spoofing, Tampering, Repudiation, Information disclosure, Denial of service and Elevation of privilege
TCP	Tactical Command Post
TLS	Transport Layer Security
TR	Technical Report

UAV	Unmanned Aerial Vehicle (drone)
UDP	User Datagram Protocol
UI	User Interface
UL	Underwriters Laboratories
V2V	Vehicle to Vehicle
V2X	Vehicle to Everything
VPN	Virtual Private Network
VTOL	Vertical Take-Off and Landing
WC	Water Closet
Wi-Fi®	Wireless Fidelity

4 Description of a general IoT Security architecture

Refer to [i.7], clause 4 for a description of the general IoT security architecture upon which the present document is based.

5 Testing and Assurance Process for IoT Applications Using the General IoT Security Architecture

Integration validation of modules is a process aimed at ensuring that the modules successfully integrate into the pilot environment and meet the required security requirements. The process involves several steps:

1) Identifying generic misuse cases relevant to the pilot (critical, high priority). These cases are grouped by processes (data collection process, storage, processing, control process, client interface).

2) Identifying pilot-specific misuse cases.

3) Identifying pilot-specific security baseline requirements addressing the generic misuse case.

4) Identifying which IoTAC modules prevent which misuse cases by implementing the security baseline requirement.

5) Checking if and how the IoTAC module is integrated into the pilot environment. To do this, the following steps are taken:

   a) Checking the architectural integration of the IoTAC modules.

   b) Checking which aspect of the security baseline requirement is implemented by the IoTAC module.

   c) Checking if the integration of the IoTAC module allows the realization of the security requirement in the context of the pilot, e.g. if the related pilot misuse case can be prevented.

The process of integrating module validation is essential in ensuring the secure integration of modules and the maintenance of the integrity and security of data and systems within the pilot environment. One of the main goals of this process is to identify and address any potential misuse cases to prevent them and guarantee the overall security of the system. To achieve this, security baseline requirements provide a set of guidelines to follow. By identifying which IoTAC modules address which misuse cases, it is possible to ensure that the appropriate measures are in place to mitigate these issues. Additionally, it is important to carefully check the integration of the IoTAC modules into the pilot environment to verify that they can effectively address the identified misuse cases and meet the security requirements.

The process of integrating module validation has two key outcomes. The first outcome is a determination of which misuse cases are covered using IoTAC modules. The second outcome is potential findings that should help the pilot's developers increase security by completely addressing their misuse cases when using the IoTAC modules.

6 Experiences with different IoT Application Domains (Case Study Samples)

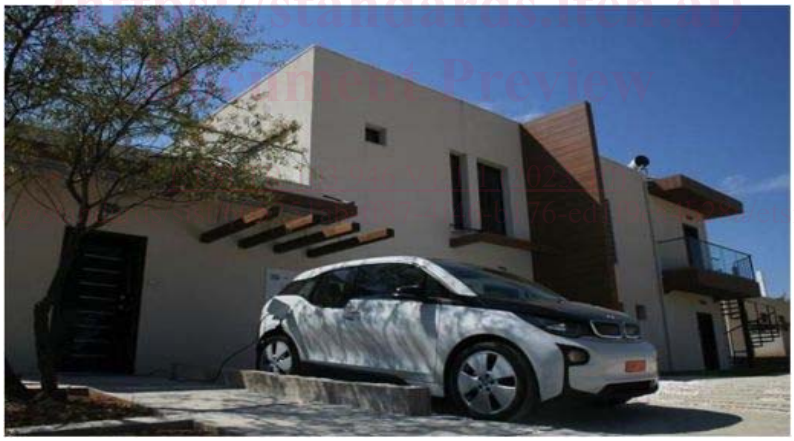
6.1 Smart Home

6.1.1 Description and Objectives

The objective of the pilot is to validate the components and services developed by the loTAC project in the smart home application domain. The Smart House of CERTH provides an ideal environment for this purpose. In order to achieve the project's objectives, a Smart Home Pilot System over the existing infrastructure of CERTH has been defined by specifying the basic functional requirements and use-cases and identifying the most important non-functional requirements as well. A STRIDE-based threat- analysis has been executed to derive security requirements.

CERTH/ITI Smart House introduces the first house in Greece that combines enhanced construction materials and intelligent ICT solutions creating a future-proof, sustainable and active testing, validating, and evaluating environment. The house is representative of a single-family, detached residential building and is already equipped with many loT, smart home solutions that provide a lot of information about its operational characteristics. More specifically, it provides various innovative smart loT-based technologies with provided Energy, Healthcare, Big Data, Robotics and Artificial Intelligence (AI) services. The Smart House is equipped with a vast variety of sensors, actuators, smart home devices and intelligent robots. The building can operate as a microgrid by utilizing the proximity PhotoVoltaic (PV) plant and the battery unit available.

The Smart House is a single two-floor building (Figure 1). It is divided into two principal sections, the main household (living room, kitchen, bedrooms, hallways, WC, bath, etc.) and three ancillary control rooms on the left and right wings of the building. It does not have physical connection with other buildings.



(Source: IoTAC project)

Figure 1: nZEB Smart House at CERTH/ITI's premises

The Smart House Infrastructure provides appliances for supporting applications of highly diverse domains, as illustrated in Figure 2.

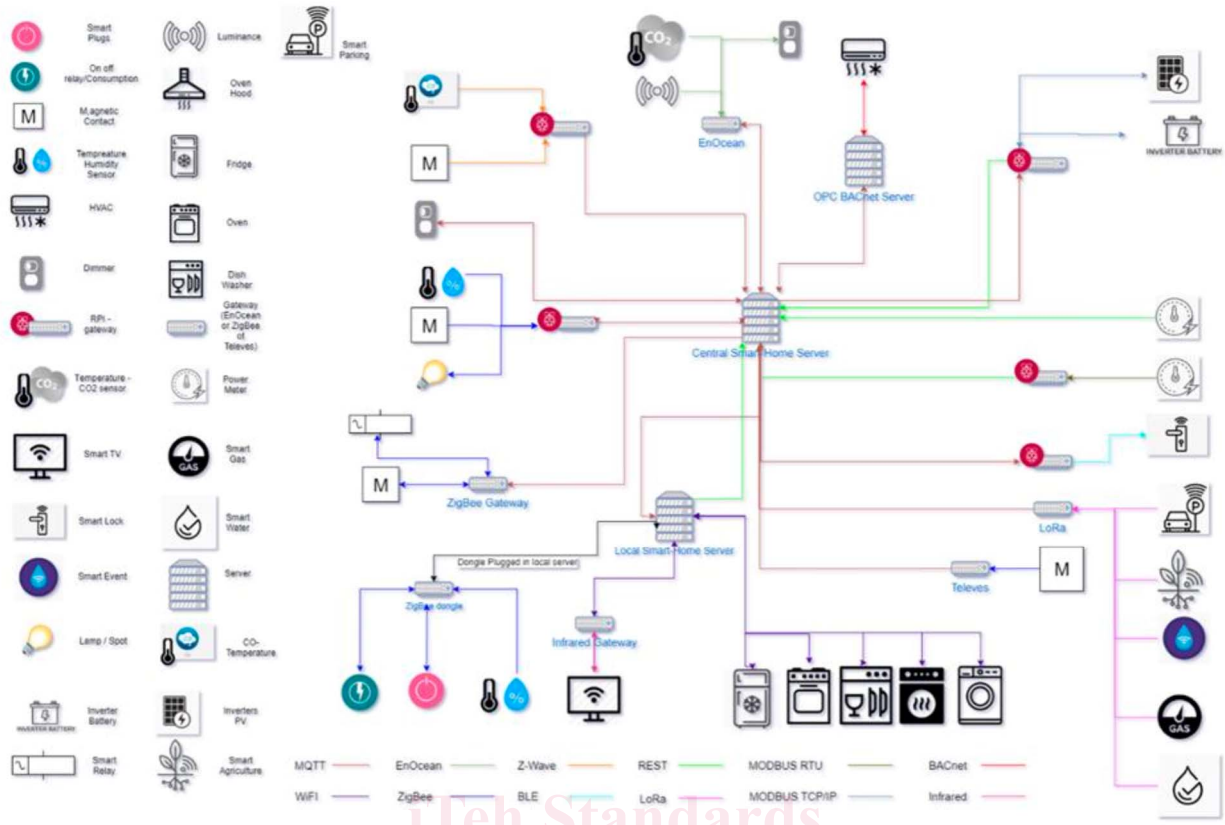


Figure 2: Smart Home infrastructure

Two domains that the CERTH/ITI Smart House supports, which are critical from a security viewpoint, are the Energy and Healthcare domains. Applications that belong to these domains are supported by the following infrastructure:

- Energy related equipment (e.g. smart meters, dimming and on/off actuators, environmental sensors, occupancy sensors, smart plugs, smart appliances, photovoltaics, batteries, etc.) that monitors the consumption, production and the conditions of the entire building, while automated algorithms can implement automation and/or efficiency scenarios while respecting occupant preferences.

- Health related equipment (e.g. blood pressure, glucose, oxygen levels, panic buttons, motion sensors, etc.) that monitors a variety of biometric attributes, a process that enables the extraction of valuable data (such as patterns and biometric attributes) through intelligent processing towards preventing or timely reacting to situations that could otherwise lead to harmful or even fatal outcomes.

6.1.2 Smart Home Pilot System

6.1.2.1 High-level Architecture

The Smart Home Pilot System comprises components and services related to the consumer energy and the healthcare domains. The context diagram of the system is shown in Figure 3.

The Smart Home has the ITI Smart Home Platform, which acts as a complete monitoring and control framework, just like a management system. Through the main web dashboard, the user can interact with the IoT Infrastructure of the Smart Home. More specifically, the platform provides several software applications in the form of standalone widgets, which allow the user to monitor data retrieved from different sensors through easy-to-understand visualizations, as well as to invoke actuators and activate appliances.

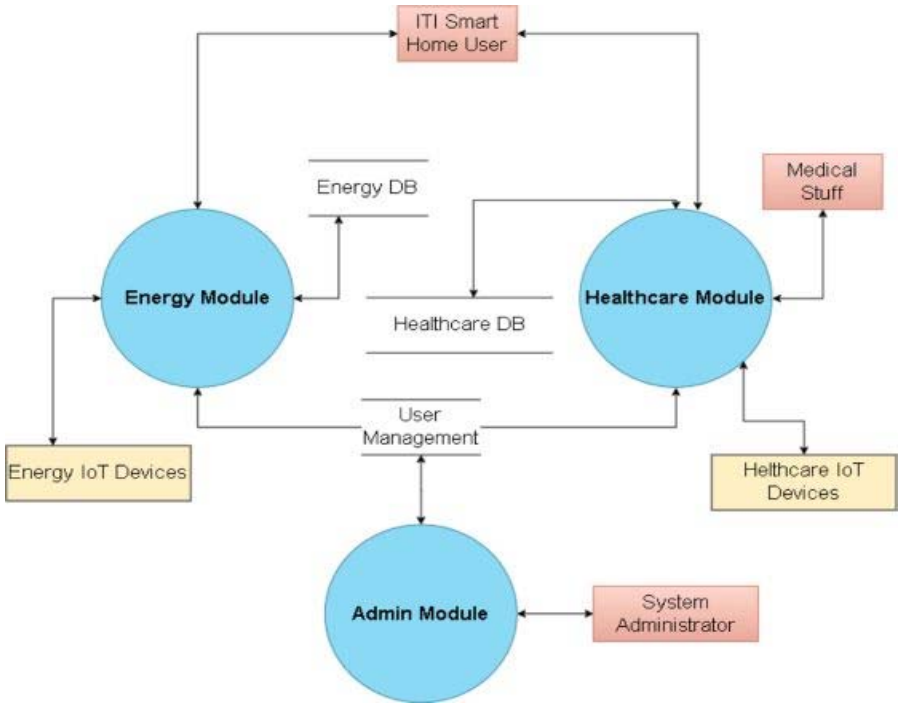


Figure 3: ITI Smart Home Pilot System DFD Diagram (first level of decomposition)

The main purpose of the ITI Smart Home Platform is to allow users to live in a comfortable environment while saving money by improving the energy efficiency and optimal health. This can be achieved by optimizing the day-to-day usage of the system to avoid unnecessary actions and overall to save money from their bills.

The high-level architecture of the ITI Smart Home Platform is based on the client-server approach. The User Interface (UI) consists of the web-based dashboard that allows user interaction with the underlying infrastructure. The back-end component provides the required services, data, and management of requests for the front-end functions to work. The high-level conceptual view of the CERTH ITI Smart Home Platform is shown in Figure 4.

The structure of the ITI Smart Home platform follows a centralized approach (i.e. all IoT components interact with the platform services via RESTful API interfaces). First, the data monitoring process accumulates all necessary data from sensors/actuators locally on gateways. Next, it propagates them to the respective databases (i.e. InfluxDB and MongoDB) via a dedicated RESTful API. Finally, the UI component retrieves the data to create intuitive plots and optimize the operation of the system. The API handles the data in JavaScript Object Notation (JSON) format, which is a standard and human-readable file format that is generally used for server communication. The UI of the platform is implemented with Angular, while the backend is written in Node.js.

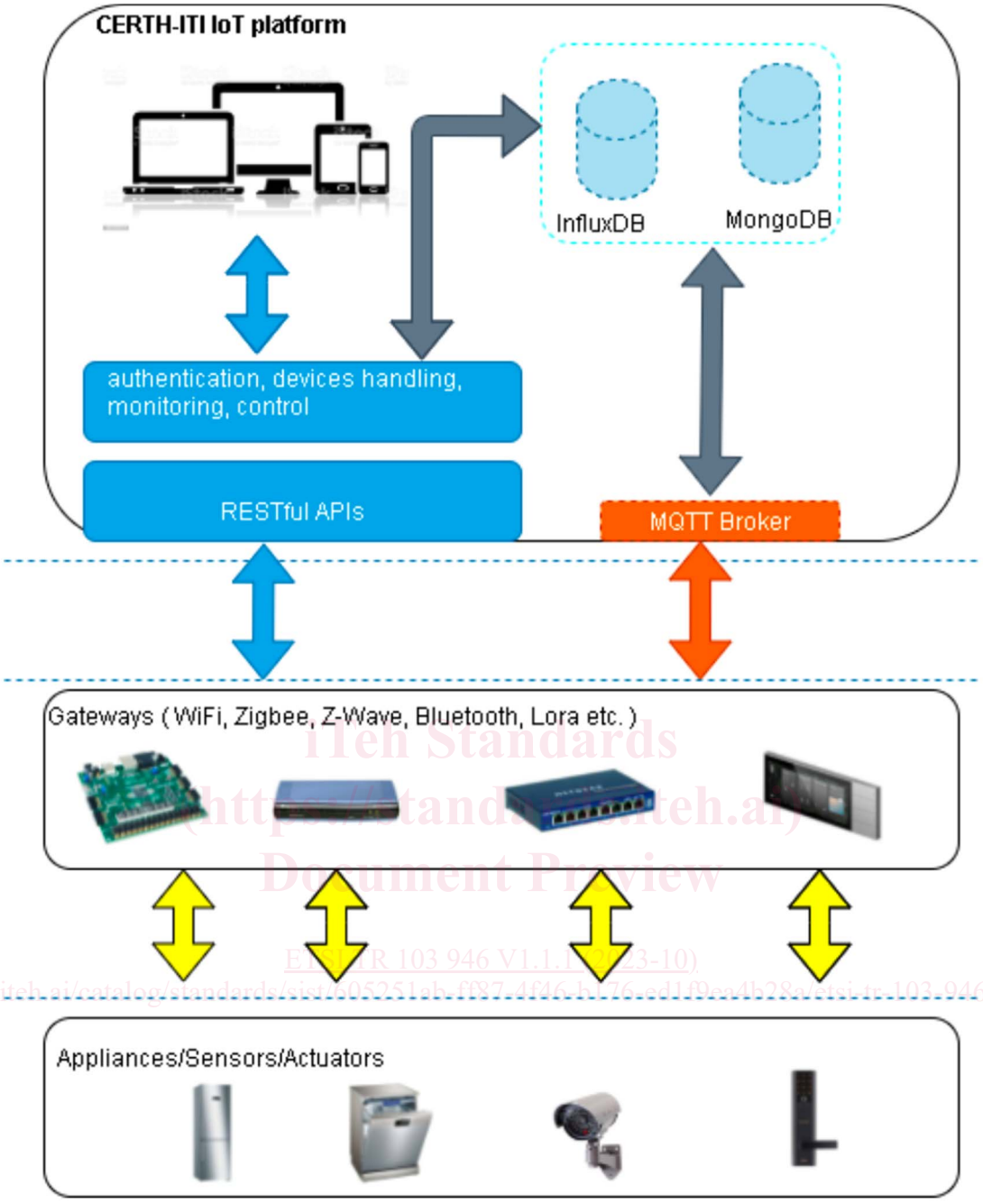


Figure 4: ITI Smart Home Platform high-level conceptual view

6.1.2.2 Detailed Description

The ITI Smart Home platform requires a user authentication to ensure data security. User authentication procedure is based in several secure encryption algorithms. ITI Smart Home login page is shown in Figure 5.