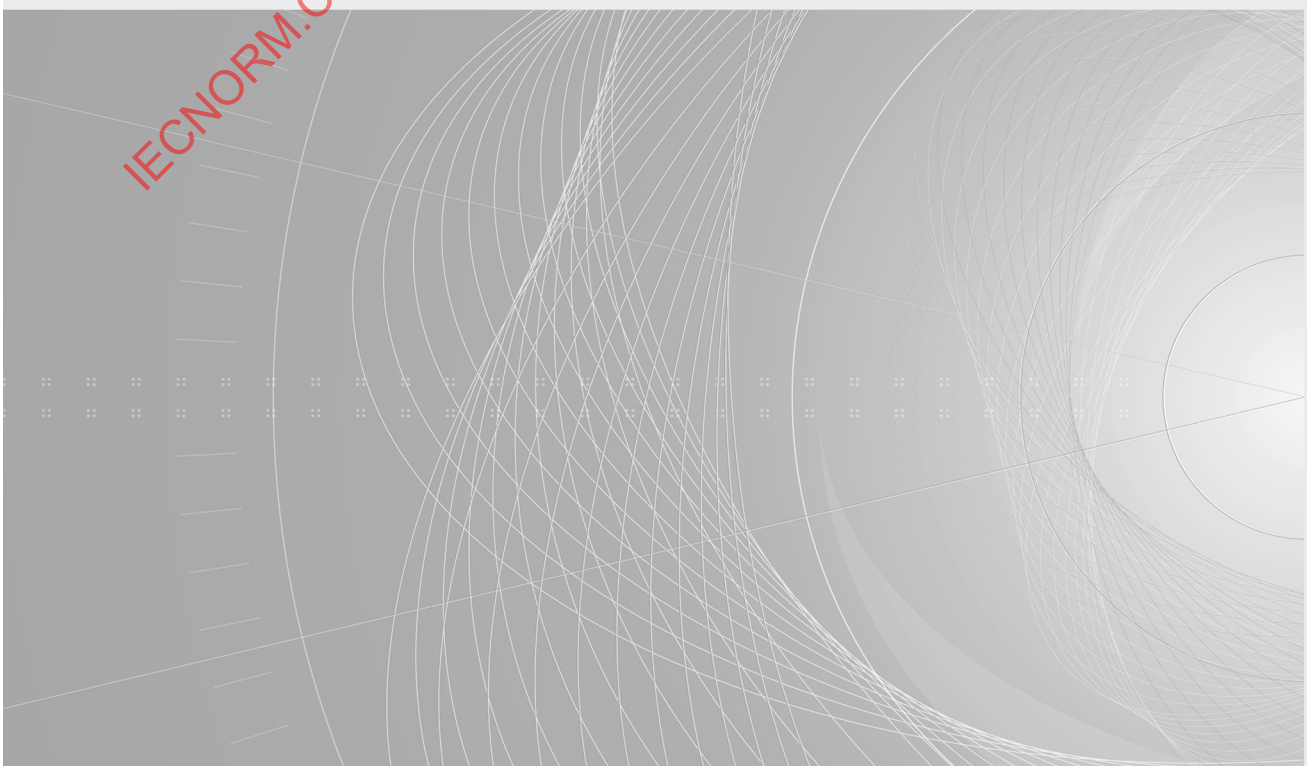
ISO/IEC TR 22417

Edition 1.0 2017-11

TECHNICAL REPORT

colour inside

Information technology – Internet of things (IOT) – IOT use cases



ISO/IEC TR 22417:2017-11(en)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

About the IEC
The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications
The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

IEC Catalogue - webstore.iec.ch/catalogue
The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

IEC publications search - www.iec.ch/searchpub
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and also once a month by email.

Electropedia - www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing 20 000 terms and definitions in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
65 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.

ISO/IEC TR 22417

Edition 1.0 2017-11

TECHNICAL REPORT

colour inside

Information technology – Internet of things (IOT) – IOT use cases

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 35.020; 35.240; 35.110

ISBN 978-2-8322-4989-5

CONTENTS

INFORMATION TECHNOLOGY – INTERNET OF THINGS (IOT) – IOT USE CASES

FOREWORD

1) ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

2) The formal decisions or agreements of IEC and ISO on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees and ISO member bodies.

3) IEC, ISO and ISO/IEC publications have the form of recommendations for international use and are accepted by IEC National Committees and ISO member bodies in that sense. While all reasonable efforts are made to ensure that the technical content of IEC, ISO and ISO/IEC publications is accurate, IEC or ISO cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.

4) In order to promote international uniformity, IEC National Committees and ISO member bodies undertake to apply IEC, ISO and ISO/IEC publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any ISO, IEC or ISO/IEC publication and the corresponding national or regional publication should be clearly indicated in the latter.

5) ISO and IEC do not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. ISO or IEC are not responsible for any services carried out by independent certification bodies.

6) All users should ensure that they have the latest edition of this publication.

7) No liability shall attach to IEC or ISO or its directors, employees, servants or agents including individual experts and members of their technical committees and IEC National Committees or ISO member bodies for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication of, use of, or reliance upon, this ISO/IEC publication or any other IEC, ISO or ISO/IEC publications.

8) Attention is drawn to the normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.

9) Attention is drawn to the possibility that some of the elements of this ISO/IEC publication may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

The main task of the joint technical committee is to prepare International Standards. However, the joint technical committee may propose the publication of a Technical Report when it has collected data of a different kind from that which is normally published as an International Standard, for example "state of the art".

ISO/IEC TR 22417, which is a Technical Report, was prepared by subcommittee 41: Internet of Things and related technologies, of ISO/IEC joint technical committee 1: Information technology.

This Technical Report has been approved by vote of the member bodies, and the voting results may be obtained from the address given on the second title page.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

INTRODUCTION

This document captures the results of a use case input process that began with the call for contributions of IoT (Internet of Things) use cases in 2015-05. The current document reflects contributions and discussions by ISO/IEC JTC 1 experts and liaison members, JTC 1 national mirror committees, and user organizations. This document also contains material gathered from reports, IoT research projects and group output from the JTC 1 working group on the Internet of Things meetings in September 2015 (Ottawa), January 2016 (Shanghai) and May 2016 (Berlin).

In total 25 IoT use cases were submitted by the end of July 2016. To start the project, the working group members were requested to submit use cases using the provided template. The use case submissions consisted of the title of the use case, a description and the origin of the use case. Contributors did not always provide information for all the fields of the template and did not necessarily revise their input when a modified use case template was introduced.

The use case template helped to group and categorize the use cases according to the identified IoT requirements and experience of users. Understanding the application of IoT systems made it easier to identify categories and highlight use case commonalities. Where multiple use cases fall in the same category and had overlapping items, they were consolidated into one section or extended use case. All selected use cases have real-world validity. Gaps were filled by adding extra use cases and future developments were also considered. Functional requirements were extracted from the use cases and have assisted in the development of the IoT Reference Architecture. There is a natural mapping from the user experience based use cases to the clustered technical use cases, where specific technical and functional requirements are expressed. Collecting the use cases allowed the working group to assess the general applicability of the IoT reference architecture in ISO/IEC 30141 to current IoT applications.

Experts from the following national committees, liaison organizations and research projects contributed use cases on IoT: Canada, China, Japan, UK, JTC 1/SC 27, JTC 1/SC 29, ISO/TC 184, and the Vicinity Project.

Technological advances have enormous potential to make the society more efficient and digitally inclusive and IoT implementations are demonstrating convergence of information and communications technology and their widespread application.

The target audience for this document includes:

- IoT service users who can understand how their IoT requirements are considered by an IoT service provider;
- IoT service providers who can learn about users IoT needs, and can also learn how to operate active assisted living systems;
- IoT application developers who can develop IoT applications according to the needs of the IoT service users;
- controllable equipment and ICT device manufacturers who want to know what the IoT interface requirements are;
- administrations and government authorities that have to act as IoT service users and IoT regulators.

INFORMATION TECHNOLOGY – INTERNET OF THINGS (IOT) – IOT USE CASES

1 Scope

This document identifies IoT scenarios and use cases based on real-world applications and requirements. This document comprises 25 use cases for Internet of Things submitted to the ISO/IEC JTC 1 working group on the Internet of Things between June 2015 and July 2016. Use cases are a well-known tool for expressing requirements at a high level and demonstrating their real-life relevance. The use cases provide a practical context for considerations on interoperability and standards based on user experience. Use cases clarify where existing standards can be applied and highlight where standardization work is needed.

An objective of this document is to assist in the identification of potential areas for standardization in the IoT environment to ensure ease of operation and interoperability.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at http://www.iso.org/obp
- IEC Electropedia: available at http://www.electropedia.org/

3.1
actor
entity that communicates and interacts

Note 1 to entry: These actors can include IoT devices, actuators, sensors, users, software applications, systems, databases.

3.2
use case
specification of a sequence of actions, including variants, that a system (or other entity) can perform, interacting with actors of the system

[SOURCE: ISO 14813-5:2010, B.1.160]

3.3
IoT use case
description of a hypothetically possible situation where IoT concepts, products and services may be specified as a set of actions associated with actors in an IoT system, which yields an observable result that is, typically, of value for one or more actors or other stakeholders of the system

Note 1 to entry: The aim is to pictorially describe a field of problems in a way that the artificial situation makes IoT approaches to solutions evident in their temporal, spatial as well as technical dimension.

3.4
role
set of behaviours displayed by an actor in an interaction with the system under discussion

3.5
context of use
area of knowledge or activity characterized by a set of concepts and terminology understood by the practitioners in that area

3.6
use case diagram
diagram that shows relations between actors and use cases

[SOURCE: ISO 14813-5:2010, B.1.161, modified – The words "within a system" have been deleted from the end of the definition.]

3.7
data flow diagram
diagram that depicts data sources, data sinks, data storage, and processes performed on data as nodes, and logical flow of data as links between the nodes

[SOURCE: ISO/IEC 2382:2015]

3.8
network function virtualization
NFV
technology that enables the creation of logically isolated network partitions over shared physical networks so that heterogeneous collections of multiple virtual networks can simultaneously coexist over the shared networks

Note 1 to entry: This includes the aggregation of multiple resources in a provider and appearing as a single resource.

[SOURCE: ITU-T Y.3011, 3.2.4, modified – The source term is "network virtualization".]

3.9
software defined networking
SDN
set of techniques that enables to directly program, orchestrate, control and manage network resources, which facilitates the design, delivery and operation of network services in a dynamic and scalable manner

[SOURCE: ITU-T Y.3300, 3.2.1]

4 Abbreviated terms

AAL	Active Assisted Living
ASD	Application Service Domain
ASHRAE	American Society of Heating and Air-Conditioning Engineers
CCTV	Closed Circuit Television
CE	Controllable Equipment
CoAP	Constrained Application Protocol
DDoS	Distributed Denial of Service
DR	Demand Response
EEG	Electroencephalogram

EGS	Energy Generation System
EMA	Energy Management Agent
EMS	Energy Management System
eNB	evolved NodeB
ERP	Enterprise Resource Planning
ESS	Energy Storage System
FBD	Function Block Diagram
FSGIM	Facility Smart Grid Information Model
GIS	Gas Insulation Switch
GPRS	General Packet Radio Service
GPS	Global Positioning System
HMD	Head Mounted Display
HRV	Heart Rate Variability
HTTP	Hypertext Transfer Protocol;
IaaS	Infrastructure as a Service
ICC	International Colour Consortium
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
IoT RA	Internet of Things Reference Architecture
IL	Instruction List
IR	Infra-red
ISO	International Organization for Standardization
JSON	JavaScript Object Notation
KPI	Key Performance Indicator
LD	Ladder Diagram
LTE	Long Term Evolution
M2M	Machine to Machine
MCS	Monitoring and Control System
MES	Manufacturing Execution System
MILP	Mixed Integer Linear Programming
MQTT	MQ Telemetry Transport
NFC	Near-Field Communication
NFV	Network Function Virtualization
NSE	Non-Shiftable Equipment
OEM	Original Equipment Manufacturer
OLED	Organic Light Emitting Diode
OMD	Operation and Management Domain
OPC-UA	Open Platform Communications Unified Architecture
OS	Operating System
PaaS	Platform as a Service
PAS	Publicly Available Specifications
PED	Physical Entity Domain

PID	Proportional-Integral-Derivative
PLC	Programmable Logic Controller
PRV	Pulse Rate Variability
QoS	Quality of Service
REM	Rapid Eye Movement
REST	REpresentational State Transfer
RFID	Radio Frequency IDentification
RID	Resource Interchange Domain
SaaS	Software as a Service
SCADA	Supervisory Control And Data Acquisition
SCD	Sensing and Controlling Domain
SDN	Software Defined Networking
SE	Shiftable Equipment
SNMP	Simple Network Management Protocol
ST	Structured Text
STN	State Transition Network
SWS	Slow-Wave Sleep
TCP	Transport Control Protocol
TR	Technical Report
UD	User Domain
UDP	User Datagram Protocol
UI	User Interface
UV	Ultra-Violet
UWB	Ultra-WideBand
VFD	Variable Frequency Device
VPN	Virtual Private Network
WAN	Wide Area Network
Wi-Fi	Wireless Fidelity

5 Summary of Use Case Scenarios

5.1 General

The use case scenarios are intended to illustrate typical IoT use cases but are not meant to be an exhaustive list of realizations within an IoT environment.

5.2 Use Cases

5.2.1 Summary

Below is a summary of the use case scenarios with a short description of the use case and the identification of the key actors described in the use case. Actors identified in the use cases are given in Annex A and interactions between Actors and IoT entities are summarized in Annex B.

Table 1 – Summary of Use Case Scenarios

Use Case Number	Name of Use Case	Short Description	Actors
1	IoT Network Security	Telcos are offering telecommunication services to IoT providers bringing various services to the market enabling rapid provisioning of IoT services as well as new agile security capabilities and functionality enabling IoT Security.	• Telco IoT cloud services (provider and tenant) • Telecom Networks • Telco Network Security application controller • Gateways • IoT endpoint
2	IoT Security threat detection and management	Telco cloud service providers are able to gather large amounts of data regarding the IoT service, endpoint, status, utilization and conduct large scale analytics. This data gathered can be used for centralized threat detection and mitigation through intelligent security policy enforcement. **Domain Role**: IoT Telco cloud service, Cloud Computing Security, NFV, Software defined networks, Data Analytics, Security as a Service.	• Telco IoT cloud services (provider and tenant) • Telecom Network • Telco Security policy controller • Data Analytics engine • Gateways • IoT endpoint
3	Remote management of large equipment in a plant	An IoT system using cloud services is deployed by the equipment manufacturer. This system is connected to all the manufacturer's deployed equipment in different plants. In this set up, the operator from the manufacturer remotely monitors the equipment. If an event or an alarm occurs, the operator could act on it remotely; for example, by sending the repair person, ordering spare parts, etc.	• Operator, • Repair personnel, • Procurement personnel, • IoT system.
4	Automated ICC profile discovery	This use case describes automatic configuration and update of colour performance of printers to reduce service and maintenance costs. Additionally it outlines safety, security and privacy requirements for the office equipment discoverability function.	• Equipment vendor • User • IT tool • Cloud service – ICC profile repository • Resources (paper, ink) • Software application
5	Tracking of farm products	This use case describes the process of farm product tracking using an IoT system to achieve the farm product safety and security.	• Public customer • Government customer • Farm product, • Employees involved in farm product activities • RFID tag and reader • Employee sensor card, • Electronic ledger • Information security support • Tracking management platform for government customer • Tracking service platform for public customer • IT system maintenance • Real-time monitoring in farm product market • Farm product information exchange platform • E-commerce platform

Use Case Number	Name of Use Case	Short Description	Actors
6	IoT application for warehouse goods monitoring	This use case describes an IoT application system, which automatically monitors and tracks goods in warehouses. By monitoring and tracking these goods the owners can accurately evaluate their assets at any given time. Therefore, such IoT systems help owners to apply for and secure the loans from banks using the assets as collateral. The IoT system also benefits the lenders (e.g. banks) by monitoring the assets of a borrower at any given time.	• RFID tag and reader • Electronic scale • Sensor with ultra-wideband (UWB) module • Laser radar which acquires the contour information • Alarm controller • IoT Gateway • Internet • On-line monitoring service system • Mortgage management system • Information resource database • Resource access system • Maintenance system • Rules management system
7	Cooperation between Factories and Remote Applications	This use case describes global cooperation between factories and remote applications for improving the efficiency of their operations.	• IoT Gateway • Remote Application • Controller • Server
8	Searching system for persons with cognitive impairment	This use case describes a secure data management system. A GPS tracker in the shoes of a patient allows GPS data to be fed to a data management centre which can then track the location of the patient when they are informed by carers that the patient is missing. The GPS location of the cognitively impaired person can be passed to police, taxi drivers etc. who can locate the person and ensure their safety.	• Patient (user) • GPS system • Carer • Data management centre • Police
9	Sleep monitoring system	This use case describes use of frequency analysis of HRV/PRV to establish the sleep stages of the patient. This can help diagnose issues such as sleep apnoea and monitor the effect of certain devices to improve breathing.	• Doctor • Patient • Pulse rate, skin temperature and motion sensors • Body area network
10	Smart glasses	This use case describes how a factory worker can use smart glasses to receive information on the shop floor to assist with setting up and maintaining machinery.	• User • Wearable smart device • Processing unit for user interaction e.g. – Gesture recognition – Voice recognition – Speech synthesis – Image analysis • Factory/enterprise database

Use Case Number	Name of Use Case	Short Description	Actors
11	IoT endpoint (sensors & actuators) monitoring systems	This use case describes a capability in the network, local or remote whose sole purpose is monitor or gather state information of sensors/endpoints on a network segment and transmits this information to a central location to enable manage, prevent failures or malfunctioning of critical IoT endpoint, as well as life cycle management of IoT endpoints.	• IoT Operations, Various industries
12	Intelligent assistive parking in urban areas	This use case presents a scalable solution for intelligent assistive parking in urban areas in order to reduce or redirect unnecessary traffic, avoid traffic congestion and reduce pollution downtown or in populated areas. It can reduce traffic-related injuries caused by less attention in looking for vacant parking space on the roadside and save drivers' time.	• Vehicle user • Vehicle • Smartphone • Parking space stakeholder • Blue light agencies • Space management sensors • Space alarm system • Cloud service • iParking • Smart city • Administration tool
13	Integrated Smart Pump System	This use case demonstrates the interoperability of IoT information exchange between applications to maintain the overall asset health in the manufacturing process and the interoperability of smart pump applications using IoT technology.	• Data acquisition application • Pump control application • Pump diagnostics application
14	Remote Health monitoring	This use case shows how a wellness or health device can be used for fall detection	• Patient • Wristband • Smartphone • Healthcare Provider • Home alarm system • Cloud service
15	Connected car analytics	This use case describes information flows and reference components used to build a framework that allows devices and users to share information with each other. It also allows individuals to get personalized recommendations based on their interactions with the devices to promote user safety and optimal operation of the device.	• Car driver • Connected car • Medical physician • Better Driver Behaviour • Application Device • Registry Device • Data Store • Enterprise User • Directory Analytics Engine • Process Management • End User Application • IoT Transformation & Connectivity

Use Case Number	Name of Use Case	Short Description	Actors
16	Real Time Motor Monitor	This use case describes an IoT platform being used to monitor motors in a production line to enable preventative maintenance; sensors in the customer device are connected to improve automation and push processes in the supply chain. Predictive maintenance using cloud services enables operations, manufacturing, production and maintenance personnel in asset-intensive industries to use predictive analytics to improve asset availability, increase throughput, minimise unplanned outages, and reduce maintenance costs.	• Technician • Supervisor • Production line motor • Motor sensors • IoT Gateway • Device registry • Predictive Maintenance and Quality application • Production line control screen
17	Smart Home Appliances	A manufacturer and its ecosystem partners can provide user remote control and better customer support for connected appliances for smart homes with appropriate IoT applications.	• Appliance Customer • Appliance Manufacturer • Appliance Service Staff • Third Party Provider • Home Appliance • Appliance Sensors • Appliance Actuators • Smart Phone • IoT Gateway • End user application • Smart Appliance • Application Manufacturer's • Customer Database • Device Registry • Appliance Analytics • Device Data Store • Third Party service interface
18	Smart Home Insurance	Smart homes with connected devices and sensors allow insurance companies to improve service for their policy holders while providing insights into risks on the home. This use case shows how an IoT platform can monitor sensors in the home.	• Homeowner • Insurance Company • Device manufacturer • Sensors • Actuators • Home Gateway • Smart home Insurance Application • Analytics Engine • Device Registry • Device Data Store • Process Management • Smart Phone Insurance Mobile Application
19	Machine Leasing	This use case describes an IoT application which would enable a machine manufacturer to monitor and track a user's remote assets in real-time. By collecting the performance, status and location data of the machines, the leasing company is able to deliver value added services such as predictive maintenance.	• RFID tag and reader • Battery, water level, temperature sensors • Machine • Information exchange systems • GPS • Cellular/WiFi

Use Case Number	Name of Use Case	Short Description	Actors
20	IoT-based Energy Management System for Industrial Facilities	This use case describes an IoT-based communication framework with a common information model which facilitates the development of a demand response (DR) energy management system for industrial customers. It also describes an IoT-based energy-management platform based on a common information model and open communication protocols, which takes advantage of integrated energy supply networks to deploy DR energy management in an industrial facility.	• Production planner or Facility Manager • Utility Power Station • Utility Meter • Energy Manager System (EMS) • Energy Management Agent (EMA) • Monitoring and Control System (MCS) • Meter • Non-shiftable Equipment (NSE) • Controllable Equipment (CE) • Shiftable Equipment (SE) • Energy Storage System (ESS)
21	Water Plant Management	This example applies IoT technology to acquire complex information from power devices, mechanical devices, firefighting equipment, safe guarding, running environment, and personnel entry and exit positions, and to perform system analysis, multiple fusion and logic decisions such as alarming, controlling and other action utilizing algorithms from a library.	• Electrical Equipment, Mechanical Equipment, Environment etc. • Temperature and moisture sensors • Water immersion sensors • Smoke sensors • Vibration sensors • RFID tags and readers • Alarm controller • Wind generation controller • Local Area Network • Wireless Base Station • IoT Gateway • Data Filtering and Fusion • Data Analysis and Diagnosis System • Resource Access Interface • Resource Database • Online Monitoring System • Assistive Controlling System • Operation System • Maintenance System • System Manager

Use Case Number	Name of Use Case	Short Description	Actors
22	Smart Home Application	This use case describes the application of smart home systems using IoT technology to achieve the enhancement of home safety and comfort.	• Family Members • Multiple Sensors • IoT Gateway • Bulbs, Main Door and Windows etc. • Door/Window sensor • Curtain Motor • Home Appliances • Mobile Phone with apps • Service Provider • Smart Home Services • Cloud Service with Database • Internet • Security Camera • Community Security System • IR Blaster • Intelligent Lock • System Maintenance • Community Management System
23	Field Gateway Bridging IoT to Legacy Devices in Factories and Plants	A field gateway bridges the protocols or networks for legacy field devices and provides data to automation applications and enterprise systems.	• Field Gateway • Application A1 • Application A2 • Field Device D1 • Field Device D2 • Sensor
24	Production Monitoring of Textile Equipment	Use of a production monitoring system enables textile firms to monitor their equipment in real-time. This is delivered by several services which include intelligent transformation, wireless communication transformation, data management, equipment monitoring. Such systems support mobile terminal access, and allow customers to follow the status of their order in real-time. The monitoring system can improve production efficiency whilst reducing personnel costs	• IoT System • Manager • Operator • Repairer • Customer
25	Remote Management of Agricultural Greenhouses	Intelligent monitoring systems in agricultural greenhouses gather the environmental parameters of the greenhouse. These parameters include air temperature, humidity, illumination, soil temperature and soil moisture. This data is used to provide intelligent decision-making regarding the real-time needs of the crops, such as the automatic activation or de-activation of specified control equipment. This system enables automatic monitoring ecological information, automatic controlling and intelligent management of facilities.	• IoT system • Manager • Operator

6 Context of Use for the IoT Use cases

6.1 Global

This denotes all space outside populated areas as well as all outdoor and on the move spaces in a populated area.

Example: Has most properties of Urban and of Public buildings except the larger geographic spread, lower protection against weather conditions and easier access by people, animals etc.

6.2 Transport infrastructure

This denotes all infrastructure related to public transportation including road, rail, maritime and air transport, for example airports, railway stations, bus stations, underground systems, highway monitoring systems, harbours, shipping channels.

6.3 Home

This denotes the private, hence highly customizable indoor area where someone lives, alone or with friends/relatives/roommates. Thus it includes dedicated infrastructure aimed to support those individuals, such as healthcare and wellness systems, building control systems, smart metering and systems for entertainment and gaming.

Example: Includes infrastructure and devices like home wireless network, routers, gateways and concentrators, audio-video equipment and systems, in-house only vehicles and walking or moving aids, in-house-only appliances and robots, CCTV, monitoring and security systems, etc.

6.4 Public buildings

This denotes all other relevant indoor environments; these are not customizable but instead equipped for generic support of the common denominator of user groups; and will thus include generic infrastructure aimed to support a large variety of individuals typically visiting any particular place;

Example: Including devices like the ones referred to in 6.3 but this can be expected to be a different selection and with a different mix of enabling functions and applications.

6.5 Offices

This denotes the room, set of rooms or building or structure for office, professional or service type transactions such as medical offices, banks, libraries, government office buildings, and corporations in which the business of a firm is done, or in which a particular kind of business, clerical work, etc. is done.

6.6 Factories

This denotes a building or buildings used principally for the manufacture of goods with equipment for the large-scale manufacture of goods. It may also include associated distribution depots or warehouses.

6.7 Process plants

This denotes the facilities and structures necessary for performing a process; the process plant is an assembly of one or more plant systems and plant items that is intended to perform a chemical, physical or transport process. A process plant is identified as a single unit for the purposes of management and ownership. A process plant has both physical and functional aspects.

6.8 Agriculture

This denotes activities related to the science or practice of farming, including cultivation of the soil for the growing of crops and the rearing of animals to provide food or other products.

6.9 Forestry

This denotes activities related to the management of forest and woodland for the commercial production of timber, including the growing and maintenance of trees, the felling of mature trees, etc.

6.10 Fishing

This denotes any industry or activity concerned with taking, culturing, processing, preserving, storing, transporting, marketing or selling fish or fish products. It includes recreational, subsistence and commercial fishing and the harvesting, processing and marketing of fish and fish or seafood products for human consumption or as input to industrial processes. It can also include fish farming.

6.11 Body and personal

This denotes the immediate area around the body.

Example: Includes personal devices like sensors and actuators worn in or on the body and also personal devices typically carried by one individual such as music players, smartphones, tablets, etc.

6.12 Healthcare

This denotes activities performed for a patient with the intention of directly or indirectly improving or maintaining the health of that patient.

6.13 Vehicles

This denotes vehicles such as cars, vans, lorries, tractors, buses and trains which can have communication and entertainment systems within them which can connect with personal or infrastructure systems.

6.14 Smart Cities

This denotes ICT-based applications that are used to manage a city's assets (e.g. public facilities, transportation systems, hospitals, power plants, water supply networks, waste management, law enforcement, and other community services). A Smart City is one that dramatically increases the pace at which it improves its sustainability and resilience, by fundamentally improving how it engages society, how it applies collaborative leadership methods, how it works across disciplines and city systems, and how it uses data and integrated technologies, in order to transform services and quality of life to those in and involved with the city (residents, businesses, visitors). Smart Cities are a new concept and a new model, which applies the new generation of information technologies, such as IoT, cloud computing, big data and space/geographical information integration, to facilitate the planning, construction, management and smart services of cities. Developing Smart Cities can benefit synchronized development, industrialization, information sharing, urbanization and agricultural modernization and sustainability of cities development. Smart City applications can vary from specific monitoring applications such as smart parking, to wider CCTV surveillance to prevent crime and from provision of emergency services, to management of utilities such as water, drainage, sewage and power systems.

7 Use Case Scenarios

7.1 IoT Network Security (Use Case number 1 in Table 1)

7.1.1 Scope and Objectives of Use Case

As IoT service providers bring various services to market across industry verticals, Telco's are thinking about how best to offer telecommunication services to IoT providers. Telco services take the shape of network connectivity, hosting of IoT application platforms as cloud services, gateways services such as 4G, enterprise or consumer edge-devices, its management, associated data analytics, security services, centralized usage and billing services among others. Telco clouds are evolving to virtualized environments (SDN/NFV) that enable rapid provisioning of IoT services as well as new agile security capabilities and functionality enabling IoT Security.

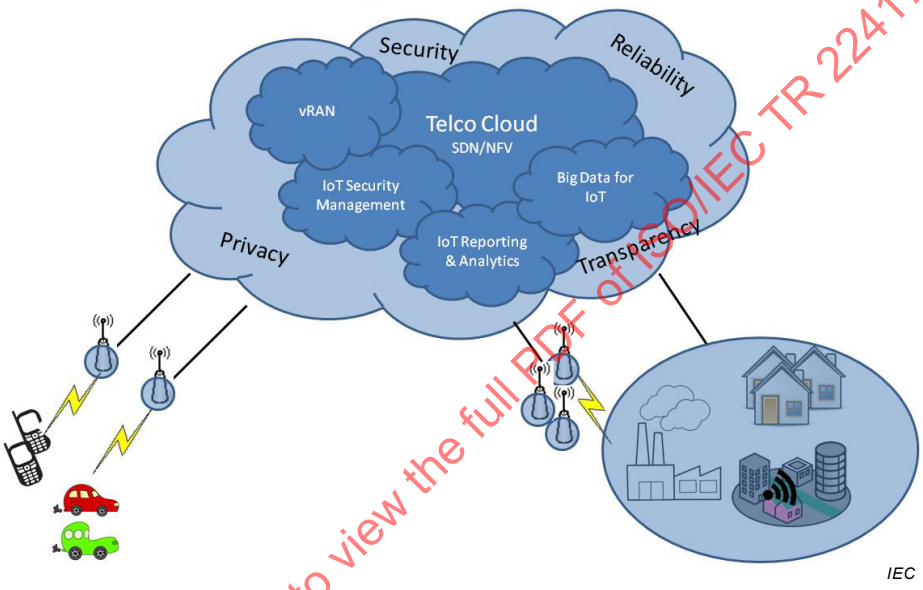


Figure 1 – Overview of IoT Security Use cases in Telco environment

7.1.2 Narrative of Use Case

7.1.2.1 Short description

Telcos are offering telecommunication services to IoT providers bringing various services to the market enabling rapid provisioning of IoT services as well as new agile security capabilities and functionality enabling IoT Security.

7.1.2.2 Complete description

Telcos offer network connectivity, cloud services and host various IoT application platforms. With Telco cloud services evolving to virtualized technologies (NFV/SDN) security intelligence can be distributed and implemented rapidly at various points of the IoT network to manage congestion and mitigate certain security incidents in the IoT ecosystem. NFV and SDN lend themselves to centralized intelligent security policy management in IoT.

For IoT services to function effectively they depend on network availability and reliability as basic requirements, but possess other security requirements. Software defined Networks enable Telco's to dynamically manage their networks via centralized policies. These policies can be disseminated to the required point in the network to mitigate traffic floods, congestion, DDoS attacks or similar.

Security policies may be applied at the gateways where traffic bottlenecks are observed to possibly offload LTE connectivity to locally available Wi-Fi®[1] connections. Figure 2 and Figure 3 depict a scenario where mobile offload thresholds maybe pre-set. For example, if flow volumes exceed 50 kbps switch traffic to Wi-Fi or vice versa. Similarly, when a congested backhaul link is observed, instead of dropping traffic, the SDN controller can route smart homes, devices and sensors in overlapping cell edges to adjacent eNBs where there is lower utilization. Additionally, SDN and NFV combined can be used to augment the saturating gateway, eNB or backhaul network with additional computing power, network bandwidth, storage, etc.

A centralized control layer allows global visibility into usage and resources across all base stations and this allows for intelligent resource management leading to management of congestion. With the dynamic nature of IoT devices, intelligent software defined networks and gateways for dynamic traffic management are necessary to enable IoT network availability and reliability.

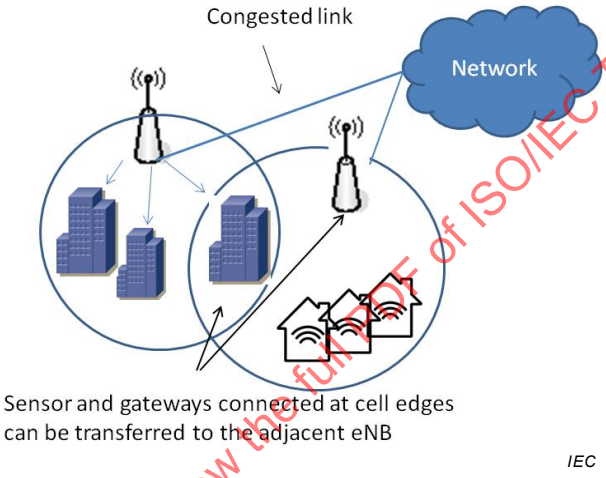


Figure 2 – Traditional LTE Network Congestion Management

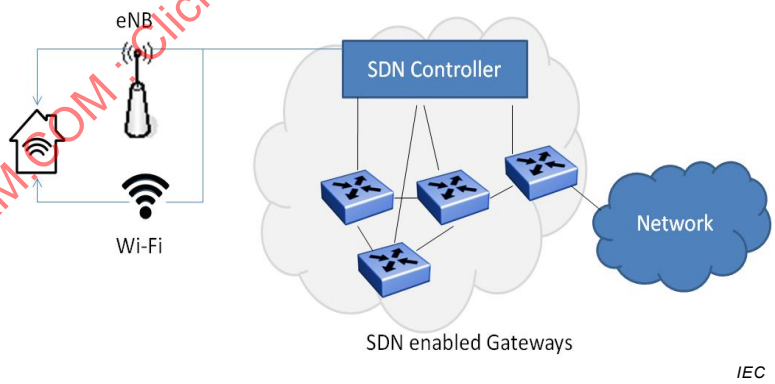


Figure 3 – SDN based congestion management at the gateways by offloading to Wi-Fi

[1] Wi-Fi is a registered trademark of Wi-Fi Alliance. This information is given for the convenience of users of this document and does not constitute an endorsement by IEC or ISO.

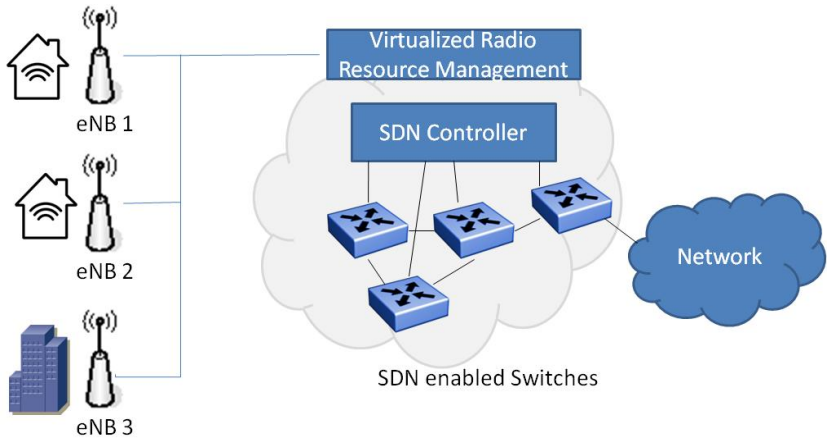


Figure 4 – SDN based congestion management in the LTE Access Network

7.1.3 Actors

Table 2 shows the actors participating in the IoT Network Security Use Case.

Table 2 – Actors for IoT Network Security

Actor Name	Actor Type	Actor Description	Used Technology
Telco IoT Cloud Services (provider and tenant)	System	Virtualized cloud service infrastructure managed by Telcos to support IoT infrastructure or provided to IoT Service providers	
Telecom Networks	Network	Interconnects and transmits information between IoT system components	
Telco Network Security Application Controller	Security Systems	Centralized Security Management Platforms	
Gateways	Intermediary system	Interconnects networks of Endpoints to Access Networks	
IoT Endpoint	Endpoint	Sensors, actuators, etc.	

7.1.4 Issues: Legal Contracts, Legal Regulations, and Constraints

None provided.

7.1.5 Referenced Standards and/or Standardization Committees

Table 3 shows referenced Standards and/or standardization committees relevant to the IoT Network Security Use Case.

Table 3 – Referenced Standards and/or Standardization Committees for IoT Network Security

Relevant Standardization Committees	Standards have to be considered in the Use Case	Standard Status
JTC 1/SC 27/SG IoT	SC 27/SG IoT work under development	
	https://www.opennetworking.org/images/stories/downloads/sdn-resources/solution-briefs/sb-wireless-mobile.pdf	

7.1.6 Relation with Other Known Use Cases

None provided.

7.1.7 General Remarks

7.1.7.1 Domain

IoT Telco cloud services, Cloud Computing Security, NFV, SDN, IaaS, SaaS, PaaS.

IoT Telco cloud services: Telecommunications service providers offer hosting services to IoT Service Providers on their infrastructure called “clouds”. These are typically Telco datacentres where Telcos offer infrastructure, services and platforms, which can include web applications, to their customers.

7.1.7.2 Role

IoT Architecture basically comprises the fundamental building blocks of things, gateways, networks (access, core) and cloud services. The IoT endpoints via their service provider interact with applications, services or platforms in telecom carrier clouds.

7.1.7.3 Scenario

Telco SDN/NFV cloud services have visibility of the traffic patterns of the IoT communication networks, as well as monitoring capabilities of IoT application or platforms they host. This intelligence can be utilized by the carrier to enforce security policies at appropriate points in the IoT network to manage traffic congestion, and even mitigate possible DDoS attacks. SDNs enable carriers to deliver just in time security to the required network points.

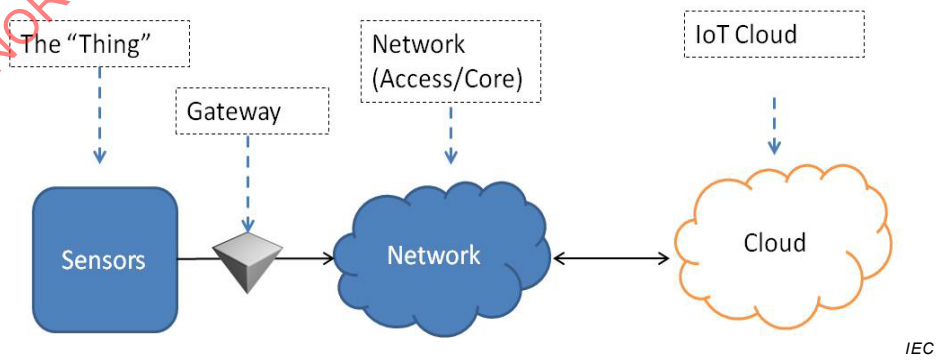


Figure 5 – IoT Basic Network

Table 4 provides the definitions of common terms used in NFV/SDN.

Table 4 – Common terms and definitions of NFV/SDN

Common terms and definitions	
Term	**Definition**
NFV	concept of replacing dedicated network appliances with proprietary hardware such as routers and firewalls – with software running on commercial off-the-shelf servers.
SDN	emerging architecture that is dynamic, manageable, cost-effective, and adaptable making it ideal for the dynamic nature of IoT applications. This architecture decouples the network control and forwarding functions enabling it to become directly programmable with abstraction of lower level functionality.

7.1.8 Security and Privacy

In cases where security is not being explicitly offered as a service (e.g. a Firewall as a service), security is an integral part of technical architectures for all IoT use cases and therefore does not need a specific chain of interactions between IoT components for its application. Security architectures should apply as matter of best practice, at different layers in the service-assets (cloud services, network, gateway, endpoint). The use case does not focus on privacy issues, but one should be aware that the telecom and IoT communication infrastructure might involve exchanges of network identifies that might create privacy issues (e.g. tracking an entity). If this is the case suitable information should be provided to the user of the infrastructure so that he assesses whether he has to carry out a privacy impact assessment. In instances where PII is collected, all services must be in compliance with applicable privacy regulations.

7.1.9 Conformity Aspects and Critical Requirements

None provided.

7.1.10 Interaction between Actors and User Requirements

None provided.

7.1.11 Diagram of Use Case

See Figure 1 for reference.

7.1.12 Data Flow Diagram of Use Case

See 7.1.2 for reference.

7.2 IoT Security Threat Detection and Management (Use case number 2 in Table 1)

7.2.1 Scope and Objectives of Use Case

Telco cloud service providers are able to gather large amounts of data regarding the IoT service, endpoint, status, and utilization with which they conduct large scale analytics. The gathered data can be used for centralized threat detection and mitigation through intelligent security policy enforcement.

7.2.2 Narrative of Use Case

7.2.2.1 Short Description

Cyber criminals and hackers are developing new methods to access home devices that have an operating system and an open IP address: DDoS attacks, botnets launch volumetric assaults on targets through the use of massive numbers of Networked IoT devices to cause required resources or service to be no longer available.

Approximately 3 million petabytes of data will be generated in the next 5 years by embedded system alone (International Data Corporation (IDC), 2013). Much of the IoT data will find its way to the cloud (internet based services and applications) for purposes of correlation of various data points from billions of IoT devices for analytics to provide the user with valuable insights. With the volumes of data generated by both machine and humans, one can expect IoT services will turn to third-party service providers to conduct large volumes of data crunching for them. These advanced data analytic can be used to detect ongoing security attacks against the IoT services in real time, and provide actionable intelligence to SDN/NFV networks for security policy enforcement at appropriate points to mitigate and remediate threats and vulnerabilities.

Malware, DDoS attacks utilizing IoT devices as well as attacks to IoT devices with millions of hijacked IoT endpoints have already been detected. Given the volumes of devices entering the network, automated security intelligence with rapid enforcement capabilities is a must.

7.2.2.2 Complete Description

Telco networks with SDN/NFV enablement have visibility into the traffic patterns of the IoT traffic and networks, as well as monitoring and mitigation capabilities of IoT application or platforms they host. These data points, typically metadata, are fed into big data analytics engine for large scale security threat detection, pattern recognition, anomaly detection and detection of security events and incidents in progress.

Some examples of the threats that can be detected and mitigated are:

- traffic anomalies to, from endpoint and network or between endpoints;
- unauthorized or dated endpoints/sensors accessing the network;
- non-standard or unexpected ports being used for data communication/transmission;
- newly installed software or non-standard protocols being used;
- anomalous or suspicious endpoint behaviours such as varied access ties, access levels, location, information requested, etc.;
- botnets, command and control traffic pattern detection.

Additionally Telcos have diverse security devices in the networks, such as firewall, IPS/IDS, VPNs, access controls that offer layers or protection to the IoT services. With centralized flexible SDN/NFV network-management, security policies including items like firewall rules, dynamic quarantine and related mechanisms can be delivered, in near real time, to the appropriate points with consistency across the overall IoT network to help respond rapidly to ongoing attacks. Remediation and counter measures could range from installing updated patches to vulnerable devices, isolating infected devices from the overall network, or even allocate processing power or increase bandwidth in part of the network as appropriate.

7.2.2.3 Scenario

IoT systems include home devices with an operating system and open IP address which are vulnerable to attack and need security measures to be implemented at different points in the IoT systems. Telcos offer some of these services with centralized detection of infected or misbehaving devices or networks and additional security services such as Big Data Analytics.

Additionally, they can provide SDN controllers to enforce security policy at appropriate points in the network.

As IoT brings a host of new endpoints to the network edge, cyber criminals and hackers are targeting these with an array of attacks taking advantage of vulnerabilities in a host of new IoT devices that are networked and present on the network edge (such as the home, home office, smart vehicle etc.). The exploits range from resource starvation of endpoints to botnets and DDoS attacks. Under such scenarios of security attack the telco is able to offer detection and mitigation, as described in this use case.

7.2.3 Actors

Table 5 shows the actors participating in the IoT Security Threat Detection and Management Use Case.

Table 5 – Actors for IoT Security Threat Detection and Management

Actor Name	Actor Type	Actor Description	Used Technology
Telco IoT cloud services (provider and tenant)	System	Virtualized cloud services infrastructure managed by Telcos to support IoT infrastructure or provided to IoT Service providers	
Telecom Networks	Network	Interconnects and transmits information between IoT system components	
Telco Network Security application controller	Security Systems	Security controllers/orchestrators	
Gateways	Intermediary system	Interconnects networks of endpoints to Access Networks	
Data Analytics engine	Analytics platform	Generates actionable intelligence through analysis of data gathered from IoT system	
IoT endpoint	Endpoint	Sensors, actuators, applications etc.	
Data Protection Officer	Human User	In charge of ensuring that resulting capabilities for security threat and management comply with privacy regulations, in particular if PII data is collected.	

7.2.4 Issues: Legal Contracts, Legal Regulations, and Constraints

None provided.

7.2.5 Referenced Standards and/or Standardization Committees

Table 6 shows referenced standards and/or standardization committees relevant to the IoT Security Threat Detection and Management Use Case.

Table 6 – Referenced Standards and/or Standardization Committees for IoT Security Threat Detection and Management

Relevant Standardization Committees	Standards have to be considered in the Use Case	Standard Status
JTC 1 SC27 SG IoT	SC27 WG4 and WG5 work under development	

7.2.6 Relation with Other Known Use Cases

https://www.opennetworking.org/images/stories/downloads/sdn-resources/solution-briefs/sb-security-data-center.pdf

http://www.lightreading.com/spit-(service-provider-it)/analytics-big-data/analytics-in-a-world-of-sdn-nfv-and-iot/d/d-id/711866

7.2.7 General Remarks

7.2.7.1 Domain

Cloud Computing Security, NFV, SDN, Big Data Analytics, SaaS.

IoT Cloud Services: Telecommunications service providers offer hosting services for IoT Service Providers on their infrastructure called “clouds”. These are typically datacentres where service provider offers infrastructure services and platforms to their customers.

While cloud services are available from a wide range of service providers, network services begin with physical infrastructure (fixed line and/or wireless) and require some form of telecommunications service provider (Telco). This gives them a unique advantage of visibility of end to end view of traffic patterns, security breaches and attacks.

7.2.7.2 Role

A Telco is essentially a service provider to IoT service providers and end users, offering network connectivity, big data analytics and security services.

7.2.8 Security and Privacy

Big Data Analytics in cloud services allow security threat detection, for example DDoS, Fingerprint matching, anomaly detection and botnet detection, see Figure 6. In cases where security is not being explicitly offered as a service, e.g. a Firewall as a service, security is an integral part of technical architectures for all use cases and therefore do not need a specific chain of interactions between IoT components for its application rather security architectures should apply as matter of best practice.

In instances where PII is collected, all services must be in compliance with applicable privacy regulations. In the case when the resulting security services necessitate collection of PII, the data protection officer must ensure that a privacy impact assessment is carried out.

7.2.9 Conformity Aspects and Critical Requirements

None provided.

7.2.10 Interaction between Actors and User Requirements

None provided.

7.2.11 Diagram of Use Case

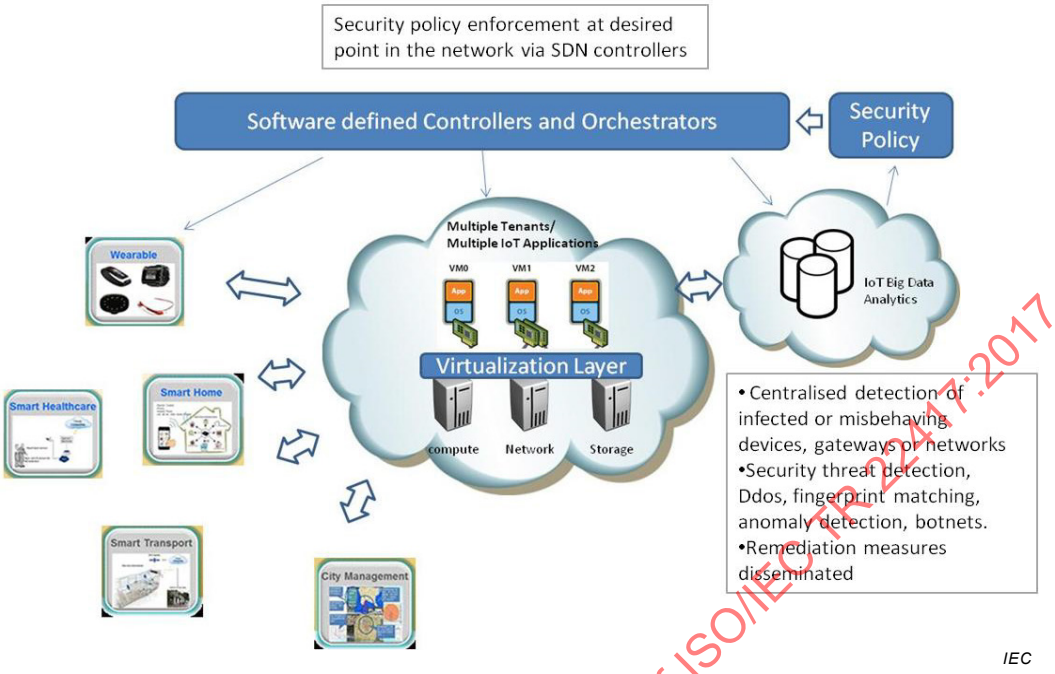


Figure 6 – IoT Security with Big Data Analytics in SDN/NFV clouds

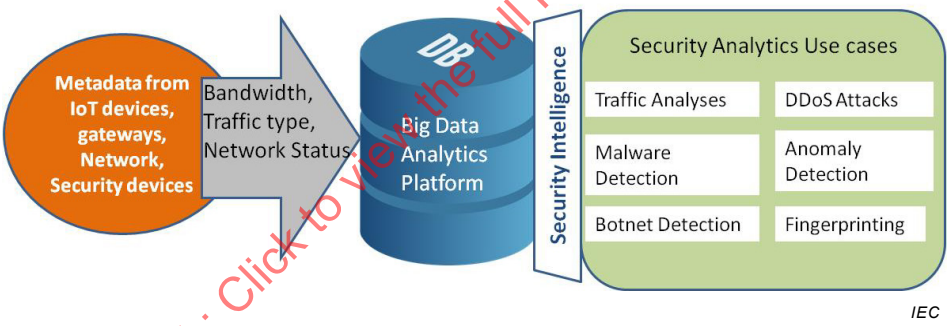


Figure 7 – IoT Data Analytics-based Security Intelligence

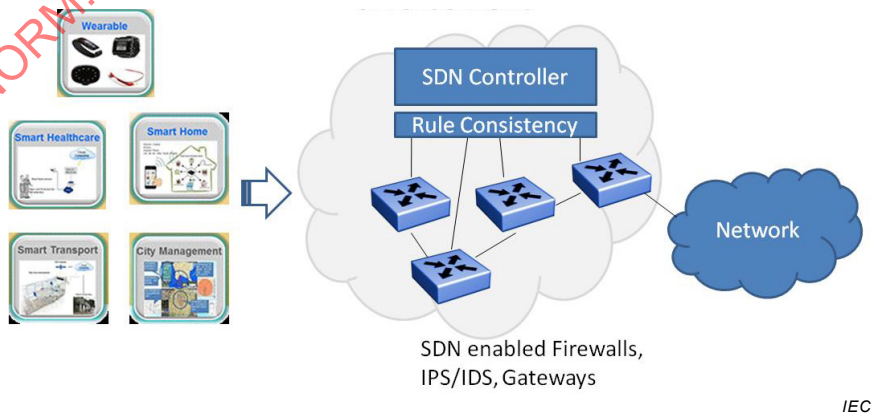


Figure 8 – SDN/NFV-based Security Policy Management

7.2.12 Data Flow Diagram of Use Case

See 7.2.2 for reference.

7.3 Remote Management of Large Equipment in a Plant (Use case number 3 in Table 1)

7.3.1 Scope and Objectives of Use Case

The large equipment in a plant is generally manufactured by different companies. It is hard for the plant to maintain it because of a lack of relevant expertise. The manufacturer has the required expertise. This use case describes how an equipment manufacturer utilizes an IoT system to manage the equipment that is deployed at the customer's plant. The IoT system enables the manufacturer to keep the equipment in good order over a long time, while making repair and procurement procedures efficient, thus reducing the plant's cost and increasing the profits of both the manufacturer and the customer.

7.3.2 Narrative of Use Case

7.3.2.1 Short Description

An IoT system using cloud services is deployed by the equipment manufacturer. The cloud services are connected to all the manufacturer's deployed equipment in different plants. In this set up, the operator from the manufacturer remotely monitors the equipment. If an event or an alarm occurs, the operator can act on it remotely; for example, by sending the repair person, ordering spare parts, etc.

7.3.2.2 Complete Description

The large equipment in a plant is manufactured by different companies. It is hard for the plant to maintain it due to the lack of relevant expertise about the equipment. The manufacturer is best placed to manage it as they have the necessary information. This use case describes how this is achieved with an IoT system. The IoT system is deployed by the equipment manufacturer. The IoT system includes cloud services that store data, process the data, and generate actionable information. The cloud services are connected to all of the equipment, usually via the Internet. The sensors measure different aspects of the equipment, actuators set up the behaviour of the equipment. Sensors and actuators are fixed on each piece of equipment forming a local mesh network, which may be wireless. The gateway of this network is connected with these cloud services through the Internet. The cloud services infrastructure stores all necessary data about all the equipment the manufacturer has sold, including the active time-series parameter data sent from each piece of equipment. The equipment, network, cloud services, and humans interacting with these form an IoT system.

Three use case scenarios are presented:

1) The operator from the manufacturer remotely monitors the equipment. If an event or an alarm occurs, the operator can act on it remotely.
2) An event or alarm triggers the service subsystem, which generates a repair request to the repair person, who executes the repair, and closes the task.
3) After some repair tasks, the parts stored at the plant go below a set limit and this fact automatically triggers the parts management subsystem, which generates an order for the purchasing personnel, who follows through and in the end closes the order task.

An application of such an IoT system is illustrated in the following narrative about a large equipment that processes pollutants. The following picture is a single system that processes various wastes. It includes many parts and pipes and uses high temperature and electric charge to break waste molecules. The system could be used to treat various pollutants and is used to process industrial wastes, dangerous material, household garbage, used medical wastes, etc. The processed wastes can be recycled for power generation, a true green solution.

Table 7 describes various scenario conditions for Remote Management of Large Equipment in a Plant Use Case.

Table 7 – Scenario conditions for Remote Management of Large Equipment in a Plant

Scenario conditions					
Scenario name	**Scenario description**	**Primary actor**	**Triggering event**	**Pre-condition**	**Post-condition**
Monitor	Certain parts of equipment need to be replaced to prevent shutdown	Operator	A failed or failing part	Parts of the equipment are worn out.	The parts are replaced
The IoT system sends the operator information that a certain part is worn out. This information could be sent straight from the sensors on the equipment, or derived by cloud services from the big data collected about the equipment. The operator issues a repair order in the IoT system. After the repair person finishes the repair and enters the result into the IoT system, the IoT system sends the operator information that the repair is done.					
Scenario name	**Scenario description**	**Primary actor**	**Triggering event**	**Pre-condition**	**Post-condition**
Repair	Certain parts of the equipment need to be replaced to prevent shutdown	Repair person	A repair order	Certain parts of the equipment are worn out. The new parts are available.	The parts are replaced
IoT system forwards the repair order to the repair man. The repair person goes to the equipment, performs the repair/part replacement. The repair person enters the repair information and completion status.					
Scenario name	**Scenario description**	**Primary actor**	**Triggering event**	**Pre-condition**	**Post-condition**
Procure	The replacement part is running low at the inventory	Procurement person	Low inventory	Low inventory	New parts ordered
IoT system generates the purchase order based on the fact that the inventory level has fallen under a threshold. Purchase the parts from the supply chain, which results in the inventory being replenished. As such the inventory low status is changed.					

7.3.3 Actors

Table 8 shows the actors participating in the Remote Management of Large Equipment in a Plant Use Case.

Table 8 – Actors for Remote Management of Large Equipment in a Plant

Actor Name	Actor Type	Actor Description	Used Technology
IoT system	System		
Operator	Human User	The person who monitors the IoT system	
Repair personnel	Human User	The person who repairs the equipment	
Procurement personnel	IT tool	The person who places orders for equipment and parts	

7.3.4 Issues: Legal Contracts, Legal Regulations, and Constraints

None provided.

7.3.5 Referenced Standards and/or Standardization Committees

None provided.

7.3.6 Relation with Other Known Use Cases

This is for an equipment vendor who switches from only selling hardware to managing the whole lifecycle of its sold equipment. The vendor, during the sale of the product, signs a contract with its customer to remotely monitor the equipment.

7.3.7 General Remarks

Traditionally a large equipment manufacturer tries to make durable products, and makes money from the sale of the product. The equipment then belongs to the plant who may or may not know much about it. A lot of cost can be incurred once it fails. Although the equipment manufacturer could make money for parts and repairs, the repairs are a problem for the customers, which leads to negative impressions of the manufacturer. The manufacturer benefits long term if the equipment can be proactively managed so that it does not break down during production. This use case describes how the manufacturer could install an IoT system to better serve the customer.

7.3.8 Security and Privacy

Remote management must be operated with appropriate access management (authentication and authorization). When necessary, confidentiality might have to be ensured.

Availability might also be an issue when a critical remote management operation must be carried out.

7.3.9 Conformity Aspects and Critical Requirements

None provided.

7.3.10 Interaction between Actors and User Requirements

None provided.

7.3.11 Diagram of Use Case

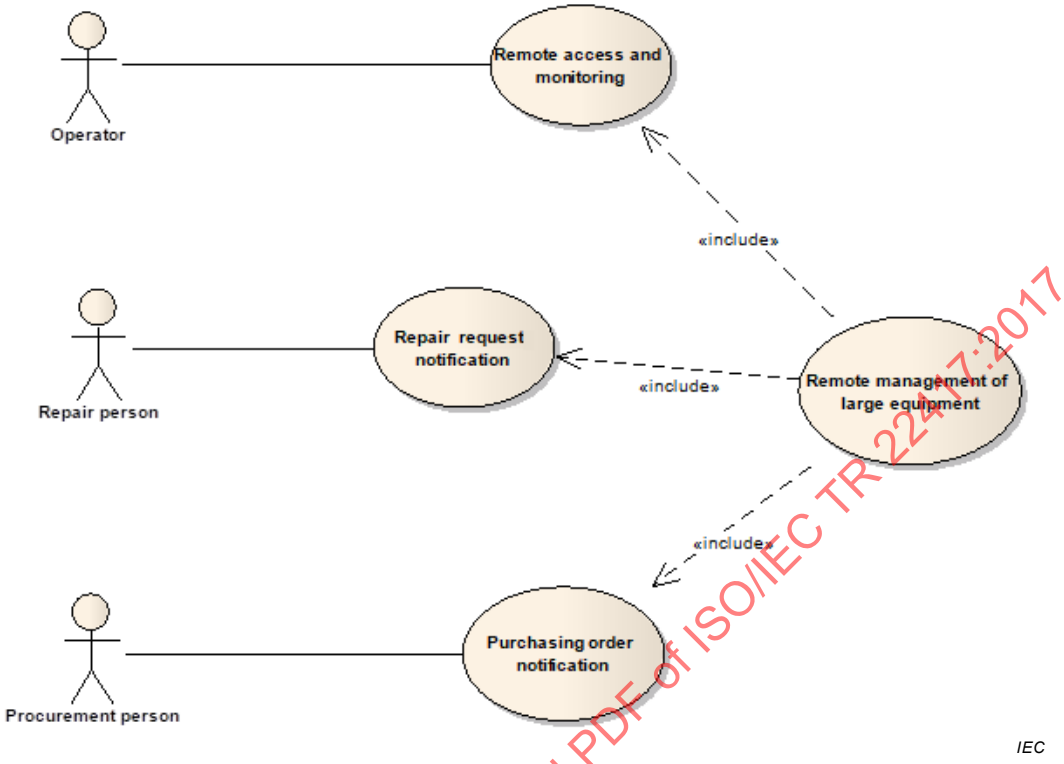


Figure 9 – Remote Management of Large Equipment in a Plant

7.3.12 Data Flow Diagram of Use Case

See 7.3.2 for reference.

7.4 Automated ICC Profile Discovery (Use case number 4 in Table 1)

7.4.1 Scope and Objectives of Use Case

This use case describes automated ICC profile discovery supporting colour performance auto-configuration and auto-update which delivers service and maintenance cost reduction in a medical office. Here the safety, security and privacy of office equipment discoverability functions are important.

Communication must be reliable and secure (encryption, authentication, etc.), Other requirements include Version Log Management, expired version detection and alarms to appropriate repository, and ontologies for devices and consumables discovery.

7.4.2 Narrative of Use Case

7.4.2.1 Short Description

John installed medical IT hardware including camera, display and printer, for remote skin disorder diagnosis.

7.4.2.2 Complete Description

John is a medical doctor in a worldwide medical care service which is capable of remote diagnosis with highly professional medical doctors. Patients sometimes have to drive or fly to visit a hospital spending many hours, but with this service, patients can be diagnosed at home, without physically visiting hospital. It is necessary for their IT hardware device profiles to be up to date, so that John can view the captured skin images from the patient's camera on his hospital display within a colour difference tolerance limit. Such limits are necessary because he has to make an assessment and calibration on skin colour to be able to detect skin diseases. He can also print the captured images and archive to his record as physical evidence.

Susan is a skin disorder patient, who gets the regular skin diagnosis at home with the help of remote diagnosis system. She has to set up the control of how and with whom her health information is shared before using the system.

7.4.3 Actors

Table 9 shows the actors participating in the Automated ICC Profile Discovery Use Case.

Table 9 – Actors for Automated ICC Profile Discovery

Actor Name	Actor Type	Actor Description	Used Technology
John	User	Medical doctor who is naive to Colour management but has high level criteria for colour reproduction accuracy in his remote diagnosis of skin disorder patient.	
Susan	User	Skin disorder patient	
Camera	IoT Device	Various types of cameras are available in terms of device cost, colour gamut size, colour accuracy, resolution,	
Display	IoT Device	Various types of displays are available in terms of device cost, colour gamut size, colour accuracy, resolution,	
Printer	IoT Device	Various types of printers are available in terms of device cost, running cost, speed, colour accuracy, resolution,	
Print paper	Consumable	Various types of papers are available in terms of cost, image quality, weight, size,	
Colour ink, toner	Consumable	Various types of inks, toners are available in terms of cost, image quality, image permanence, stability,	
Cloud service	ICC profile repository	Various types of repositories are available such as OEM, Third party, Consortium (e.g. ICC),	
Software	Application	Various types of applications are available such as OEM bundled in OSs, Profile provider (e.g. ColorBase),	

7.4.4 Issues: Legal Contracts, Legal Regulations, and Constraints

None provided.

7.4.5 Referenced Standards and/or Standardization Committees

Table 10 shows referenced standards and/or standardization committees relevant to the Automated ICC Profile Discovery Use Case.

Table 10 – Referenced Standards and/or Standardization Committees for Automated ICC Profile Discovery

Relevant Standardization Committees	Standards have to be considered in the Use Case	Standard Status
ICC, CIE Div. 1, CIE Div. 8, ISO/TC 42, ISO/TC 130, IEC TC 100/TA 2, ISO/IEC JTC 1/ SC 27, SC 28, SC 29, W3C	Colour characterization standards, Cloud service and web standards, Information security standards,	

7.4.6 Relation with Other Known Use Cases

None provided.

7.4.7 General Remarks

When the system is in operation everything works automatically without any user interaction. The remote monitoring application is a cloud service and can communicate with the IT hardware devices. A local router, situated for example in a smartphone, may be needed to translate between a local communication method such as Bluetooth Low Energy and the mobile network or Wi-Fi, but at application level end-to-end security and communication through firewalls are achieved. The communication must be reliable. User interaction is not required.

7.4.8 Security and Privacy

User must be in control of how and with whom information is shared, i.e. only uploading to an authorized device profile provider that is approved by the user.The device/user must be authorized to access a certain device profile provider, i.e. protection against fake devices and malicious users.

Confidentiality of information must be assured. No un-authorized entity should be able to get access to the data. This is typically solved by encrypted transport across the communications networks. Integrity of information must be assured. This means that it should not be possible to modify the data being sent.

Privacy must also be taken into account. The very fact that an external observer detects that an ICC profile is being updated can be an indication that the user (PII principal) has a health issue. In instances where PII is collected, all services must be in compliance with applicable privacy regulations.

7.4.9 Conformity Aspects and Critical Requirements

The system must be reliable in all aspects, for example, the cloud service application must be able to detect if any failure occurs, for example if contact is lost with the active system components.

7.4.10 Interaction between Actors and User Requirements

Proposal for sequence description that could contain the following parts for a system set-up:

- Description/Overview
  - The assumption is that IT tools should have discoverability and auto-configuration capabilities according to the ISO/IEC 30141[2] IoT reference architecture, so that a set-up and update of device profiles should be done without having user interference which means the system set up and authorization process through the device's web browser or a through a native application running in the devices.
- Pre-conditions
  - A set of IoT devices connected to cloud services.
  - Device with user interface, e.g. a laptop or a smartphone connected to cloud services.
- Flow
  - User logs in to service provider web site. If the user has an existing account, e.g. web-based service providers or social platforms, this could be used for the log in process.
  - User starts set-up process by specifying the IoT devices to form a system.
  - User approves that the system is used for the remote diagnostic application.
- Post-condition
  - The system is active through the diagnostic operation.

7.4.11 Diagram of Use Case

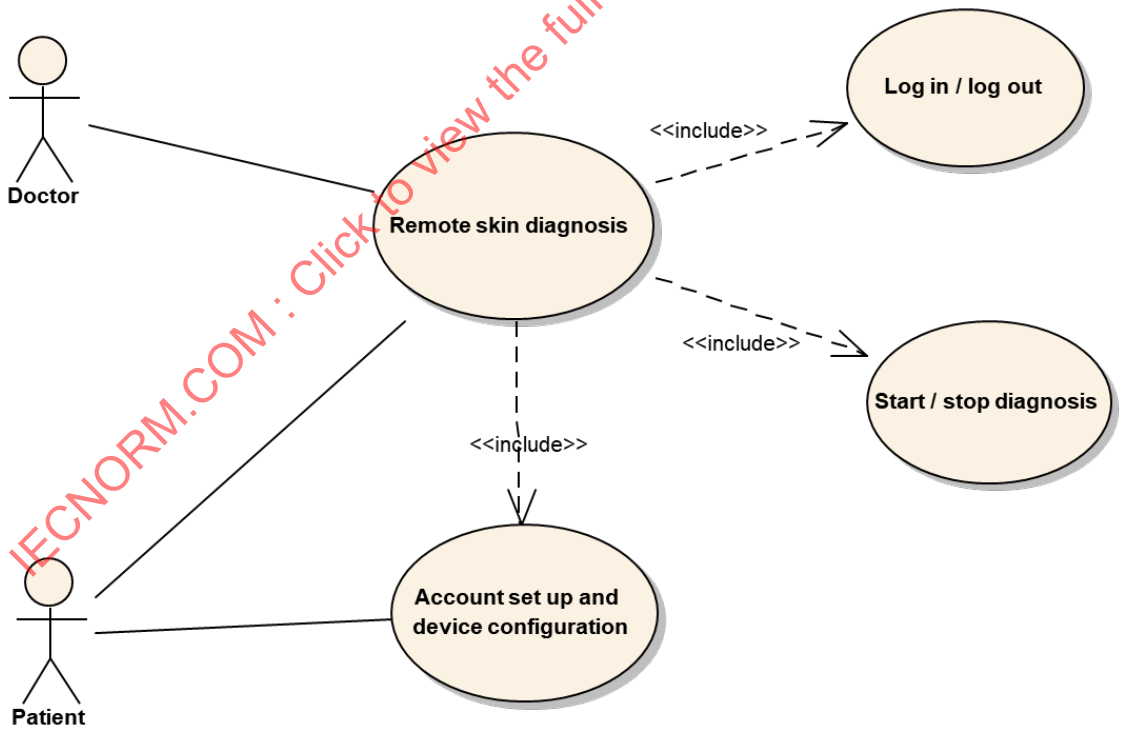


Figure 10 – Automated ICC Profile Discovery

[2] Under preparation. Stage at time of publication: ISO/IEC CDV 30141:2017.

7.4.12 Data Flow Diagram of Use Case

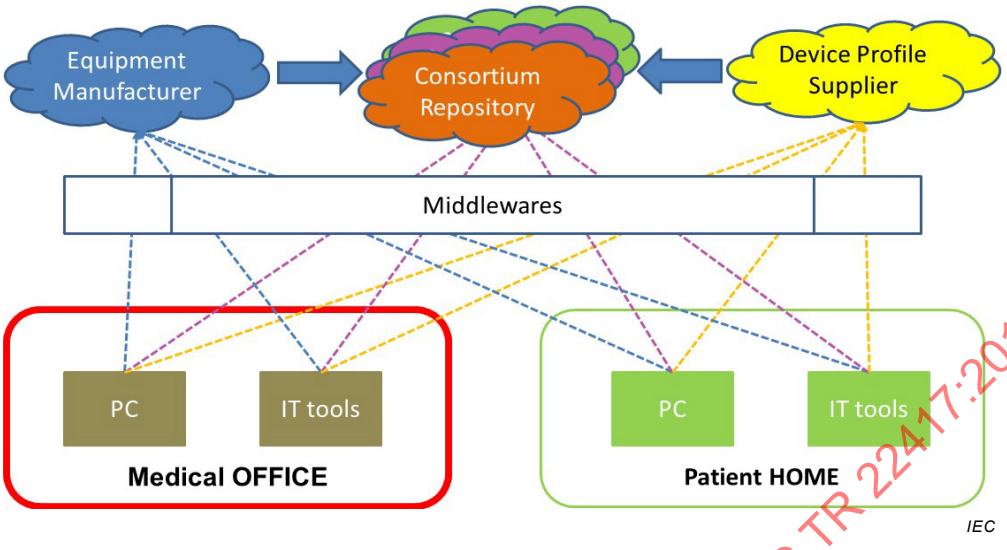


Figure 11 – Data Flow of Automated ICC Profile Discovery

7.5 Tracking of Farm Products (Use case number 5 in Table 1)

7.5.1 Scope and Objectives of Use Case

This use case describes the process of farm product tracking using an IoT system to achieve the supervision of farm products and ensure their safety.

The use case is within the scope of monitoring and supervision throughout the farm product supply chain, including production, processing, transportation, circulation, sale, etc.

The use case guarantees the safety and security of the farm products for the consumers. Meanwhile, it facilitates the management of the farm products for the businesses involved in the supply chain. Food safety and security is becoming increasingly important in countries such as China, and the ability to track farm products from origin to destination is becoming a very important topic. The tracking of the farm products effectively manages the farm product supply chain for the government and industry and benefits the consumer.

In order to achieve effective farm product tracking IoT technology can be used to realize the monitoring and supervision of the products throughout the entire farm product supply chain, including production, processing, transportation, circulation, sale, etc. The IoT system collects the specified information of the farm products via sensors at every stage of the farm product supply chain. The data are stored and aggregated in the IoT system. The system provides an enquiry service for the customers. The reliability and security of the system is guaranteed by the operation and maintenance management systems. Data interchange can be achieved through interaction with other systems.

7.5.2 Narrative of Use Case

7.5.2.1 Short Description

This use case describes the process of farm product tracking using an IoT system to achieve the farm product safety and security.

7.5.2.2 Complete Description

Table 11 shows various scenario conditions for the Tracking of Farm Products Use Case.

Table 11 – Scenario conditions for Tracking of Farm Products

Scenario conditions					
Scenario name	**Scenario description**	**Primary actor**	**Triggering event**	**Pre-condition**	**Post-condition**
Inspection on meat production	Collection of specified data during the meat production process	Object, sensing and controlling system, IoT gateway	Regular quarantine, vaccination, injection of medicine, quarantine after slaughtering		
Tracking of meat on the retail market	Inspection of meat status during the retail process	Object, sensing and controlling system, IoT gateway, service provider, operation and maintenance management, resource interchange	Delivering, weighing, storing, processing of meat and checking freshness		

7.5.3 Actors

Table 12 shows the actors participating in Tracking of Farm Products Use Case.

Table 12 – Actors for Tracking of Farm Products

Actor name	Actor type	Actor description	Further information specific to this use case
Government customer	Organization	Government customers are agricultural bureau, business bureau, etc.	
Public customer	Human user	Public consumer	
Farm product	Physical entity	Meat, vegetables, milk, etc.	
Employees involved in farm product activities	Human user	People involved in the farm product activities	
RFID tag and reader	Device	It reads or writes information of farm products during the supply chain management procedures of farm products. The information can be tracked by the customer.	
Employee sensor card	Device	It collects information relating to employees involved in the farm product activities.	
Electronic ledger	Application	Sensor data is input to the electronic ledger under authentication by a third-party.	
IoT gateway	Gateway	It encapsulates and converts the format of the sensor data	

Actor name	Actor type	Actor description	Further information specific to this use case
Information security support	System	It provides statistical data processing and analysis for the agricultural products and gives early warning when abnormal data is identified.	
Tracking management platform for government customer	System	It provides the monitoring management service for the government customer and achieves supervision of the farm product in the market.	
Tracking service platform for public customer	System	It provides enquiry service for the public customers via web, 2-D barcodes scanning, etc. It also supports responding to the customers' complaints on food safety.	
IT system maintenance	System	It performs the management and maintenance of the IoT devices, so as to guarantee the reliability and security of the IoT system.	
Real-time monitoring in farm product supply chain	System	It offers real-time monitoring during the production, processing, transportation, circulation, sale, etc. of the agricultural products.	
Farm product information exchange platform	System	It provides sharing and interchange of the IoT system data with other systems.	
E-commerce platform	System	It offers a financial interchange service between the IoT system and other systems	
IoT System provider	System Provider	It sells or leases the IoT System to the farmer and provides privacy management capabilities	

7.5.4 Issues: Legal Contracts, Legal Regulations, Constraints

None provided.

7.5.5 Referenced Standards and/or Standardization Committees

None provided.

7.5.6 Relation with Other Known Use Cases

None provided.

7.5.7 General Remarks

None provided.

7.5.8 Security and Privacy

The IoT system is collecting data on employees. Suitable assurance that the system complies with applicable privacy regulations must be obtained. This might involve proper consent management procedures.

7.5.9 Conformity Aspects and Critical Requirements

None provided.

7.5.10 Interaction between Actors and User Requirements

Table 13 shows information exchanged between domains in interactions in the Tracking of Farm Products Use Case.

Table 13 – Interaction for Tracking of Farm Products

Information exchanged			
Information exchanged, ID	**Name of information**	**Description of information exchanged**	**Requirement, R-IDs**
UD and OMD	Operation status of user system	UD enquires operation status of the user system and get feedback from OMD, including the basic user information, user priority, etc.	
UD and ASD	Enquiry service, complain report	ASD provides inquiry service for the UD; UD can feedback complaint report to ASD	
UD and RID	Request and response of resource interchange with other systems	RID and UD exchange information of farm product	
OMD and ASD	Control instructions, operation status	OMD transmits control instructions to ASD, ASD feeds back the operation status to OMD	
ASD and RID	IoT resource, resource from other system	ASD and RID exchange IoT resource and resource from other systems	
OMD and SCD	Heterogeneous sensor data, device and system status	SCD provides heterogeneous sensor data to OMD, SCD feeds back operation status to OMD	
ASD and SCD	Heterogeneous sensor data, control and request data	SCD provides heterogeneous sensor data to ASD, ASD transmits control and request data to SCD	
RID and SCD	Heterogeneous sensor data, resource from other systems	SCD provides heterogeneous sensor data to RID, RID transmits resource from other systems to SCD	
SCD and PED	Sensor data	SCD obtains sensor data from PED	

7.5.11 Diagram of Use Case

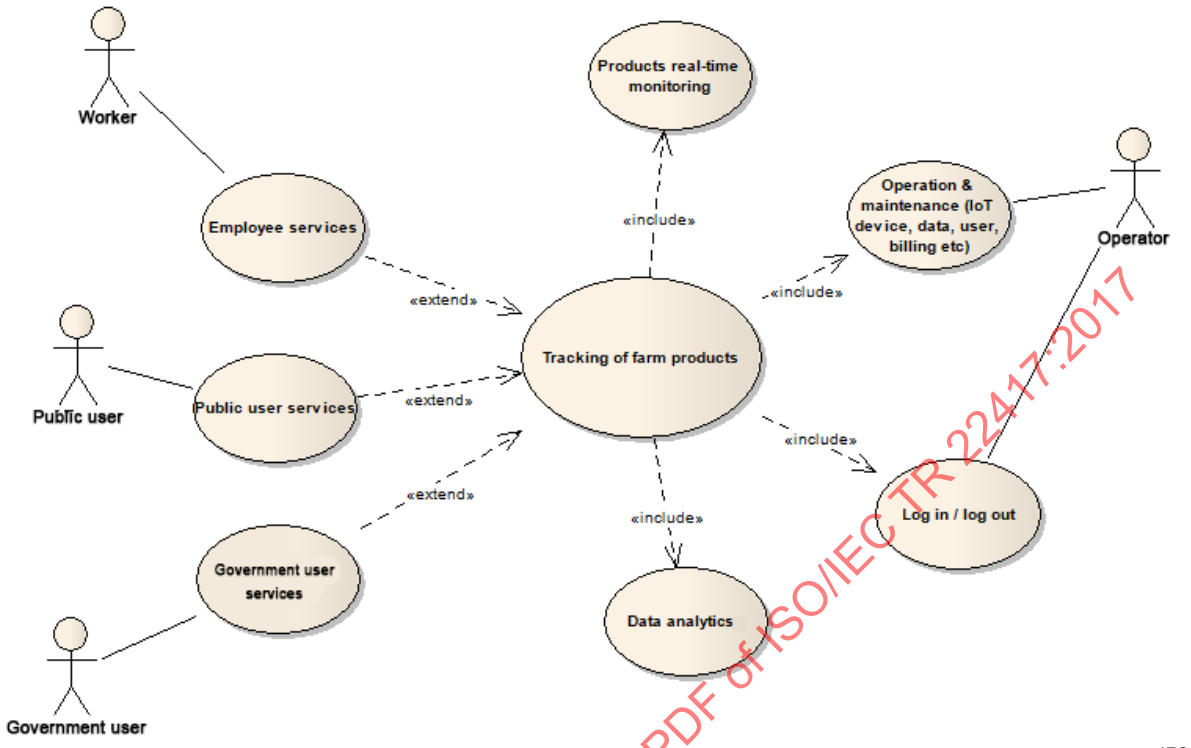


Figure 12 – Tracking of Farm Products

7.5.12 Data Flow Diagram of Use Case

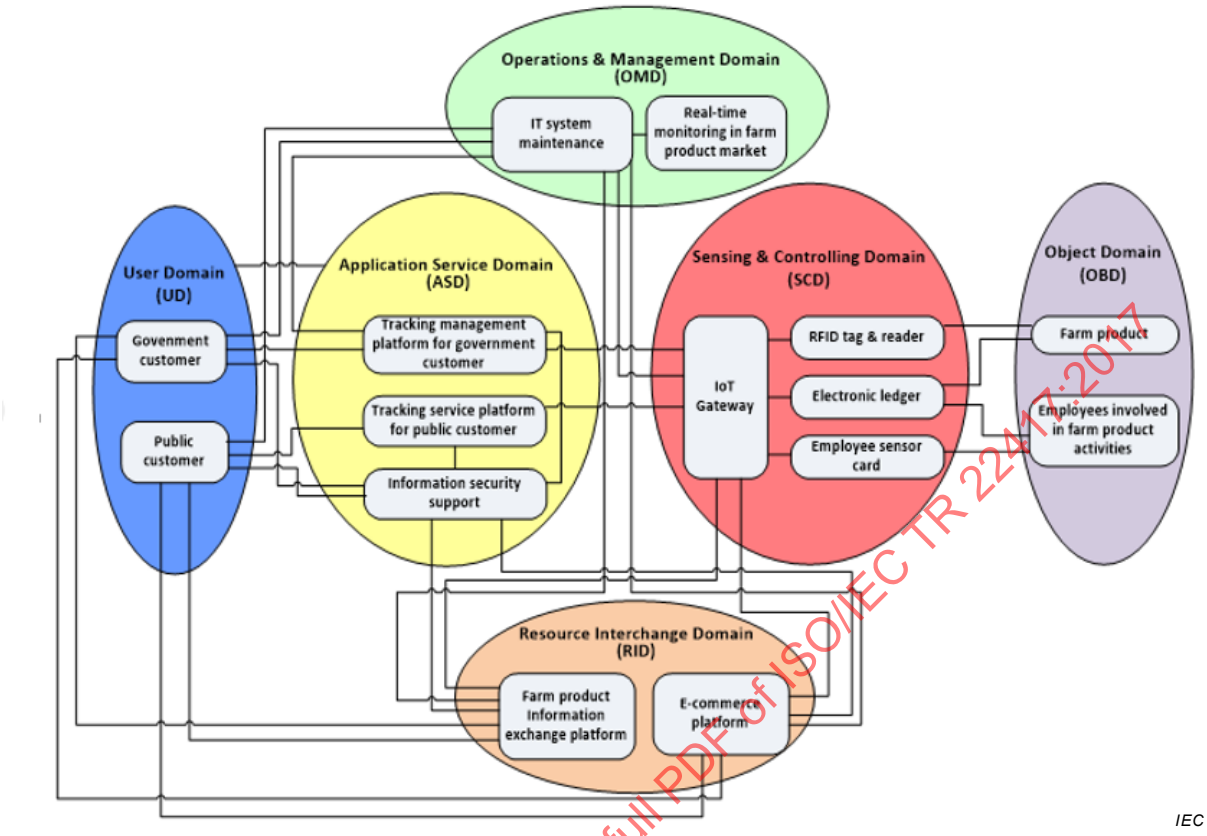


Figure 13 – Data Flow of Tracking of Farm Products

7.6 Warehouse Goods Monitoring (Use case number 6 in Table 1)

7.6.1 Scope and Objectives of Use Case

This use case describes an IoT application system, which automatically monitors and tracks goods in warehouses. By monitoring and tracking these goods the owners can accurately evaluate their assets at any given time. Therefore, such IoT systems help owners to apply for and secure the loans from banks using the assets as collateral. The IoT system also benefits the lenders (e.g. banks) by monitoring the assets of a borrower at any given time.

7.6.2 Narrative of Use Case

7.6.2.1 Short Description

This use case describes the accurate monitoring of goods in a warehouse as part of financial management and ensures movements in and out of stock are only done with appropriate authorization. This IoT application benefits both the owners of the goods and the bank; thus, it provides a new financial mode of IoT technology used for dynamic property supervision.

7.6.2.2 Complete Description

Previously, when an enterprise, which owns goods, applied for loans from a bank; the owner of the enterprise needed to value their assets and submit loan application documents along with the warehouse manager's verification of goods in the warehouse to the lending bank. With the value of the goods as collateral, the bank's loan officer would decide whether or not to approve the loan based on the application documents provided by the enterprise owner and the warehouse manager. If the information in the application was incorrect or falsified or the goods were removed from the warehouse by illegal activity, the bank that had already loaned the funds to the enterprise would have no way of knowing if such situation had occurred and

therefore might not be able to recover any portion of the money that was loaned to the enterprise owner.

A warehouse goods monitoring system is an application realized by IoT technology to automatically monitor and track significant quantities of goods. Figure 11 shows the IoT applications for monitoring the goods in the warehouse. This information includes when goods are moved in and out of the warehouse, the weight of all the boxes and containers of the goods, the types of the goods in the different boxes and containers, and the location from which they are being collected. If the goods are moved out of the warehouse without authorization, it would be considered illegal activity and would therefore trigger the alarm system to alert the warehouse security office and/or monitoring operator.

Therefore, this IoT system allows the owners of the goods to secure the loans from banks as it benefits the bank to have the confidence in the collateral, which reduces the risk and potential loss associated with the loans.

Figure 14 – IoT Applications for Monitoring the Goods in the Warehouse

7.6.3 Actors

Table 14 shows the actors participating in the IoT Application for Warehouse Goods Monitoring Use Case.

Table 14 – Actors for IoT Application for Warehouse Goods Monitoring

Actor Name	Actor Type	Actor Description	Further Information specific to this use case
RFID tag and reader	Devices	RFID tags attached on boxes and containers have the recorded information about goods. Using RFID readers, all the information about the goods is collected.	
Electronic scale	Device	Electronic scale acquires the weight of all the goods individually or in boxes or containers.	

Actor Name	Actor Type	Actor Description	Further Information specific to this use case
Sensor with UWB module	Device	Using sensors with a UWB module, the location of the goods in the warehouse can be calculated and recorded.	
Laser radar	Device	Laser radar acquires the contour information when boxes are placed in the warehouse, and the system can perform the contour change detection and raise an alarm when the change is more than 15% which can indicate that some of the boxes have been moved.	
Alarm controller	System	When boxes are illegally moved out of the warehouse, it triggers the alarm controller. This produces a sound and light alarm, and additionally send alarm information to the service platform to alert the security officers or the security monitoring operator.	
IoT gateway	Device	IoT gateways connect all types of sensors, sensor nodes, and RFID tag information, which is read by RFID readers, and other outside networks. It also collates gathers the information and manages the local network.	
Internet connectivity	Network	Internet connectivity enables the information relating to goods to be exchanged between the service platform, user system, and other platforms.	
On-line monitoring service system	System	The on-line monitoring service system collects the information on the goods in the warehouse including name, originating warehouse or supplier, location where the goods are placed in the warehouse, and the weight of goods. It also registers the workers that go in and out of the warehouse including their name, identification or employee number, etc. It manages the warehouse information and provides an information service for the bank and the enterprise.	

Actor Name	Actor Type	Actor Description	Further Information specific to this use case
Collateral service system	System	The collateral service system performs a collateral service for banks and enterprises, and it manages the collateral information, including goods in the warehouse, warehouse, owners, banks, the values of the goods, etc.	
Resource access system	System	The resource access system connects to, and gets data from, third-party systems. The third party systems include commercial exchange systems that can provide the goods' real-time price information with the collateral management system in the ASD. End-users, being the banks and the enterprise owners, can acquire the value of the collateral goods and can compare this with the value of loan in real-time.	
Information resource database	Application	The information resource database categorizes all the sensor and device data in terms of the types of goods, stores all the data and allows authorized data exchanges with other services.	
Maintenance system	System	The maintenance system manages the entire warehouse goods monitoring system ensuring stable and safe operation. It records all the systems' operational states, device states, and provides maintenance services.	
Rules management system	System	This provides the rules for the management of collateralized goods and commercial trade. For example, if the goods are already guaranteeing a current loan the system will inform the service provider not to provide the loan service using the same goods as collateral.	

7.6.4 Issues: Legal Contracts, Legal Regulations, Constraints

None provided.

7.6.5 Referenced Standards and/or Standardization Committees

None provided.

7.6.6 Relation with Other Known Use Cases

None provided.

7.6.7 General Remarks

None provided.

7.6.8 Security and Privacy

Operations must be carried out with proper access management to ensure that unauthorized parties do not access the system. IoT devices impersonation must be prevented.

7.6.9 Conformity Aspects and Critical Requirements

None provided.

7.6.10 Interaction between Actors and User Requirements

None provided.

7.6.11 Diagram of Use Case

See Figure 14 and 15 for reference.

7.6.12 Data Flow Diagram of Use Case

Data flow of warehouse goods monitoring from architectural viewpoint is shown in Figure 15.

- PED
  - The objects in this IoT application system are the goods stored in the warehouse and the workers that moved the goods.
- UD
  - The end-users of the system are the enterprise and the bank.
- SCD
  - The devices can sense information relating to the goods in the warehouse and trigger alarms in certain conditions (e.g., illegal activity, or where the weight of a container does not match with the recorded weight, etc.).
- ASD
  - Service providers use service platforms to collect the information and provide information services to the end-users.
- RID
  - Service providers need information from other third-party information system to provide services, such as getting commercial exchange information through the resource exchange platform in the RID, to perform the commercial evaluation services of the goods.
- OMD
  - System managers manage the whole system through the operation and management platform.

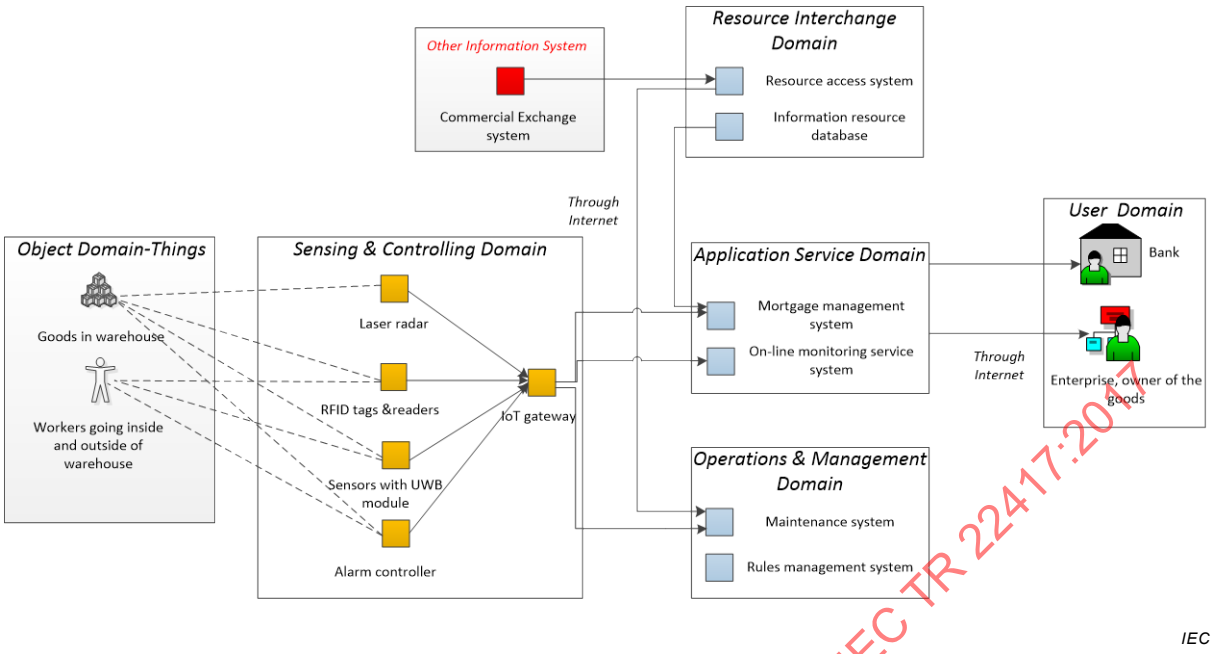


Figure 15 – Data Flow of Warehouse Goods Monitoring from architectural viewpoint

7.7 Cooperation between Factories and Remote Applications (Use case number 7 in Table 1)

7.7.1 Scope and Objectives of Use Case

This use case describes global cooperation between factories and remote applications for improving the efficiency of their operations. The scope of this use case is global cooperation between factories and an IoT application, which allows manufacturers to optimize operations in their factories by monitoring and controlling production lines running on a remote server. This use case describes how a remote server IoT application exchanges data with specific factories through a wide area network in order to optimize operations in those factories.

7.7.2 Narrative of Use Case

7.7.2.1 Short Description

This use case describes how an IoT application running on a remote computing environment exchanges data with factories through a wide area network in order to optimize operations by monitoring and controlling production lines. In this case, an IoT gateway located in a factory provides connectivity between the IoT application and production line controllers (e.g. MES, SCADA, PLC) in those factories. The IoT gateway has to dynamically translate different transmission protocols.

In factories deploying several types of networks with different protocols an IoT application running on a remote computing environment exchanges data with those factories through a wide area network. In this case, a factory IoT gateway provides connectivity between the IoT application and the factory production line controllers. The IoT Gateway should be able to address unexpected events, such as throughput degradation of a wide area network connection, rapid increase of the amount of information data in a factory.

7.7.2.2 Complete Description

Nowadays IoT technologies aim to solve business problems. In an industry field, global cooperation between factories and a remote application can optimize operations in those factories. Potential applications of such remote systems would be product line optimization which enables operational efficiency of the factories, and stock control optimization among the factories. In factories, having automated production lines using IoT technology, behaviours of individual devices are controlled dynamically according to monitored sensor

data. In order to achieve a necessary level of control, dedicated network technologies, which provide real-time and high reliability transmission for communications among sensors, devices, and controllers are required. Figure 14 shows a concept of this cooperation between factories and a remote application.

There are different categories of networks in factories which have different transmission attributes and such transmission attributes are categorized by priorities of the transmission data. For example, in many applications, motion control commands for devices should have the first priority, device and network (re-)configuration commands should have the second priority, and information data such as a log file transfer should have the third priority. Priorities will depend on the types of the data, data sources and their destinations. For instance, while strict requirements (e.g. zero or small delay, periodicity, or no lost packets) are necessary for the control commands, such strict requirements are not necessary for the less critical log information. Figure 15 shows an example of network structure for this global cooperation. In the structure, there are four types of networks each having different transmission attributes while the IoT gateway provides connectivity to a remote application. Figure 16 shows an example of data amount and real time capability in each network domain.

This use case shows that a remote application exchanges data with factories through a wide area network in order to optimize operations in those factories by monitoring and controlling production lines. In this case, an IoT gateway located in a factory provides connectivity between the remote application and the controllers in the factory. The IoT gateway has to dynamically translate different transmission protocols. The IoT gateway should be able to address unexpected events, such as throughput degradation of a wide area network connection, rapid increase of the amount of information data in a factory.

Therefore, the IoT Gateway has the following potential requirements:

1) An IoT Gateway shall have QoS functionalities such as a priority control, traffic shaping, and traffic policing.
2) An IoT Gateway shall be able to observe network conditions on a wide area network in order to provide feedback control for its own transmission function.

Table 15 shows various scenario conditions for cooperation between Factories and Remote Applications Use Case.

Table 15 – Scenario conditions for Cooperation between Factories and Remote Applications

Scenario conditions			
Individual factories are deploying several types of networks having different transmission attributes for controlling and managing equipment. A remote application program manages individual factories to optimize their operations and is connected through a wide area network to the factories.			
Scenario name	**Scenario description**	**Primary actor**	**Triggering event**
Prioritized transmission	This scenario describes how an IoT gateway deployed in a factory behaves when it receives high priority information during normal data transfer to a remote application	IoT gateway	Event Notification

Table 16 shows specific steps in a prioritized transmission scenario in the Cooperation between Factories and Remote Applications Use Case.

Table 16 – Specific steps in Prioritized Transmission Scenario

Event	Name of process/ activity	Description of process/ activity	Information exchanged	Information producer (actor)	Information receiver (actor)
Periodic transfer	Log file transfer	A server sends collected log information for a certain period to a remote application through an IoT gateway periodically.	Log file: Log files contain records of behaviour, status, and failures for monitored equipment in a factory.	Server	IoT Gateway
Normal transfer	File transfer	The IoT gateway forwards a large amount of low priority data to a remote application.	Log file:	Server	IoT Gateway
Event Notification	High priority event	While the server sends large amounts of log information to the remote application, a controller sends an emergency event (e.g. a performance degradation of equipment) to the remote application through the IoT gateway.	Event Notification: Information concerning emergency events, which are published by controllers in a factory.	Controller	IoT Gateway
Prioritized transmission	Selective transmission in order of priority	Even though the IoT gateway has been forwarding a large amount of data from the server, the IoT gateway detects receipt of high priority data from the controller, and forwards them before low priority data. The IoT gateway then resumes forwarding the rest of low prioritized data.	Event Notification, Log file	IoT gateway	Remote Application

7.7.3 Actors

Table 17 shows the actors providing cooperation between Factories and Remote Applications Use Case.

Table 17 – Actors for Cooperation between Factories and Remote Applications

Actor name	Actor type	Actor description	Further information specific to this use case
IoT Gateway	Gateway	It interconnects networks and exchanges data between controllers in a factory and remote applications.	
Remote Application	Application of monitoring system	It monitors operation of production lines in factories, and provides feedback control of the production lines.	
Controller	System	It controls equipment including production lines.	
Server	System	It collects log information of equipment deployed in a factory.	

7.7.4 Issues: Legal Contracts, Legal Regulations, Constraints

None provided.

7.7.5 Referenced Standards and/or Standardization Committees

None provided.

7.7.6 Relation with Other Known Use Cases

None provided.

7.7.7 General Remarks

This use case describes factories which deploy several types of networks having different transmission attributes, an IoT application running on a remote computing environment exchanges data with those factories through a wide area network in order to optimize operations in those factories by monitoring and controlling production lines. In this case, an IoT Gateway located in a factory provides connectivity between the remote IoT application and controllers (e.g. MES, SCADA, PLC) in those factories. The IoT Gateway dynamically convert between different protocols on local and wide area networks.

7.7.8 Security and Privacy

The overall communication facility between applications and factories must comply with the availability needs. Further remote applications should be authenticated.

7.7.9 Conformity aspects and Critical Requirements

None provided.

7.7.10 Interaction between Actors and User Requirements

Table 18 shows information exchanged between domains in interactions in the Cooperation between Factories and Remote Applications Use Case.

Table 18 – Interaction for Cooperation between Factories and Remote Applications

Information exchanged			
Information exchanged, ID	**Name of information**	**Description of information exchanged**	**Requirement, R-IDs**
PED and ASD and OMD	Log file	Log files contain records of behaviour, status, and failures for monitored equipment in a factory.	
SCD and OMD	Event Notification	This information carries emergency events, which are published by controllers in a factory.	

7.7.11 Diagram of Use Case

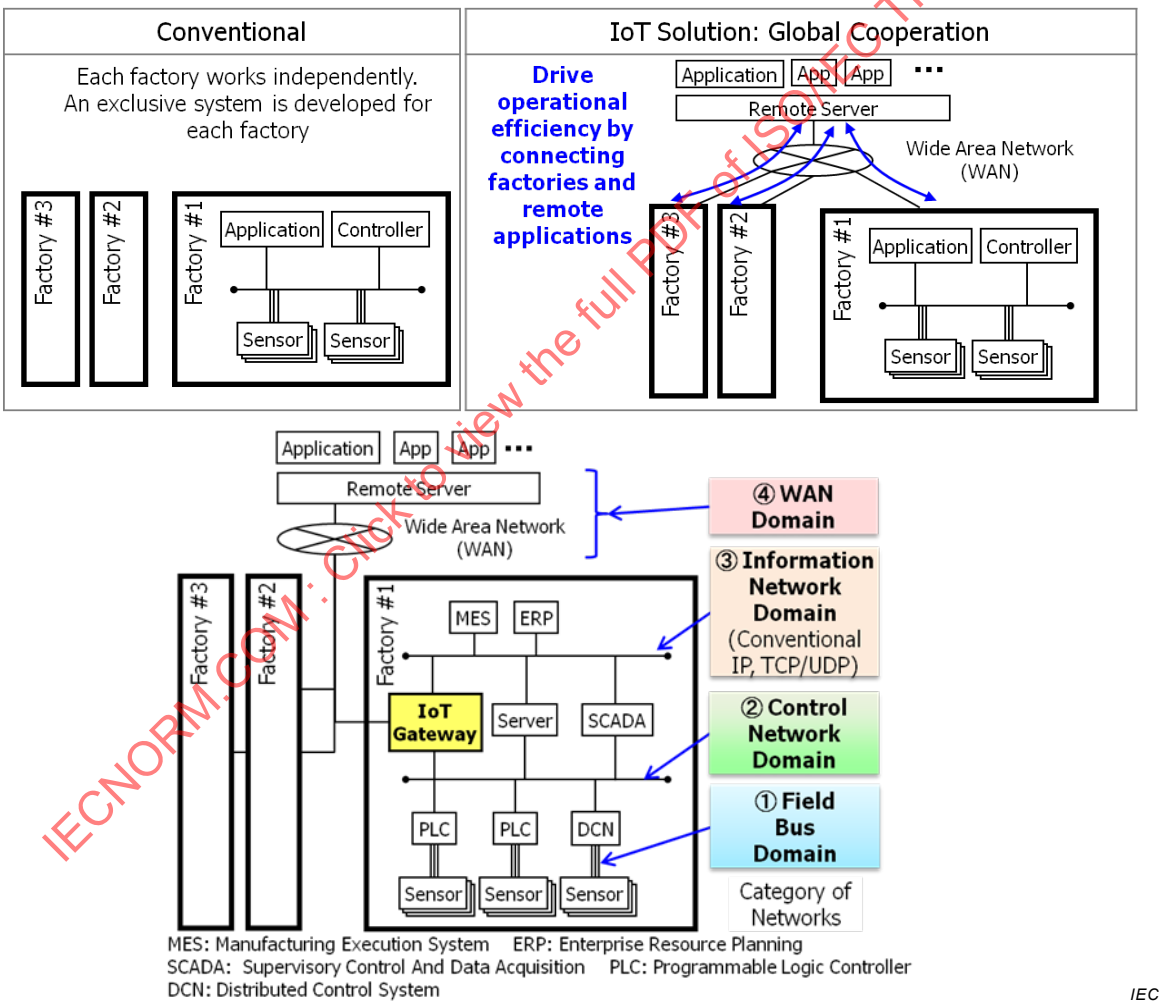


Figure 16 – Cooperation between Factories and Remote Applications

7.7.12 Data Flow Diagram of Use Case

See 7.7.2 and Figure 16 for reference.

7.8 Searching System for People with Cognitive Impairment (Use case number 8 in Table 1)

7.8.1 Scope and Objectives of Use Case

To allow a cognitively impaired patient to be located and tracked when reported missing by a carer.

7.8.2 Narrative of Use Case

7.8.2.1 Short Description

This use case describes a secure data management system. A GPS tracker in the shoes of a patient allows GPS data to be fed to a data management centre which can then track the location of the patient when they are informed by carers that the patient is missing. The GPS location of the cognitively impaired person can be passed to police, taxi drivers etc. who can locate the person and ensure their safety.

7.8.2.2 Complete Description

A carer reports that a patient is missing from their home or care facility. Because the patient has a GPS device in their shoes this can be used to locate and track them. When the carer notifies the information centre that the patient is missing the call handler establishes the location of the patient. The call handler can then notify a responsible person, such as a family member, carer or police officer, to fetch the patient, and can update them if the patient moves during the retrieval process.

7.8.3 Actors

Table 19 shows the actors participating in the Searching System for People with Cognitive Impairment Use Case.

Table 19 – Actors for Searching System for People with Cognitive Impairment

Actor Name	Actor Type	Actor Description	Used Technology
Patient	User	Cognitively impaired individual e.g. someone affected by Alzheimer's or dementia	
Carer	User	Individual providing caring service to patient	
Call Handler	User	Receives a telephone notification of the missing person	
Information system	System	Information system used by call handler to coordinate the rescue and safe return of the patient.	
GPS	Device and System	Used to locate patient	
Police Officer/Carer	User	Responds to information supplied by the call handler and actually physically locates and retrieves the patient.	

7.8.4 Issues: Legal Contracts, Legal Regulations, Constraints

Table 20 identifies issues for Searching System for People with Cognitive Impairment Use Case.

Table 20 – Issues for Searching System for People with Cognitive Impairment

Issue – here specific ones	Impact of Issue on Use Case	Reference – law, standard, others
Personal data protection	Patient or the carer need to give informed consent for sharing of personal information	

7.8.5 Referenced Standards and/or Standardization Committees

Table 21 shows referenced standards and/or standardization committees relevant to the Searching System for People with Cognitive Impairment Use Case.

Table 21 – Referenced Standards and/or Standardization Committees for Searching System for People with Cognitive Impairment

Relevant Standardization Committees	Standards that have to be considered in the Use Case	Standard Status
JTC 1/SC 27	ISO/IEC 29151: Code of practice for personally identifiable information protection.	ISO/IEC standard

7.8.6 Relation with Other Known Use Cases

RFID technology is used for tracking and locating animals and in some countries it is a legal requirement to chip horses, dogs and other pets. When the microchip is read the tag reader sends the relevant data to an information database so that the identity of the owner can be established, or the “pet passport” checked.

7.8.7 General Remarks

None provided.

7.8.8 Security and Privacy

This use case requires informed consent from the patient or carer for personal data to be released to, or accessed at, the call centre. Suitable privacy and consent management must be provided. In instances where PII is collected, all services must be in compliance with applicable privacy regulations.

7.8.9 Conformity aspects and Critical Requirements

None provided.

7.8.10 Interaction between Actors and User Requirements

None provided.

7.8.11 Diagram of Use Case

Figure 17 – Searching System for People with Cognitive Impairment

7.8.12 Data Flow Diagram of Use Case

See description in 7.8.2 above.

7.9 Sleep Monitoring System (Use case number 9 in Table 1)

7.9.1 Scope and Objectives of Use Case

This use case describes use of frequency analysis of HRV/PRV to establish the sleep stages of the patient. This can help diagnose issues such as sleep apnoea and monitor the effect of certain devices to improve breathing.

Pulse wave sensor, temperature sensor and 3-dimensional accelerator inside package worn on the chest.

Bluetooth connection to tablet display

IEC

Figure 18 – Sleep Monitoring Systems

7.9.2 Narrative of Use Case

7.9.2.1 Short Description

Fitness and sleep tracking is another application for IoT systems. There is a growing awareness of sleep as a health concern because alterations of sleep duration and architecture have been associated with increased morbidity and mortality, and specifically linked to chronic cardiovascular disease and psychiatric disorders, such as type 2 diabetes or depression. Measurement of sleep quality can assist in the diagnosis or treatment of these diseases and others such as sleep apnoea.

Monitoring sleep patterns in the home is useful for individuals concerned about their sleep quality, for care givers checking patients, and for medical personnel diagnosing sleeping issues. Being able to monitor sleep at home can be less disruptive than attending a sleep clinic even if the accuracy of some of the measurements is reduced.

Many devices allow sleep statistics to be uploaded to the internet for analysis with increasing integration and connectivity between personal tracking hardware and cloud services software.

7.9.2.2 Complete description

Recent advances in electronic technologies and sensor interfaces have allowed for a significant reduction in the size and weight of recording equipment and made self-application feasible. This allows assessment of sleep quality in the home where a patient's sleep patterns can be objectively quantified in their normal sleeping environment using wearable recorders or sensors in the bed.

For example, a biometric sensor can be placed under a mattress without any wires or leads and there is no disruption to the patient's physical environment. The sensor detects heart rate, breathing rate, motion, and presence in bed while the person sleeps normally. A common method used for personal sleep tracking devices is actigraphy, a non-invasive way of monitoring human rest and activity cycles usually with a wrist-worn device which measures and records bodily motion. Additional sensors can measure pulse rate and EEG. Signals acquired from the forehead can provide total time and percentage sleep, REM and SWS, sleep efficiency, total and average number of cortical, sympathetic and behavioural arousals, and the frequency and intensity of snoring.

7.9.3 Actors

Table 22 shows the actors participating in the Sleep Monitoring System Use Case.

Table 22 – Actors for Sleep Monitoring System

Actor Name	Actor Type	Actor Description	Used Technology
John	User	Person having sleep monitored	
Medical Professional	User	Person reviewing results for medical diagnosis	
Accelerometer sensor	Sensor	Various types of accelerometers are found in mobile phones, and wellness and medical bracelet devices.	
Audio sensor	Sensor	Sensor measures snoring intensity and duration	
EEG sensor	Sensor	Sensor measures EEG	
Pulse rate sensor	Sensor	Sensor measures pulse rate	
Processing unit	Device	Processes raw sensor data to provide traces etc.	
Data analysis tool	Application	Analyses and displays sensor information	

7.9.4 Issues: Legal Contracts, Legal Regulations, Constraints

This use case may be affected by national medical regulations. For example, in some countries the transmission of medical information must comply with the HIPAA (Health Insurance Portability and Accountability Act) privacy/security rule.

7.9.5 Referenced Standards and/or Standardization Committees

The ISO/IEEE 11073 series enables communication between medical devices and external computer systems. This standard and corresponding IEEE 11073-104zz standards address a need for a simplified and optimized communication approach for personal health devices, which may or may not be regulated devices. These standards align with, and draw upon, the existing clinically focused standards to provide easy management of data from either a clinical or personal health device. The work is done in ISO/TC 215 and IEEE.

1) ISO/IEEE 11073-00103 provides an overview of the personal health space and defines the underlying use cases and usage models.
2) ISO/IEEE 11073-10101 documents the nomenclature terms that can be used.
3) ISO/IEEE 11073-10201:2004 documents the extensive domain information model (DIM) leveraged by this standard.
4) ISO/IEEE 11073-104xx standards define specific device specializations. For example, ISO/IEEE 11073-10404 defines how interoperable pulse oximeters work.

7.9.6 Relation with Other Known Use Cases

None provided.

7.9.7 General Remarks

None provided.

7.9.8 Security and Privacy

Health and wellness monitoring systems, such as sleep monitoring systems, collect personal data (PII) and the use of this will be subject to appropriate security and privacy regulations. In instances where PII is collected, all services must be in compliance with applicable privacy regulations.

7.9.9 Conformity Aspects and Critical Requirements

None provided.

7.9.10 Interaction between Actors and User Requirements

None provided.

7.9.11 Diagram of Use Case

See 7.9.1 and Figure 18.

7.9.12 Data Flow Diagram of Use Case

See use case description above.

7.10 Smart Glasses (Use case number 10 in Table 1)

7.10.1 Scope and Objectives of the Use case

This use case describes how a factory worker can use smart glasses to receive information on the shop floor to assist with setting up and maintaining machinery.

7.10.2 Narrative of Use Case

7.10.2.1 Short Description

Smart glasses are used on factory floors in a number of ways to provide information to the user; for example, a camera can scan barcodes so the user can see specific information based on individual customer requirements, as well as enabling precise positioning during installation or maintenance. This use case describes how a factory worker can use smart glasses to receive information on the shop floor to assist with setting up and maintaining machinery.

7.10.2.2 Complete Description

Smart glasses enable factory workers to have essential information provided in a hands-free way so that they can undertake assembly or maintenance operations. With some smart glasses, workers can beam what they are seeing across the world and receive visual instructions as they work. Field and warehouse employees will be among the early adopters for these wearable technologies aimed at increasing productivity and safety while reducing employee errors.

Wearable-computing technologies such as Smart Glasses require a constant and smooth interaction between humans and machines. They allow users to perform tasks while simultaneously executing commands and are functional in situations where tasks have to be performed at a distance from traditional desktop computing.

In a field-service, maintenance, and trouble-shooting role, Smart Glasses can be used to deliver information on installed equipment and diagnose problems, eliminating the need for service engineers to make site visits.

Head-mounted displays (HMDs) are becoming more streamlined and ergonomically appropriate compared to the bulky ones that were available in the recent past and as they are becoming more cost effective they are becoming increasingly widespread. Next-generation OLED micro displays and retinal displays are expected to further increase adoption as they support many capabilities. There are near-eye 2D/3D video see-through displays and video-recording capabilities resident in an eyeglass frame based on gyro and acceleration sensors as well as advances in proximity and ambient light sensors in HMDs.

7.10.3 Actors

Table 23 shows the actors participating in the Smart Glasses Use Case.

Table 23 – Actors for Smart Glasses

Actor Name	Actor Type	Actor Description	Used Technology
Smart glasses	Wearable Device		
Camera	Device		
Display	Device		
User interface		Supports voice, touch and gesture commands	
Enterprise network	Network	Enterprise network allowing access to product data and assembly instructions	
Cloud service	Service	Product data and work instructions repository	

7.10.4 Issues: Legal Contracts, Legal Regulations, Constraints

None provided.

7.10.5 Referenced Standards and/or Standardization Committees

Table 24 shows referenced standards and/or standardization committees relevant to the Smart Glasses Use Case.

Table 24 – Referenced Standards and/or Standardization Committees for Smart Glasses

Relevant Standardization Committees	Standards to be considered in the Use Case	Standard Status
JTC 1/SC 29	ISO/IEC 23005: Media Context and Control (MPEG-V) Parts 1 – 7 ISO/IEC 15938: Multimedia Content Description Interface (MPEG-7) Parts 1-10 Exploration on Internet of Media Things and Wearables (IoMTW)	

7.10.6 Relation with Other Known Use Cases

Table 25 shows relationships with other known use cases for the Smart Glasses Use Case.

Table 25 – Relation with Other Known Use Cases for Smart Glasses

Known use case	Source	UC Status
Use case of QR code recognition with hand held device or smart glasses	JTC 1/SC 29/WG 11	
Augmented museum visit with smart glasses providing additional information to user	JTC 1/SC 29/WG 11	

7.10.7 General Remarks

None provided.

7.10.8 Security and Privacy

Product data is sensitive information and needs to be secure and therefore access to important information needs to be controlled. Additionally some applications for Smart Glasses may involve Health and Safety aspects and are therefore critical systems.

It is potentially feasible that a system interacting with smart glasses collects data on the person wearing the glasses. Suitable assurance is needed to ensure that no PII is collected. In instances where PII is collected, all services must be in compliance with applicable privacy regulations.

7.10.9 Conformity Aspects and Critical requirements

None provided.

7.10.10 Interaction between Actors and User Requirements

None provided.

7.10.11 Diagram of Use Case

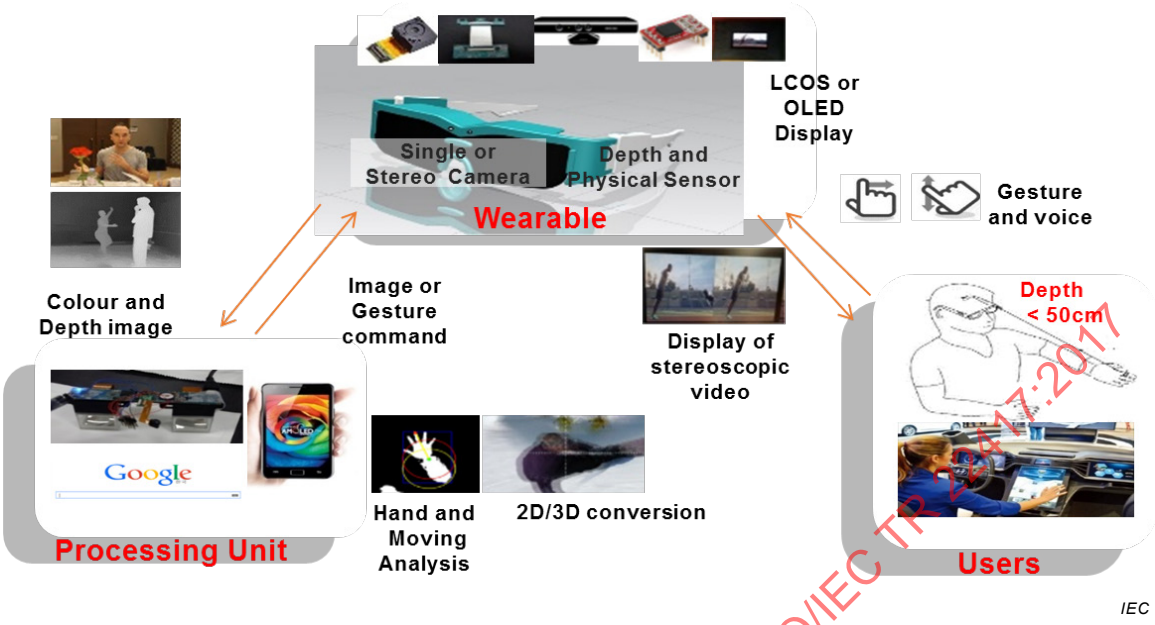
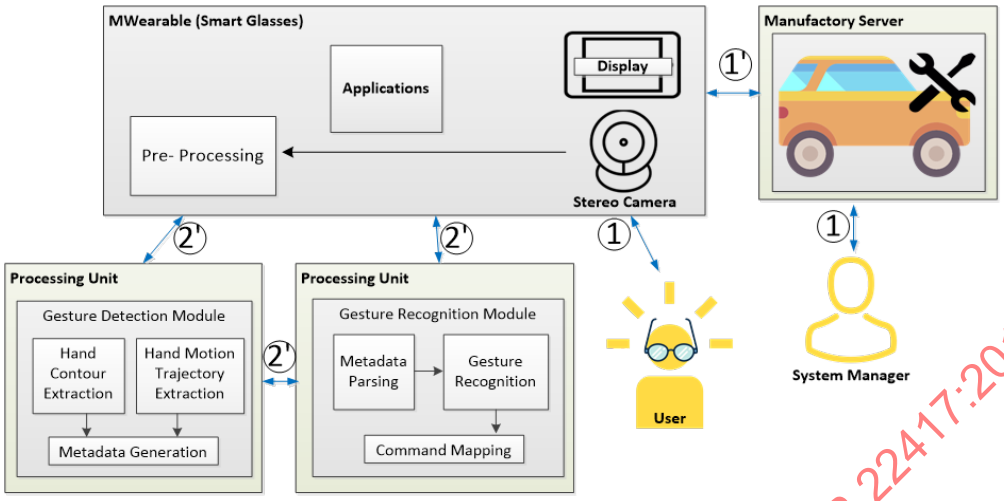


Figure 19 – Smart Glasses

7.10.12 Data Flow Diagram of Use Case



From/To	User	End User	Camera	Gesture Detection Module	Gesture Recognition Module	Factory Server	Display
User			Setup Info ①			-Setup Info -Approve the authority ①	
EndUser			-Setup Info -Gesture -Image sequence -Barcode ②			-Approve the authority 1'	
Camera				-Gesture sequences 2'			
Gesture Detection Module					-Encoded Metadata 2'		
Gesture Recognition Module							Command 2'
Factory Server							Information of the maintenance manual 1'

IEC

Figure 20 – Data Flow of Smart Glasses

7.11 IoT Endpoint (Sensors and Actuators) Monitoring Systems (Use case number 11 in Table 1)

7.11.1 Scope and Objectives of Use Case

IoT endpoints (sensors and actuators) of various types and capabilities are distributed where IoT systems are deployed. Many of these endpoints each serve a single purpose and are in remote locations. These IoT endpoints can be fragile and are often low power but they provide critical functions through the data they gather and transmit or services they provide in the IoT system. IoT endpoints are sometimes unable to report their own state (power/battery life, on/off, failure to wake up, performance profile or security profile). This use case describes the introduction of a capability in the network, local or remote whose sole purpose is to monitor or gather state information of sensors or endpoints on a network segment and transmit this information to a central location to enable management, prevention of failures or malfunctioning of critical IoT endpoints, as well as life cycle management of IoT endpoints.

7.11.2 Narrative of Use Case

7.11.2.1 Short Description

With billions of IoT endpoints and sensors going live, it will become extremely complicated to monitor and manage the health of an endpoint sensor, especially if it is constrained, remote and critical to other systems. Today, most sensor malfunctions and failures are detected only

after they occur in a reactive manner. For critical infrastructure and IoT systems that impact human lives this would no longer be viable.

7.11.2.2 Complete description

Availability of constrained endpoints is a security requirement that is important to critical IoT systems and solutions. IoT endpoints vary widely in capability and they typically work in concert with a wider network of IoT endpoints and infrastructure that can be placed locally or remotely. These remote placements can sometimes be inhospitable or inaccessible. Status monitoring, life-cycle management, upgrades and patch management status can be difficult. Some embedded systems in sensors are designed to last for up to 10 or more years and keeping track of their upgrade status, software patches or battery life status and being aware if they fail, become defective or are compromised can be challenging. Manually managing thousands of endpoints in the field can be cumbersome and in some cases impossible, but IoT sensor monitoring systems can help alleviate this. Placing a security function in sensor networks whose sole purpose is to monitor sensors within its reach and transmit data continuously, intermittently or periodically subject to the requirement of the IoT solution can help significantly with endpoint lifecycle management. It can help prevent critical safety and security failures, which would otherwise be detected only after the fact and allows for pro-active remediation, repairs, replacement or decommissioning of endpoints.

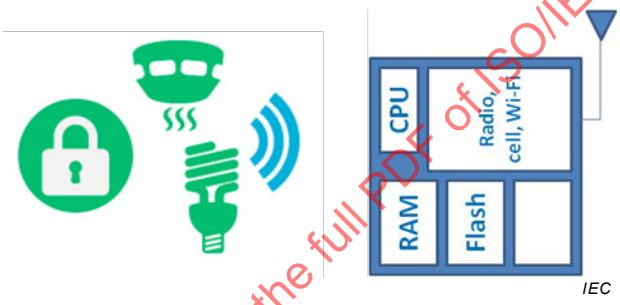


Figure 21 – Basic Endpoint/sensor components

7.11.3 Actors

Table 26 shows the actors participating in the IoT Endpoint Monitoring Systems Use Case.

Table 26 – Actors for IoT Endpoint Monitoring Systems

Actor Name	Actor Type	Actor Description	Used Technology
IoT endpoints (sensors, actuators, etc.)		IoT endpoints work in concert with one another and other infrastructure.	
Endpoint monitoring sensor	Device	Special purpose endpoint can be configured to monitor required parameters such as battery life, patch status, security, failure state, etc.	
Gateway	Device	Device interconnecting local IoT endpoints to wider communication channels	
Telecom Network	Network	Interconnects IoT infrastructure	
Control system	System	Cloud service monitoring platform or central monitoring server	
Cloud service	Service	Option for monitoring system	

7.11.4 Issues: Legal Contracts, Legal Regulations, Constraints

None provided.

7.11.5 Referenced Standards and/or Standardization Committees

Table 27 shows referenced standards and/or standardization committees relevant to IoT Endpoint Monitoring Systems Use Case.

Table 27 – Referenced Standards and/or Standardization Committees for IoT Endpoint Monitoring Systems

Relevant Standardization Committees	Standards that have to be considered in the Use Case	Standard Status
	Dependency: IoT sensor monitoring systems could successfully functions where interoperability standards are in place and work effectively between the monitoring endpoints and the target sensors in scope	

7.11.6 Relation with Other Known Use Cases

None provided.

7.11.7 General Remarks

The health of critical IoT systems will become progressively more important. As society moves towards reliance on IoT systems for automation and critical functions, be it in factories, smart cities, remote field sites or in medical devices then the availability, reliability and security of such systems becomes crucial. The most vulnerable component of the IoT system is generally the endpoint or sensor, that is often unprotected and low cost; nevertheless the infrastructure relies on the consistency and availability of this endpoint and its unfailing performance. This introduces a need for monitoring systems to ensure the health of the IoT endpoint, sensor or device.

A monitoring sensor or device placed amidst other functional sensors to gather and keep track of sensor status can function by either periodically detecting the presence of the set of sensors on the network, polling the sensors or tapping into the data being sent by the sensors on its designated communication path. The monitoring sensor could be configured with an auto-detect capability or with a pre-programmed set of data points that the monitoring sensor could update. Additionally, maintenance records, in terms of replacement, software version or latest patch upgrade status may also be recorded. In instances where a sensor fails to wake up, respond or ceases to transmit critical data, the monitoring sensor can generate alarms which are sent to central management locations. In instances where average battery life is known and tracked the monitoring endpoint could proactively forecast when various sensors are due for a battery refresh, thus allowing for proactive maintenance preventing segments of sensor networks from becoming unnecessarily unavailable. This type of sensor monitoring or surveillance is a preventative security measure to ensure critical IoT system availability and reliability.

7.11.8 Security and Privacy

IoT systems can be vital and vulnerable but endpoint sensors are frequently only monitored for expected and normal operational indicators. An endpoint failure may be detected only after the failure has occurred and may have a cascading impact on the IoT system that it interacts with. While reactive remediation may be adequate in most cases, in certain cases this would be unacceptable and could impact critical infrastructure or human life quite severely. Examples of critical failures include a chip malfunctioning in an implanted medical device in a

patient, an unresponsive sensor in a self-driving car which can cause havoc in traffic, or malfunctioning pressure and temperature sensors in remote mining, oil and gas sites on which IoT automated systems make decisions can all have serious repercussions.

Monitoring capabilities must be suitably protected so that cybersecurity attacks are not possible through them. Further these capabilities might collect PII data, and in cases where PII is collected all services must be in compliance with applicable privacy requirements.

7.11.9 Conformity aspects and Critical Requirements

None provided.

7.11.10 Interaction between Actors and User Requirements

- Domain
  - IoT system availability, reliability and safety, monitoring and life cycle management, upgrades and patch management status can improve security. Sensor monitoring systems may be proprietary or generic and can be offered by Telcos as a cloud monitoring service.
- Role
  - This monitoring solution is focused on the current state of the endpoints and their functionality. This data is collated locally and sent via traditional networks to either a central server location for monitoring activity or to a service provided via a Telco cloud monitoring service. The solution may also invoke automated or manual remediation and alerts, for instance by communicating with security elements.
- Scenario
  - With billions of IoT endpoints and sensors going live, it will get extremely complicated to monitor and manage the health of an endpoint sensor, especially if it is constrained, remote and critical to other systems. Currently, most sensor malfunctions and failures are detected only in a reactive manner after the fact. For critical infrastructure and IoT systems that impact human lives this would no longer be viable.

7.11.11 Diagram of Use Case

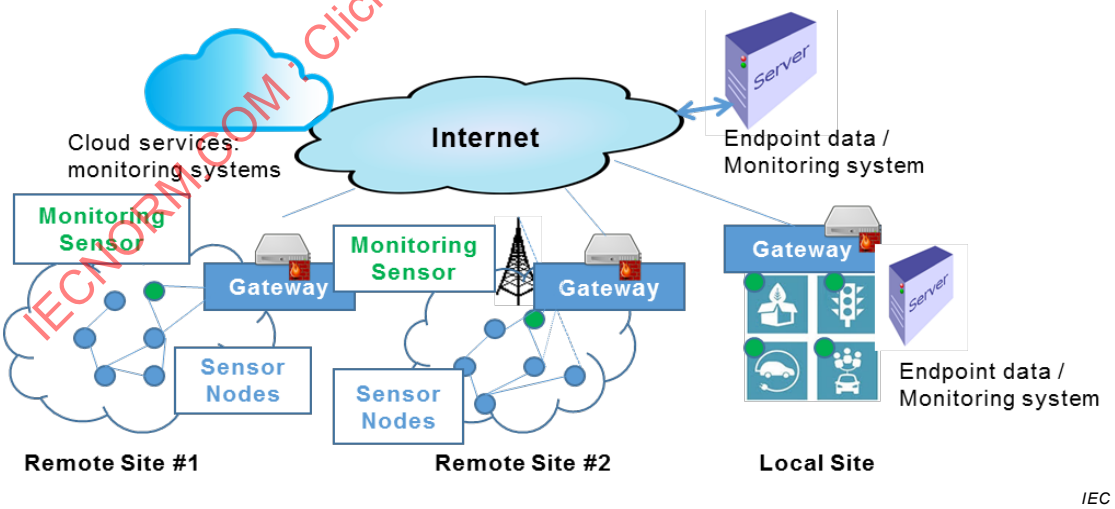


Figure 22 – IoT Endpoint Monitoring Systems

7.11.12 Data Flow Diagram of Use Case

See use case description above.

7.12 Intelligent Assistive Parking in Urban Areas (Use case number 12 in Table 1)

7.12.1 Scope and Objectives of Use Case

This use case presents a scalable solution for intelligent assistive parking in urban areas in order to reduce or redirect unnecessary traffic, avoid traffic congestion and reduce emissions in populated areas. It can reduce traffic-related injuries caused by a lack of attention when looking for vacant parking spaces on the roadside and save drivers' time.

Many car owners and citizens possess something that is of great value to others; areas that can be used as parking space. They do not use this space during normal workdays, as they are using their car to drive to their workplace, resort, etc. These privately owned vacant spots could help solve many of the challenges associated with lack of free parking spaces in urban areas.

User groups which may benefit from this solution:

- private owners of parking spaces or similar vacant areas wishing to profit from renting out available parking spaces;
- drivers in search of a parking space who will have access to a larger resource pool;
- car park owners, markets and event managers who will be able to offer this solution as an extra service to their customers, in addition to identifying nearby spaces that are still vacant.

City officials may benefit from smart city tools as they can get a real time view of occupancy of available parking spaces, and reduced traffic and pollution in urban areas. This may, additionally, provide access to statistical information about parking.

7.12.2 Narrative of Use Case

7.12.2.1 Short Description

John is 60 years old and late for his meeting. He lives in rural area of City A and needs his car to travel to his customers in City B. He has invested in the new SmartParking app to be able to park as close as possible to his customers. Parking spaces are normally full after 10 a.m., but this app guides him to the closest private parking space, which is free when Bill, the home owner, is away for work. Home owners benefit from a reimbursement of costs for sharing their parking spaces.

7.12.2.2 Complete Description

This use case demonstrates the integration of transport information between different systems to achieve increased usage of the infrastructure and parking spaces. Intelligent parking for residents with particular needs is especially helpful for health buildings and clusters of housing estates tailored for user groups such as cancer patients and people with various physical disabilities, including wheelchair dependency.

In order to address the needs of the individual residents, management of parking spaces and their proximity to access points can be tailored to user-defined profiles. Safety, predictability, reliability, accessibility are elements that can be incorporated when implementing load balancing and resource administration of parking spaces and available areas. Access control and appraisal systems are functions that need to be supported. This will be affected by what kind of user wants to use the parking space. Visitors should be kept separate from residents, but the needs of the user and preferred actions will have an impact on the recommended parking space. Moreover, healthcare and blue-light agencies ought to receive priority.

In the demonstrated solution, prioritized parking spaces, parking space booking, traffic analysis, customized and messaging services based on biometric data will be adjusted according to pre-determined rules. Home control centres can operate both locally and by interacting with external services and communication units. The sensors report proximity and

temperature, and this information is provided to the health facility and made available to the virtual neighborhood. Such mobile apps can report the status of the parking space and the health home. Both booking and configuration of units in the virtual neighborhood will be available through the mobile app.

Three potential outcomes of this use case are:

- traffic reduction through an increase in available parking spaces throughout the day, this may affect infrastructure around public and private buildings, districts and smart cities;
- monitoring traffic in certain areas of a smart city which may lead to vehicle access restrictions and may also be implemented for testing and measurement purposes;
- provision for unusual events, i.e. accidents, concerts, festivals, that may temporarily require extra parking spaces, and this could impact blue light agencies and other municipal vehicles.

In order to achieve successful results, appropriate business models can provide owners of relevant parking space with incentives to make them available:

- Private sharing and renting of parking spaces, with some restrictions or caveats being applied, may promote a sharing economy.
- Contracts between users and municipalities or other organizations would permit them to offer available outdoor and indoor parking space for a pre-determined fee.
- Extra incentives for companies and agencies that actively support employees and stakeholders in contributing to green efforts.

It is important to offer professional and user friendly applications to facilitate successful adoption of the parking space sharing software, making everything as simple and transparent as possible when it comes to access control (authorization and authentication), booking and billing, administration with data mining, balancing traffic/routes and offering real-time data. The data would also be part of Smart City KPIs for climate, environment, traffic, noise and other social issues related to traffic and lack of environmental qualities.

7.12.3 Actors

Table 28 shows the actors participating in the Intelligent Assistive Parking Use Case.

Table 28 – Actors for Intelligent Assistive Parking

Actor Name	Actor Type	Actor Description	Used Technology
Vehicle user	User	Person that needs a parking space close to their destination.	
Vehicle	Real-time positioning device	Moving vehicle tracking in a street network to locate available parking spaces in the vicinity.	
Smartphone	Mobile device	Device used to set up the system and map to the parking space.	
Parking space stakeholder	User	Property owner having one or more parking spaces available at certain times during the week.	
Blue light agencies	Public	Certain agencies that must have access to parking spaces when on emergency calls.	
Space management sensors	Technology	A network of sensors collaborating to establish whether a space is free or in use.	
Space alarm system	System	Traditional alarm system which makes a loud noise when an illegal entity tries to occupy an empty space without booking.	
Cloud service	Service	Runs the cloud service application that manages parking monitoring system set up and operation.	
Smart Parking	Mobile app	Connects the driver with the owner and offers option to book, report and administrate the parking spaces.	
Smart city	Management system	System allowing municipality to exploit available resources in order to reduce traffic congestion and pollution thereby improving living conditions and policing regulations.	
Administration tool	Software	The system that offers information and administration of available parking spaces.	

7.12.4 Issues: Legal Contracts, Legal Regulations, Constraints

Table 29 identifies issues for Intelligent Assistive Parking Use Case.

Table 29 – Issues for Intelligent Assistive Parking

Issue – *here specific ones*	**Impact of Issue on Use Case**	**Reference –** *law, standard, others*
Involving human participants and cover real use scenarios related to health monitoring, home management, governance, energy consumption and other various human activity and behaviour analysis –related data gathering purposes. For some of the activities to be carried out by the project, it may be necessary to gather basic personal data (e.g. name, background, contact details, interest, IoT units and assigned actions), even though the project will avoid collecting such data unless data is necessary for the application.	NDA and privacy contract needs to be made available to participants. All personal data collection efforts of the project partners will be established after giving subjects full details on the experiments to be conducted, and obtaining from them a signed informed consent form. Certain guidelines will be implemented in order to limit the risk of data leaks: – keep anonymized data and personal data of respondents separate; – encrypt data if it is deemed necessary by the local researchers; – store data in at least two separate locations to avoid loss of data; – limit the use of USB flash drives; – save digital files in one the preferred formats (see Annex 1); and – label files in a systematically structured way in order to ensure the coherence of the final dataset	EU's Data Protection Directive 95/46/EC "on the protection of individuals with regard to the processing of personal data and on the free movement of such data" and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

7.12.5 Referenced Standards and/or Standardization Committees

Table 30 shows referenced standards and/or standardization committees relevant to the Intelligent Assistive Parking Use Case.

Table 30 – Referenced Standards and/or Standardization Committees for Intelligent Assistive Parking

Relevant Standardization Committees	**Standards that have to be considered in the Use Case**	**Standard Status**
ISO/TC 204 ITS – All parking space elements will be stored and presented in a format that adheres to ISO/TS 21219-14: "Intelligent transport systems – Traffic and travel information via transport protocol experts group, generation 2 (TPEG2) – Part 14: Parking information application (TPEG2-PKI)"	Cloud service and web standards: IETF protocols, JavaScript, URLs, REST, JSON, OAuth	ISO standard
JTC 1/SC 27	ISO/IEC 29151: Code of practice for personally identifiable information protection.	ISO/IEC standard

7.12.6 Relation with Other Known Use Cases

None provided.

7.12.7 General Remarks

IoT devices involved:

- Multi-sensorial network for monitoring and control of parking space DAMs: Energy consumption/emission reduction, Operational status (e.g. vacancy/booking, visual feedback, permissions, etc.), Location aware parking suggestion, User actions (booking, matching, transaction).
- Multi-sensorial network for vacancy detection: Motion Detection, proximity, IR sensors, location detection, Bluetooth, RFID, NFC, etc. – for individual tracking/permissions.
- Infrastructure and traffic load monitoring: Low-cost, fault tolerance, sturdy, intelligent packaging, mesh technology, Open data describing predicted/booked events, curvature, route planning.
- Weather conditions and forecasting, pollution and other kinds of information retrieved from open data source.
- Integration of security, safety and alarm systems in IoT implementation.

In addition, other devices that can contribute to authenticating the vehicle may be integrated in the setup:

- camera for reading license plates of vehicles to confirm authorization;
- fingerprint reader for temporary biometric access;
- printer and reader for temporary access cards.

7.12.8 Security and Privacy

A preliminary impact assessment must have been carried out by the organization that deployed the application, in order to ensure that privacy regulations are met. In instances where PII is collected, all services must be in compliance with applicable privacy regulations.

The user must be in control of with whom the information is shared, i.e. only uploading to an authorized parking space provider that is approved by the user.The user or vehicle ought to be authorized to access a certain parking space provider, i.e. protection against fake devices and malicious users.

Confidentiality of information needs to be assured. No unauthorized entity should be able to gain access to the data. Integrity of information also needs to be ensured. Thus modification of the data being sent should not be possible.

7.12.9 Conformity Aspects and Critical Requirements

The system should be reliable in all aspects, for example:

- The cloud service application should be able to detect failures, for example if contact is lost with the parking space sensors.
- The smartphone app should be able to detect when battery level is below a certain threshold value and then send an alarm message to the cloud service application.

7.12.10 Interaction between Actors and User Requirements

Proposal for a sequence description containing the following parts for a system set-up:

- Description/Overview
  - The assumption is that parking sensors lack a visual user interface (UI) or have a very limited user interface. During the operation of the system no UI is needed but another device, with a UI, must be used for the system set up and authorization process through the device's web browser or a through a native application running in the device.
- Pre-conditions
  - Parking sensors connected to cloud services.

  - Device with UI, e.g. a laptop or a smartphone connected to cloud services.
  - Control system connected to device with UI through some kind of local connectivity method, e.g. Bluetooth or USB.
- Flow
  - User (or person assisting user) logs into parking space management web site. If the user has an existing account, e.g. web-based service providers or social platforms, this could be used for the log in process.
  - User starts set-up process by pressing a button at the smartphone.
  - User approves that the control system is used with the remote parking space application.
- Post-condition
  - Parking sensor is actively monitoring which vehicle is using the space and the system prepares billing when booked time is exceeded and informs the car owner of this and whether additional fees apply.

7.12.11 Diagram of Use Case

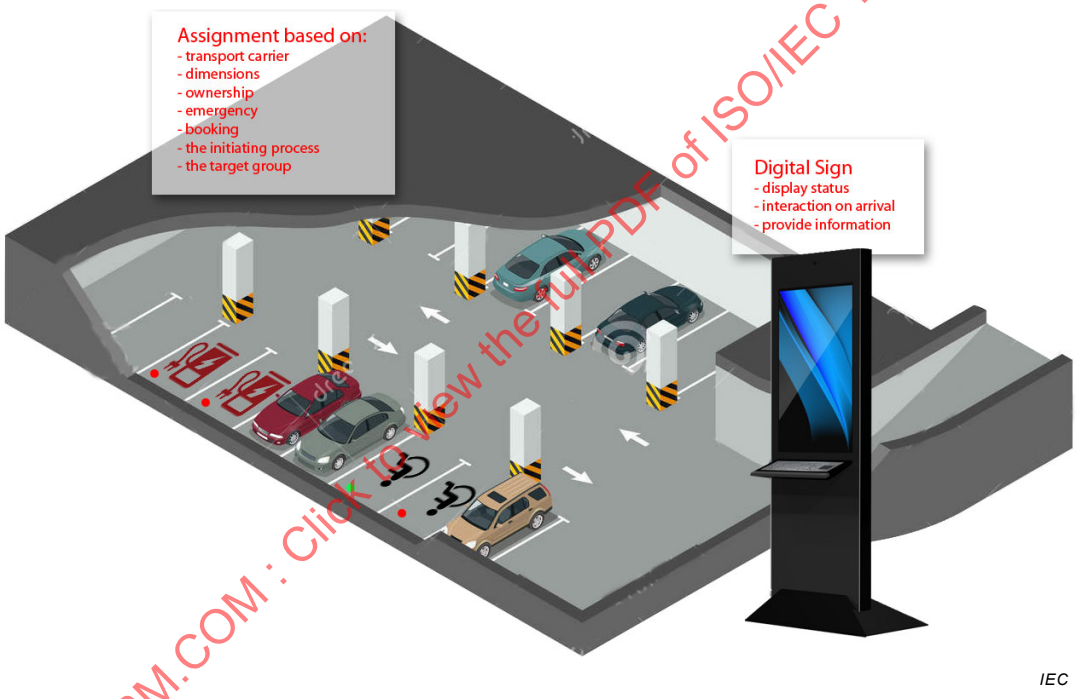


Figure 23 – Car Park Scenario

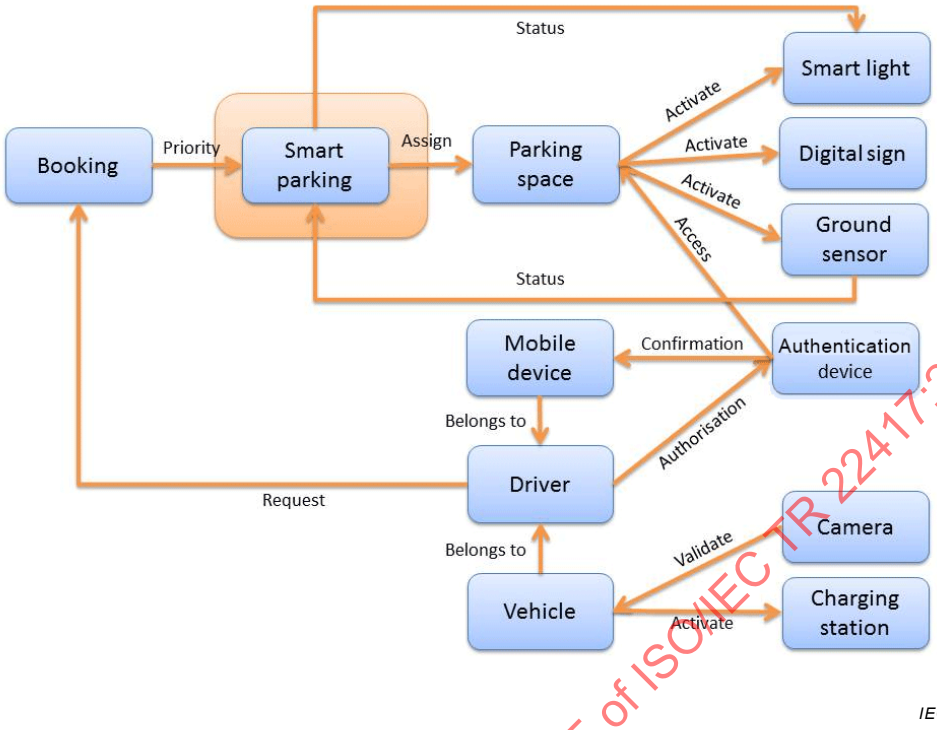


Figure 24 – Interactions in Smart Parking Scenario

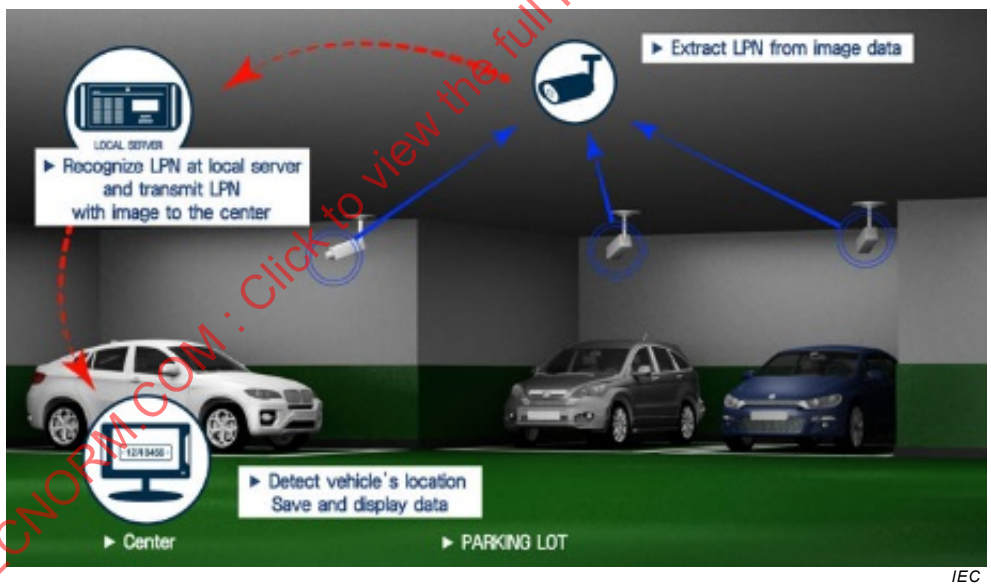


Figure 25 – Camera based detection of occupancy

IEC

Figure 26 – Camera based identification of traffic load at key points in the infrastructure

IEC

Figure 27 – Smart parking is an integrated part of smart cities

In iParking, a network of sensors and traffic data from different sources (Traffic Control Centrals, camera monitoring the traffic, open traffic data from web-based service providers and satellite navigation systems, etc.) establish a picture of the current traffic situation.

IEC

Figure 28 – Ground-based sensor detecting proximity, temperature and humidity

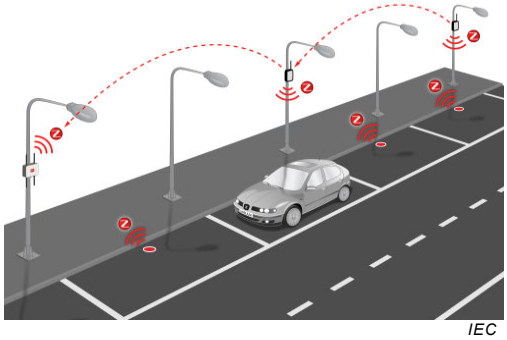


Figure 29 – Sensor communicates through mesh-technology with repeaters mounted on roadside installation

The Smart City supplies real time information about the availability and position of vacant spaces. Expert systems assist in balancing the parking requirements and offering prioritized parking space tailored to specific user groups based on identification, restrictions, and needs.

7.12.12 Data Flow Diagram of Use Case

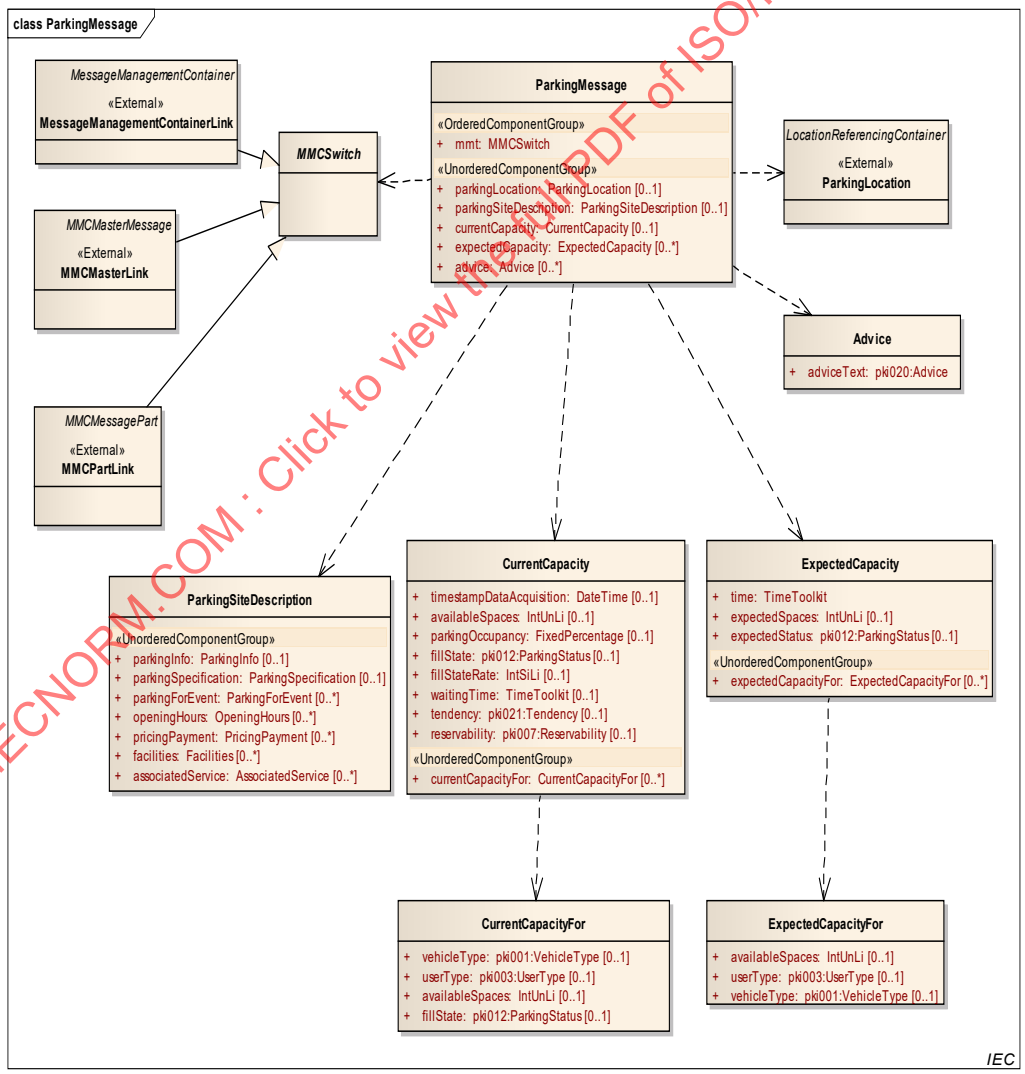


Figure 30 – Data Flow of Smart Parking

7.13 Integrated Smart Pump System (Use case number 13 in Table 1)

7.13.1 Scope and Objectives

The use case describes the interoperability of smart pump applications using IoT technology. It provides a demonstration of information exchange over IoT systems allowing interoperability between applications and maintaining the overall asset health in the manufacturing process.

7.13.2 Narrative of Use Case

7.13.2.1 Short Description

This use case describes the interoperability of manufacturing applications resulting in an integrated smart pump system using IoT technology.

7.13.2.2 Complete Description

7.13.2.2.1 General

There is growing interest in the early detection of degradation or malfunction, which can help predict machinery failure. Diagnostics techniques can be effectively coupled with control techniques in the context of a smart motor-pump-control system. An integrated smart system for pumping applications can sense the operating condition and health of a hydraulic system and automatically change the control of the motor-pump components utilizing IoT technology. The operation of a smart system in an integrated, coordinated manner can achieve important capabilities for protecting critical processes, process equipment, operations personnel, and the environment.

7.13.2.2.2 Step by Step Analysis of Use Case – Overview of Scenarios

Table 31 shows various scenario conditions for the Integrated Smart Pump System Use Case.

Table 31 – Scenario conditions for Integrated Smart Pump System

Scenario conditions						
No.	**Scenario name**	**Scenario description**	**Primary actor**	**Triggering event**	**Pre-condition**	**Post-condition**
1	Data Acquisition	Sensor data acquisition running on PLC1	Data Acquisition	Pump system running	Data Acquisition application is running	Sensor readings (flow, pressures, temperature)
2	Speed/PID Control	Pump Speed/PID control running on PLC1	Pump Control	Input from User Domain (desired flow or pressure)	Current sensor readings	Regulated flow
3	Diagnostics	Pump diagnostics running on PLC2	Pump Diagnostics	Sensor readings acquired by Data Acquisition	Current sensor readings	Cavitation status, Pump Health Indicator
4	Control Adjustment	Adjust the pump operation per diagnostics	Pump Control	Pump diagnostics performed by Pump Diagnostics	Cavitation Condition	Pump running in cavitation avoidance mode

7.13.2.2.3 Step by Step Analysis of Use Case – Scenarios

Table 32 shows a detailed analysis of scenarios for the Integrated Smart Pump System Use Case.

Table 32 – Scenarios for Integrated Smart Pump System

Scenario								
Scenario name:		**No. 1 – Data Acquisition**						
Step No.	**Event**	**Name of process/ activity**	**Description of process/ activity**	**Service**	**Information producer (actor)**	**Information receiver (actor)**	**Information exchanged (IDs)**	**Requirement, R-IDs**
1	Pump System running	Data Acquisition	Sensor data acquisition	Sensor data acquisition	Data Acquisition	Pump Control	1	
Scenario name:		**No. 2 – Speed/PID Control**						
Step No.	**Event**	**Name of process/ activity**	**Description of process/ activity**	**Service**	**Information producer (actor)**	**Information receiver (actor)**	**Information exchanged (IDs)**	**Requirement, R-IDs**
1	User input	PID	PID loop	Closed loop feed-back control	Pump Control	Pump Diagnostics	2	
Scenario name:		**No. 3 – Diagnostics**						
Step No.	**Event**	**Name of process/ activity**	**Description of process/ activity**	**Service**	**Information producer (actor)**	**Information receiver (actor)**	**Information exchanged (IDs)**	**Require-ment, R-IDs**
1	Sensor Data Acquisition	Pump diagnostics	Perform pump diagnostics using pump curves and sensor data to avoid pump cavitation. Calculate pump health.	Pump cavitation calculation Pump health estimation	Pump Diagnostics	Pump Control	3	
Scenario name:		**No. 4 – Control Adjustment**						
Step No.	**Event**	**Name of process/ activity**	**Description of process/ activity**	**Service**	**Information producer (actor)**	**Information receiver (actor)**	**Information exchanged (IDs)**	**Requirement, R-IDs**
1	Diagnostics calculation	Adjust pump speed	Adjust pump speed to avoid pump system health degradation (avoid pump cavitation)	Modifying the control to avoid cavitation condition	Pump Control	Pump Diagnostics	4	

7.13.2.2.4 Step by Step Analysis of Use Case – Information Exchanged

Table 33 shows types of information exchanged in the Integrated Smart Pump System Use Case.

Table 33 – Information exchanged for Integrated Smart Pump System

Information exchanged			
Information exchanged, ID	**Name of information**	**Description of information exchanged**	**Requirement, R-IDs**
1	Sensor data	Flow, Pressures, Temperature	
2	Sensor data	Flow, Pressures, Temperature	
3	Pump Speed Pump Health	Recommended speed to avoid pump system health degradation (avoid cavitation)	
4	Sensor data	Flow, Pressures, Temperature data due to a different pump operating point	

7.13.3 Actors

Table 34 shows the actors participating in the Integrated Smart Pump System Use Case.

Table 34 – Actors for Integrated Smart Pump System

Actor name	Actor type	Actor description	Further information specific to this use case
Data Acquisition	Application	Sensor data acquisition (part of PID control application)	
Pump Control	Application	PID control application running on Programmable Logic Controller	Conforming to IEC 61131-3
Pump Diagnostics	Application	Pump diagnostics application running on Programmable Logic Controller	Conforming to IEC 61131-3

7.13.4 Issues: Legal Contracts, Legal Regulations, Constraints

None provided.

7.13.5 Referenced Standards and/or Standardization Committees

Table 35 shows referenced standards and/or standardization committees relevant to the Integrated Smart Pump System Use Case.

Table 35 – Referenced Standards and/or Standardization Committees for Integrated Smart Pump System

Relevant Standardization Committees	Standards have to be considered in the Use Case	Standard Status
ISO/TC 184		
IEC TC 65/SC 65B	IEC 61131-3 EC 61131-3:2013 specifies the syntax and semantics of a unified suite of programming languages for programmable controllers (PCs). This suite consists of two textual languages, Instruction List (IL) and Structured Text (ST), and two graphical languages, Ladder Diagram (LD) and Function Block Diagram (FBD)	

7.13.6 Relation with Other Use Cases

7.13.6.1 Key Performance Indicators (KPI)

Table 36 shows KPIs for the Integrated Smart Pump System Use Case.

Table 36 – KPI for Integrated Smart Pump System

Key performance indicators			
ID	Name	Description	Reference to mentioned use case objectives
	Pump Health	Pump Health Indicator	3

7.13.6.2 Use Case Conditions

Table 37 shows use case conditions for the Integrated Smart Pump System Use Case.

Table 37 – Use case conditions for Integrated Smart Pump System

Use case conditions
Assumptions
Pump system is pumping low viscosity fluid (not solid or sludge)
Pre-requisites
Flow, pressure and temperature sensors are measuring the flow, suction and discharge pressure, and fluid temperature
Pump speed is controlled by the motor and the variable frequency drive

7.13.7 General remarks

Integrating diagnostics and control provides many unique and important capabilities. Significant development has occurred which enhances the ability to continuously monitor industrial machinery during operation and establish the health of a machine. The integration

of diagnostics and control effectively leverages off these developments and enables new opportunities for intelligent control. An integrated, intelligent control provides a method to identify desirable and undesirable machinery states and then to control the system to avoid such problematic states. Examples of undesirable operating states to be avoided include excessive vibration such as occurs with resonant frequencies and pump cavitation. In addition to avoiding these undesirable operating states or delaying the time for a failure to occur, further enhancement of the control specification with other process and business information may be attained. IoT is a fundamental enabler for industrial integration.

7.13.8 Security and Privacy

None provided.

7.13.9 Conformity Aspects and Critical Requirements

None provided.

7.13.10 Interaction between Actors and User Requirements

Table 38 shows common terms and definitions applied to the Integrated Smart Pump System Use Case.

Table 38 – Common terms and definitions for Integrated Smart Pump System

Common terms and definitions	
Term	**Definition**
Programmable Logic Controller (PLC)	digital computer used for automation of typically industrial electromechanical processes, such as control of machinery on factory assembly lines. PLCs are used in many machines, in many different industries.
Pump curve	data about a given pump's ability to produce flow against certain head
Pump cavitation	formation of vapour cavities in a liquid that are the consequence of forces acting upon the liquid. It usually occurs when a liquid is subjected to rapid changes of pressure that cause the formation of cavities where the pressure is relatively low. When subjected to higher pressure, the voids implode and can generate an intense shock wave. Cavitation is a significant cause of wear in pumping system
Variable Frequency Drive (VFD)	type of motor controller that drives an electric motor by varying the frequency and voltage supplied to the electric motor. Other names for a VFD are variable speed drive, adjustable speed drive, adjustable frequency drive, AC drive, and inverter

7.13.11 Diagram of Use Case

See Figure 33 for reference.

7.13.12 Data Flow Diagram of Use Case

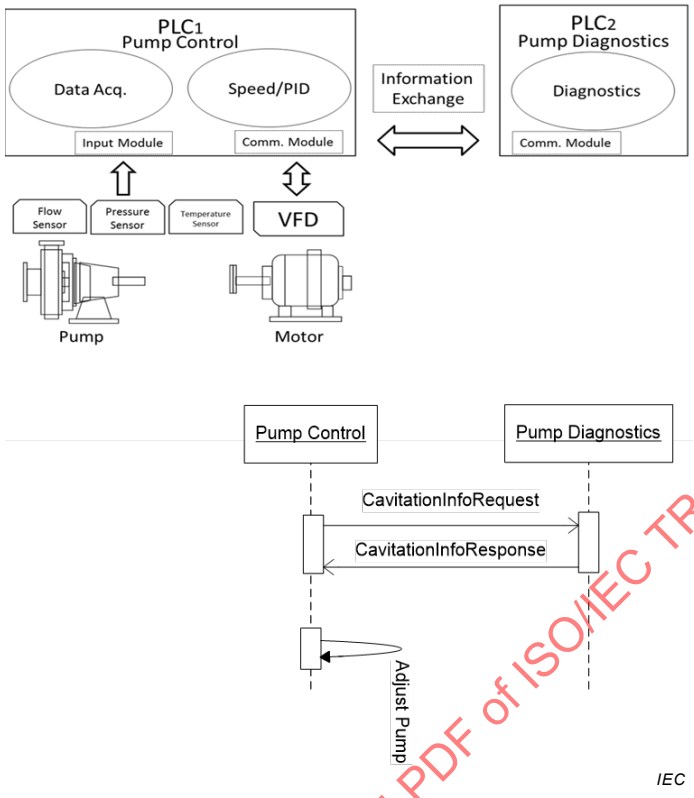


Figure 31 – Data Flow of Integrated Smart Pump System

7.14 Remote Health Monitoring: Example of an AAL Use Case Relevant to IoT (Use case number 14 in Table 1)

7.14.1 Scope and Objectives of Use Case

This use case supports active ageing by demonstrating how wearable devices and a house alarm system can provide health monitoring and an alert system. Such services enable patients to live independently for longer provided that reliable and secure communication networks are available to link the patient with the alarm monitoring service and the healthcare monitoring service.

7.14.2 Narrative of Use Case

7.14.2.1 Short Description

A patient who lives alone and has medical conditions which need to be regularly monitored has a wearable device to measure certain vital signs. The wearable device provides the collected information to a health information system which provides the healthcare service which can react to detected anomalies. Additionally, the patient has access to a home alarm system which has emergency pull cords and a wearable alert device, often worn as a necklace.

7.14.2.2 Complete Description

None provided.

7.14.3 Actors

Table 39 shows the actors participating in the Remote Health Monitoring Use Case.

Table 39 – Actors for Remote Health Monitoring

Actor Name	Actor Type	Actor Description	Used Technology
Patient	User	Individual that needs a remote health monitoring system	
Wristband	Device	Monitors falls, heart rate, irregular heart rhythms, blood glucose, etc. Issues health status and alarms to healthcare service	
Smartphone	Device	Device used to set up the system as the Wristband has no UI or a very limited UI	
Healthcare Provider	Management	Manages the Cloud service with the healthcare information system	
Home alarm system	IoT endpoint	Traditional alarm system with which elderly or handicapped people are able to call for assistance. For example, the user wears a necklace with a button that the user presses when assistance is needed	
Cloud service	Service	Runs the healthcare application that manages the remote monitoring system set up and operation	

7.14.4 Issues: Legal Contracts, Legal Regulations, Constraints

This use case may be affected by national medical regulations. For example, in some countries the transmission of medical information must comply with the HIPAA (Health Insurance Portability and Accountability Act) privacy / security rule.

7.14.5 Referenced Standards and/or Standardization Committees

Table 40 shows referenced standards and/or standardization committees relevant to the Remote Health Monitoring Use Case.

Table 40 – Referenced Standards and/or Standardization Committees for Remote Health Monitoring

Relevant Standardization Committees	Standards have to be considered in the Use Case	Standard Status
	Cloud and web standards: IETF protocols, JavaScript, URLs, REST, JSON, OAuth	
IEC SyC-AAL	Terminology and Reference architecture	

7.14.6 Relation with Other Known Use Cases

Table 41 shows relationships with other known use cases for the Remote Health Monitoring Use Case.

Table 41 – Relation with Other Known Use Cases for Remote Health Monitoring

Known use case	Source	UC Status
Gateway Security for AAL	JTC 1/SC 27	

7.14.7 General Remarks

When the system is in operation everything works automatically without a specific user interface. The remote monitoring application is a cloud service and can communicate with the wristband. A local router, situated for example in a smartphone, may be needed to translate between a local communication method such as Bluetooth Low Energy and the mobile network or Wi-Fi, but at the application level end-to-end security and communication through firewalls can be achieved. The communication needs to be reliable and the power consumption in the wristband low to achieve long battery life. User interaction is only required during system installation. The user, or another trusted person, e.g. a relative, health care personnel or personal assistant, has to use a web browser, on another device, to log in to the remote monitoring application and the user has to approve that the application is given access to their wristband.

7.14.8 Security and Privacy

- A preliminary impact assessment must have been carried out by the organization that deployed the application, in order to ensure that privacy regulations are met. Example privacy protection rules can be found in the HIPAA Privacy Rule.
- The user should be in control of with whom information is shared, i.e. only allowing uploading of data to an authorized health care provider that is approved by the user.
- The device or user needs to be authorized to access a certain health care provider, i.e. protection against fake devices and malicious users.
- Confidentiality of information needs to be assured. No un-authorized entity should be able to get access to the data. This is typically solved by encrypted transport.
- Integrity of information needs to be assured. This means that it should not be possible to modify the data being sent.
- In instances where PII is collected, all services must be in compliance with applicable privacy regulations.

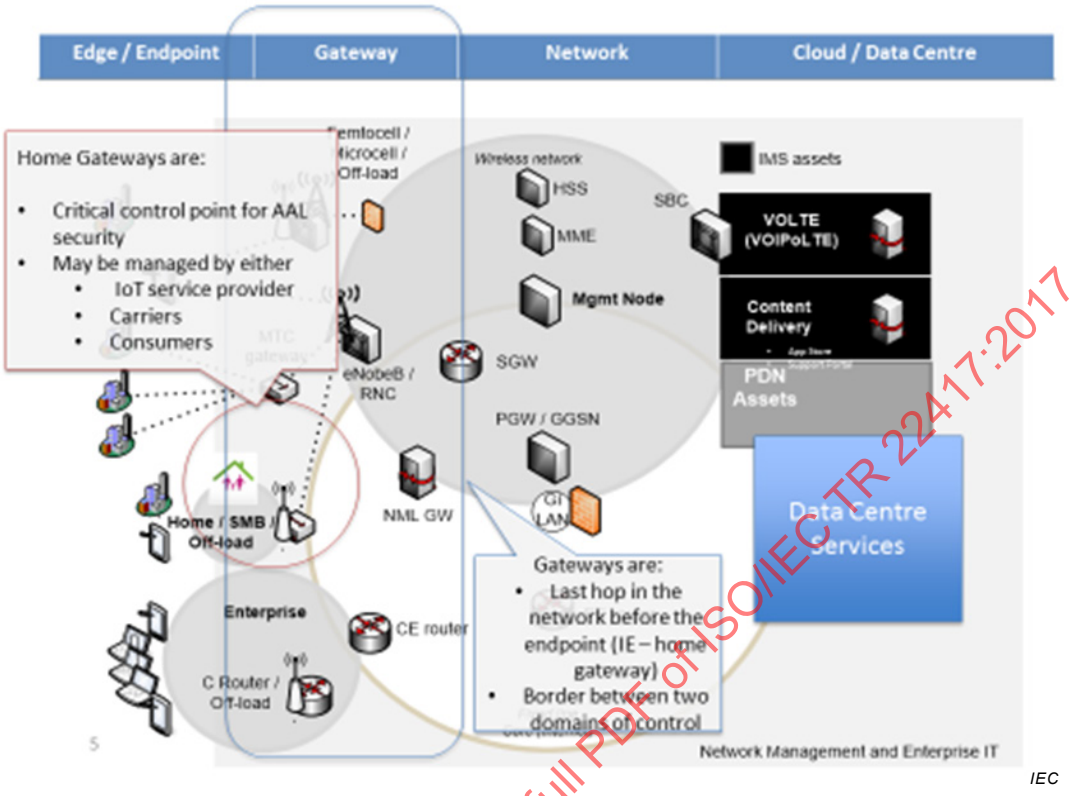


Figure 32 – Gateway Security Architectural Diagram

The Home Gateway is often the first point of reliable security in an IoT system, including AAL and this gateway must often perform security operations on behalf of constrained endpoints such as: Device Identity and Key Management, Session crypto, and In-home IPS (to protect devices from: “on-net” attacks from other local devices; effects of defective local devices)

7.14.9 Conformity Aspects and Critical Requirements

The system must be reliable in all aspects, for example:

- The cloud service application needs to be able to detect if any failure occurs, for example if contact is lost with the wristband of a user.
- The wristband needs to be able to detect when battery level is below a certain threshold value and then send an alarm message to the cloud service application.

7.14.10 Interaction between stakeholders/devices/services/system including user requirements

Proposal for a sequence description containing the following parts for a system set-up:

- Description/Overview
  - The assumption is that wristband lacks a visual user interface or has a very limited user interface. During the operation of the system no user interface is needed but another device, with a user interface, must be used for the system set up and authorization process through the device’s web browser or a through a native application running in the device.
- Pre-conditions
  - Wristband connected to cloud services via a home gateway or other IoT gateway.
  - Device with UI, e.g. a laptop or a smartphone connected to cloud services.

  - Wristband connected to device with UI through some kind of local connectivity method, e.g. Bluetooth or USB.
- Flow
  - User (or person assisting user) logs in to health care provider web site. If the user has an existing account, e.g. Google or Facebook, this could be used for the log in process.
  - User starts set-up process by pressing a button at the wristband.
  - User approves that the wristband is used with the remote health monitoring application.
- Post-condition
  - Wristband is actively monitoring health vital signs of user.

7.14.11 Diagram of Use Case

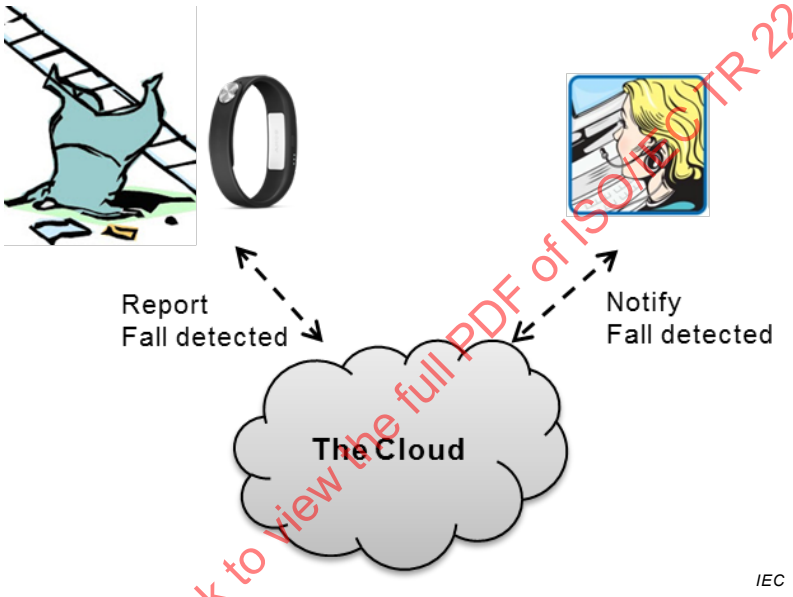


Figure 33 – Fall detection Use Case

7.14.12 Data Flow Diagram of Use Case

See use case description above.

7.15 Connected Car Analytics (Use case number 15 in Table 1)

7.15.1 Scope and Objectives of Use Case

This use case reflects a real-world implementation in a customer project performed by IBM and describes information flows and reference components used to build an IoT framework. This framework allows devices and users to share information with each other and allows individuals to get personalized recommendations based on their interactions with the devices. This promotes user safety and optimal operation of the device.

This use case aims to promote better driver safety and improve driving conditions for car drivers. It also has a second set of objectives to improve driver health and lower healthcare costs.

The context of use involves instrumenting and monitoring both the car that is driven and also instrumenting the driver, combining both sets of information gathered to offer two sets of advice:

- advice to the driver about best routes to follow, driving style to adopt, warnings about road conditions;
- health advice follows from the monitoring of vital statistics, with the aim of detecting health concerns at an early stage and offering lifestyle choices to improve health outcomes.

7.15.2 Narrative of Use Case

7.15.2.1 Short Description

This use case aims to improve driver safety and driving conditions for car drivers, while at the same time improving driver health and lowering healthcare costs.

7.15.2.2 Complete Description

7.15.2.2.1 General

A male driver, 75 years of age, has a heart condition and wears a fitness tracker to monitor vital signs like heart rate. A female driver, 35 years of age, has an active lifestyle, wears an connected watch, and has chosen to share information from her device. Both drivers register for a “Better Driving Behaviour Program”.

The drivers have a profile based on their hometown location, driving records, daily driving route, speed, current weather, and road conditions. Based on these and other features, a known driver profile is created. These relate to a set of KPI that provide a metric on how to measure such features. The driver opts into a better driving behaviour program so we are able to monitor devices the individual has given access to. This information is shared between the drivers, their emergency contacts and their doctor’s office.

When the drivers drive and interact with their devices, the IoT framework picks up all data points. The analytics engine evaluates changes in driving behaviour and any anomalies that must be acted upon or that the system needs to learn as a normal or a new behaviour that needs to be acted upon in the future.

7.15.2.2.2 Steps in the Flow of the Use Case

1) Users register, create a profile in the enterprise user directory, link existing social media accounts, and add a doctor’s network.
2) Users’ record is updated in the enterprise user directory.
3) Users connect their vehicle to a device registry service and to a global network of devices for identification and broadcast message.
4) Users’ record is updated with the devices in the device data store.
5) Users update their preferences such as data capture setup, special alerts, thresholds, emergency contacts, and application settings.
6) The device captures motion, telemetry, and geospatial data. Interactions from the fitness tracker, connected watch, and cell phone usage are captured.
7) Using edge services, the user application sends data from the Internet such as social media accounts or weather and road conditions.
8) The transformation and connectivity service enables secure connectivity to IoT registered devices such as vehicle, fitness tracker, and connected watch.
9) Devices from male driver record abnormal medical stress and driving pattern. Devices from female driver record phone call and erratic driving pattern. Application correlates information, evaluates next action, and saves in corporate data store. Both drivers are sent appropriate alerts. The application follows the escalation path as defined in preferences.

10) The analytics engine implements machine learning and applies heuristics, statistics, classifiers, dimensional reduction, and collaborative filtering for anomaly detection and remediation. It updates in-memory processors for quick processing of real-time transactions.

11) The transformation and connectivity service allows for secure connection to enterprise systems to look up event information.

12) The enterprise application maintains business models such as customer experience and risk evaluation. It is used for lookup, transaction processing, or publishing a new event rule, audit processing. This data is loaded in memory for access to analytics engine.

13) This service manages process workflow and coordinates the REST-based services that are used in your applications.

14) The IoT governance maintains policies and terminology of the business applications and the rules for accessing that information.

15) Visualization provides active descriptive reports and dashboards to user.

16) The user application provides the engagement model for the user as a mobile or web application.

7.15.2.2.3 Basic information on the use case

Table 42 shows basic information related to the Connected Car Analytics Use Case.

Table 42 – Basic information for Connected Car Analytics

Source(s) / Literature	Link	Conditions (limitations) of Use
IBM Cloud Architecture Centre	https://www.ibm.com/devops/method/content/architecture/iotArchitecture/connected_car_analytics	No limitations Attribution required.

7.15.3 Actors

Table 43 shows the actors participating in the Connected Car Analytics Use Case.

Table 43 – Actors for Connected Car Analytics

Actor Name	Actor Type	Actor Description	Used Technology
Car driver	Human	Person who is a car driver and signs up for "Better Driver Behaviour" program	Personal devices such as fitness tracker, connected watch, Smart Phone. Connected car
Connected car	System	The car driven.	The car is instrumented with various sensors which provide location, speed, temperature, conditions.
Medical physician	Human	The personal doctor for the car driver	Have IT systems that can receive alerts about the car driver, that can be used to analyse car drivers vital signs and report potential conditions.
Better Driver Behaviour Application	Application	Application which correlates information and evaluates next actions, including alerts and messages.	Application runs in a cloud service, with appropriate scalability and connectivity.
Device Registry	Database	Holds registration information for all devices in the system.	Standard SQL database
Enterprise User Directory	Database	Holds profiles for all the car drivers registered with the Better Driver Behaviour program	Standard SQL database
Device Data Store	Database	Holds data received from the various sensors and devices registered in the system	Standard SQL database
Analytics Engine	Service	Provides analysis of both real-time data streams and historical data looking for patterns and anomalies.	
Process Management	Service	Provides process workflow for the system	
End User Application	Application	Application which provides an interface to the system for the car driver	Smart Phone
IoT Transformation & Connectivity	Service	Enables communication between the devices and the applications & services in the system.	

7.15.4 Issues: Legal Contracts, Legal Regulations, Constraints

None provided.

7.15.5 Referenced Standards and/or Standardization Committees

Table 44 shows referenced standards and/or standardization committees relevant to the Connected Car Analytics Use Case.

Table 44 – Referenced Standards and/or Standardization Committees for Connected Car Analytics

Relevant Standardization Committees	Standards have to be considered in the Use Case	Standard Status
ISO/IEC JTC 1, OASIS	ISO/IEC 20922, MQTT	ISO/IEC and OASIS standard

7.15.6 Relation with Other Known Use Cases

None provided.

7.15.7 General Remarks

None provided.

7.15.8 Security and Privacy

A preliminary impact assessment must have been carried out by the organizations involved in the application, in order to ensure that privacy regulations are met (e.g. consent management, data protection).

Given that this system involves personal data relating to the car drivers, some of the data being sensitive health data, protection of personal data is a major issue for this use case. In instances where PII is collected, all services must be in compliance with applicable privacy regulations.

There is a need to protect data flowing from the devices to the applications and services – it must be encrypted and have integrity checking applied. Data in the Device Data Store must be protected – it should be encrypted and requires strict access control.

7.15.9 Conformity Aspects and Critical Requirements

None provided.

7.15.10 Interaction between Actors and User Requirements

None provided.

7.15.11 Diagram of Use Case

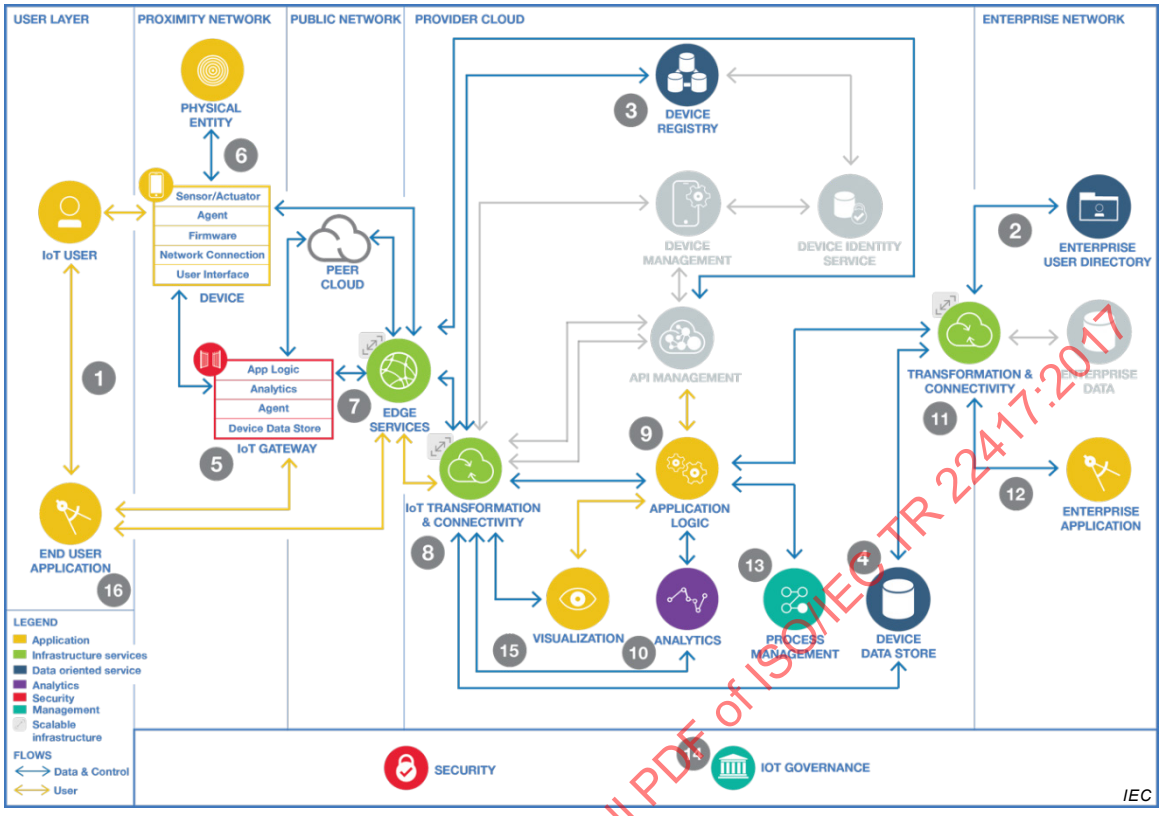


Figure 34 – Connected Car Analytics Use Case Diagram

7.15.12 Data Flow Diagram of Use Case

See 7.15.2.2.2 and Figure 34 for reference.

7.16 Real Time Motor Monitor (Use case number 16 in Table 1)

7.16.1 Scope and Objectives of Use Case

This use case describes using an IoT platform to monitor motors in a production line to enable preventative maintenance; it uses sensors to ensure that the customer device is connected to the IoT system which can improve automation and push processes in the supply chain. Predictive maintenance by cloud services enables operations, manufacturing, production and maintenance personnel in asset-intensive industries to use predictive analytics to improve asset availability, increase throughput, minimize unplanned outages, and reduce maintenance costs.

7.16.2 Narrative of Use Case

7.16.2.1 Short Description

Predictive maintenance offered as a cloud service enables operations, manufacturing, production, and maintenance personnel in asset-intensive industries to use predictive analytics to improve asset availability, increase throughput, minimize unplanned outages, and reduce maintenance costs.

7.16.2.2 Complete Description

7.16.2.2.1 Steps in the Flow of the Use Case:

1) User can interact with a machine, in this case a servo motor via sensor, to monitor its performance attributes to enable preventive maintenance.
2) The IoT gateway converts the data into MQTT format and sends it to APIs in the customer application running on a cloud service.
3) The APIs and the IoT devices are authenticated in the cloud service.
4) API and device authorization pass the received data to the Predictive Maintenance and Quality (PMQ) application.
5) Check for exceptions, boundary conditions, and other anomalies in real time.
6) Workflow integration with Asset Management application and notify a service representative.
7) Complete business process automation running as a cloud service.

7.16.2.2.2 Basic Information to Use Case

Table 45 shows basic information related to the Real Time Motor Monitor Use Case.

Table 45 – Basic information for Real Time Motor Monitor

Source(s) / Literature	Link	Conditions (limitations) of Use
IBM Cloud Architecture Centre	https://www.ibm.com/devops/method/content/architecture/iotArchitecture/real_time_motor_monitor	No limitations Attribution required.

7.16.3 Actors

Table 46 shows the actors participating in the Real Time Motor Monitor Use Case.

Table 46 – Actors for Real Time Motor Monitor

Actor Name	Actor Type	Actor Description	Used Technology
Technician	Human	Responsible for the maintenance of the production line motors	
Supervisor	Human	Oversees the operation of the production line	Production line control screen
Production line motor	Physical Entity	The entity that is being monitored for its performance	
Motor sensors	Sensor	Sensors measuring vital characteristics of the production line motor	
IoT Gateway	IoT Gateway	Gathers motor sensor data and forwards it to cloud services and applications	Proximity network + Internet connection using MQTT as the transport protocol
Device registry	Database	Holds registration information for all devices in the system.	Standard SQL database
Predictive Maintenance and Quality application	Application	Application which analyses the incoming device data and historical data to provide advice on next steps to take.	
Production line control screen	End user application	Application which provides an interface for the Supervisor to interact with the system.	

7.16.4 Issues: Legal Contracts, Legal Regulations, Constraints

None provided.

7.16.5 Referenced Standards and/or Standardization Committees

Table 47 shows referenced standards and/or standardization committees relevant to the Real Time Motor Monitor Use Case.

Table 47 – Referenced Standards and/or Standardization Committees for Real Time Motor Monitor

Relevant Standardization Committees	Standards have to be considered in the Use Case	Standard Status
	MQTT	ISO standard OASIS standard

7.16.6 Relation with Other Known Use Cases

None provided.

7.16.7 General Remarks

None provided.

7.16.8 Security and Privacy

A preliminary impact assessment must have been carried out by the organization that deployed the application, in order to ensure that privacy regulations are met. Security and privacy management to protect enterprise and personnel information must be provided.

7.16.9 Conformity aspects and Critical Requirements

None provided.

7.16.10 Interaction between Actors and User Requirements

None provided.

7.16.11 Diagram of Use Case

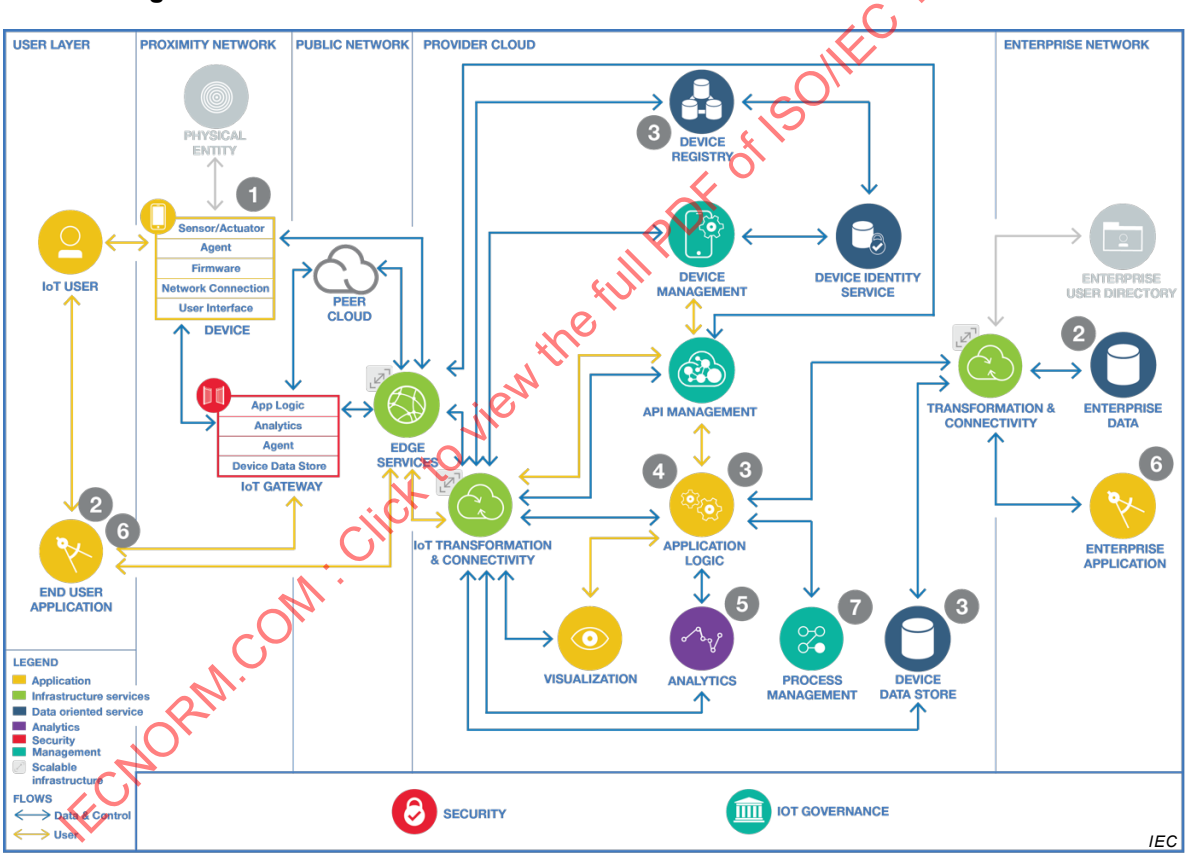


Figure 35 – Real Time Motor Monitor Use Case Diagram

7.16.12 Data Flow Diagram of Use Case

See 7.16.2.2.1 and Figure 35 for reference.

7.17 Smart Home Appliances (Use case number 17 in Table 1)

7.17.1 Scope and Objectives of Use Case

A manufacturer and its ecosystem partners can provide user remote control and better customer support for connected appliances in smart homes.

7.17.2 Narrative of Use Case

7.17.2.1 Short Description

The business drivers of this use case are to:

- Improve customer support and satisfaction.
- Streamline work of customer service and warranty service.
- Generate additional revenue by improving sales of partner services

7.17.2.2 Complete Description

7.17.2.2.1 Steps in the Flow of the Use Case

1) Smart phone application registers customer ownership of appliance and provides the user with the ability to control the appliance.
2) Customer registration details are recorded in the manufacturer's systems of record.
3) The appliance is registered in the cloud service provider's registry and appropriate security permissions are established.
4) While in the house, the user uses the smart phone app to check the status of the appliance and to send commands to the appliance, such as adjusting a temperature setting. In this situation, the application connects directly to the appliance.
5) Devices embedded in the appliance send data to the application and respond to its commands.
6) The application can communicate with the cloud service to offer the same capabilities when the user is not physically in the house. In this situation, the device also communicates with the cloud service.
7) Application logic can be used to influence or control the appliance. For example, a washer or dryer might not start immediately, but delay to get a better energy rate.
8) Usage and operational data can be collected from the devices in the appliance and stored in a device data store.
9) This data can be analysed, either in real time or retrospectively, for one or more of the following: preventive maintenance; understanding what features are used from appliance (for future marketing or cross selling); for rental or lease of the appliance (pay as you go).
10) Third party ecosystem providers can connect through API management to offer further services, such as selling accessories or consumables.

7.17.2.2.2 Functional Requirements

- Customer should easily register and claim their appliance for warranty and service support.
- Customer opted-in to share location with manufacturer, retail distributor, and service provider.
- For preventive maintenance, customer provides access to usage data and customer support can determine if any part needs service or replacement.
- Customer should be able to check status of appliance and be able to operate it from their smart phone, even outside of the house.
- Remote troubleshooting by service engineer.

7.17.2.2.3 Basic Information to Use Case

Table 48 shows basic information related to the Smart Home Appliances Use Case.

Table 48 – Basic information for Smart Home Appliances

Source(s) / Literature	Link	Conditions (limitations) of Use
IBM Cloud Architecture Center	https://www.ibm.com/devops/method/content/architecture/iotArchitecture/smart_home_appliances	No limitations Attribution required.

7.17.3 Actors

Table 49 shows the actors participating in the Smart Home Appliances Use Case.

Table 49 – Actors for Smart Home Appliances

Actor Name	Actor Type	Actor Description	Used Technology
Appliance Customer	Human		Smart Phone
Appliance Manufacturer	Organization		
Appliance Service Staff	Organization		
Third Party Provider	Organization		
Home Appliance	Physical Entity	The smart home appliance	
Appliance Sensors	Sensors	Sensors in or attached to the smart home appliance, monitoring its operation	Proximity network
Appliance Actuators	Actuators	Actuators associated with the smart home appliance, able to affect its operation (e.g. switch on, alter power consumption, etc)	Proximity network
Smart Phone	End user device		Proximity network Access network
IoT Gateway	IoT Gateway	Home Gateway device, connecting local appliance devices to the cloud services and applications.	Proximity network Access network
End user application	Application	Provides the appliance customer with an interface to interact with the appliance, the appliance manufacturer and with Third Party providers.	Smart Phone Wireless connectivity
Smart Appliance Application	Application	Application which drives the smart home appliances and supports the end user application.	
Manufacturer's Customer Database	Database	Holds information about customers and appliances registered into the system	Standard SQL Database
Device Registry	Database	Holds registration information for all devices in the system.	Standard SQL database
Appliance Analytics	Service	Analyses data streaming from various sources including the appliances, weather data, electrical usage and pricing data.	

Actor Name	Actor Type	Actor Description	Used Technology
Device Data Store	Database	Holds data received from the various sensors and devices registered in the system	Standard SQL Database
Third Party service interface	Service	Interface which permits Third Party providers to connect their services	API Management

7.17.4 Issues: Legal Contracts, Legal Regulations, Constraints

None provided.

7.17.5 Referenced Standards and/or Standardization Committees

Table 50 shows referenced standards and/or standardization committees relevant to the Smart Home Appliances Use Case.

Table 50 – Referenced Standards and/or Standardization Committees for Smart Home Appliances

Relevant Standardization Committees	Standards have to be considered in the Use Case	Standard Status
	MQTT	ISO standard OASIS standard

7.17.6 Relation with Other Known Use Cases

None provided.

7.17.7 General Remarks

None provided.

7.17.8 Security and Privacy

In instances where PII is collected, all services must be in compliance with applicable privacy regulations. This system involves personal data relating to the appliance customer and so requires appropriate protection applied to this data. This includes encryption of the data in transit and (for example) the pseudonymization and encryption of the data held in the databases.

Security is significant in the case of Actuators, which should only be usable by authorized actions either deriving from the appliance customer or from the smart appliance application. Safety must be a major consideration in the system design.

7.17.9 Conformity aspects and Critical Requirements

None provided.

7.17.10 Interaction between Actors and User Requirements

None provided.

7.17.11 Diagram of Use Case

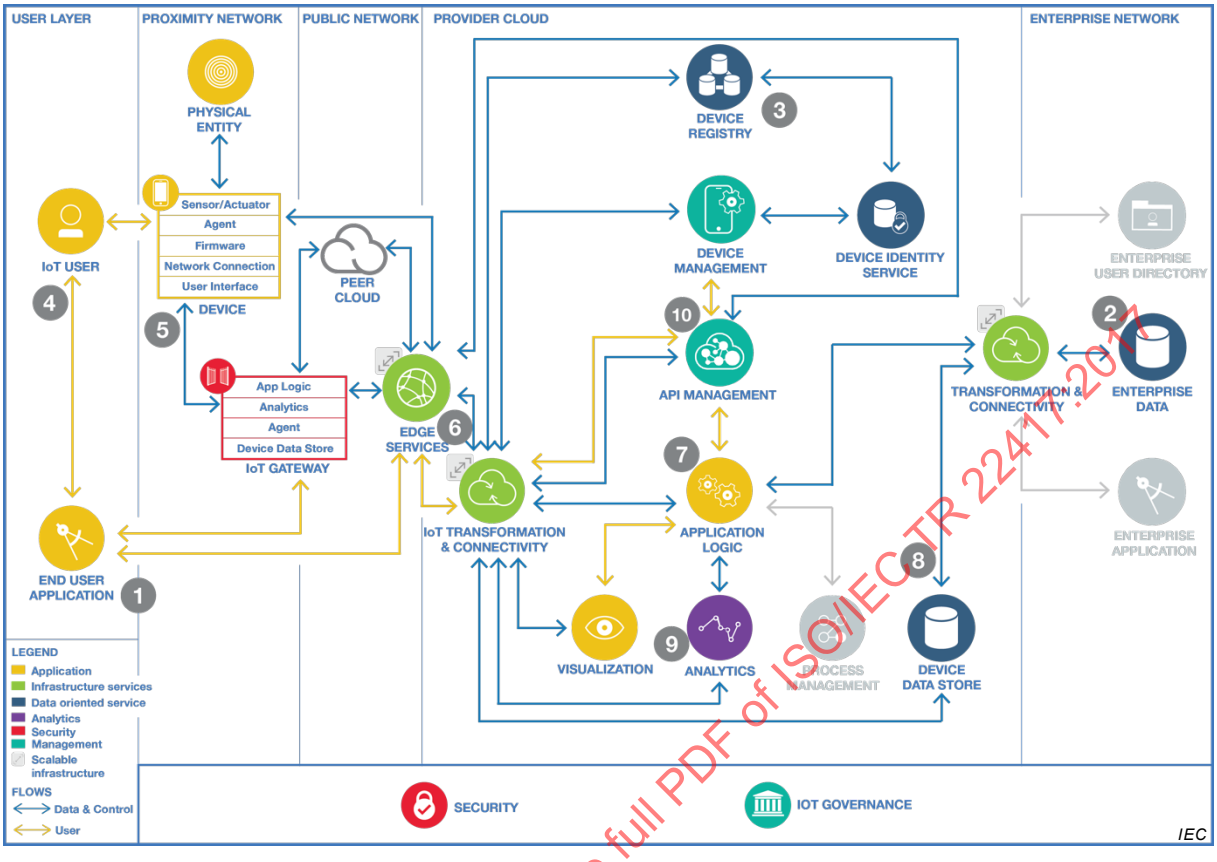


Figure 36 – Smart Home Appliance Use Case Diagram

7.17.12 Data Flow Diagram of Use Case

See 7.17.2.2.1 above.

7.18 Smart Home Insurance (Use case number 18 in Table 1)

7.18.1 Scope and Objectives of Use Case

The scope of the use case is to improve the insurance experience for a homeowner using instrumentation in the home allied to analytic applications provided as cloud services.

7.18.2 Narrative of Use Case

7.18.2.1 Short Description

Smart homes with connected devices and sensors allow insurance companies to improve service for their policy holders while providing insight into risks to the home. This use case shows how an IoT platform can monitor sensors in the home.

7.18.2.2 Complete Description

7.18.2.2.1 General

By connecting an instrumented home and ecosystem partners, insurers, and services such as weather reporting, the IoT for Insurance solution enables a home insurance company improve their service and the experience of the homeowner. A solution like this lets the policy holder receive notification of potential danger to the home and engage with the insurer in a more proactive manner. For example, leak-detection sensors and valves can monitor for water leaks and protect the home from resulting damage. The device maker is responsible for the life cycle of the devices and the insurance company benefits from access to the device data so it can provide an improved experience to its policy holders.

7.18.2.2.2 Steps in the Flow of the Use Case:

1) Sensors are set up, deployed in the home, and attached to the device maker's cloud service. These sensors could include water leak detection, water flow, temperature, and automatic water shutoff valves.
2) The home owner logs into the insurance company's mobile application and authorizes the insurance service to access the device maker's cloud service and device data. The mobile application sends the authorization token and insurance company identifier to the cloud service. This information is used to map the user, devices, and insurance policy within the cloud service. The device cloud service is used because the device maker owns the life cycle of the devices as well as the user experience with the devices.
3) The insurance cloud service receives authorization, device details, and insurance ID from the insurance mobile application and processes this in several nodes (application logic, device registry and device data store). The devices are registered with the device registry and data mapping is updated in the application logic component.
4) The insurance service application connects to the device maker's cloud service using the authorization token and requests the data. The application is set up to pull data on a configured interval. In addition to device data, the application is configured to access other data sources such as a weather data service for use in analysis.
5) Data from devices and other sources such as the weather service are continually updated and sent to analytics to determine if a potential risk threshold has been exceeded. This data is analysed to determine if there is a potential for damage to the home (including water damage, freeze potential, etc).
6) Once it is determined that there is a problem, using the analysis from step 5, notifications are sent to the home owner and to the insurance company. The home owner can then take an action to respond to the notification and determine if damage has occurred, and the insurance company can initiate the claim process.
7) If damage has occurred, the insurance business process of claims management is initiated. The insurance business processes can be accomplished in the cloud service, the company's enterprise applications, or its mobile applications. This is dependent on how and where the insurance company decides to perform the business logic.

7.18.2.2.3 Functional Requirements

- Easy to use, secure mobile application.
- User opted-in to share location and other information.
- Home equipped with a network of sensors and gateway devices.
- Cloud services IoT platform with robust device management, data identity services, and analytics.
- Enterprise network, containing existing enterprise applications, services, and data.

7.18.2.2.4 Basic Information to Use Case

Table 51 shows basic information related to the Smart Home Insurance Use Case.

Table 51 – Basic information for Smart Home Insurance

Source(s) / Literature	Link	Conditions (limitations) of Use
IBM Cloud Architecture Center	https://www.ibm.com/devops/method/content/architecture/iotArchitecture/smart_home_insurance	No limitations Attribution required.

7.18.3 Actors

Table 52 shows the actors participating in the Smart Home Insurance Use Case.

Table 52 – Actors for Smart Home Insurance

Actor Name	Actor Type	Actor Description
Homeowner	Human	Owner of the home and customer of the insurance company
Insurance Company	Organization	Insurance company offers home insurance services to the homeowner
Device manufacturer	Organization	Provides actuator and sensor devices which the home owner installs around the home
Sensors	Sensor	Sensor devices installed in the home, such as water leak detector, water flow meter, thermometer
Actuators	Actuator	Actuator devices installed in the home to enable control, for example, water shutoff valves, heating control system
Home Gateway	IoT Gateway	Gateway connecting home devices to the device manufacturer cloud services and to the insurance company cloud services. Also provides local connectivity for the end user application.
Smart Home Insurance Application	Application	Analyses data from the home sensors, combined with other data such as weather information to drive the system
Analytics Engine	Service	Analyses data streaming from home sensors and from other sources, combined with historical data, to predict potential for damage to home or its contents.
Device Registry	Database	Holds registration information for all devices in the system.
Device Data Store	Database	Holds data received from the various sensors and devices registered in the system
Process Management	Service	Initiates insurance business process workflow for the system

Actor Name	Actor Type	Actor Description
Smart Phone	End user device	
Insurance Mobile Application	Application	Application which provides an interface to the insurance system for the home owner

7.18.4 Issues: Legal Contracts, Legal Regulations, Constraints

None provided.

7.18.5 Referenced Standards and/or Standardization Committees

None provided.

7.18.6 Relation with Other Known Use Cases

None provided.

7.18.7 General Remarks

None provided.

7.18.8 Security and Privacy

A preliminary impact assessment must have been carried out by the organizations involved in the application, in order to ensure that privacy regulations are met (e.g. consent management, data protection).

This system involves personal data relating to the homeowner and so requires appropriate protection applied to this data. This includes encryption of the data in transit and (for example) the pseudonymization and encryption of the data held in the databases.

Security is significant in the case of Actuators, which should only be usable by authorized actions either deriving from the appliance customer or from the smart appliance application. Safety must be a major consideration in the system design.

7.18.9 Conformity Aspects and Critical Requirements

None provided.

7.18.10 Interaction between Actors and User Requirements

None provided.

7.18.11 Diagram of Use Case

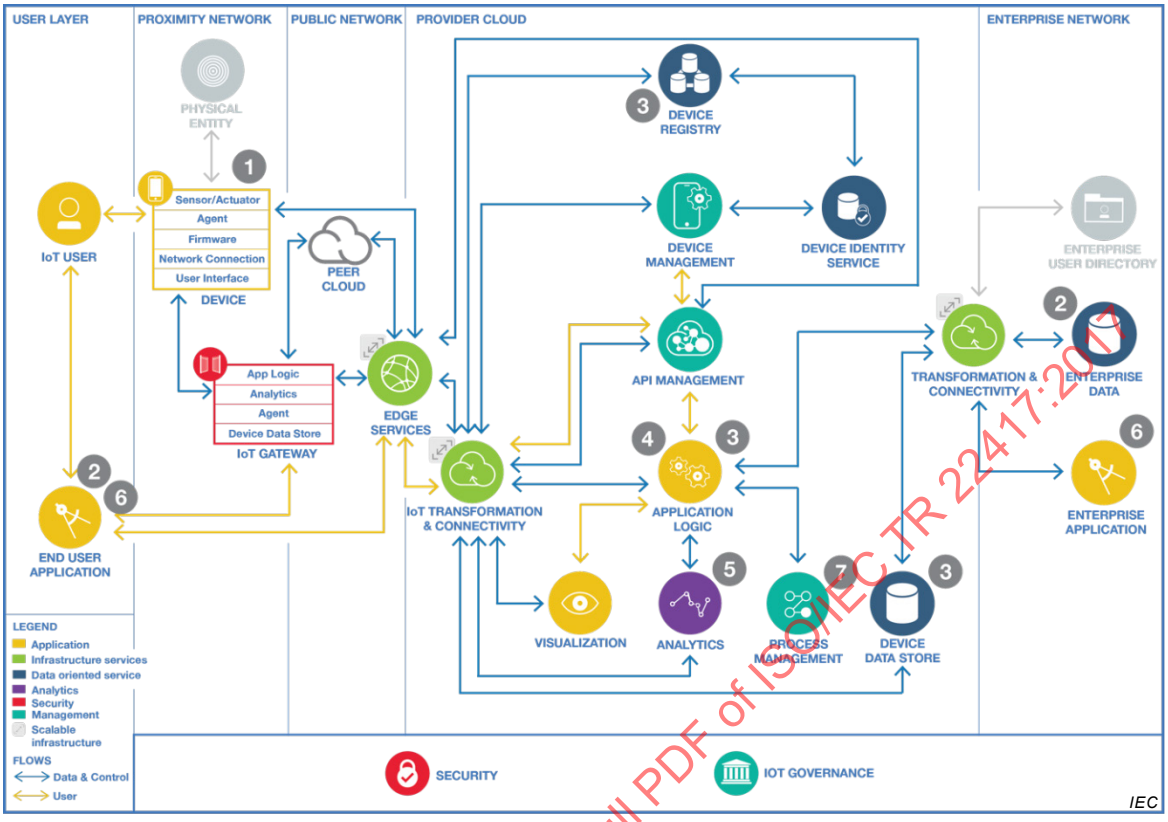


Figure 37 – Smart Home Insurance Use Case Diagram

7.18.12 Data Flow Diagram of Use Case

See 7.18.2.2.2 above.

7.19 Machine Leasing (Use case number 19 in Table 1)

7.19.1 Scope and Objectives of Use Case

This use case describes an IoT application which would enable a machine manufacturer to monitor and track a user's remote assets in real-time. By collecting the performance, status and location data of the machines, the leasing company is able to deliver value added services such as predictive maintenance.

7.19.2 Narrative of Use Case

7.19.2.1 Short Description

In the past, the machine manufacturer would sell machines to users; however, because the machines were expensive, users would have to get financial support from banks or use their own capital for these purchases, which restricted expansion of the business. Without current information regarding the machines it was difficult for banks to approve the financial applications from either manufacturers or users.

The Machine Financial Leasing System is an IoT application which enables a machine manufacturer to monitor and track a machine's performance and situation in real-time, and this system could provide the data to the banks. The machine manufacturer could also collect the data from the key parts of the machines or spare part purchases to analyse the performance of the machines. This would enable predictive maintenance to minimize the

downtime of the machine. Analysing the data can provide additional statistics and key performance data such as average operation cost.

Therefore, the Machine Financial Leasing System helps the machine manufacturer to secure the asset loan when leasing machines to users, and could also benefit the bank by increasing confidence in approval of lease financing and reducing potential risk.

7.19.2.2 Complete Description

The IoT system architecture view of machine leasing is shown in Figure 38.

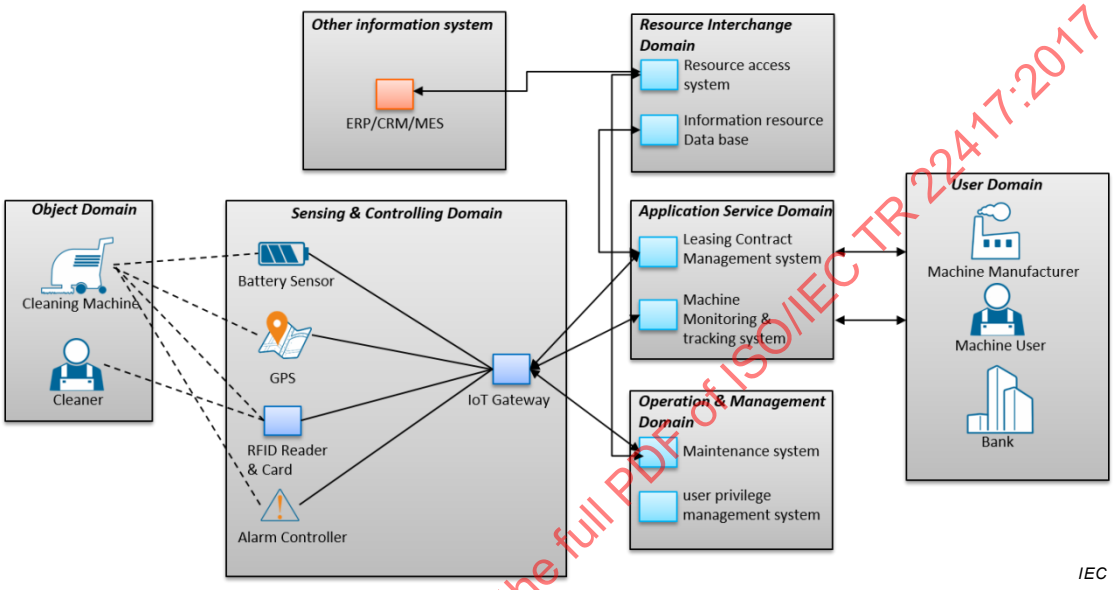


Figure 38 – IoT system architecture overview of machine leasing system

- User Domain (UD)
  - The end users of the system are the machine manufacturer, leasing company, users, and the bank.
- Sensing and Controlling Domain (SCD)
  - Devices can sense information about the machine, such as lithium ion battery level, temperature, charging status and times, water box level, detergent level, location information, clean area and RFID and trigger an alert in certain conditions, such as an illegal operation, malfunction, or moving the machine out of operation area.
- Application Service Domain (ASD)
  - The service platform collects information from the machines and provides it to the end users.
- Resource Interchange Domain (RID)
  - The service provider needs information from a third party information system to provide services, such as acquiring commercial information from the Customer Relationship Management (CRM) system and machine delivery information from the Enterprise Resource Planning (ERP) system of the machine manufacturers and manufacturing information from the Manufacturing Execution System (MES).
- Operation and Management Domain (OMD)
  - System managers are able to manage the whole system through the operation and management platform.

7.19.3 Actors

Table 53 shows the actors participating in the Machine Leasing Use Case.

Table 53 – Actors for Machine Leasing

Actor Name	Actor Type	Actor Description	Used Technology
Sensor	Device	Sensors collects the data from key spare parts of the machine, e.g. battery level and temperature, water level, etc.	
GPS	Device	GPS provides the real-time positioning information of the machines to service application	
RFID card and reader	Device	RFID reader installed on the machine reads the information inside the RFID card to give the card holder access to operate the machine. This information should include RFID card holder information, valid time, etc.	
Alarm controller	Device	When a machine is moved out of the operation area, malfunctions, key spare parts drop below a pre-set value, an alert is sent to the service platform.	
IoT gateway	Gateway	An IoT gateway connects all types of sensor, alarm controller and RFID reader, and gathers this information and manages the local network.	
Internet connectivity function	Network	Internet connectivity enables the information from the PED to be exchanged by the SCD, UD, ASD, OMD and RID.	
Resource access system	System	The resource access system connects to third-party systems to retrieve data These third party systems include ERP, CRM and MES systems of the machine manufacturer.	
Information resource database	Database	The information resource database categorizes and stores all the sensor and device data.	
Machine monitoring and tracking system	System	This collects the operating condition information from the machines, and provides data analysis and visualization services to end users such as machine manufacturer, machine users, banks.	

Actor Name	Actor Type	Actor Description	Used Technology
Maintenance system	System	The maintenance system manages the entire machine leasing system ensuring stable and safe operation. It records operational and device states of all the machines and provides the system maintenance service.	
User privilege management system	System	The user privilege management system allows user to have access to different level of information according to their access privileges. It prevents an unauthorized person from gaining access to sensitive data.	

7.19.4 Issues: Legal Contracts, Legal Regulations, Constraints

None provided.

7.19.5 Referenced Standards and/or Standardization Committees

None provided.

7.19.6 Relation with Other Known Use Cases

None provided.

7.19.7 General Remarks

None provided.

7.19.8 Security and Privacy

Operations must be carried out with proper access management to ensure that unauthorized parties do not access the system.

IoT devices impersonation must be prevented.

There could be cases where a privacy impact assessment should be carried out

7.19.9 Conformity aspects and Critical Requirements

None provided.

7.19.10 Interaction between Actors and User Requirements

None provided.

7.19.11 Diagram of Use Case

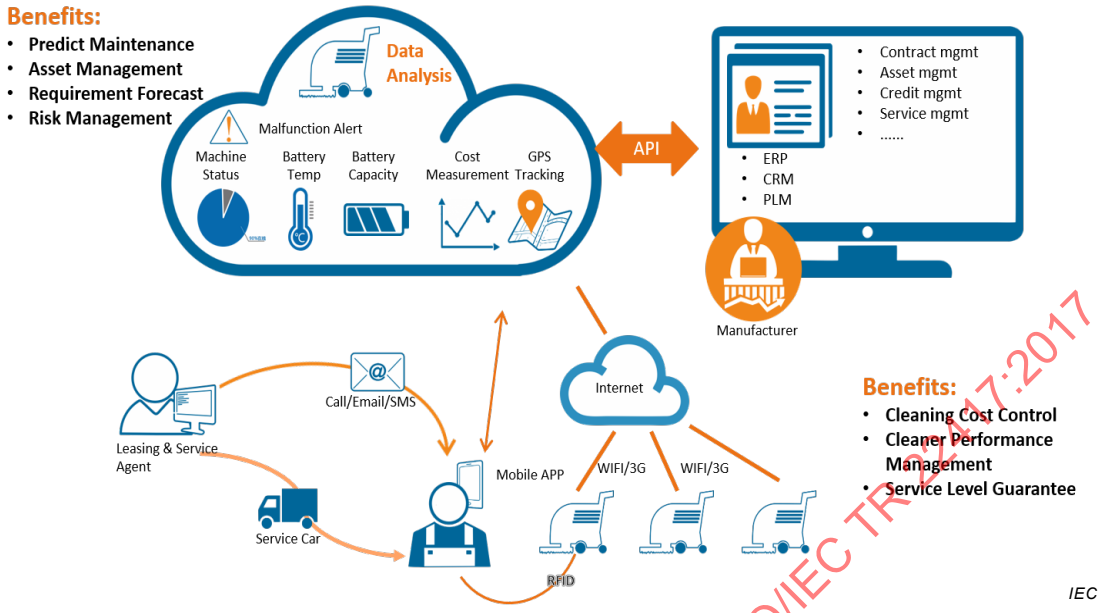


Figure 39 – IoT Application for Cleaning Machine Leasing

7.19.12 Data Flow Diagram of Use Case

See use case description above.

7.20 IoT–based Energy Management System for Industrial Facilities (Use case number 20 in Table 1)

7.20.1 Scope and Objectives of Use Case

Energy management is the proactive, organized and systematic coordination of procurement, conversion, distribution and use of energy to meet specific requirements, taking into account environmental and economic objectives. However, the variety of energy management systems results in a lack of interconnectivity and interoperability, therefore a simple and common strategy for exchanging energy-related information is required. This use case defines an IoT-based communication framework, and an IoT-based energy-management platform. The IoT-based strategy can exchange energy-related information among the entities in a facility, which not only allows the integrated energy management system to become interconnected and interoperable but also reduces the energy costs of industrial facilities.

7.20.2 Narrative of Use Case

7.20.2.1 Short Description

This use case describes an IoT-based communication framework with a common information model which facilitates the development of a demand response (DR) energy management system for industrial customers. It also describes an IoT-based energy-management platform based on a common information model and open communication protocols, which takes advantage of integrated energy supply networks to deploy DR energy management in an industrial facility.

7.20.2.2 Complete description

Industry is the largest consumer of electricity among all end-user sectors. According to statistics from the International Energy Agency, in 2012, the consumption of electricity worldwide by the industrial sector was 42,3 % of total energy produced. This has led to

significant interest in the development of industrial energy management around the world in recent years.

Nowadays, IoT technologies are deployed to solve business problems. In an industry field, one promising approach is the assurance of interconnectivity and interoperability in industrial energy management systems in order to allow the communicating entities to interact with each other using a common information model. The IoT system includes an energy management system (EMS) that runs the DR algorithm, an energy management agent (EMA) that manages industrial tasks, a monitoring and control system (MCS) that monitors and controls the industrial processes, an energy storage system (ESS) that stores energy that can be delivered at a later time, a solar energy generation system (EGS) that generates electrical energy by using the sun's radiation, an industrial Ethernet backbone network to provide reliable communication, and a wireless field network based on 6LoWPAN, and provides the possibility to reduce the development cost of an industrial network.

Because of the high electricity consumption in industrial applications, it is imperative to establish an industry-centric energy management system as well as to make sure that this system is utilized in a proper way. Thus an effective information model is needed. The Facility Smart Grid Information Model (FSGIM) is utilized to represent the energy consumption, production, and storage systems in an industrial facility. As a result, a level of interoperability is ensured because the data formats have been standardized.

Current study shows that the IoT-based architecture and FSGIM-based information models can play an important role in providing interconnectivity and interoperability between devices and equipment, which guarantees simpler implementation, installation, operation and management of integrated energy management systems in a facility. It also offers a simple and common strategy for exchanging energy-related information between the entities in a facility.

7.20.3 Actors

Table 54 shows the actors participating in the IoT–based Energy Management System for Industrial Facilities Use Case.

Table 54 – Actors for IoT–based Energy Management System for Industrial Facilities

Actor Name	Actor Type	Actor Description	Used Technology
Production Planner /Facility Manager	Human	Responsible for carrying out production plans	
Utility Power Station	The power system	Acts as an energy supplier and energy information provider	
Utility Meter	Device	Measures energy consumption or generation, and provides this information to the utility company	
Energy Manager System (EMS)	System	Provides the functions of energy management, control and planning in conjunction with responsible facility management	
Energy Manager Agent (EMA)	System	Monitors the electricity consumption and controls the electric load of each task	
Monitoring and Control System (MCS)	System	Designed to monitor and control the operation of each device	
Meter (M)	Device	A physical device or subsystem onto which an electric meter is defined	
Non-shiftable Equipment (NSE)	Device	A device whose energy demand must be met immediately	
Controllable Equipment (CE)	Device	A device that has multiple operating levels, resulting in differences in electricity demand	
Shiftable Equipment (SE)	Device	A device that can be switched on or off based on the electricity demand	
Energy Storage System (ESS)	System	Store electrical energy, then deliver it at a later time.	

7.20.4 Issues: Legal Contracts, Legal Regulations, Constraints

None provided.

7.20.5 Referenced Standards and/or Standardization Committees

The requirements of semantic interoperability are now being met on the customer side by the use of the Facility Smart Grid Information Model (FSGIM). The FSGIM is a specification that is currently under development by the American Society of Heating and Air-Conditioning Engineers (ASHRAE).

To implement the FSGIM in industrial facilities, the protocols for both the backbone and wireless networks need to be considered.

In the physical and data link layers, the proposed standards include PROFINET, EtherCAT, Ethernet Powerlink, RAPIEnet and EPA. As for the field network, the industrial radio stacks are built on IEEE 802.15.4, where the referenced standards include ISA100.11a, WirelessHART and WIA-PA. In the network layer, the proposed standards include IPv4, IPv6 and 6LoWPAN. In transport layer, the proposed standards include TCP and UDP. In the industrial wired part, the proposed application layer standards include Hypertext Transfer Protocol (HTTP) and Simple Network Management Protocol (SNMP). The sensors can be defined as MIBs and SNMP can read data from the sensors.

For the industrial wireless part, the proposed standards include Constrained Application Protocol (CoAP), which is used as the application layer protocol for implementing the scheme.

7.20.6 Relation with Other Known Use Cases

None provided.

7.20.7 General Remarks

The main goal in the integration of energy management systems is to allow the communicating entities to interact with each other using a common information model. A simple and common strategy for exchanging energy-related information among the entities in a facility is needed. By using the IoT to interconnect the devices, industrial production will be made more intelligent and efficient.

The results of current studies show that the IoT-based architecture and FSGIM-based information models have a vital role in providing interconnectivity and interoperability between devices and equipment, which guarantees simpler implementation, installation, operation and management of integrated energy management systems in a facility. It also offers a simple and common strategy for exchanging energy-related information between the entities in a facility.

7.20.8 Security and Privacy

Operations must be carried out with proper access management to ensure that unauthorized parties do not access the system.

IoT devices impersonation must be prevented.

There could be cases where a security and/or privacy impact assessment should be carried out.

7.20.9 Conformity Aspects and Critical Requirements

None provided.

7.20.10 Interaction between Actors and User Requirements

None provided.

7.20.11 Diagram of Use Case

7.20.11.1 General

In Figure 40, there are 7 related sub-case studies that have been conducted.

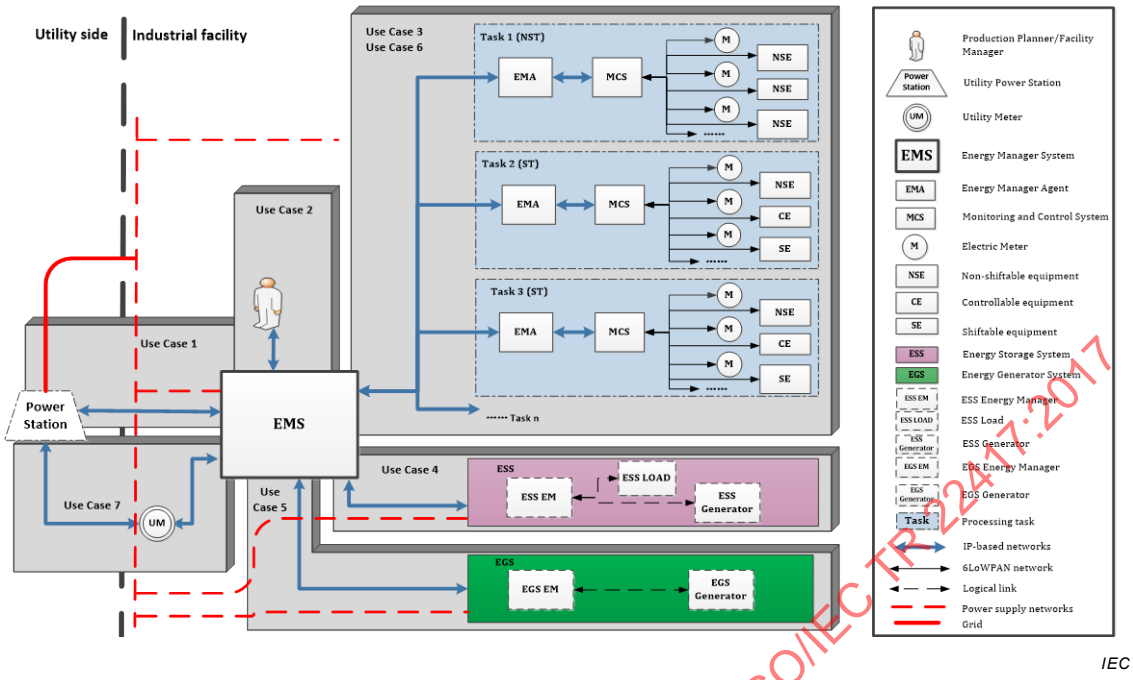


Figure 40 – Structure of IoT-Based Energy Management System with FSGIM

7.20.11.2 Sub-Use Case 1: Determining Energy/demand Price Information

In this use case, the power station provides dynamic pricing to the facility. These price data are developed by the power station using internal procedures to maintain a balance between generation and supply near the time of use. The communication between the utility power station and the EMS is based on using a wide area network (WAN), in which TCP/IP can guarantee reliability of packet transfer.

7.20.11.3 Sub-Use Case 2: Determining DR Parameters

In this use case, the EMS prepares the parameters of the DR algorithm and makes the DR decision. The algorithm is formulated using the STN model and mixed integer linear programming (MILP).

7.20.11.4 Sub-Use Case 3: Managing the Operation Point of Each Time Interval to Minimize Cost

In this use case, the facility manages the operating point of each time interval to minimize cost. After making a decision, the EMS provides the EMA of each task, the optimal operating point of the task and the operating time of that operating point. The EMA proposes operating levels of the equipment in each task and sends this information to the MCS, which ultimately controls the equipment according to the commands scheduled by the EMA.

7.20.11.5 Sub-Use Case 4: Determining the Utilization of ESS

In this use case, the facility decides to buy, power or utilize the ESS within each time interval. After determining the energy price information and the DR parameters, the EMS specifies the ESS operating mode in the next stage and the operating duration of that mode, which is an IES decision. The communication between the EMS and ESS is based on TCP, which guarantees reliability of packet transfers.

7.20.11.6 Sub-Use Case 5: Determining the Utilization EGS

In this use case, the facility decides to buy power from the grid or use the EGS within each time interval. After making a decision, the EMS specifies the EGS operating mode in the next stage and the operating duration of that mode, which is an IES decision. In a high-electricity-

price period, it encourages the EMS to command the EGS to supply electricity to some or all of the processing tasks. This decreases the electricity demand of the industrial facility.

7.20.11.7 Sub-Use Case 6: Measuring Equipment Power Consumption

In this use case, the facility measures equipment power consumption for each task and each load. The facility measures the power consumption of a particular electrical device and each task. Prior to its use, the operation manager installs a meter to measure energy at a device or for each task. Periodically, the meter measures the energy consumption of each device and sends an energy measurement message to the MCS to track the ongoing energy use of the load. The MCS sends the energy consumption of related loads to the EMA. The EMA sends the energy consumption of each task to the EMS. The EMS supplies the energy consumption to the facility manager.

7.20.11.8 Sub-Use Case 7: Measuring all Energy Consumption in a Factory

In this use case, the facility measures all equipment power and provides this information to the utility power station and the EMS. The utility meter measures the whole energy consumption of the factory. The utility meter sends the energy measurement message to the EMS to track the ongoing energy use of the factory. The EMS provides the energy consumption information to the facility manager. The utility meter sends the energy measurement message to the utility power station, which is used by an energy provider to track facility or equipment performance and analyse requirements.

7.20.12 Data Flow Diagram of Use Case

None provided.

7.21 Water Plant Management (Use case number 21 in Table 1)

7.21.1 Scope and Objectives of Use Case

This use case describes an IoT application for comprehensive management of a water plant in Shanghai, China, which is a demonstration application project. In the water plant, various types of sensor, which are in collaborating networks, perceive the information of device status and running environment of the water plant, and transmit this data to the IoT gateway which collects and formats the data. The application software can analyse, process, and fuse the data to provide convenient and reliable services for the managers and operators, such as device monitoring, running environment monitoring, asset management, personnel behaviour management, safe guard management, actions with alarms, and interact with other business systems. With the IoT application for this water plant, it contributes to the technical support for secure, reliable, highly effective operation and promotes the technical progress of the water plant industry.

7.21.2 Narrative of Use Case

7.21.2.1 Short Description

This example applies IoT technology to acquire complex information from power devices, mechanical devices, firefighting equipment, safe guarding, running environment, and personnel entry and exit positions, and to perform system analysis, multiple fusion and logic decisions such as alarming, controlling and other action utilizing algorithms from a library.

7.21.2.2 Complete Description

Traditional management and operations of the water plant is largely based on labourers' field inspection by seeing, hearing, touching, smelling, and oversight of the machine and ambient environment in the plants. However, with low efficiency methods and a lack of qualified workers the problem cannot be solved without using technology. Nowadays, many new devices and technologies are applied in water plants and therefore smarter and leaner management capabilities need to be evolved.

Through the use of IoT technology, comprehensive and smart monitoring and controlling systems for the water plant can be developed. In the front end, sensor networks sense the environment parameters which impact the ordinary running and real-time status of devices. All this information is transmitted to the service platform to be processed and analysed, and can be used to produce the visualization interface which displays the data and central controlling system. The IoT smart water plant monitoring system, assembled from subsystems including: safe guarding, electronic device monitoring, mechanical device status monitoring, production environment monitoring, personnel positioning, asset management, alarm generating, and assistive controlling, to allow for smart detection, judgment, management, and verification, thus improving management.

Smart monitoring and assistive controlling systems in water plant can greatly reduce the work load and improve the quality of operation and management. This can prevent or reduce the failures caused by missing safe guards, over-worked staff, weak asset management, defective devices, inappropriate operation, and environment parameter exceeding normal setting range. Thereby greatly improving work efficiency and reducing operation and maintenance costs.

The information in the smart monitoring and assistive controlling system of the water plant is monitored, and can provide the following services:

- Safe guarding
  - perimeter intrusion prevention, smoke detection, intruder detection through use of camera surveillance, vibration sensors, IR sensor, theft-proof bolts, etc.
- Electronic device monitoring
  - temperature monitoring of substation equipment, resistance current monitoring and harmonic current detection of lighting arrestor, GIS (Gas Insulation Switch) SF6 leakage detection, etc.
- Mechanical device monitoring
  - vibration of the water pump, temperature of the axis, and the status of switches and valves.
- Ambient environment monitoring
  - heating and ventilation, water supply and drainage, harmful gas monitoring, water immersion, and water level detection,
- Personnel and asset position
  - GPS for personnel and assets.
- Alarm with action
  - sound and light alarms and notification of a manager who can take action when the re-set condition occurs.
- Other function
  - prevention alarm, visual data presentation and central direction for emergency.

7.21.3 Actors

Table 55 shows the actors participating in the Water Plant Management Use Case.

Table 55 – Actors for Water Plant Management

Actor name	Actor type	Actor description	Further information specific to this use case
Electrical equipment, mechanical equipment, environment, etc.	Physical Entity	Their attributes are monitored and controlled by users.	
Temperature and moisture sensors	IoT Device	Acquisition of temperature and moisture of ambient environment	
Water immersion sensors	IoT Device	Water immersion detection	
Smoke sensors	IoT Device	Smoke concentration detection	
Vibration sensor	IoT Device	Detection of the vibration	
RFID tags and readers	IoT Device	The tags attached on the assets and the helmets of personnel record the corresponding position information which be transmitted to the management system for personnel's motion authentication beforehand.	
Alarm controller	IoT Device	Triggered when sensed data is beyond the pre-set values, or the position of human and asset is out of scope. Furthermore the alarm information can be sent to managers who can take action	
Wind generation controller	IoT Device	When high concentration of harmful gas is detected by sensors, this controller will start to ventilate the area	
Local Area Network	Network	Connects the IoT gateway, service platform, and other business systems in the water plant to allow data interaction	
Wireless base station	IoT Device	Connects data from various sensors, and transmits data to IoT gateway	
IoT gateway	IoT Device	Collects the data from wireless base stations, some sensor network stations, and RFID servers, transforms this data to a common format for service platforms and other systems	
Data filtering and fusion	System	Filters the incomplete or destroyed data, and fuses the data from different sensors which are monitoring the same object, to produce comprehensive device status data	

Actor name	Actor type	Actor description	Further information specific to this use case
Data analysis and diagnosis system	System	Provides data mining and data trend analysis, and diagnoses the health of the equipment	
Resource Access Interface	system	Interchanges data with external systems such as emergency fire and security systems	
Resource database	system	Stores the data which needs to interchange with external system	
On-line monitoring system	system	On-line and real-time representation of the device status information, environment information, personnel and asset information, etc.	
Assistive Controlling system	system	Send command to controlling systems such as the alarm controller, wind generation controllers, etc.	
Operation system	system	Management system which supports the whole system allowing it to run stably and reliably	
Maintenance system	system	Manages the device status and arranges their repair when errors occur, and manages the maintenance tools used in terms of authorization	
System manager	User	End-users, who get the information relating to equipment or environment, perimeter security status, and alarms in case of error or intrusion, and manage the devices, asset and personnel automatically	

7.21.4 Issues: Legal Contracts, Legal Regulations, Constraints

None provided.

7.21.5 Referenced Standards and/or Standardization Committees

None provided.

7.21.6 Relation with Other Known Use Cases

None provided.

7.21.7 General Remarks

None provided.

7.21.8 Security and Privacy

Personnel safety and environmental safety aspects are involved in this use case. In instances where PII is collected, all services must be in compliance with applicable privacy regulations.

7.21.9 Conformity Aspects and Critical Requirements

None provided.

7.21.10 Interaction between Actors and User Requirements

None provided.

7.21.11 Diagram of Use Case

Figure 41 – Monitoring and Control System in Water Plant project in Shanghai

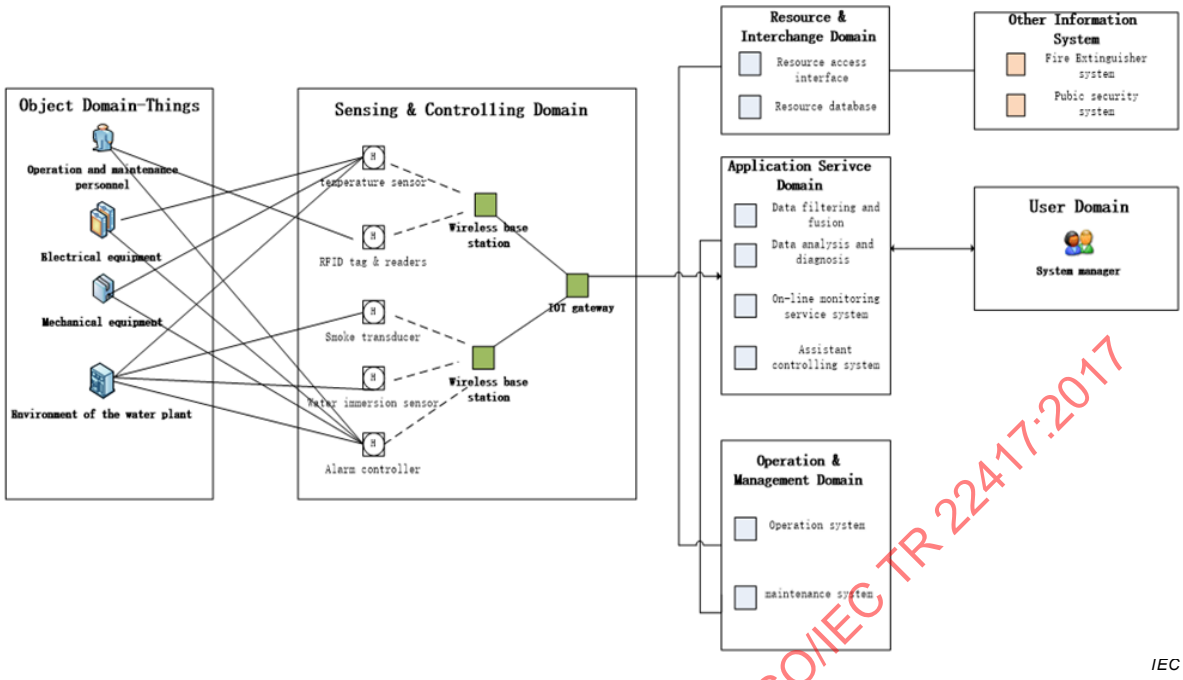


Figure 42 – System Architecture of Smart Water Plant Monitoring System

7.21.12 Data Flow Diagram of Use Case

See system architecture diagram and detailed actor descriptions above.

7.22 Smart Home Application (Use case number 22 in Table 1)

7.22.1 Scope and Objectives of Use Case

The use case relates to the monitoring and controlling of what happens in and round the house to provide a convenient home service for people. Basically, a smart home can be defined as an overarching system that can access or control many of a home's systems including appliances, security, climate, and video monitoring from a remote or centralized location. It aims to provide not only convenience, but also security, accessibility and efficiency.

- Convenience
  - Convenience is one of the main reasons that people build and purchase smart homes. These homes give users remote access to systems including heating and cooling systems, intercoms, music and multimedia devices throughout the home. Integrated hardware allows homeowners to watch video or listen to audio in any room; video intercoms make it easy to communicate with others in the home or visitors at the door. All of these smart home technologies streamline everyday tasks.
- Security
  - Smart homes include advanced security systems with cameras, motion sensors and a link to the local police station or a private security company. Smart homes may also use key cards or fingerprint identification in place of conventional locks, making it harder for someone to break in.
- Accessibility
  - For elderly or disabled residents, a smart home may feature accessibility technologies. Voice-command systems can perform tasks, such as controlling lights, locking doors, operating a telephone or using a computer. Home automation allows an individual to set a schedule for automatic tasks including closing the curtains, watering the lawn, removing the need to perform these labour-intensive tasks on a regular basis.

- Efficiency
  - Smart homes offer enhanced energy efficiency. Lights can shut off automatically when no one is in a room, and the thermostat can be set to let the indoor temperature drop during the day before returning it to a more comfortable level just before residents arrive in the evening. All of these automated tasks, along with modern, energy efficient appliances, combine to reduce usage of electricity, water and natural gas, thereby reducing the strain on natural resources.

7.22.2 Narrative of Use Case

7.22.2.1 Short Description

This use case describes the application of smart home systems using IoT technology to achieve the enhancement of home safety and comfort.

7.22.2.2 Complete Description

A Smart Home is expected to provide comfort, security, energy efficiency (low operating costs) and convenience to the homeowner at all times, regardless of whether anyone is at home.

"Smart Home" is the term commonly used to define a residence that has appliances, lighting, heating, air conditioning, TVs, computers, entertainment audio and video systems, security, and camera systems that are capable of communicating with one another and can be controlled remotely by a time schedule, from any room in the home, as well as remotely from any location in the world via phone or internet.

Examples are given as follows:

Dad arrives home. He presses his finger on the intelligent lock and the finger information is sent to the gateway and is verified and then the gateway orders the opening of the lock. Meanwhile the notification of Dad's coming back has been sent to the mobile app.

Dad opens the door of the house which is equipped with a Door sensor. The sensor sends a message to the system and then the window curtains open as has been pre-set. The sun shines in.

The sensors in the room continuously monitor the brightness, temperature, humidity and other environmental states. When the temperature is higher than the pre-set number, the system will automatically turn the air conditioning on with an IR blaster; when the brightness is too low, the lights will also turn on.

The family is ready for travelling. With only one press, the house will be in Away Mode and the door will lock; some appliances switch to sleep mode, and some are powered down. If a stranger tries to break into the house by destroying the intelligent lock, the system will send a message to the cloud service and then to the homeowner's mobile app. The homeowner will be informed and turn on the security camera recording the abnormal situation. This abnormal situation will also be sent to the security system of the community allowing someone to investigate.

Figure 43 – Smart Home Systems

7.22.3 Actors

Table 56 shows the actors participating in the Smart Home Application Use Case.

Table 56 – Actors for Smart Home Application

Actor name	Actor type	Actor description	Further information specific to this use case
Multiple sensors	IoT Device	Read the brightness, vibration, UV, temperature, humidity, and motion.	
IoT Gateway	IoT Device	Encapsulates and converts the format of the sensor data.	
Bulbs, Main Door & Windows etc.	Physical Entity	The Physical Entity that is monitored and controlled.	
Door/window sensor	IoT Device	Reports the status of a door or window.	
Curtain motor	IoT Device	Drives the curtain when it is opened or closed.	
Home appliances	Integrated Physical Entities & IoT Device(with sensors and controllers)	Smart devices can report their status through integrated sensors or a controlling unit which can change the status or motion according to the reset model.	

Actor name	Actor type	Actor description	Further information specific to this use case
Mobile phone with application software installed	Application Interface Device	Receives report data or notifications from the IoT system and sends back the user's instructions.	
Service provider and Smart home services	Stakeholder & software	Provides convenient smart home services for family users.	
Family members	Human User	Human users of the whole IoT system.	
Cloud service with database	Information system	Collects, stores and analyses the sensed data and controlling data from the house.	
Internet connectivity	Communication network	Enables information exchange between the service platform and user application.	
Security camera	IoT device	A camera which is used to monitor an area for security purposes.	
Security system of community	Service System	Connects with the individual smart home system of every house in the community and provides with security monitoring services.	
IR Blaster	IoT device	Converts digital instructions into IR signals.	
Intelligent lock	IoT device	Digital locks with fingerprint reader and keypad which communicates with the IoT gateway.	
System maintenance	Management	Manage the devices network and performs repairs if anything malfunctions or fails.	
Community Management System	Management	Manages community services such as security, public energy consumption and provides better logistical servicing of community.	

7.22.4 Issues: Legal Contracts, Legal Regulations, Constraints

None provided.

7.22.5 Referenced Standards and/or Standardization Committees

Table 57 shows referenced standards and/or standardization committees relevant to the Smart Home Application Use Case.