Deliverable 3: Internet of Things Risk Analysis and Assessment

PROJECT RISIoT: MARKET ANALYSIS AND RISK ASSESSMENT TO ACCELERATE THE ADOPTION OF THE INTERNET OF THINGS IN AUSTRIAN ENTERPRISES

Sandra König, Stefan Schiebeck, Stefan Schauer, Martin Latzenhofer, Peter Mayer, Geraldine Fitzpatrick
MAY, 2017
The project RISIoT - MARKET ANALYSIS AND RISK ASSESSMENT TO ACCELERATE THE ADOPTION OF THE INTERNET OF THINGS IN AUSTRIAN ENTERPRISES – is conducted between September 2016 and August 2017 by the following consortium:
IDC Central Europe GmbH
Austrian Institute of Technology GmbH
Technical University of Vienna
Austrian Computer Society

The RISIoT project is co-funded under the „ICT of the Future“ programme by the Austrian Ministry for Transport, Innovation and Technology and the Austrian Research Promotion Agency (FFG). Project number: 855450
# TABLE OF CONTENTS

Table of Contents .......................................................................................................................................................2  
List of Figures.............................................................................................................................................................3  
List of Tables .............................................................................................................................................................3  
1. Introduction ...........................................................................................................................................................0  
   1.1 IoT Domains, Use Cases and Related Incidents .................................................................................... 1  
   1.2 Characteristics of IoT Systems ........................................................................................................... 9  
   1.3 IoT Related Research Projects and Studies .................................................................................. 11  
2. IoT Standards and Reference Models ...........................................................................................................0  
   2.1 ISO 30141 – Internet of Things Reference Architecture (IoT RA).................................................. 1  
   2.2 Reference Architecture Model Industry 4.0 (RAMI 4.0) ................................................................... 8  
   2.3 Industrial Internet Reference Architecture (IIRA) ........................................................................ 11  
   2.4 Internet of Things Architectures ................................................................................................... 14  
   2.5 ITU-T Y.2060 Overview of the Internet of Things ...................................................................... 15  
   2.6 The ISO 31000 Family .................................................................................................................... 17  
   2.7 The ISO 27000 Family .................................................................................................................... 21  
   2.8 NIST SP800-160 – Systems Security Engineering ....................................................................... 24  
   2.9 NIST SP800-183 – Networks of Things ......................................................................................... 25  
   2.10 ISA/IEC-62443 .......................................................................................................................... 27  
3. IoT High Level Risks ...........................................................................................................................................0  
4. Categorization of IoT-related risks .....................................................................................................................2  
   4.1 Risk Matrices ................................................................................................................................. 2  
   4.2 High-level IoT Risk Matrix .............................................................................................................. 3  
5. Domain-Specific IoT Risks .............................................................................................................................0  
   5.1 An Illustrative Use Case .................................................................................................................. 0  
   5.2 Risk Assessment for the Project’s Use Cases ............................................................................. 4  
   5.3 Domain Specific IoT Risk Matrices .............................................................................................. 7  
6. Conclusion ..........................................................................................................................................................0  
7. References ..........................................................................................................................................................0  
8. Annex ..............................................................................................................................................................7
LIST OF FIGURES

Figure 1 - IoT Mind Map, 2014 (ISO/IEC JTC 1/WG 10, 2014) ................................................................. 2
Figure 2 - IERC Vision for IoT integrated environment and ecosystem (cf. (Vermesan and Friess, 2016)) .... 13
Figure 3 – IERC future IoT challenges (Vermesan and Friess, 2016) ........................................................ 14
Figure 4 - The IERC Activity Chains (Vermesan and Friess, 2016) ............................................................ 14
Figure 5 - Creating specific System Architectures (SA) and Application Areas (AA) (ISO, 2016b, p. 46) ........ 1
Figure 6 - Big Picture for IoT Concepts of the CM (ISO, 2016b, p. 67) ....................................................... 2
Figure 7 - Systematic Approach to IoT Security (ISO, 2016b, p. 66) ......................................................... 3
Figure 8 - Relation between IoT Conceptual Model (CM), Reference Model (RM), and Reference Architectures (RA) ......................................................................................................................... 3
Figure 9 – Relation between Concept Model (CM) and Reference Model (RM) (ISO, 2016b, pp. 70, 73, 77) .... 4
Figure 10 - IoT RA functional view (ISO, 2016b, p. 41) .............................................................................. 5
Figure 11 - IoT RA system view (ISO, 2016b, p. 44) ................................................................................... 5
Figure 12 - IoT RA communications view (ISO, 2016b, p. 47) .................................................................. 6
Figure 13 - Type of information related to domains (ISO, 2016b, p. 49) ....................................................... 7
Figure 14 - Structure of information (ISO, 2016b, p. 49) ......................................................................... 7
Figure 15 - Roles and activities during the IoT product life-cycle (ISO, 2016b, p. 58) ................................. 8
Figure 16 - Structure of the RAMI 4.0 object worlds ............................................................................... 9
Figure 17 - Concepts of an RAMI 4.0 asset ................................................................................................. 9
Figure 18 - Reference architecture model Industry 4.0 (RAMI 4.0) ............................................................. 11
Figure 19 - ISO/IEC/IEEE 42010:2011 - Architecture Description .......................................................... 12
Figure 20 - Relationship among IIRA Viewpoints, Application Scope and System Lifecycle Process ......... 13
Figure 21 - Risk management framework and risk management process according ISO 31000 (ISO, 2009a, fig. 1) .......................................................... 18
Figure 22– System Life Cycle Processes (Ross et al., 2016) according (ISO, 2015b) ................................. 25
Figure 23 - Example model of a NoT’s dataflow (Voas, 2016, fig. 4) ......................................................... 27
Figure 24 - 62443 Elements (ISA, 2016, fig. 1) ..................................................................................... 28
Figure 25 - High Level Risk Matrix ............................................................................................................ 4
Figure 26– Use Case Specific Risk Matrix .................................................................................................. 7

LIST OF TABLES

Table 1: OWASP framework considerations for IoT component types (OWASP, 2016c) ...................... 12
Table 2: Abbreviations .............................................................................................................................. 8
1. INTRODUCTION

The Term “Internet of Things” was first used in 1999 by Kevin Ashton (Mchugh, 2004), who worked on Radio-Frequency Identification (RFID) for logistics applications. Meanwhile, thousands of somewhat similar definitions of IoT have emerged.

Oxford defines the Internet of Things as “A proposed development of the Internet in which everyday objects have network connectivity, allowing them to send and receive data.” (Oxford University Press, 2017).

The authors of this document share a broader definition of the IoT, namely “a network of items, embedded with sensors and actuators”.

We particularly consider security aspects and potential safety harms that result from intentional security breaches. Safety aspects in regards to environmental or unintentional harms of IoT ecosystem use cases are beyond the scope of this study.

Since its first introduction in 1999, major developments have been

- the release of IPv6 (Deering and Hinden, 1998), the internet protocol that will support the IoT,
- the announcement of various OS for IoT devices (e.g., (“RIOT - The friendly Operating System for the Internet of Things,” 2017), Windows 10 for IoT (Microsoft, 2017), VxWorks (“VxWorks,” 2017), Google Brillo (Android, 2017), ARM mbed (ARM, 2017),
- the widespread availability of M2M communication devices (e.g., Bluetooth, ZigBee, low-power WiFi),
- the announcement of a new generation of chips for smart devices (e.g., Intel Joule (“Make Amazing Things Happen in IoT and Entrepreneurship with Intel Joule,” 2017), Samsung (“Meet the Expanded Samsung ARTIK Smart IoT Platform,” 2016), NXP (NXP Semiconductors, 2017), Texas Instruments (“SimpleLink Wi-Fi CC3100/3200 | Ecosystem | Wi-Fi | TI.com,” 2017), ARM (ARM, 2017)), and
- the widespread availability of networked microcontrollers serving as sensors or actuations (Postscapes, 2017a).

During the past years, some industries have gone beyond the basic concept of the IoT, incorporating various other applications within the IoT ecosystem. For example, the Referenzarchitekturmodell Industrie 4.0 (Reference Architecture Model Industry 4.0 – RAMI 4.0, (Plattform Industrie 4.0, 2017)) extends IoT concepts to handle manufacturing and logistics applications.

The rise of the Internet of Things, a trend sometimes called “the next Industrial Revolution”, has led to a situation where humans won’t be the only ones powering the internet by feeding it with information. A multitude of sensors and cyber-physical systems will monitor and interact with the environment, creating innovative services by harnessing information that has previously not been utilized. IoT will undoubtedly boost a tremendous amount of innovation, efficiency, quality and value across all industries, but with something as complex as the IoT development stack, how much effort will be employed in regards to security when organizations keep struggling to decrease time-to-market of their IoT applications?

The IoT market is already starting to change consumer, business and industrial processes and practices and is subject to various forecasts [IoT forecasts and trends, (Postscapes, 2017b)]. A recent study (Knud Lasse Lueth,
IoT Risks

2017) summarized individual forecasts by Cisco, Ericsson, Gartner, IDC, Harbor Research, ABIresearch, Global Insight, GE, McKinsey and various other organizations along four major metrics. It is estimated that, by 2020:

- the number of connected devices will reach up to 50 billion
- the generated revenue via IoT will reach up to 7 trillion USD
- the total economic value of IoT will reach up to 15 trillion USD
- the amount of IP-traffic will reach up to 2.3 Zeta Byte (0.87 ZB by 2015 (“The Zettabyte Era,” 2016)), tripling worldwide internet traffic.

One of the prevailing challenges regarding the development of IoT applications is the fundamental lack of an internationally accepted reference architecture for planning, design, implementation and operation of IoT ecosystems. Various organizations have begun to adopt IoT characteristics for many of their products and systems, resulting in thousands of different frameworks, methods, protocols as well as software and hardware implementations.

1.1 IoT Domains, Use Cases and Related Incidents

In order to establish a common understanding of the domains and use cases that the IoT will likely encompass, the following sections provide a grouped summary of applications [cp. (ISO/IEC JTC 1/WG 10, 2014)].

Within most domains one of the most important international standards in regards to information security is ISO 27001 (ISO, 2013a), allowing organizations to certify their efforts in establishing organization-wide management of technical and organizational information security risks. Special requirements are marked separately within the next sections.

Due to general considerations in regards to globalization, industrialization and future developments of Industry 4.0 concepts, most organizations may be wise to consider ISO 28000 on supply chain security (ISO, 2007a), especially if their products require extensive 3rd party support.

In the following we review a number of domains with a view to the impact of IoT.
1.1.1 Healthcare

Through IoT, the healthcare domain will most likely gain remote diagnostics and examinations, patient monitoring, tracking and telemetry applications, remote treatment and surgery, patient prescription management, medical asset tracking with cryptographic assurance features, centralized medical records and increased patient accessibility, including multi-lingual support and various interfaces for people with disabilities.

Important international standards in regards to information security in this domain include ISO 14971 (ISO, 2007b, risk management for medical devices) and ISO 27799 (ISO, 2016a, usage of ISO 27001 in healthcare).

Concerns related to the security of medical devices already started in 2008, when researchers published a document titled: Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defences (Halperin, 2008). The researchers outlined privacy issues, the ability to change device settings and even the possibility to deliver a shock to the patient. In 2012 it was claimed that a pacemaker can be hacked to either shut it down completely or to remotely send a 830-volt shot to the patient (Kirk, 2012).
1.1.2 Information and Communication Technology (ICT) Industry

The domain of Information and Communication Technologies will likely encounter increased network device tracking, inventory, automation and remote/predictive management as well as low level security and monitoring features in regards to wires, fibres, junctions, telecom vaults, backup power supplies and access control.

In a recent example from November 2016 (Chazan, 2016), malicious hackers tried to hijack broadband routers of the German Telekom AG into the Mirai botnet, by exploiting vulnerabilities in widely distributed IoT devices within their network - Zyxel and Speedport routers. Due to a misconfiguration of the malware infection attempt, 900,000 of the 20,000,000 devices crashed, leaving customer broadband connections, including mobile line, TV or internet services disrupted for days.

1.1.3 Manufacturing and Heavy Industry

The manufacturing and heavy industry will be impacted by process, equipment, health and safety monitoring and management, production management, inventory management, tracking, defect and recall management, proactive servicing and warranty features relying on big data analytics, product-service bundles and mating \(^1\) as well as access control and monitoring for employees, suppliers and contractors entering premises.

The evolution of large scale Supervisory Control and Data Acquisition (SCADA) systems, robotics and interconnected production line systems (Industry 4.0), autonomous industrial-use aerial systems (e.g., delivery, monitoring) and ground systems (e.g., drilling rigs, hauling trucks) will increase productivity as well as the vulnerability exposure of those industries dramatically.

According to IBM’s Cyber Security Intelligence Index (IBM, 2016), the manufacturing industry is now one of the most frequently hacked industries, second only to health care. The most common cybersecurity incident occurs from unauthorized access that is usually launched by spear phishing attacks. Besides industrial espionage, ransomware and social engineering attacks (e.g., the “fake president” fraud) have increased.

In 2014 a cyberattack on the ICS system of a German steel mill caused multiple components to fail. This circumvented the regulation of critical process in the furnace and caused physical damage to the system and the complete plant (Lee et al., 2014).

1.1.4 Finance and Banking

In the finance and banking domain, retail Point of Sale (POS) terminals and remotely located Automated Teller Machines (ATMs) will provide local financial services to customers, while desktop and mobile devices will continue to increase their service features.

With the emergence of telematics (in-vehicle communication devices), cars are now able to transmit data about driver behaviour back to insurance companies, enabling risk-based assessment of premiums. The same principle will enable homeowners to voluntarily provide data about their households for insurance purposes. Fitness tracking and health monitor devices will enable healthcare providers and insurers to get a much more detailed picture about a customer’s well-being. The IoT has the potential to dramatically change how society will gather

\(^1\) i.e. a service that allows your couch to tell you when your car keys have slipped into the crack
and share data, including how financial services companies interact with their customers. This may also have impacts on consumers’ access to banking and financial services.


Due to its intrinsic value, the financial services industry will likely remain one of the most interesting targets across all domains for the foreseeable future. Recent reports (Seals, 2016) even show the potential of cyberattacks to destabilize a country’s financial system, combined with targeted disinformation and social media propaganda campaigns about the banks’ financial stability.

1.1.5 Food and Farming
Within the food and farming sector, the evolution of IoT will be noticed through increased usage of field sensors indicating chemical and environmental conditions, monitoring of produce, livestock, and processed foods for quality and defect management, spoilage, and expiry and the automation of ordering and delivery of services.

In a report on the worldwide adoption of IoT in smart and connected farms (Beecham Research, 2015), the potential to cut costs and improve production has been estimated to boost food production by 70% by 2050. The possibility to monitor production, processing and distribution across the whole supply chain will give companies and customers the means to fight food fraud.

1.1.6 Transportation
With assisted driving and autonomous-driving technologies on the rise, smart trains, planes, automobiles, boats and spacecraft, traffic signals that respond to traffic conditions, infrastructure monitoring that reports wear and tear for proactive (predictive) maintenance, vehicle-to-vehicle (V2V) communication and Road Side Units (RSUs) for safety, including crash prevention, the transportation sector will encounter dramatic improvements during the next decades.


Widespread international efforts (e.g., P.E.A.R.S. (Page et al., 2015), Project Pegasus (Köster et al., 2016)) are starting to harmonize political and regulatory requirements for safety & security testing in regards to vehicle security, road safety and advanced driver assistance systems.
With the first report of an automobile autopilot allegedly killing a driver in June 2016 (Golson, 2016) and hackers discovering vulnerabilities in 471,000 automotive entertainment systems (Greenberg, 2015) allowing them to remotely control dashboard functions, steering, brakes and transmission, many safety and privacy concerns have risen amongst the industry’s players. Widespread international efforts (e.g., P.E.A.R.S. (Page et al., 2015); Project Pegasus (Köster et al., 2016)) are starting to harmonize political and regulatory requirements for safety & security testing in regards to vehicle security, road safety and advanced driver assistance systems.

In May 2015, a cybersecurity consultant even hacked into computer systems aboard airliners (Perez, 2015) up to 20 times, managing to control aircraft engines during a flight.

Back in 2008, although these devices have not been connected to the internet back then, German railway switches have been manipulated by a 14 year old youth using an infrared TV remote (Knop, 2008), who was able to derail four trains and injure several people. In the US, distribution of equipment related to the manipulation of various control devices mainly used in transportation (traffic signals, switches, etc.) has already been declared illegal under federal legislation since 2005, because several companies where selling devices to, e.g., “change red lights to green in 2-3 seconds” (“The Mirt Traffic Light Control Device,” 2003).

### 1.1.7 Domestic

IoT innovations in home automation like heating, ventilation and air conditioning, lighting control, leak detection, smoke and carbon monoxide detectors, security and monitoring, smart appliances and intelligent renewable energy systems will make homes more integrated and adaptive to our daily needs, increase energy efficiency and self-sufficiency.

Home automation devices that enable older adults and people with disabilities to remain at a higher level of independence (called assistive domotics) include activity monitoring, home treatment and remote diagnostics.

The increase of connected devices in domestic homes has already proven to be a potential disruptive force, ranging from baby monitor exposures and vulnerabilities (Stanislav and Beardsley, 2015), multiple reports of wearable products that introduce privacy concerns (Open Effect, 2016) to powerful Distributed-Denial-of-Service (DDoS) attacks that are powered by a hacked web cameras, DVRs, TVs and many other domestic devices (Krebs, 2016).

Another example is a smart video doorbell (Layden, 2016) that is meant to be installed outside of a house, enabling attackers to dismount the device, put it into setup mode and read the shared secret key that was used to connect the doorbell to the home’s wireless network.

### 1.1.8 Water

Water systems, both large-scale municipal water distribution and waste systems, as well as their smaller in-house counterparts will become increasingly connected, providing remote administration, alerting as well as sensory and automated treatment to ensure drinking quality as well as corrosion and sediment management of involved pipework.

In 2016 Hackers breached a water utility system and manipulated systems responsible for water treatment and flow control (Kovacs, 2016). The compromised systems allowed hackers to alter settings related to water flow and the amount of chemicals used to treat the water.
Researchers at the Georgia Institute of Technology have even demonstrated the capability of ransomware (Khandelwal, 2017) to take down critical infrastructures (Georgia Institute of Technology, 2017) and demand ransom payment.

1.1.9 Education
The realm of education will also benefit from AR/VR applications, remote education and engagement options and the availability of real-time empirical data from study topics (e.g., live data feeds from marine probes to study ocean biology).

Regular devices like smartphones, tablets and laptops will increasingly be used for education to provide computer-aided learning experiences, but also dedicated educational toys will offer more functionality by being interconnected.

Back in 2013, students in Indiana and California showed that limitations imposed on educational IT devices inhibit students' natural curiosity, which lead them to hack their school issued iPad’s and circumvent unwanted security restrictions (Watters, 2013).

In 2015, a Chinese educational toy company with revenues of over US$2 billion has suffered a data breach where the personal information of five million customers, both parents and children, were stolen (Lui, 2015).

1.1.10 Energy
IoT devices will enable coordination of energy generation, distribution, storage and usage through IoT devices within the energy system infrastructure and through smart appliances in homes. This of course will enable or require energy systems to monitor various environmental aspects, raising the potential for behavioural analysis as well as remote administration, which eventually allows hackers to shut down energy supply or even overload and destroy certain components.

Cyber-attacks on a smart grid, Supervisory Control and Data Acquisition (SCADA) and Programmable Logic Controller (PLC) systems that support national critical infrastructure components have been made public through demonstrations like the Aurora Generator Test in 2007 (Meserve, 2007), showing that a cyber-attack could destroy physical components of the electric grid. This was followed by incidents such as Stuxnet (Kushner, 2013), where malicious code aimed at upsetting Iran’s nuclear development program by sabotaging centrifuge systems, and the hack of Ukraine’s power grid (Zetter, 2016) that left 230.000 residents in the dark for several hours. Several months after the attack some controls still have to be operated manually, because attackers overwrote firmware on critical devices, leaving them unresponsive.\(^2\)

\(^2\)The process of corrupting firmware is also called to „brick“ electronics – since devices cannot function any more without working firmware, they are technologically useful as a brick.
1.1.11 Entertainment and Sports
The entertainment and sports sector will benefit from enhanced realities for gaming (e.g., augmented/virtual reality (AR/VR)), tourism (e.g., multi-lingual tours for sites and monuments, simulated physical locations) and sports (e.g., ticketing and admission management, player stats and health, equipment and material information).

Besides the potential for being used for Distributed Denial of Service (DDoS) attacks due to their numbers, entertainment and educational systems will primarily introduce privacy related problems. For example, it was noticed that Samsung’s smart TV privacy policy included some rather troubling warnings. Owners are informed that they shouldn’t have personal conversations around the TV, because it’s listening and may transmit their personal information to third parties (Whitwam, 2016).

1.1.12 Public Safety and Military
In the line of public safety and military applications, the IoT will enhance border and perimeter surveillance and protection, asset tracking and localization, remote asset control (e.g., robots, unmanned aerial vehicles (UAVs)), weapons tracking and identification as well as disaster management and response.

The importance of cyber security in the military domain has been shown by various incidents, e.g., the recent attempt to infiltrate the military networks of South cyber command (Paganini, 2016), as well as public research programs like the “Hack my Army” initiative, where the US Government invites hackers to attack US Army domains.

Due to the mainstream availability of small drones (Unmanned Aerial Vehicles) and the subsequent increase of related domestic incidents, safety and privacy issues became apparent. Researchers have already shown how to use even these systems for IoT device reconnaissance, mapping out large geographic areas of IoT products that are running certain radio frequency protocols.

Military applications in the UAV sector alone cover highly armed Battlefield UAVs, endurance UAVs (e.g., DARPA’s Vulture (DARPA, 2010), a solar powered aircraft designed to remain uninterrupted for more than five years) as well as Miniature and Micro UAVs (MAVs), providing beyond-line-of-sight situational awareness for infantry (reconnaissance using visual, thermal, infrared, radar and/or several RF frequencies) (e.g., US Air Force Wasp (US Air Force, 2007)).

Other notable infantry targeted applications include the infantry helmet HeadUp display, providing information on the location of friendly forces, vehicles, and aircraft in the vicinity (Hoffman, 2014), and various interconnected gunfire detection systems that provide information about potential attacker range, direction and ballistics (Crane, 2006).
1.1.13 Retail and Hospitality
The domain of retail and hospitality will most likely gain IoT ecosystems for inventory management and logistics, support highly targeted promotions based on physical location and environmental conditions, anti-theft and fraud and enable facilities monitoring and management.
Interactions with customers based on their physical location will likely raise privacy concerns (e.g. retail in-store applications like smart shopping carts, product suggestion based on third party wearable devices, contactless checkout, smart price tags, etc.). Insufficiently secured inventory management and logistics applications (e.g. RFID inventory tracking, purchase orders, asset identification and signage), will be exposed to adversary manipulation. Facilities monitoring and management applications supported by IoT ecosystems may enable electronically assisted burglary (circumvent electronic locks, disable alarm systems, interference with wireless transmissions, etc.) as well as industrial espionage.

Retail applications will also be highly connected to smart home concepts, enabling (preventive) maintenance of parts and accessories, grocery management and various digital content delivery (e.g. on-screen advertisements) as well as options for online purchasing.

During the last years it has been recognized that malware attacks also impose a serious threat to the retail industry (Alvarez, 2015). As in other domains, infection by malicious emails or manipulated links and documents are the most common forms of attack.
In 2016 a clothing store has fallen victim to a malware attack that allowed the attacker to access customer payment data (Ankeny, 2016).

1.1.14 Government
The ability to enable online management of government-related administrative procedures (e.g. compulsory registration, tax payments, election management, etc.) will likely be affected by various IoT ecosystems providing authentication and payment services, asset tracking and management as well as remote service delivery and compliance monitoring.
Other features concerning Smart City concepts will enable real-time environmental monitoring (air quality, water levels and pollution, earthquakes), municipal water, sewer and distribution network monitoring and control, logistics asset tracking and inventory as well as building and property management and maintenance.
Many of those systems will be publicly available, thus being physically exposed and easier to attack – traffic lights, environmental sensors, digital billboards, pedestrian warning devices, elderly monitoring and emergency management systems of smart cities are likely to be targeted by malicious hackers.

As examples with national security implications, Russia allegedly hacked the US election in November 2016, contributing to the election outcome in Donald Trump’s favour (Fisher, 2016) and Lithuania’s cyber security service has identified several computer system infections of national agencies, where passwords and classified documents have leaked to IP addresses involving the Russian secret service (DPA, 2016).
1.2 Characteristics of IoT Systems

The following section gives an overview of common characteristics and related problems of IoT products and ecosystems, based on (CSA, 2016), that are shared across the domain.

1.2.1 Deployed in Insecure or Physically Exposed Environments

Many IoT edge or intermediary devices are left physically exposed to being stolen or accessed (e.g., Smart Meters) and reverse engineered to identify secrets (e.g., shared keys, passwords) or vulnerabilities within the software. Developers should also anticipate that wireless routers, home computers and mobile devices that are part of the IoT ecosystems’ data flow may be old, unpatched and configured insecurely.

1.2.2 Resource Constraints in Embedded Systems Limit Options

Within the IoT ecosystems, especially concerning edge devices, there are some highly constrained devices when it comes to implementing secure cryptographic functions. The chair of the Federal Trade Commission (Ranger, 2015) recently warned that the small size and limited processing power of many connected devices could limit the use of encryption and other security measures; it may also be difficult to patch flaws in low-cost and essentially disposable IoT devices.

1.2.3 Low IoT Device Prices Increase Adversary Pool

The low cost of consumer IoT devices will make it simpler for both security researchers and malicious attackers to identify security issues by being able to physically examine the device. Unless safeguards are applied to handle tamper identification/resistance of hardware components and logical access control of physical ports, it is highly likely that a reverse engineer will be able to extract the firmware as well as cryptographic keys of the device. If the IoT ecosystem relies on shared keys, the attacker would likely also gain access to all data within other devices that share the same key. If the attacker is able to find software vulnerabilities or default passwords within the devices firmware/software, he would – given that the vulnerability can be triggered remotely – potentially be able to compromise similar devices reachable via the network.

1.2.4 Lack of Internationally Recognized Standards

New technology companies that are implementing pieces of the IoT are spanning across the globe in several domains, making use of various architecture frameworks, hardware and software platforms, communication protocols, technical security features and distinct process maturities. Due to the public attention that the IoT market is gaining, literally thousands of standards and best practices have been proposed, creating a jungle of competing standards. The lack of internationally accepted reference architecture amongst Original Equipment Manufacturers (OEMs) results in the inability of technologies and protocols to cooperate seamlessly between vendors. Additionally, interaction between standards is missing. Various domains use various standards and even though they may be constructed from the same base, this may result in complications. For example in the case of construction machines, it is possible to follow two standards at the same time (basic vehicles follow ISO 26262 while construction equipment machinery safeties ISO 13849) and the basic safety standard IEC61508 is used to resolve uncertainties. In the case of security each domain is developing their own approach and in a connected IoT world this means that systems following different security approaches need to interact and trust each other.
In addition, standards normally follow the development of the state of the art and, in the case of rapidly evolving technological fields, there is a gap between new developments and standards.

1.2.5 Security is Not a Business Driver
It is well known that especially technology start-ups and their investors are typically interested in getting their products to the market quickly and ensuring that the core functionality works - everything else would likely lead to competitive disadvantage due to time and resource constraints.
In order to make product usage for customers as easy as possible, the enforced adaption of configuration changes (e.g., change of default credentials) or any other technical or operational security measures that require user intervention are often overlooked.

1.2.6 Security in the IoT Domain is New to the Industry
The production of IoT devices requires many manufacturers that have never had to deal with security in the past to establish resources, skills and processes to engineer and develop products in a secure manner. The basic concept of “secure by design” and “privacy by design” should be considered by following best practices (e.g., Microsoft SDLC, BSIMM, OpenSAMM), including training programs for the development team, participation in threat sharing initiatives (e.g., Information Sharing and Analysis Center, ISAC) and integrating security testing (e.g., threat modelling, code reviews, penetration tests, DevOps/DevSecOps) into the development process.

1.2.7 Security Skills are Rare
Many IoT development staff are already constantly challenged with learning and incorporating new technologies without additionally worrying about software vulnerabilities, reverse engineering and hardware attacks.
Without sufficient IoT security training efforts, organizations will continue to have difficulties recruiting and retaining necessary IoT development skills.
In addition, even professional users of IoT systems, as example operators of industrial machinery, may be unaware of the importance of security skills in their daily business and use systems with the same universal trust to received information as in the past, unconnected world. Further, it is important to maintain cybersecurity along the complete lifecycle of IoT devices, design and implementation, but also operation, maintenance and disposal. Currently operators are largely unaware of cybersecurity.

1.2.8 People are not used to being in charge of their digital privacy and security
The majority of end users are not aware of privacy and security risks introduced by IoT ecosystems, nor are they used to think about security when setting up their newest IT equipment. Therefore, most vendors won’t forcibly bother their customers with important security configurations (e.g. change of default passwords). Especially when things need to be easily configured and highly usable without restrictions, security concerns are often neglected.

3 DevOps/DevSecOps are methods for integration and improvement of secure software and hardware development
1.3 IoT Related Research Projects and Studies

In this section we give an overview on ongoing research projects and studies, including some standardization efforts.

1.3.1 OWASP IoT Project

The OWASP IoT Project is one of several widely known publications by OWASP (Open Web Application Security Project) that currently provides information on the following IoT topics:

- Principles of IoT Security (OWASP, 2016a), summarizing 16 principles for secure IoT ecosystem design and development
- IoT Attack Surface Areas (OWASP, 2015), providing a list of high-level IoT attack surfaces and related vulnerabilities that can be used as a basis for risk assessment
- IoT Testing Guides (OWASP, 2016b), providing lists of generic assessment items to help software testers
- IoT Security Guidance (OWASP, 2017) for manufacturers, developers and consumers of IoT products
- IoT Framework Assessment (OWASP, 2016c), covering general security related concerns based on the IoT component type (edge, gateway, cloud, mobile)

The following table gives a summary of framework considerations based on the IoT Framework Assessment component types that can be used as a list of generic safeguards.

<table>
<thead>
<tr>
<th>Edge</th>
<th>Gateway</th>
<th>Cloud</th>
<th>Mobile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encrypted communications</td>
<td>Multi-directional encrypted communications</td>
<td>Encrypted communications</td>
<td>Ensure mobile component enforces authentication requirements equal or greater to other components</td>
</tr>
<tr>
<td>Storage encryption</td>
<td>Strong authentication of components (edge, platform, user)</td>
<td>Secure web interface</td>
<td>Local storage security considerations</td>
</tr>
<tr>
<td>Strong logging</td>
<td>Storage</td>
<td>Authentication</td>
<td>Capabilities to disable or revoke mobile components in the case of theft or loss</td>
</tr>
<tr>
<td>Automated updates and/or version reporting</td>
<td>Denial of service and replay attack mitigation</td>
<td>Secure Authentication Credentials</td>
<td>Strong audit trail of mobile interactions</td>
</tr>
<tr>
<td>Update verification</td>
<td>Logging and alerting</td>
<td>Encrypted storage</td>
<td>Mobile application should perform cryptographic verification and validation of other components</td>
</tr>
<tr>
<td>Cryptographic identification capabilities</td>
<td>Anomaly detection and reporting capabilities</td>
<td>Capability to utilize encrypted communications to the storage layer</td>
<td>Encrypted communication channels</td>
</tr>
<tr>
<td>No default passwords</td>
<td>Use latest, up-to-date third party components</td>
<td>Data classification capabilities and segregation</td>
<td>Multi-factor authentication</td>
</tr>
<tr>
<td>Strong local authentication</td>
<td>Automatic updates and/or version reporting</td>
<td>Security event reporting and alerting</td>
<td>Capability to utilize mobile component to enhance authentication and alerting for other components</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Edge</th>
<th>Gateway</th>
<th>Cloud</th>
<th>Mobile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Offline security features</td>
<td>Automatic updates and update verification</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configurable root trust store</td>
<td>Use latest, up-to-date third party components</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device and owner authentication</td>
<td>Plugin or extension verification, reporting and updating</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transitive ownership</td>
<td>Interface segregation and</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Considerations</td>
<td>OWASP Framework Considerations</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Isolation based on utility</td>
<td>(device, management interface, user interface, etc.)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Defensive capabilities</td>
<td>Application level firewall and defensive capabilities (IP blocking, throttling, account management, etc.)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Plugin or extension verification, reporting and updating</td>
<td>Ensure ecosystem segregation in case of multi-tenant solutions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Secure M2M capabilities</td>
<td>Stack security considerations (no web UI to execute arbitrary code)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Secure web interface</td>
<td>Audit capability</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Utilize established, tested networking stacks and protocols</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use latest, up-to-date third party components</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Capability to utilize hardware devices</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Support multi-factor authentication and functionality</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tracks and contains data from potentially tainted (insecure) sources</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Written in a safe programming language or subject to scrutiny</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Does not employ secrets in code</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device monitoring and management capabilities</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 1: OWASP framework considerations for IoT component types (OWASP, 2016c)

1.3.2 European Research Cluster on the Internet of Things (IERC)
The European Cluster on the Internet of Things (IERC) is an interest group consisting of over 50 European research projects (mostly from FP 7, FP 6 and FP 5). The cluster was founded in 2007 with the original goal to strengthen the research on Radio Frequency Identification (RFID) on Europe. This objective changed over time towards defining a common vision of the IoT technology (cf. Figure 2). Due to the large number of various IoT-related projects in the EU, establishing an ongoing communication and exchange of ideas among these projects is an important mechanism for a secure, safe and privacy preserving deployment of IoT in Europe. Therefore, the main goals of the IERC are to (IERC, 2017):

- Establish a cooperation platform and develop a research vision for IoT activities in Europe and become a major entry and contact point for IoT research in the world.
- Define an international strategy for cooperation in the area of IoT research and innovation and have an overview of the research and innovation priorities at the global level.
IoT Risks

- Coordinate the cooperation activities with other EC Clusters and ICT projects.
- Coordinate and align the Strategic Research and Innovation Agenda (SRIA) at the European level with the developments at the global level.
- Organize debates/workshops leading to a better understanding of IoT and Future Internet, 5G, cloud technology, and adoption.

The IERC also serves as a platform to go beyond the European level and share knowledge, best practices and business models in the IoT area all over the world.

A major result from the IERC’s efforts is the Strategic Research and Innovation Agenda (SRIA). The SRIA has been extended over the last years (Vermesan et al., 2011, 2014, 2014) and addresses the main IoT priorities for European industry to stay competitive in the global market. It is originating from numerous discussions among the stakeholders and project members involved in the IERC’s activities over the past years. In the SRIA, the most important challenges for the IoT technology are summarized and a roadmap for the future research and development activities regarding the IoT concept and paradigm is described. With the SRIA, IERC also focusses in particular on upcoming developments and emerging trends in the field of IoT, which will also bring new challenges onto the screen. In detail, IERC sees such new challenges in the fields of the architecture and

Figure 2 - IERC Vision for IoT integrated environment and ecosystem (cf. (Vermesan and Friess, 2016))
IoT Risks

ecosystem for IoT technologies, including integration issues, as well as the need for novel business models (cf. also Figure 3). Hence, the IERC has the objective to collect known but also emerging challenges into SRIA and thus provide an incrementally updated overview on the high-priority topics in the field of IoT.

In addition to the SRIA, the IERC also defines Activity Chains, which should focus the research in different fields towards the main objectives of the cluster (cf. Figure 4). In detail, these chains summarize technical activities from a specific field of application, which are carried out by working groups of different IERC partners. As an output, these chains should produce a deliverable or an asset targeted at least at one of the IERC objectives. Furthermore, the activity chains are also used to foster the cooperation with other IoT related interest groups, e.g., the IoT Cluster, the IoT European Platforms Initiative (EPI) or the Alliance for Internet of Things Innovation (AIOTI).
The IERC provides a good overview on their activities, achievements and strategic forecasts in several articles and books available on their website (IERC, 2017). Therein, the general vision of the cluster is shown together with an in-depth description of the SRIA.

1.3.3 Study on Smart Appliances (SMART) study

In 2015, the “Study on Semantic Assets for Smart Appliances Interoperability” (Daniele et al., 2015; “Smart Appliances Project,” 2015) was published by the European Commission DG Communications Network, Content and Technology and carried out by Netherlands Organisation for Applied Scientific Research (TNO). This study deals with household appliances as main power consumers in today’s households and specifies a reference ontology for these appliances with the goal to simplify the interaction and interoperability of different devices and sensors and thus increase the power efficiency of these appliances. Although there are currently a huge variety of standards dealing with smaller parts of this problem, they do not define a consolidated data model. Hence, the main objectives of the study were to:

- Provide an overview of existing explicit or implicit semantic assets and use case assets.
- Perform a detailed analysis of the existing semantic assets or requirements in an exhaustive way.
- Define a proposal for a unified ontology to be contributed to the European Telecommunication Standard Institute (ETSI) for consideration as a future standard.
- Compile a documentation of the proposed the ontology into the ETSI M2M architecture.

To achieve this, a number of already existing assets (which is used in a broad sense in the study, i.e., referring to everything from a project to a document or a working group up to a single website) was identified. Those assets were described based on their semantic coverage and an initial semantic mapping was performed. In a next step, a subset of these assets was translated into ontologies using the Web Ontology Language (OWL) to share a common basis. Mappings among the resulting ontologies were applied to identify the most common concepts. This was done in an iterative process, updating the common ontology based on the individual models being translated. In the final step, the first version of this common ontology was created, which included the recurring concepts of all assets from the smart appliances domain as well as the main relations between these concepts.

As a result, the Smart Appliances Reference Ontology (SAREF) was defined (TNO, 2015). SAREF is built on four major principles, i.e., reuse and alignment, modularity, extensibility and maintainability. In other words, SAREF reuses the concepts and relationships already defined in existing models, allows a separation and recombination of different parts of the ontology as well as further growth of the ontology. Additionally, SAREF facilitates the identification and the correction of defects as well as the accommodation of new requirements and the adjustment to changes in the ontology.

1.3.4 ETSI Standards for smart M2M

The technical committee (TC) of the European Telecommunication Standard Institute (ETSI) provides several IoT-related standards. Recently, two reference ontologies have been published focusing on smart Machine-to-Machine (M2M) interaction.
In 2016, the oneM2M base ontology has been specified in (ETSI, 2016). It provides the basic concepts and defines the relationships between them. Thus, it enables interoperability of the oneM2M system with external systems also described by ontologies. The main classes in oneM2M are Thing, ThingProperty, Variable, Device, Functionality, Service and Operation. The main object properties are hasThingProperty and hasThingRelation. For example, a room can be modelled as a Thing with ThingProperty room temperature and ThingRelation “isAdjacentTo” that describes a relation to another room modelled as a Thing. The technical specification also contains a list of principles that should be applied when the base ontology is mapped to other ontologies.

The most recent reference (ETSI, 2017) provides a standardized framework for the Smart Appliances Reference ontology (SAREF) that can be a basis for more specific extensions in particular domains. It resulted from the SMART study described in Section 1.3.3. The SAREF model provides building blocks that support separation and recombination of different parts in the smart appliances domain. The main objects are devices performing different services, typically household devices, which are able to communicate with each other and may be controlled via the internet (and thus can be seen as part of the IoT). In this document, the SAREF ontology is introduced and an equivalence mapping to the oneM2M base ontology from (ETSI, 2016) is defined. The aim of this ontology is to facilitate the matching of existing assets (such as standards, protocols etc.) in the smart appliances domain. To this end, the SAREF ontology contains a list of simple functions that can be combined such that the device can accomplish its tasks.

1.3.5 Smart City Architectures

As IoT focuses on interconnected objects, devices, machines as well as people, it is quite natural to investigate how it can be applied to not just make houses smarter but also cities. Typical questions involve how to improve efficiency of mobility, how to enhance safety, how to reduce energy consumption or how to handle sensitive data (e.g., in the context of elections).

The international technical working group on IoT-enabled smart city framework (IES-City Framework) is currently developing a consensus framework for smart city architectures (IES-City Framework, 2016). The main challenges in the development of smart cities are twofold: on one side, a common taxonomy has not yet been established which hampers a fruitful collaboration. On the other side, there exist many different smart city architectures that are hardly comparable. These challenges are also the main barriers that prevent development of efficient solutions and increase doubts among stakeholders potentially applying IoT in the field of smart cities. Thus, the main objective of the working group is to discover common structures in existing smart cities frameworks and promote development of standards.

Several smart city initiatives exist in the EU, involving Amsterdam (Amsterdam Smart City, 2017), Barcelona (Barcelona City Council, 2017), Berlin (Senate Department for Urban Development and the Environment, 2015), Dublin (Smart Dublin, 2017), Helsinki (HRI, 2017) and Manchester (Manchester City Council, 2017). In Austria, similar projects are currently running (Climate and Energy Fund, 2017).
1.3.6 International Telecommunication Union Telecommunication Standardization Sector (ITU-T)

The International Telecommunication Union Telecommunication Standardization Sector (ITU-T) has set coordination activities on aspects of IoT topics. They usually propose focus groups to provide a working environment for a quick development of standards for specific areas. They are initiated by technical study groups developing recommendations (in fact standards) for the international telecommunication area. ITU-T published a vision on the Internet of Things (IoT) first in 2005 (UIT, 2005) as part of a series of ITU reports on the internet. Beside others, two groups are of note.

Technically oriented, the ITU-T Focus Group M2M of the Study Group 11 “Signalling requirements, protocols, test specifications and combating counterfeit products” studied standardization activities for Machine-to-Machine (M2M) service layer specifications between January 2012 and December 2013. They identified a minimum set of common requirements of vertical markets, e.g., health-care, logistics, transport, utilities, etc. Five deliverables summarize current standardization activities, further gap analysis, enabled ecosystem and use cases for e-health, and requirements, architectural framework, APIs and protocols for the service layer (ITU, 2017a).

The Study Group 20: “Internet of Things, smart cities and communities” was established in June 2015 and coordinates all standardization activities within ITU-T concerning the Internet of Things (IoT). Initially the focus lies on IoT applications in smart cities and communities, resuming the experience of the ITU-T Focus Group on Smart Sustainable Cities (FG-SSC) of Study Group 5 “Environment, climate change and circular economy” which concluded its activities in May 2015. It includes machine-to-machine communications, ubiquitous sensor networks, end-to-end architectures, and interoperability mechanisms for IoT applications and datasets. The important objective of the study group is to address the impact of IoT technologies on urban-development challenges (ITU, 2017b).

1.3.7 AIOTI – Alliance for Internet of Things Innovation

The Alliance for Internet of Things Innovation (AIOTI) was launched by the European Commission (AIOTI, 2017) to develop and support the dialogue and interaction among the IoT stakeholders in Europe. It aims to build IoT ecosystems that address the current challenges of IoT including standardisation and interoperability.
2. **IoT STANDARDS AND REFERENCE MODELS**

The need for standardization as a basis for an efficient and successful use of IoT has been recognised and has led to a vast number of proposed standards and reference models. The Joint Technical Committee 1 (JTC 1) of ISO / IEC works on developing ICT related standards, including IoT related standards. Besides the already published ISO/ICE 29341 (ISO, 2015a) standard on management of devices, the Austrian Standards Institute (ASI) (Austrian Standards Institute, 2017) lists the following standards under development:

- ISO/IEC WD 30141 – Internet of Things Reference Architecture (IoT RA)
- ISO/IEC CD 20924 Information technology -- Internet of Things -- Definition and Vocabulary
- ISO/IEC FDIS 29341-30-2 Information technology -- UPnP Device Architecture -- Part 30-2: IoT management and control device control protocol -- IoT management and control device ISO/IEC FDIS 29341-30-1 Information technology -- UPnP Device Architecture -- Part 30-1: IoT management and control device control protocol -- IoT management and control architecture overview
- ISO/IEC FDIS 29341-30-10 Information technology -- UPnP Device Architecture -- Part 30-10: IoT management and control device control protocol -- Data store service
- ISO/IEC FDIS 29341-30-11 Information technology -- UPnP Device Architecture -- Part 30-11: IoT management and control device control protocol -- IoT management and control data model service
- ISO/IEC FDIS 29341-30-12 Information technology -- UPnP Device Architecture -- Part 30-12: IoT management and control device control protocol -- IoT management and control transport generic service
- ISO/IEC AWI 18574 Information technology -- Internet of Things (IoT) in the supply chain -- Containerized cargo
- ISO/IEC AWI 18575 Information technology -- Internet of Things (IoT) in the supply chain -- Products & product packages
- ISO/IEC AWI 18576 Information technology -- Internet of Things (IoT) in the supply chain -- Returnable transport items (RTIs)
- ISO/IEC AWI 18577 Information technology -- Internet of Things (IoT) in the supply chain -- Transport units
- ISO/IEC 29161 Information technology -- Data structure -- Unique identification for the Internet of Things
2.1 ISO 30141 – Internet of Things Reference Architecture (IoT RA)

The Joint Technical Committee 1 (JTC 1) of ISO / IEC is currently developing the ISO / IEC 30141 - Internet of Things Reference Architecture (ISO, 2016b), shortly IoT RA. This standard identifies and specifies a Conceptual Model (CM), Reference Model (RM), and Reference Architecture (RA) for IoT systems and has the goal to provide guidance to facilitate the design and development of IoT systems and promote open and common guiding architecture to establish seamless interoperability of IoT systems.

The Reference Architecture is described by different architectural views (systems, communications, information, functional, usage), in order to generically represent IoT systems. The standard provides various types of architectural elements (subsystem platforms, functional entities) as well as building blocks to develop application-specific architectures, as shown in Figure 5.

2.1.1 Conceptual Model (CM)

The Conceptual Model (CM) provides common UML structure and definitions for describing the concepts of and relationships among

- the IoT entities and domains,
- Identities (Identifiers),
- services, components, and endpoints,
- IoT Users,
- physical entities, digital entities, and IoT devices,
- security and privacy.

The model diagram in Figure 6 provides the big picture of all key IoT entities defined in this CM, their relationships and interactions.

![Figure 6 - Big Picture for IoT Concepts of the CM (ISO, 2016b, p. 67)](image)

The CM considers security and privacy implications using a systematic approach as shown in Figure 6, recommending identifying and mitigating threats and risks early on, in order to reduce support costs during the life of the product/solutions.
2.1.2 Reference Model (RM)

Figure 7 shows the architecture continuum from CM, entity-based RM, domain-based RM, to a number of different views of RA.

It is suggested to maintain evolutionary updates over time based on this continuum as an effective way of documenting the architecture descriptions. Figure 9 shows the relation between the two reference models, which are consistent with each other. Based on the previous high level IoT CM, an entity-based RM is described (see Figure 9, upper left corner), illustrating the interactions between the major entities using arrowhead lines. Security and
privacy elements (authentication, authorization, certificates, encryption, key management, logging and auditing, anonymization, pseudonymization) apply across the complete IoT system. The domain-based RM (see Figure 9, upper right corner) supports planning and organization of interconnected networks to model point-to-point links in or between IoT systems, both inter- and intra-domain, as well as with other systems and organizations.

Figure 9 – Relation between Concept Model (CM) and Reference Model (RM) (ISO, 2016b, pp. 70, 73, 77)

### 2.1.3 Reference Architecture (RA)

Based on the domain-based RM, the IoT RA is described by the following five views:

1. **IoT RA functional view**
The functional view as shown in Figure 10 describes a technology-agnostic view of the intra- and cross-domain functions (and dependencies) necessary to form the IoT system and support activities described by the user view.

**Figure 10 - IoT RA functional view** (ISO, 2016b, p. 41)

2. **IoT RA system view**

The system view as shown in Figure 11 describes the generic physical system components (devices, sub-systems, networks), the general architecture (structure, distribution of components, network topology) and a technical description of the components behaviour and other properties.

**Figure 11 - IoT RA system view** (ISO, 2016b, p. 44)
3. **IoT RA communications view**

The communications view as shown in Figure 12 describes the separated communication networks (proximity, access, services, user) and the entity-end-points they connect to. Each communication network can be described by means of different technologies and configurations, depending on the requirements of the IoT system.

![Figure 12 - IoT RA communications view (ISO, 2016b, p. 47)](image-url)
4. **IoT RA Information View**

The information view describes the format-agnostic type of information on a conceptual level, as shown in Figure 13. The structure (relations, attributes, services) of information is described based on Entity Relationship Diagrams (ERD) as shown in Figure 14.

![Figure 13 - Type of information related to domains (ISO, 2016b, p. 49)](image1)

![Figure 14 - Structure of information (ISO, 2016b, p. 49)](image2)
5. **IoT RA usage view**

The user view focuses on how the IoT system is developed, tested, operated and used from a user perspective. This is done by describing roles and sub-roles, as well as their activities and required services during the whole life-cycle of the IoT system. An example of applicable roles during the product life-cycle is shown in Figure 15.

![Figure 15 - Roles and activities during the IoT product life-cycle (ISO, 2016b, p. 58)](image)

The generic IoT RA becomes an application-/service-specific system architecture when all CM, RM and RA descriptions are tailored to a specific set of requirements.

### 2.2 Reference Architecture Model Industry 4.0 (RAMI 4.0)

The Reference Architecture Model Industry 4.0 (RAMI 4.0, IEC 65/XYZ/PAS) defines a structure for modelling and documentation of all aspects of any asset (and combination of assets) used within the manufacturing process.

In the object world of Industry 4.0, assets from the information world and the physical world are considered. The information world is divided into the model world (meta-documents, concepts, production plans, etc.), the state world (current state) and the archive world (recorded state & life cycle information). The physical world includes all physical products, installations, resources, hardware and software. People are also modelled as assets, are part of the physical world and participate in the information world.

---

4. Assets in the context of Industry 4.0 are whole installations or parts thereof, electronic modules, subsystems and systems, machinery, plants and networks, services, concepts and ideas, plans, archives and programs.

5. The algorithm itself belongs to the information world, but the executable program loaded to a system is part of the physical world.
### 2.2.1 Asset concept

Each asset has a lifecycle (commissioning, production, provision, usage, maintenance, repair, disposal) during which it serves its purpose. In regards to the information world, assets can be characterized as shown in Figure 17.

#### Figure 17 - Concepts of an RAMI 4.0 asset

<table>
<thead>
<tr>
<th>Model world</th>
<th>State world</th>
<th>Archive world</th>
<th>Physical world</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Meta-documents (standards, directives)</td>
<td>- Current measurements</td>
<td>- Life cycle documentation</td>
<td>- Products</td>
</tr>
<tr>
<td>- Technical documentation (functional diagrams, plant diagrams, product descriptions, procedural descriptions)</td>
<td>- Effective target values</td>
<td>- Events</td>
<td>- Resources</td>
</tr>
<tr>
<td>- Operative plans (production plans, project plans)</td>
<td>- Current configuration parameters</td>
<td>- Status histories</td>
<td>- Production systems (equipment items, sensors, actuators)</td>
</tr>
<tr>
<td>- Business process description</td>
<td></td>
<td>- Project histories</td>
<td>- IT systems, control systems (computer, programs, data carriers, cables)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Processes</td>
<td>- Cabinets, paper</td>
</tr>
</tbody>
</table>

#### Figure 16 - Structure of the RAMI 4.0 object worlds

- Model world
- State world
- Archive world
- Physical world

**Human world**

<table>
<thead>
<tr>
<th>Human</th>
<th>Human</th>
</tr>
</thead>
</table>

**Information world**

**Physical world**
This concept allows the definition of:

- the means by which an asset is actively presented, or made known, in the information system. Assets can be classified as unknown (in the information world), anonymously known (by type), individually known (by means of identification) or administered as an entity (assets that process objects of their own, administered via component managers in the information world).

- the state in an asset’s lifetime (“vita”)
  During its lifetime, assets are considered as types and instances. The type of an asset defines the sum of the properties which are characteristic for all instances of that particular asset. An instance is an identifiable asset that is characterized by the properties of a type.

- communication capabilities
  Assets can have communication capabilities in the physical world as well as in the information world and are classified in terms of presentation (see above) and communication capability (none, passive\(^6\), active\(^7\), I4.0-compliant service\(^8\))

- virtual representations
  This encompasses all data and properties which characterize an associated asset or represent important information for other assets

- technical functions
  The description of the functions of an asset representing its actual “technical” functionality.

### 2.2.2 Reference architecture model

The RAMI 4.0 model establishes a terminology and structure for defining assets along three axes as shown in Figure 5, covering

- the architecture axis (“Layers”), with six layers to represent information that is relevant to the role of the asset (IEC 62264-1, IEC 61512-1), covering\(^9\) properties, system structures and functions in regards to
  - Business,
  - Function,
  - Information,
  - Communication,
  - Integration, and the
  - Asset;

---

\(^6\) e.g. RFID, barcode
\(^7\) The asset actively identifies itself on making contact with the network and logs in to participate in communication.
\(^8\) An component that is connected to the information system (passively or actively) and provides I4.0 compliant communication based on a service-oriented architecture (SOA).
\(^9\) Layers do not have to have content.
- the “Life cycle & value stream” axis to represent the lifetime of an asset and the value-based process (IEC 62890), used to describe an asset at a particular point in time during its lifetime;
- the “Hierarchy levels” axis for assigning functional models to specific levels, based on the reference architecture model for a factory along the lines of IEC 62264-1 and IEC 61512-1 (integrating enterprise IT and control systems).

![Figure 18 - Reference architecture model Industry 4.0 (RAMI 4.0)](image)

2.3 Industrial Internet Reference Architecture (IIRA)

This technical report (IIC, 2017) describes the Industrial Internet Reference Architecture (IIRA), for Industrial Internet of Things (IIoT) systems. It further specifies a framework, the Industrial Internet Architecture Framework (IIAF), to aid in the development, documentation and communication of the IIRA. It mainly focuses on different viewpoints using standard-based frameworks.

The report is authored by the Industrial Internet Consortium, an open membership organization with currently about 260 members. It was formed in 2014 by AT&T, Cisco, General Electric, IBM and Intel to accelerate the development of interconnected machines and devices and intelligent analytics.

To address several needs like the coverage of the whole lifecycle and the high complexity, the ISO/IEC/IEEE 42010:2011 is used to define the IIAF.
2.3.1 Industrial Internet Reference Architecture

The Industrial Internet Reference Architecture (IIRA) documents the outcome of applying the Industrial Internet Architecture Framework (IIAF) to Industrial Internet of Things systems (IIoT systems). It organizes the most important architectural concerns along with their stakeholders in viewpoints to get an abstract architectural representation.

2.3.2 Industrial Internet Viewpoints

There are four IIRA viewpoints: business viewpoint, usage viewpoint, functional viewpoint and the implementation viewpoint. Those have been designed after analysing various IIoT use cases developed by the IIC and elsewhere. Those four viewpoints form the basis for a detailed analysis of the individual sets of IIoT system concerns. They could be extended by architects to include special system requirements. This concept is designed to offer a framework for system designer to think iteratively through important common architectural issues in IIoT system creation as shown in Figure 20.
Business Viewpoint
The business viewpoint deals with the business visions of the stakeholders. By designing an IIoT System as a solution for business problems, basic items like business value, expected return of investment, cost of maintenance and product liability are to be evaluated. This is done by using a vision and value driven model, focusing on key objectives. The fundamental capabilities, a high level specification of the essential ability of the system to complete specific major business tasks, are also taken in account.

Usage Viewpoint
The usage viewpoint is concerned with how an IIoT system realizes the key capabilities identified in the business viewpoint. It takes care of the key capabilities identified in the business viewpoint. It is using activities to describe how the system is used. Those are described using tasks which are carried out by a party assuming a role. A functional map is used to describe the relation between a task and functions or functional components. An implementation map describes the components a task relies on for its execution. An activity is defined as a specific coordination of tasks including elements like triggers, workflow, constraints etc.

Functional Viewpoint
The functional viewpoint deals with the functional components of an IIoT system, focusing on the structure and interrelation, the interfaces and interactions between them and the relation and interaction with external components.
To achieve this, a typical IIoT System is decomposed in five functional domains: control domain, operations domain, information domain, application domain and business domain. Data and control flows take place in and between those functional domains.
Implementation Viewpoint
The implementation viewpoint focuses on the technologies which are needed to implement the functional components prescribed in the functional viewpoint, including their communication schemes and their lifecycle procedures. It also takes into account the activities which are specified in the usage viewpoint and the system capabilities specified within the business viewpoint (cost, go-to-market time, business strategies, etc.).

Beside the general architecture and a technical description of the components, the implementation view also describes an implementation map of the activities identified in the usage viewpoint and an implementation map of the key system characteristics.

2.4 Internet of Things Architectures
While the term IoT getting famous and frequently used, commonly agreed definitions are still missing. However, such a common language would be of great benefit especially when facing many different fields of application. Different approaches exist; we here focus on two well-founded models that are frequently used.

2.4.1 The IoT-A Reference Model
IoT-A was an EU lighthouse project in the seventh Framework Programme (FP7), running from beginning of September 2010 to end of November 2013, involving partners from Belgium, Finland, France, Germany, Italy, Switzerland and the United Kingdom.

The main motivation behind this project was the fact that through IoT very different networks become connected. The network providers are mainly utility companies, in particular energy, while applications in other fields such as logistics and health are increasing. Despite that fact, a common language is still missing. Thus, consequences of connecting such networks are often unclear and might amplify existing risks as well as cause new ones.

Further, IoT involves objects talking to each other without user consent (or even interaction) which increases the uncertainty about existing risks and consequences. Thus, there is a need for education to raise awareness about potential risks. Still, many people will be affected by IoT while not realizing it. This might also cause privacy problems when storing and analysing data.

Considering all these aspects, the goal of IoT-A was to define a set of key entities and afterwards to construct a reference model describing the most fundamental concepts and relations between these entities. Based on this general reference model, specific reference architectures can be built for a concrete use case. The identified Architectural Reference Model (ARM) for the internet of things has been presented in (Bassi et al., 2013). Additionally, guidelines on how to apply the constructed ARM to generate concrete architectures are given.

The IoT Reference Model (RM) provides concepts and definitions on which the actual IoT Architecture Reference Model is built. The defined RM consists of several interacting sub-models with the IoT Domain Model as its core. It defines the main concepts of IoT including their attributes and thus provides a common language for the constructed architecture. Based on this, the information model is
built that defines the structure of IoT related information. Both components then contribute to the IoT functional model that identifies groups of functionalities of the IoT. One of these groups contains the trust, security and privacy model (TSP) that is responsible for ensuring security and privacy of IoT-A-compliant systems. However, it seems that security is not a central concern. In short, the RM provides terminology, basic concepts, models and relationships for the Architecture Reference Model.

2.4.2 The AIOTI Architecture
In 2016 the Alliance for Internet of Things Innovation (AIOTI, cf. Section 1.3.7) proposed a High Level Architecture (HLA) for IoT systems (AIOTI, 2016). The HLA gives recommendations on the Domain Model (derived from the IoT-A Domain Model) and the Functional Model. The latter describes functions and interactions in the considered domain. The AIOTI WG3 recommends building architectures based on ISO 42010 that defines the terms and concepts in use.

2.5 ITU-T Y.2060 Overview of the Internet of Things
In 2012, the International Telecommunication Union (ITU) published recommendation Y.2060 giving an overview of the internet of things (ITU, 2012). This document identifies characteristics and requirements for IoT and provides an IoT reference model. It aims to provide the basis for future standardization.

2.5.1 Terms and Definitions
In their document ITU defines IoT as a “global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies” (ITU, 2012). In this context a “thing” is characterized by its capability of being identified and integrated into a communication network. In that context, IoT is seen as third dimension (“thing”) to ICTs already having dimensions “time” and “place” (see Figure 1 in (ITU, 2012)). Generally, things are either part of the physical world or of the information world and correspondingly called physical or virtual.

Further, a device is defined as “a piece of equipment with the mandatory capabilities of communication and optional capabilities of sensing, actuation, data capture, data storage and data processing” (ITU, 2012). It is characterized by its ability to collect information and afterwards provide it to the information and communication network. Especially in IoT it is a necessary requirement for a device to support communication capabilities. Devices are categorized as follows:

- **Data-carrying devices** indirectly connect a physical thing with the communication networks
- **Data-capturing devices** read or write and interact with physical things, either directly or indirectly.
- **Sensing and actuating devices** may convert information about the environment into digital electronic signals as well as digital electronic signals into operations.
- **General devices** have processing and communication capabilities. These include equipment and appliances for different IoT application domains (e.g., industrial machines or smart phones).
Equipped with these terms and definitions, a reference model is described.

### 2.5.2 Fundamental Characteristics of IoT
The following fundamental characteristics of IoT have been identified in (ITU, 2012).

- **Interconnectivity**: anything can be interconnected with the global information and communication infrastructure
- **Things-related services**: IoT enables providing things-related services (subjected to constraints due to e.g. privacy issues)
- **Heterogeneity**: IoT devices differ with regard to their hardware platforms and networks
- **Dynamic changes**: states of IoT devices as well as their environment change dynamically
- **Enormous scale**: the number of devices communicating with each other is huge and so is, accordingly, the amount of generated data

### 2.5.3 High-level Requirements
Amongst others, the following key high-level requirements relevant for IoT have been identified in (ITU, 2012).

- **Identification-based connectivity**: the connectivity between a thing and the IoT is based on the thing’s identifier
- **Interoperability**: heterogeneous systems need to be able to exchange information
- **Autonomic services provisioning**: it is necessary to be able to provide automatic communication and data processing in order to automate services
- **Security**: due to the high connectivity confidentiality, authenticity and integrity of both data and services are threatened and different security policies need to be integrated
- **Privacy protection**: private information about users contained in the collected data need to be protected (especially during transmission, storage and processing of data)

### 2.5.4 Reference Model
The IoT reference model proposed in (ITU, 2012) consists of four different layers:

- The **Application layer** contains IoT applications.
- The **Service support and application support layer** can be divided into two parts, namely generic and specific support capabilities. While generic capabilities are general and can be used by different applications (e.g., data processing or storage), specific capabilities provide support for particular applications only.
- The **Network layer** can be divided into two parts, namely network capabilities and transport capabilities. While the former supports network connectivity, the latter provides connectivity for the transport of services and information.
- The **Device layer** can be divided into two parts, namely device capabilities and gateway capabilities. Device capabilities include direct and indirect interaction with the communication network (including gathering and receiving information), ad-hoc networking and sleeping
mechanisms. The gateway capabilities on the other hand include support of multiple interfaces (including wired and wireless technologies) as well as protocol conversion.

All these layers are associated with management capabilities and security capabilities. While the management capabilities cover the fault, configuration, accounting, performance and security (FCAPS) management classes, the security capabilities include authorization, authentication, access control and data confidentiality. Both groups contain general and specific capabilities.

2.6 The ISO 31000 Family
In 2009, the International Standards Organization (ISO) published the international standard for risk management ISO 31000:2009 (ISO, 2009a) which is based on national approaches from Australia and New Zealand AS/NZS 4360:2004 (Joint Technical Committee OB-007 et al., 2004) as well as from Austria ONR 49000:2004 (Österreichisches Normungsinstitut, 2004). This standard evolved to a global and widely accepted leading standard until today. Due to the explicit generic approach the authors have been following, this standard can be ubiquitously applied on every kind of organization, regardless of its type, perspective or size (ISO, 2009b). The ISO 31000 is organized as a standard family, consisting of several components which focus on different aspects (ISO, 2009a):

  All terms and definitions were subsumed. A new edition is planned for the end of 2017.
  This standard provides the fundamental principles and generic guidelines for risk management. A new edition with quite more content is expected at the end of 2017.
  This component provides guidance for implementation of ISO 31000 risk management structures. It discusses concepts and principles of the framework in detail.
  This part of the standard family introduces selected procedures for risk assessment and discusses possibilities of their application.
- ISO 31020 – Managing Disruption Related Risk (Draft, 2014)
- ISO 31021 – Managing Supply Chain Risk (Draft, 2015)

2.6.1 ISO 31000 – A Generic Risk Management Approach
A distinct characteristic of ISO 31000 is the two-tier structure with a risk management framework on the one hand, and the operative risk management process on the other hand (cf. (ISO, 2009a)). These two life cycles are linked by the activity “implementing risk management” in the framework. The risk management framework represents the top down approach, ensures the consistent embedding of risk management in the organization based on a quality management perspective. It follows an iterative and continuous improvement cycle according the general plan – do – check – act (PDCA) cycle. On the other hand, the operative risk management process supports the bottom-up approach, which puts the
concrete risks in an organizational context, assesses and treats them. During the whole risk management process, two guiding sub-processes ensure communication and consultation as well as monitoring and review. The first one interacts with the stakeholders, the latter enables performance measure. Figure 21 visualizes the components of both cycles and reflects the relationship as described above (Schauer et al., 2015, p. 18f).

The ISO 31000 postulates eleven principles (International Organization for Standardization (ISO), 2009, p. 7f), interpreting risk management as an interdisciplinary task on all levels which has to be transparently integrated in consisting overall organizational structures. These eleven principles lead in the risk management framework, consisting of five components (Austrian Standards Institute, 2010, p. 14ff; Schauer et al., 2015, p. 13f) (Schauer et al., 2015, p. 13f) which can be seen on the left side of Figure 2.

1. **Mandate and commitment**
   An explicit and strong commitment of the management is a prerequisite for a successful implementation of effective risk management structures. A rigorous strategic planning ensures the consistent embedding in the organizational structure. The integration is enforced on a strategic level
and mainly affects organization’s culture, commitment of stakeholders, availability resources and compliance (Austrian Standards Institute, 2010, p. 15f).

2. **Design of framework for managing risk**
   The risk management framework must be designed consistently in the internal and external context of the organization. Additionally, it emphasizes the interaction with the stakeholders. A risk management policy defines the objectives for risk management in written form. A risk management plan enables the integration of risk management into organizational processes and thus implements the risk management policy. Furthermore, responsibilities are defined and resources are required. Finally, internal and external communication and reporting are set up (Austrian Standards Institute, 2010, p. 16ff).

3. **Implementing risk management**
   The organization enforces the required activities in line with the implementation of the risk management framework, i.e., applying of the risk management policy, conducting the risk management process, fulfilling the compliance requirements, ensuring decision making, interacting with stakeholders and communicating in general. According to the risk management process, the defined risk management plan is conducted on all relevant levels in all functions of the organization (Austrian Standards Institute, 2010, p. 18f).

4. **Monitoring and review of the framework**
   Indicators, progress measurement of conducting the risk management plan, risk reports and reviews of design and effectiveness of the applied risk management measures implement an ongoing effectiveness monitoring of the framework (Austrian Standards Institute, 2010, p. 19).

5. **Continual improvement of the framework**
   A continuous improvement process ensures an iterative development of the risk management framework, the risk management policy, and the risk management plan – in fact all levels of implementation (Austrian Standards Institute, 2010, p. 19).

The following step after establishing the risk management framework is focused on setup of the risk management process, hence the operative implementation of risk management. The necessary process activities (Austrian Standards Institute, 2010, p. 19ff) (Schauer et al., 2015, p. 14ff) are illustrated on the right side of Figure 2.

1. **Establishing the context**
   The organization embeds the risk management process into existing structures and specifies the aspects defined in the risk management framework in more detail and process-oriented. It subsumes the external environment, internal and external context or influence factors, and methodological prerequisites in order to consistently set up the environment.

2. **Risk assessment**
   Risk assessment in sense of the ISO 31000 standard subsumes the complete process of risk identification, risk analysis and risk evaluation. During the first phase risk identification, the organization identifies sources of risk, areas of impacts, risk events and their consequences (Austrian Standards Institute, 2010, p. 15f).
The risk analysis phase concentrates on the causes and sources of risk, and thus on the classical attributes potential consequences and likelihood. The risk criteria defined in the risk framework cycle are applied. A reasonable modelling of the results, especially the amount of risk considering all of the influence factors is the main objective of this step. The uncertainty and diversity of the expert’s opinion need to be documented, because determining only one numerical value is not sufficient in many cases (Austrian Standards Institute, 2010, p. 24) (Schauer et al., 2015, p. 16). The third component of risk assessment is risk evaluation. It prepares the results of the risk analysis and subsequently develops a prioritization for the risk treatment. Hence, the amount of risk determined before is compared to the defined risk criteria. This comparison reveals the necessity for a risk treatment. The evaluation considers the generic circumstances, the risk attitude of the organization and the risk tolerance of the stakeholders (Austrian Standards Institute, 2010, p. 23) (Schauer et al., 2015, p. 16).

3. Risk treatment
The selection and implementation of one or more options for modifying risks follows a cycle process, in which the risk treatment is decided, the residual risk is determined, a new risk treatment measure is designed and its effectiveness assessed. ISO 31000 suggests seven fundamental risk treatment strategies, which are not mutually exclusive: avoiding, taking, removing the source, changing the likelihood or the impact, sharing, or retaining the risk (Austrian Standards Institute, 2010, p. 25) (Schauer et al., 2015, p. 16). A risk treatment plan documents how and why the defined measures need to be implemented. Furthermore, it defines order, priority, need for resources, responsibility, performance measure, time and implementation plan, and suggests monitoring measures (Austrian Standards Institute, 2010, p. 25f) (Schauer et al., 2015, p. 16f).

4. Communication and consultation
This guiding sub-process deals with the communicative interaction from and to the stakeholders. A communication plan defines the corresponding activities, and decides about causes, impacts and treatments (Austrian Standards Institute, 2010, p. 20f) (Schauer et al., 2015, p. 17).

5. Monitoring and review
A core element is monitoring and review by performing regular and situation-based checks of all aspects and general performance measures during all phases of the risk management process. The main part here is the appropriateness and effectiveness, as well as the further development based on new findings or as a reaction to the changing circumstances (Austrian Standards Institute, 2010, p. S26f) (Schauer et al., 2015, p. 17).

One advantage of ISO 31000 is its fundamental structure. The division of risk management framework on the one side and the operative risk management process on the other side reveals several connecting points across different levels of an organization. The generic systemic approach enables an application also for small organizations by selecting the appropriate aspects. Hence, it is possible for them to adapt the appropriate costs for risk management. The ISO 31000 provides a reliable process which is easily and robust applicable on each task. The process-oriented holistic structure supports the important integration in a management system, especially of others propagated by ISO. Additionally, the ISO 31000
contributes to a consistent terminology of risk management (Schauer et al., 2015, p. 18f). For IoT aspects, ISO 3100 should be considered due to its significance and broad acceptance when it comes to risk management.

### 2.6.2 ISO 31010 – A Collection of Risk Assessment Techniques

This substandard of the ISO 31000 family substantiates the process activities introduced in ISO 31000 by discussing several possibilities of implementation and determining influence factors. Additionally, ISO 31010 provides guidance on an optimized selection and application of specific systematic risk assessment techniques. Hence, this standard can be interpreted as a guideline how to implement the requirements of the ISO 31000 standard in practice by summarizing a variety of distinct risk assessment techniques for application within the different risk management phases or risk life cycle stages. The risk assessment techniques can be differed by (ISO, 2009b, p. 21):

- the applicability within the different process activities determining the technique type,
- the complexity of the problem and the analysing method,
- the nature and the degree of uncertainty based on the information available,
- the extent of the required resources (time, expertise, data, cost), and
- the ability of the method to generate quantitative output.

Thereby, 31 techniques are categorized and roughly assessed in this way. Every method is narratively described by providing a short overview of the method, discussing their application, determining necessary inputs, documenting the formal process, defining the outputs and concluding with strengths and limitations.

The advantage of ISO 31010 is that it structurally describes different risk assessment techniques and that it provides guidance for which risk process activities and which purpose it can be deliver useful results. It can be applied as a catalogue. The descriptions are rather rough and not formalized, so that specific literature needs to be consulted when analysing details. Nevertheless it provides a good starting point defining appropriate risk assessment methods when having certain application scenarios in mind. All these risk assessment techniques should be taken into consideration to develop IoT risk scenarios.

### 2.7 The ISO 27000 Family

The International Standards Organization (ISO) (International Organization for Standardization (ISO), 2017) and the International Electrotechnical Commission (IEC) (IEC, 2017) summarized all information security related best practice recommendations and standards to the information security management system (ISMS) standards to design a management system for information security. The objective is to manage information risks by information security means. The main part evolves originally from the British Standard BS 7799 from 1995 (part 1) and 1999 (part 2) (British Standard Institute, 1995), which was published as ISO 17799:2000 (Standardization and Commission, 2005) as first international standard in this context. Meanwhile, the ISO/IEC 27000 family consists of a wide range of specific security management standards (IsecT Ltd, 2017):
2.7.1 ISO 27001 and ISO 27002 – Guidelines for Information Security

The core of an information security management framework are spanned by both ISO/IEC 27001 (ISO, 2013a) – subsuming all the certification requirements – and ISO/IEC 27002 (ISO, 2013b), which discusses the implementation possibilities to address these postulated aspects. Hence, the certification standard is restricted to define distinct general objectives to address information security from a broader top-down perspective. It is structured in the following subsections (ISO, 2013a, p. 2ff)

- Context of the organization
- Leadership with commitment, policy, roles, responsibilities and authorities
- Planning subsuming actions to address risks and opportunities, risk assessment and treatment
- Support with resources, competence, awareness
- Communication

  All terms and definitions used in the ISO/IEC 27000 family were introduced here.
  This standard reflects all requirements on ISMS. It evolved from part 2 of BS 7799.
  It gives recommendation for security controls. This part was originally derived from part 1 of BS 7799 and ISO 17799.
  This standard document provides an implementation guideline for the requirements of ISO 27001.
- ISO/IEC 27005 – Information security risk management (last version 2011, refers to ISO 31000)
- ISO/IEC 27006 – Requirements for bodies providing audit and certification of ISMS (2015)
- ISO/IEC 27007 – Guidelines for information security management systems auditing (2011)
  focusses on the management system perspective.
- ISO/IEC 27010 – 27019 contains sector-specific sub standards; e.g., finance, telecommunications, security governance, cloud computing, personal information, energy industry, etc.
- ISO/IEC 27030 – 27044 cover technical issues of information security e.g., business continuity, cybersecurity, network security, application security, information security incident management etc.
- ISO 27799 Health informatics (2016)
• Documented information with aspects of creating, updating, and controlling
• Operation with planning and control, risk assessment and treatment
• Performance evaluation
• Internal audit
• Management review
• Improvement in a continuous way

The Annex A lists different 14 security control clauses collectively containing 35 main security categories and 114 controls (ISO, 2013a, p. 10ff):
1. Information Security Policy
2. Organization of Information Security
3. Human Resource Security
4. Asset Management
5. Access Control
6. Cryptography
7. Physical Environmental Security
8. Operations Security
9. Communications Security
10. System Acquisition, Development and Maintenance
11. Supplier Relationships
12. Information Security Incident Management
14. Compliance

This structure reflects the structure of Annex A of the requirements and discusses in ISO/IEC 2002 appropriate control implementations which are able to meet the defined objectives in general, additionally giving other relevant information. The organizations need to find a suitable way of implementing appropriate control activities following the standardized control objective. This might be different for the organizations depending on their size, branch, legal entity, degree of complexity and requires know how to find a balance between effort, cost and effectiveness.

The overall objective when implementing these controls is to set up a sustainable management system for information security in order to streamline all information security activities of an organization and to ensure a consistent approach. It defines a sector-independent set of minimal quality criteria for information security. Hence, the certification is useful in order to get a transparent seal of approval by independent auditors generating confidence of the customers, minimizing processing costs, reducing risks and improving competitiveness. ISO 27001 is widely accepted across all sectors operating information and communication technology means and recognized as THE comprehensive standard for information security management systems. Consequently, these standards also set up core topics for
information security for IoT challenges, even though some aspects which were established since the mid-1990s evolved and further became more important for distinct IoT requirements.

2.8 NIST SP800-160 – Systems Security Engineering

Starting with an initial draft in 2014, the National Institute of Standards and Technology (NIST) announced in 2016 a first draft of its Special Publication SP 800-160, entitled with Systems Security Engineering (Ross et al., 2016). This publication was announced as a “new guidance on how to judge the cybersecurity of devices in the Internet of Things” and propagating a consequently engineering-driven perspective in system security design of IoT devices (Federal Times, 2016).

The SP 800-160 is structured as described in the following. After the introduction and definition chapter (chapter 1), the second section discusses in detail system engineering specialties and fundamentals and the security perspective and concepts. Additionally it proposes a systems security engineering framework. The third chapter enhances the international systems and software engineering standard ISO/IEC/IEEE 15.288 (ISO, 2015b) with security engineering considerations, contributions, and extensions compared to the standardized system life cycle process. Additionally supporting appendices provide detailed information for the effective application of the concerned activities and tasks suggested by the SP 800-160.

The main focus of this contribution is to strengthen the cybersecurity of the devices connected to the internet. It implies the consequent application of systems security engineering methods, practices, and techniques during systems and software engineering activities addressing the growing complexity. It covers all types of systems along the life cycle stages:

- New systems;
- Reactive modification and planned upgrades of systems;
- Dedicated or special-purpose systems, either security-dedicated or security-purposed systems or high-confidence, dedicated-purpose systems;
- System-of-systems;
- Evolution systems; and
- Retirement systems.

Each one of the components needs to be assessed against a distinct level of trustworthiness in order to increase their ability to persist penetrations from external attacks. The second aspect is to consider the life cycle of each device and the impact on the stakeholders. Figure 22 shows the system life cycle processes and their application across all stages. It is structured into the four process categories

- Agreement processes
- Organization-project enabling processes,
- Technical management processes, and
- Technical processes.
Each life cycle process description follows the same format introducing purpose, outcomes, detailed activities and tasks with elaboration, references and related publications to ISO/IEC/IEEE 15288 sections other standard publications. This overall structure helps stakeholders and developers to apply well-established international systems engineering standards, tailor and implement the necessary processes also in concurrently applied tasks performed by sub-teams, develop required qualifications to design the devices, all the way from the requirements definition to the business analysis. The overall objective is to make the devices as resilient as it need to be seen from a stakeholder needs perspective, to develop an assurance level for the different application areas of the IoT devices, see (Federal Times, 2016) and (Ross et al., 2016, p. ii). The publication is also going hand-in-hand with an IoT cyber-security guideline issued by the Department of Homeland Security of the US government (U.S. Department of Homeland Security, 2016).

### 2.9 NIST SP800-183 – Networks of ‘Things’

Other activities of the National Institute of Standards and Technology (NIST) aim on the categorization of basic building blocks for a network of “things” giving an underlying and fundamental understanding of
IoT. The special publication SP800-182 entitled with “Network of Things” (Voas, 2016) defines five core primitives of typical distributed systems which allows to sense, compute, communicate and actuate. It presents a vocabulary in order to get a better understanding of IoT. This postulated generic approach categorizes the function of IoT elements addressing the rapid developments in this area. Internet of things (IoT) is seen here as an instantiation of a network of things (NoT), other variants of a NoT are e.g., local area network (LAN), social media network, or a sensor network. In defining this abstraction level, a differentiation of different IoTs is possible. By categorizing the basic building blocks of a network, a further differentiation of NoTs is a consequent extension of this concept.

It enables analysts to apply a clearer distinction between the different “things”. The aforementioned primitives of NoTs are (Voas, 2016):

- **Sensor**
  An electronic utility measures physical properties like temperature, acceleration, weight, sound, location, presence, identity.

- **Aggregator**
  This is a software implementation which transforms raw data into aggregated data. Aggregators could be further characterized as cluster or sensor cluster for grouping issues and weight reflecting the impact of data on an aggregator’s behaviour.

- **Communication Channel**
  It represents the medium by which the data is transmitted from the sensors to the aggregators.

- **External Utility (eUtility)**
  An eUtility is a software or hardware product or service, and thus rather broad to subsume future services. It could execute one or more aggregator implementations.

- **Decision trigger**
  A decision trigger creates final results to fulfill purpose, specification, and requirements of a specific NoT, often represented as if-then-clauses.

There may rarely exist NoTs not containing all of these basic building blocks. Figure 3 shows an example of a possible primitive’s network. For all primitives a set of basic properties, assumptions, recommendations and general statements are listed.
The model additionally introduces six elements which determine the degree of trustworthiness that a NoT can provide (Voas, 2016):

- Environment as the universe, essentially the operational profile the primitives operate in, especially for sensors and aggregators
- Cost in terms of money and time for building and operation
- Geographic location where a sensor or eUtility operates in
- Owner of the primitives in terms of persons or organizations
- Device Identity as a unique identifier for each primitive
- Snapshot as instant in time

Additional considerations and scenarios concerning reliability and security conclude the special publication SP800-183. The five primitives and six elements impact the behaviour of a NoT providing some kind of a design catalogue for IoT-based technology (Voas, 2016).

2.10 ISA/IEC-62443

The IEC 62443 series of standards (ISA, 2016) is a joint development by the ISA99 committee and IEC Technical Committee 65 Working Group 10 (TC65WG10). The goal is to design cybersecurity robustness and resilience into industrial automation control systems (IACS). As far as possible IEC 62443 tries to use existing and established standards for general purpose information technology systems (mainly ISO/IEC 27000 series), while addressing the special issues and challenges for industrial control systems. One of the major differences is that cybersecurity risks within IACS may have Health, Safety or Environment (HSE) impact. Therefore every response and cybersecurity measure should be coordinated and
integrated into existing risk management practices. The standard series is structured in four areas with multiple parts per area.

![Figure 24 - 62443 Elements (ISA, 2016, fig. 1)](image)

Parts in the general area introduce common concepts, models and terminology used throughout the complete standard, security conformance metrics and a potential security life-cycle. The second area “Policies and Procedures” describe requirements and implementation of a cyber security management system, based on the ISO 27000 series, in IACS environments, patch management and requirements for suppliers. The parts in the system area present security technologies for IACS systems, security risk assessment and system design methods and system security requirements, based on security levels. The final “components” area contains requirements for the product development and guidance on how to breakdown high-level security requirement to IACS components.

The standard series is not yet completely available; some parts are still in draft status.
3. IoT HIGH LEVEL RISKS
Taking a step back, it becomes transparent that all prevailing IoT challenges share common high level risks, based on what kind of data is being collected, processed and transmitted, cyber-physical capabilities of the devices, their location and accessibility and the overall technical and organizational level of information security of the IoT ecosystem.

3.1 IoT Devices May Compromise Privacy
A lot of use cases have the potential to create privacy issues, especially if the design and implementation of the IoT ecosystem didn’t account for privacy from the beginning. These issues can arise from technological choices (e.g., Bluetooth 4.2 protocol privacy features (Open Effect, 2016)), incorrect usage of encryption or protocol features, insecure software design and development and general business considerations on the collection and usage of personally identifiable information.

3.2 IoT Devices are Poorly Secured and Vulnerable to Attack
Typically investors and technology start-ups are not concerned with the security of their products, but primarily with getting their products to market quickly. On the customer side there are also trade-offs between product usability and security, as shown by thousands of digital surveillance cameras and other IoT products with default usernames and passwords. The initial inconvenience of having to manually change the default credentials of a product may lead to serious implications, if not properly addressed technically (e.g., forced change of login credentials at the setup process, password complexity requirements, etc.).

3.3 IoT Devices May Introduce Safety Hazards
With the US Government Aurora Generator Test in 2007 a cyber-attack was demonstrated to be able to cause a generator to self-destruct, exposing millions of security issues within the electronic industry (Meserve, 2007).
But not only blind destruction can lead to safety hazards – imagine the malicious manipulation of automated assembly machines for production (e.g., producing car chassis with missing welding points), energy and smart grid applications or transportation systems in general.

3.4 IoT Devices May be Misused to Launch DDoS Attacks
With the historically largest botnet attack consisting of IoT devices in October 2016 (Krebs, 2016), the potential of massive DDoS attacks has been shown. Investigations showed (Herzberg et al., 2016) that even a relatively small set of botnet devices (~50,000 devices, mostly CCTV cameras) can have a global impact on companies such as Twitter, Amazon, Tumblr, Reddit, Spotify, Netflix and many others.
3.5 UAVs/Drones Are Used as a Platform for IoT Device Reconnaissance
While security research has already shown the potential of drones to be used as platforms for large scale RF\textsuperscript{10} protocol reconnaissance, it can be assumed that various public IoT databases covering geolocation maps will emerge during the next years supporting the geo-discovery of IoT services.

3.6 IoT Devices May Interfere With Critical National Infrastructure
Due to the increased connectivity and sharing between national and public IoT infrastructures as well as the continuous integration of IoT components into critical national infrastructure (e.g., smart grid, transportation, facility management, etc.), the potential of interferences between the ecosystems rises.

The EU directive 2016/1148 on security of network and information systems (NIS) (EU, 2016) requires security assurances across different sectors, listing providers of digital services (online marketplaces, search engines, cloud computing and internet service providers), energy (electricity, oil and gas), transportation (air, rail, ship, road), bank and finance, healthcare, water and digital infrastructure.

\textsuperscript{10} Radio Frequency as well as other frequency bands of the electromagnetic spectrum used for communication purposes (e.g. GSM/LTE, WIFI, GPS, GPRS/CDMA, etc.)
4. CATEGORIZATION OF IoT-RELATED RISKS

The Risks identified in the last section can be categorized with the help of risk matrices. This representation allows comparison of the different risks regarding their impact and their likelihood of occurrence. This ranking of risks also allows a prioritization in the sense that risks with both a high impact and a high likelihood of occurrence are the most dangerous ones and thus need to be dealt with first.

In this section we first give a short summary on risk matrices before applying this tool to the high-level IoT risks identified earlier.

4.1 Risk Matrices

The risks should be visualised in the most common way of a risk matrix. The two-dimensional description presents the likelihood of occurrence (in quantitative classes) on the x-axis. The y-axis describes the impact or the loss depicted by the impact classes. In order to consistently achieve this matrix presentation the following prerequisites must be considered.

Likelihood class

Accordingly, the likelihood for occurrence is qualitatively assessed as well. A narrative description in order to choose the right likelihood class is necessary. The scale might be adjusted according the damage assessment for all risks. The amount and names should be the same for all damage indicators. A possible classification could be frequency per year or – perhaps more intuitive – “one time in x years”. However, for many risks only plausibility estimation is applicable.

Damage Indicators

For further risk analysis, especially for the assessment and a compatible presentation it is useful to apply a restrict categorization structure. The damage should be divided in specified groups according to the corresponding protection needs. Thus, the damage indicators can be defined as follows:

- Person
- Environment
- Economy
- Society

These four damage indicators provide a sufficient categorization for further analysis. It is feasible to define subgroups in order to describe partial aspects which can be affected by a risk event. By applying these damage indicators the damage potential can be estimated more accurately for the different use case areas.

The damage indicator Person can be described by possible fatalities, or causalities/patients who need support longer than 24 hours, e.g. through treatment in hospital or ambulant first aid. Other persons needing support up to 24 hours and people in need for food, water, accommodation, etc. are other influencing factors.
The damage indicator *Economy* describes damages which affect water or air quality, use of space or land by agriculture, industry, and society as well as the ecosystems related to biodiversity, change of gene pool or the like.

The damage indicator *Environment* subsumes all kinds of pecuniary loss. It describes primary damages, which were caused directly by the risk event, and the cost for reparation and reconstruction. Additionally, it includes secondary damages like losses in value and image, cascading effects, restriction of the supply chain or the complete supply chain network; as well as the reduction of the economic performance, i.e., restriction for the production of goods and services.

Finally, the comparatively broad damage indicator *Society* includes any impacts on the public confidence in national’s ability to act and the societal instruments, e.g., law and public order and domestic security, outbreak of panic; on the daily life, e.g. restriction of communication, mobility, means of payment, restriction of the territorial integrity; on the individual’s life, e.g., shortage of water and food; or on the societal security like religion, cultural identity, migration, political impacts etc. Furthermore, damages or losses of cultural assets as well as in general the resilience of public institutions were considered for fulfillment of citizen’s demand.

**Impact classes**

For the assessment of the impact, a scale must be defined which is applied for each damage indicator. This is done mostly in a qualitative way, which means that the impact class is described in written form with as distinct parameters as possible. It is advisable to define explicit threshold values in order to decide for an impact class. The threshold value can be different for each damage indicator, but it should be consistently applied over all risks. An even number of assessment classes can address the tendency to mediocrity, i.e. there is a relative frequency of the assessor to choose the category located in the middle of the scale with odd amount of impact classes.

The estimated impact values of a risk event can now be visualized in a risk matrix. It is necessary to summarize the estimated image values of each of the image indicators in a single value. There can be different methods applied for, but this might have some consequences – especially for extreme high or extreme low damage values – to be aware of. These methods could be summation, arithmetic mean, Euclidean norm, more complex functions in order to weight parameters, or conversion to a money amount.

**4.2 High-level IoT Risk Matrix**

This risk matrix can be applied to the high-level IoT risks from Section 3 to get a deeper understanding of the relation between the risks and to compare then in terms of impact and likelihood. Such an analysis is most conveniently done for each domain individually since risks are easier to assess when thinking about a concrete setting. On the other hand, some domains are very similar and can be grouped together in order to increase the visibility of the differences to other domains. As for the domains identified in Section 3, we consolidated the domains Water, Energy, Retail and Hospitality as well as Government together to the area Smart Cities.
Therefore, 11 different risk matrices have been developed based on discussions with experts. For the sake of simplicity and to give a clear overview the results of these different assessments are represented in one single matrix as shown in Figure 23. There is a positive correlation between likelihood and impact representing the fact that - from the perspective of an intentional threat actor – the higher the impact, the greater the motivation and thus the likelihood of an attack.

In a survey conducted in 2017 by the RISIoT project team, stakeholders from different fields were asked to assign both likelihood and impact to the high-level risks on a scale from 1 (low) to 10 (high) for the domains Domestic, Healthcare and Education. This survey with 109 participants confirmed our findings in the sense that there is a positive correlation between likelihood and impact: in all three areas the maximal values of likelihood were assigned to the same risk as the maximal values of impact. However the ordering among the different risks sometimes deviated, for example in the domestic domain the risk of DDoS attack was scored highest (instead of safety hazard by experts).
5. DOMAIN-SPECIFIC IoT RISKS
In order to illustrate the rather abstract high-level risks related to IoT we consider a specific use case that describes the problems appearing in real life application of IoT.

5.1 An Illustrative Use Case
As starting point we give a brief description of three areas for which risks will be discussed:

- Smart Homes
- Healthcare
- AAL

This will provide a basis for understanding the later specified risks. The AIOTI WG05 report (AIOTI WG5, 2015) discusses in depth the links between IoT and Smart Living Environments for Ageing Well (Elderly Care and Health and Smart Home / Home Automation), related EC policies and research initiatives.

In Health and AAL applications IoT solutions seem promising to help detect onsets if decline before people become really dependent (frail, ill) and so to provide adapted care and assistance as needed to prolong independence as much as possible with good Quality of Life (QoL). This has been discussed e.g. in (Dohr et al., 2010) very early.

Overall the exemplary use cases span clinical health environments with professional involvement, to private homes, to again institutional or nearly institutional environments like senior residences or sheltered homes. A big difference for IoT related risks can be seen in the existence or lack of professional support for the applied technologies depending on the field of application. Another distinction can be made for AAL where the older users are usually less motivated and able to decide for themselves about technology supporting their needs.

5.1.1 Smart Homes
The idea of means to control and monitor the living environment for comfort, security and safety was first introduced long ago as a vision of future driven by emerging technological advances and first driven by luxury and building automation and electronics hobbyists. This vision was, further advanced in the early 2000s by adding interactivity between the user and his/her environment to the concept which led to things in the environment becoming “smart” and supportive. Together with IoT the concept of a networked smart environment was extended from Smart Homes to Smart Cities, sustainable use of resources and energy saving. Smart Homes also were adopted in the upcoming AAL movement described below and tele-services and mobile connectivity were added e.g. for medicine or care. The concept of Smart Home typically spans the applications of Home Automation, Security, Home Entertainment, Energy Management and AAL. All the areas together are expected to see a Compound Annual Growth Rate (CAGR) of +34.2% until 2021 (Statista, 2017). If AAL specifics are ignored for the moment, the Smart Home Market is largely based on individual decisions of people to purchase certain
products and on the other hand on products pre-installed in buildings (e.g. for comfort, security and energy management). Recent discussions include risks of smart homes and IoT in general (Greenfield, 2017), (Manwaring, 2017).

5.1.2 Healthcare (at home)

IoT can be applied in clinical (hospital) environment for stationary patients to improve the data collection from few intermittent routine measurements by staff to continuous monitoring of physiological parameters. This helps to gain a clearer and richer data less prone to individual errors, allows earlier detection of complications and reduces the work load of staff and the comfort of patients. When governed by the professional medical directives it can be expected that risks will be properly addressed even if IoT introduces some new aspects because of the increase in complexity of the tools used.

Instead of futuristic hospital buildings and huge devices, disruptive technologies injected into small, almost invisible objects will set the trends in medicine. Such devices will create smart households bringing healthcare home. A shift toward IoT and apps in the field of healthcare allows companies to essentially become ‘healthcare providers’.

In Section 1.1.1 the likely increase in remote application of healthcare was already mentioned. This in part is driven by expectations for health services to become cheaper and more efficient when at least partly outsourced from medical institutions to extramural services. The World Health Organization lists chronic diseases as a leading cause of death worldwide. Therefore new technological trends like IoT are promoted as a chance to combat the risk factors and provide early detection. Applied both, indoor and outdoor, risk monitoring together with accorded prevention measures, assistance for medication and treatment, and support for a healthier life style are seen as big opportunities for the future. Main target disease segments of the eHealth market are diabetes, hypertension and heart failure. Studies like (marketsandmarkets, 2015) estimate the global Internet of Things (IoT) healthcare market to grow at a Compound Annual Growth Rate of 38.1 % during the period 2015 to 2020.

Main applications of IoT in Healthcare are in:

- Clinical care permanent monitoring
- Remote monitoring for early intervention/prevention
- Telehealth (transmission of medical information over telecommunication)
- Self-care

Hospitals, practitioners, and healthcare device manufacturers are using the IoT to keep patients remotely connected to healthcare providers and services. By tracking patient vital signs and health status indicators using connected healthcare devices, they are improving patient outcomes, enabling providers to serve more patients, and reducing hospital visits and lowering overall healthcare costs. This future vision is also reflected in the European Horizon 2020 research programme which includes the broad challenge “Health, demographic change and wellbeing”, covering aspects of Healthcare and AAL. Like in many studies, in (Teresa Villalba et al., 2016) an architecture for patients monitoring based on smartphones, Bluetooth and some wearable vital signs or activity sensors (partially dedicated devices
like pulse oximeters but also consumer devices like e.g. the FitBit flex wristband) is discussed. A security analysis presented according to (Avancha et al., 2012) found several important security risks and vulnerabilities impacting users of such architectures, especially if they include cloud-based services offered by the manufacturers of such devices. As soon as personalised data is transferred to or integrated into medical databases the strict medical and data protection regulations have to be applied. This poses a problem because the mobile segment including several devices with or without MDD compliance and the many wireless links (often Bluetooth, WiFi, GSM/LTE) and Internet services are hard to secure and even sometimes have to be used without proper in-depth documentation on what is collected when and how it is transmitted.

5.1.3 AAL – Ambient/Active Assisted Living

Countering the effects of a growing elderly population, declining fertility rates and rising life expectancy, and the shrinking relation of percentage of people in-work to that retired, Ambient Assisted Living (AAL) as an emerging multi-disciplinary field, aimed at exploiting information and communication technologies in personal assistive systems has been established. To support activities in this field a dedicated research support program (AAL-JP) has been created in Europe under the slogan “ICT for ageing well”. The focus was later extended to AAL standing for “Active and Assisted Living”, including broader aspects of older people’s everyday lives, typically starting from age 55+ until old age including their work, health, learning and leisure related activities. AAL applications are usually comprised of several sensors and optionally actuators plus user interfaces typically within the home or living environment. They are products and services which help older users to stay safe, autonomous and independent as long as possible in their own private environment (including sheltered homes or senior residences) maintaining social contacts by easy to use communication functions. According to (Fitzpatrick et al., 2015): “Among AAL/telecare solutions and service offerings, there is a huge diversity in the different configurations of technologies and in the degree of involvement of healthcare professionals. However, they all tend to encompass some or all of the following features: monitoring of safety and security, e.g. to detect water left running, via sensors that operate in isolation and generate alerts when events are detected; monitoring of activities of daily living (ADL) and lifestyle monitoring via a network of sensors in the home, again with some alerting function, e.g. for fall detection; and physiological monitoring, which usually involves some direct participation of the users, e.g. in taking blood pressure measurements.” (p306).

AAL applications are not meant as replacement for personal contacts and assistance but rather as a supplement. The application of AAL technology is expected to gain cost savings for the public but also an improvement in quality of life for the person. Compared to the healthcare sector, the AAL sector, while using similar technology, is a shift from professional medical towards self-care and professional care provision. While many research projects have been and are being funded (thus many studies were conducted and prototypes built), only few products or services have reached the market which is characterized by subsidies based procurements and services run by non-profit organizations.
In some countries, mainly US, UK and Scandinavia, AAL-like solutions have been (before AAL became popular) and still are pooled under the headings of "Telecare", “Telehealth” and/or “Telehealthmonitoring”.

The aims of AAL can be summarized as follows (AAL-JP):
- extending the time people can live in their preferred environment by increasing their autonomy, self-confidence and mobility;
- supporting the preservation of health and functional capabilities of the elderly,
- promoting a better and healthier lifestyle for individuals at risk;
- enhancing security, preventing social isolation and supporting the preservation of the multifunctional network around the individual;
- supporting carers, families and care organisations;
- increasing the efficiency and productivity of used resources in the ageing societies.

A well-known, and probably starting level of AAL technology in widespread in use are senior alarm systems, either with only an emergency push button or additional sensors like for fall detection. According to (Statista, 2017), the global market for Ambient Assisted Living (AAL), which is the smallest segment of the smart home market, is expected to show strong growth of 58% CAGR to 2021. In that year, the size of the global market is expected to reach US$5.6 billion. Europe will remain the second largest market after US in comparison with about US$1.6 billion in 2021 after a growth phase with a 71% CAGR with an expected number of 4.7 million AAL households in Europe. Worldwide household penetration with AAL is at 0.3 % in 2017 and is expected to hit 1.3 % in 2021 (Statista, 2017).

Use Cases for IoT in the AAL sector might be (note the partly identical items to smart home and healthcare):
- Comfort functions (automation or remote control of appliances – door lock, lights, blinds, entertainment)
- Energy saving
- Security like burglar, fire and gas alarms
- Safety (of people living alone) e.g. senior alarms, fall detectors, non-activity detection
- Activities of Daily Living support like reminders for medicine, drinking water, appointments and general coaching
- General self-monitoring of health and wellbeing by sensors with or w/o connection to medical services
- Tele-medical support including monitoring of vital signs and activity
- Tele-rehabilitation monitoring and support
- Tele- and self-care support and knowledge base
- Cognitive training and learning support
- Coaching of persons with mild dementia
- Communication and Entertainment/Remote gaming
IoT technologies are seen as promising building blocks around which powerful monitoring, alarm, counseling, communication and support system can be built with many similarities to the field of Smart Homes and also to Healthcare. This implies that most of the risks identified for these areas also apply to the broad AAL area. A complicating factor though is that the primary end users of AAL technology are neither health nor care professionals nor interested and technically skilled consumers. This makes the risks even bigger than in general IoT applications, a) given the already identified risks because of technically vulnerable IoT systems (or parts) which also form the basis for AAL technologies, unsecure communication protocols, cost pressures and numerous involved parties, and b) especially also in an area where personal information is collected, health related information is transmitted and safety relevant functions are to be provided 24/7. In the last years the introduction of service robotics in AAL has added a new risk in form of a mobile physical element which acts as an independent player making potentially hazardous situations even more complex to analyse. As a reaction, a dedicated standard ISO 13482:2014 “Robots and robotic devices – Safety requirements for personal care robots” (ISO, 2014) has been created. A very specific additional risk stems from the fact that primary AAL users mostly do not choose the implemented technology by themselves but are provided a solution which someone else is selecting and financing for them. In this situation people do not have the skills to understand the technical background, therefore are excluded from the selection process and are also mostly not provided with any means to assess or control the ongoing processing in an installed system. Their only anchor are contacts to relatives or representatives of (mostly non-profit) care organisations, who are considered trustworthy and able and willing to explain the work principle in simple language, take away hidden fears and take care for wanted adaptations and necessary maintenance, and to do this over the whole use time of the devices, which creates new costs above the mere procurement costs of the product. It is an often emphasized fact that because of economic constraints current technology in the field is almost never developed based on approaches like Value Sensitive Design or Privacy by Design so it does not properly take into consideration the interests of all stakeholders, especially the end users and not of older end users.

5.2 Risk Assessment for the Project’s Use Cases

After a gap analysis of 39 current IoT platforms and a survey among 350 experts in Finland, the following recommendations for the development of IoT middleware were given (Mineraud et al., 2016):

- leaning on standardized communication protocols to interface heterogeneous devices,
- adding the provisions for handling and processing data locally,
- adding uniform data models, data catalogs, and the edge analytics capabilities
- offering streamlined APIs
- introducing cross-platform brokers and financial incentives for ecosystem players
- developing dedicated IoT marketplace(s)
While these recommendations apply to all IoT systems, as will become evident in the following detailed discussion, many of the use case specific risks described in this section can be attributed to one of the recommended actions.

### 5.2.1 IoT Devices May Compromise Privacy

With the increasing amount of sensors collecting data about potential hazards but also the daily activities of the user it becomes more and more possible to infer in much detail what the user is doing when. This starts with simple presence at home and goes to detailed activity profiles based even on indirect “uncritical” data like energy consumption. Access to these data therefore should be under the control of the user and based on informed consent after evaluation of benefits and risks. Access to private data may also be misused to generate false or faked data, e.g. for causing (financial or health) damage or for blackmailing purpose.

In (Baldini et al., 2016) a policy-based framework is described which allows the end user and his/her context to be involved in privacy configuration instead of one-time „by design“ pre-scribed solutions. Such advanced concepts however, are not applied in current products.

Data protection is also emphasized in the new EC regulations and duties for providers under the new regulation entering into force in 2018 (EU regulation 2016/679, Datenschutz Grundverordnung - DSGVO). Although long time known to come up many providers are still not well prepared to properly deal with main requirements as:

- Anonymized and pseudonymized data, only use those personalized data which are required
- Required consent
- Privacy by design & Privacy by default
- Duty to document use of data and to report any breaches

### 5.2.2 IoT Devices Are Used by Inexperienced People

Many problems are caused accidentally due to deficient understanding of technology or due to improper configuration. Human errors are a main source for failure of IoT devices and make up a significant part of all risks. Therefore, IoT used for AAL purposes has to put special emphasis on actively reducing such risks.

Users of AAL technologies often are not able or interested to select and purchase these by themselves. Often relatives or professionals from medical or care services will recommend or prescribe something, which then often is funded (in part) by the social insurance system. As a consequence, there exists a regulated market, funded products or services can be selected only from official lists. In parallel, an increasing number of new products is offered (often from startups), which set up their own infrastructure that is hard to assess from a security perspective.

The inexperienced end users of AAL devices would need an easy understandable but detailed documentation of the functions of a device which is rarely available. This particularly applies for regular maintenance (e.g. battery, calibration) and update instructions, which in the typical consumer market is the task of the end user. In the extreme it is even possible that the awareness of users about the installed AAL system and its functions is low or over time the system’s presence is forgotten at all.
IoT Risks

In reality, the provision of services based on AAL products is nowadays often split. For example, relatively simple senior alarm systems are based on proven devices from some manufacturers which are rented to the user via non-profit organizations like the Red Cross, Johanniter, Caritas, Hilfswerk etc. The organization installs the device in the home of the user and does the initial configuration and training, but the call center behind the service might be run by another company. It can be imagined that with rising complexity of systems, maintenance, updating and repair will no longer be done by employees of the non-profit organization but have to be outsourced to specialized companies. These are confronted with a growing number of different products which should be individually configured according to users’ needs and wishes.

5.2.3 IoT Devices May Introduce Safety Hazards
Incorrect use or handling of IoT devices by elderly and most likely not very experienced people may cause safety hazards because of blind trust in the perfect function of technology despite its limitations. Besides the missing knowledge, it is also possible that the user has no access to the configuration and is not able to adjust the device her/himself to changing needs and is reluctant to ask for help.

5.2.4 IoT Devices are Poorly Secured and Cheaply Produced
Often IoT devices are produced cheaply and purely secured based on readily available standards components. Thus they are especially vulnerable to attacks exploiting existing (and even well-known) vulnerabilities. None or insufficient updating, which often happens in real life, increases this risk. Additionally, cheap products are not intended to be used unattended 24/7 which is often a requirement in AAL. To keep product costs low, self-check, redundancy and backup solutions are often not implemented which may also yield to malfunctioning of the devices over time.

5.2.5 Social Impact
Often users of IoT devices in AAL do not feel comfortable using these devices (generally any technology). They may cause anxiety, which results in trying to “outsmart” the technology, and especially elderly people may be worried about losing personal contacts by being fobbed off with technology instead. On the other side, some users are also happy to not have to rely on personal assistance (not needing to bother others, not being supervised by people) because of the technology serving them. Regarding QoL the technology, if well designed and applied, offers a perspective for longer autonomy and independence of users instead of early institutionalization.

While such social consequences are usually not part of a classical risk management they are important for users and should thus be considered in a comprehensive analysis of the use of IoT in AAL because they may interfere with the intended use.
5.3 Domain Specific IoT Risk Matrices

The 5 main risks associated with use of IoT in the use case “Smart Homes/Healthcare/AAL” are detailed in Figure 25 based on current situation i.e. mostly without recommended risk reduction measures. Additional to the general risks, domain specific, important risks have been added to make better visible the special influence factors in the area.

Results from the survey (see also Section 4.2) show that among the respondents to the survey the probability and effects of privacy risks for HEALTHCARE applications (covers medical to AAL) are also considered rather high (on average and by relative number of “very high” = 10/1-10 votes) compared to other areas. This leads to high risk rating of impact together with high likelihood (1). The inexperienced users in the field are a given fact and introduce very likely high risks not typical for other IoT application areas (2).

In contrast, the vulnerability of devices is not considered much different (or maybe somewhat lower, maybe because of higher trust in medical applications) to other fields by the responders to the survey. This correctly lines up with the fact that more and more the base technology is the same over all areas. The resulting rating is split, because safety hazards related to security faults (4) are especially critical because of the unaware users so the resulting impact is potentially bigger (3).

The negative social impact of IoT as a risk stems from technology potentially becoming a (cheaper) substitute for personalized care. It is rather likely because of the end users being often not part of the decisions which support is provided. This impact is somewhat limited because current technology cannot replace all personalized services (5) but may become more important in future. On the other hand, technology can also have positive social impact because, if introduced properly, it can support the end users (as well as their carers) and their social participation.

If one adds to this informal coarse risk assessment the special situation of users of AAL technologies who rely on third parties to select, fund and service the devices (and handle the data collected), it becomes
immediately clear that the overall risk without special measures is both, unforeseeable and unmanageable, for the average user in this area. While the typical informed consumer is free to give up comfort and fun from devices when risks become known and unbearable, users in the AAL field are depending on their support and in general are less informed about the risk/benefit balance.

As expressed by the participants of the RISIoT workshop, the risks of application of IoT based services need to be handled by cautionary measures applied from design to use phase. In all areas but especially in the AAL field there should be standards created which allow assessment of risks based on harmonized criteria and an explicit responsibility of the manufactures and providers of equipment and related services to deal with risk management during the whole lifespan of the products.
6. CONCLUSION

Internet of Things (IoT) affects an increasing variety of areas. Numerous products, systems and technologies with the label IoT were already launched on the market. This enormous number of different devices and services makes it difficult to find a consistent definition and structure for these forms and hamper developing an application-independent information security architecture for IoT products. This lack of paradigmatic classification causes inherent deficiencies and vulnerabilities of the products and services. Many of the manufacturer and the users are not aware of the threats and relating risks.

The presented publication tries closing this gap by analysing different frameworks and its implications for IoT, discussing different application domains and conceptually elaborates high-level risks. Initially, the characteristics of IoT systems were pointed out and IoT-related research projects and studies adequately discussed. The 14 different IoT application domains, which have been applied for risk assessment later, are sketched by requirements, stakeholders, application domains, use cases, and technologies and were categorized by ISO/IEC JTG 1 / WG 10. This will be the starting point for the development of an IoT reference architecture, intended to publicized as ISO/IEC 30141 (ISO/IEC JTC 1/WG 10, 2014) (ISO, 2016b). Various standards and reference models were analysed by this working group for implications on IoT, a small number of the most important ones are introduced in this publication as well. It leads to the setup of six different high-level risks that can be related to the application domains, suggesting a high-level risk matrix, which provides a rough overview of generic risks in the area of IoT. The objective here is not to conduct a detailed risk analysis for one technology or a specific application area, rather to stimulate general awareness for all IoT involved risk fields. The classification of the risk and the visualisation in a risk matrix according the influence factors impact potential and likelihood has been conducted in a workshop with the project members.

Considered in detail, the risk matrix shows that the highest risk was revealed if danger of life is evident, e.g., health, transport, public safety and military. It is followed by the area of retail and hospitality as well as partly food. Finance, manufacturing and heavy industry provide dispersed data depending on the high-level risk, same for specific risks in food. Rather less estimated risks are linked with entertainment and sports and education. Finally, three selected use cases were introduced to illustrate the generic high-level risk and round-off this approach for a comprehensive presentation of the complex field of IoT risks. In order to derive empirically more meaningful theses and results, this phase could be re-performed with more experts and stakeholders from more different sectors with broader perspectives. An empirically acceptable amount of statements helps to assure the obtained findings and to indicate a sustainable trend for general IoT risks.
7. REFERENCES


AIOTI WG5, 2015. Smart Living Environment for Ageing Well.


IoT Risks


ETSI, 2017. TS 103 264 - SmartM2M; Smart Appliances; Reference Ontology and oneM2M Mapping.

ETSI, 2016. TS 118 112 - oneM2M; Base Ontology (V2.0.0).


IBM, 2016. Reviewing a year of serious data breaches, major attacks and new vulnerabilities.
IES-City Framework, 2016. IoT-Enabled Smart City Framework.
ISA, 2016. The 62443 series of standards.

Plattform Industrie 4.0, 2017. Referenzarchitekturmodell Industrie 4.0 (RAMI 4.0).


8. ANNEX

8.1 Abbreviations

<table>
<thead>
<tr>
<th>Term</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIOTI</td>
<td>Alliance for Internet of Things Innovation</td>
</tr>
<tr>
<td>AKA</td>
<td>Authentication and Key Agreement</td>
</tr>
<tr>
<td>AR</td>
<td>Augmented Reality</td>
</tr>
<tr>
<td>ARM</td>
<td>Architectural Reference Model</td>
</tr>
<tr>
<td>ATM</td>
<td>Automated Teller Machine</td>
</tr>
<tr>
<td>BSIMM</td>
<td>Building-Security-In Maturity Model</td>
</tr>
<tr>
<td>CCTV</td>
<td>Closed-circuit Television</td>
</tr>
<tr>
<td>CPS</td>
<td>Cyber Physical Systems</td>
</tr>
<tr>
<td>CPU</td>
<td>Central Processing Unit</td>
</tr>
<tr>
<td>DDoS</td>
<td>Distributed Denial of Service</td>
</tr>
<tr>
<td>Dev</td>
<td>Development</td>
</tr>
<tr>
<td>EPI</td>
<td>IoT European Platforms Initiative</td>
</tr>
<tr>
<td>ETSI</td>
<td>European Telecommunications Standards Institute</td>
</tr>
<tr>
<td>FIB</td>
<td>Focused Ion Beam</td>
</tr>
<tr>
<td>FIPS</td>
<td>Federal Information Processing Standard</td>
</tr>
<tr>
<td>GDPR</td>
<td>General Data Protection Regulation</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and Communication Technologies</td>
</tr>
<tr>
<td>IDE</td>
<td>Integrated Development Environments</td>
</tr>
<tr>
<td>IEC</td>
<td>International Electrotechnical Commission</td>
</tr>
<tr>
<td>IERC</td>
<td>European Cluster on the Internet of Things</td>
</tr>
<tr>
<td>IES</td>
<td>Internet-Enabled Services</td>
</tr>
<tr>
<td>IMEI</td>
<td>International Mobile Equipment Identifier</td>
</tr>
<tr>
<td>IMSI</td>
<td>International Mobile Subscriber Identifier</td>
</tr>
<tr>
<td>IoT</td>
<td>Internet of Things</td>
</tr>
<tr>
<td>IPv6</td>
<td>Internet Protocol Version 6</td>
</tr>
<tr>
<td>ISAC</td>
<td>Information Sharing and Analysis Center</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization</td>
</tr>
<tr>
<td>ITU</td>
<td>International Telecommunication Union</td>
</tr>
<tr>
<td>JTAG</td>
<td>Joint Test Action Group</td>
</tr>
<tr>
<td>JTC</td>
<td>Joint Technical Committee</td>
</tr>
<tr>
<td>M2M</td>
<td>Machine-to-Machine</td>
</tr>
<tr>
<td>MAV</td>
<td>Miniature Unmanned Aerial Vehicle / Micro Unmanned Aerial Vehicle</td>
</tr>
<tr>
<td>MCU</td>
<td>Micro Controller Unit</td>
</tr>
<tr>
<td>ME</td>
<td>Mobile Equipment</td>
</tr>
<tr>
<td>MISRA</td>
<td>Motor Industry Software Reliability Association</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Full Form</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------</td>
</tr>
<tr>
<td>NFC</td>
<td>Near Field Communication</td>
</tr>
<tr>
<td>NIS</td>
<td>Network and Information System</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>NoT</td>
<td>Network of Things</td>
</tr>
<tr>
<td>OEM</td>
<td>Original Equipment Manufacturer</td>
</tr>
<tr>
<td>OpenSAMM</td>
<td>Open Software Assurance Maturity Model</td>
</tr>
<tr>
<td>Ops</td>
<td>Operations</td>
</tr>
<tr>
<td>PCB</td>
<td>Printed Circuit Board</td>
</tr>
<tr>
<td>PDCA</td>
<td>Plan – Do – Check – Act</td>
</tr>
<tr>
<td>PIA</td>
<td>Privacy Impact Analysis</td>
</tr>
<tr>
<td>PLC</td>
<td>Programmable Logic Controller</td>
</tr>
<tr>
<td>POS</td>
<td>Point-of-Sale</td>
</tr>
<tr>
<td>PUF</td>
<td>Physically Unclonable Functions</td>
</tr>
<tr>
<td>RA</td>
<td>Reference Architecture</td>
</tr>
<tr>
<td>RAMI</td>
<td>Referenzarchitekturmodell Industrie 4.0 (Reference Architecture Model Industry 4.0)</td>
</tr>
<tr>
<td>RF</td>
<td>Radio Frequency</td>
</tr>
<tr>
<td>RFID</td>
<td>Radio-Frequency IDentification</td>
</tr>
<tr>
<td>RM</td>
<td>Reference Model</td>
</tr>
<tr>
<td>RSU</td>
<td>Road Side Units</td>
</tr>
<tr>
<td>RTOS</td>
<td>Real Time Operating Systems</td>
</tr>
<tr>
<td>SAE</td>
<td>Society of Automotive Engineers</td>
</tr>
<tr>
<td>SAREF</td>
<td>Smart Appliances Reference Ontology</td>
</tr>
<tr>
<td>SCADA</td>
<td>Supervisory Control and Data Acquisition</td>
</tr>
<tr>
<td>SDLC</td>
<td>System Development Life Cycle</td>
</tr>
<tr>
<td>SoC</td>
<td>System on a Chip</td>
</tr>
<tr>
<td>SRIA</td>
<td>Strategic Research and Innovation Agenda</td>
</tr>
<tr>
<td>TC</td>
<td>Technical Committee</td>
</tr>
<tr>
<td>TNO</td>
<td>Netherlands Organisation for Applied Scientific Research</td>
</tr>
<tr>
<td>TPM</td>
<td>Trusted Platform Module</td>
</tr>
<tr>
<td>UART</td>
<td>Universal Asynchronous Receiver Transmitter</td>
</tr>
<tr>
<td>UAV</td>
<td>Unmanned Aerial Vehicle</td>
</tr>
<tr>
<td>UE</td>
<td>User Equipment</td>
</tr>
<tr>
<td>UICC</td>
<td>Universal Integrated Circuit Card</td>
</tr>
<tr>
<td>US</td>
<td>United States</td>
</tr>
<tr>
<td>USB</td>
<td>Universal Serial Bus</td>
</tr>
<tr>
<td>USD</td>
<td>United States Dollar</td>
</tr>
<tr>
<td>V2V</td>
<td>Vehicle-to-Vehicle</td>
</tr>
<tr>
<td>VR</td>
<td>Virtual Reality</td>
</tr>
</tbody>
</table>

Table 2: Abbreviations