SCOTT:

Secure COnnected Trustable Things

Market Roadmap

Document Type	Deliverable
Document Number	D22.2
Primary Author(s)	Maunya D. Moghadam | University of Oslo Josef Noll | University of Oslo
Document Version / Status	4.0 | final
Distribution Level	PU (public)

Project Acronym	SCOTT
Project Title	Secure COnnected Trustable Things
Project Website	www.scottproject.eu
Project Coordinator	Michael Karner | VIF | michael.karner@v2c2.at
JU Grant Agreement Number	737422
Date of latest version of Annex I against which the assessment will be made	2020-05-29

SCOTT has received funding from the Electronic Component Systems for European Leadership Joint Undertaking under grant agreement No 737422. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme and Austria, Spain, Finland, Ireland, Sweden, Germany, Poland, Portugal, Netherlands, Belgium, Norway.

CONTRIBUTORS

Name	Organization	Name	Organization
Jan Pedro Rimala	Eye Networks	Manish Shrestha	University of Oslo
Geir Arne Rimala	Eye Networks	Sinéad Scully	Tyco
Maghsoud Morshedi	Eye Networks		
Maunya D. Moghadam	University of Oslo		
Josef Noll	University of Oslo		
Christian Johansen	University of Oslo		
Elahe Fazeldehkordi	University of Oslo		

FORMAL REVIEWERS

Name	Organization	Date
Linda Firveld	EyeNetworks	2020-09-12
Boning Feng	OsloMet	2020-09-09

DOCUMENT HISTORY

Revision	Date	Author / Organization	Description
1.0	2019-05-15	Maunya D. Moghadam	Initial TOC with inputs
1.1	2019-05-20	Maunya D. Moghadam	Contributions from partners
2.0	2020-06-30	Josef Noll	Added Wifi6 Sensor
3.0	2020-08-10	Josef Noll	Basis for review
4.0	2020-09-13	Josef Noll	Review recommendations included

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 EXECUTIVE SUMMARY

This SCOTT deliverable focusses on the market roadmap for managed wireless. Wireless has traditionally been based on best-effort networks, assuming that the delivered bandwidth will satisfy the customer needs.

However, the more stringent requirements in Internet of Things (IoT), automated systems, Industry 4.0 and future homes have established the need for monitoring. While mobile networks had device and network monitoring as part of the initial design, wireless networks did not have these features.

The trends for indoor communications address 5G network deployment in buildings, security- and privacy-demanding applications in future homes, as well as upcoming WiFi sensor standards. All these trends increase the need for managed wireless. This report will focus solely on managed WiFi, knowing that experiences from managed WiFi will be applicable to other sensor networks.

The report starts with an overview over trends in wireless, and especially the user demand for reliable services at high quality. Aspects being addressed are Smart WiFi, 5G requirements and demands for industrial wireless networks.

The report will then address how Europe can gain leadership and open market opportunities by focussing on security, privacy and trustability in wireless networks. There are several advantages seen from a European perspective, both the relatively high education, the societal structure in Europe, the leadership of the Nordic and Baltic regions in digitisation, and last but not least the success of the privacy regulations through GDPR. This report goes beyond, by providing examples on how the focus on Societal Security and on empowering the users in Europe will contribute to new market opportunities. Just as an example, the World's fastest mobile network is in Norway, with an average(!) speed of 75.4 Mbit/s as measured from the user side. Denmark provides broadband services to the home guaranteeing 500 Mbit/s both within the home and out to the public Internet. Latvia is market leader when it comes to end-customer costs for mobile broadband.

SCOTT, the largest JU project in the area of trust, security and privacy for IoT, has a number of achievements contributing to trusted wireless networks. Chapter 5 provides an overview on contributions from SCOTT both from the use cases, and from the building blocks. A total of 3 use cases and 12 building blocks address the need for managed wireless, and thus contribute to the European leadership in Managed Wireless. The three use cases are led by companies from Finland, Norway and The Netherlands, and cover the heterogeneous sensor integration for indoor air quality monitoring, managed wireless for excellent Quality of Service (QoS) in home networks, and integrated health-care using on-body sensors.

Key words: managed wireless, Internet of Things, roadmap, WiFi, trustability

2 INTRODUCTION AND OBJECTIVES

Internet of Things (IoT) extends the traditional IT networks with many new connected devices. It is estimated that the number of connected IoT devices grow to nearly 125 billion connected devices by 2030 in various domains such as homes and buildings, e-health, industry applications, entertainment, transportation. 79% of the Internet's traffic is expected to run through WiFi and mobile by 2022 [1] and the number of Internet-connected devices is expected to reach 50 per home with four members in 2022 [2].

In the current IoT market, manufacturers are mainly focus on technology development and sending the product to the market. However, there is a supplementary requirement to pay attention to service development in terms of security and privacy aspects and trustworthiness. In fact, it is essential to perform security and privacy risk assessment of the IoT products and the products should get updates to compensate security and privacy vulnerabilities unless it leads to degreased security and privacy level in a timely manner.

In homes, users have been surrounded by new technologies and services in their everyday life. Meantime, new technologies and services delivered wirelessly to provide convenience and ease of use. However, deploying connected things in homes raises security and privacy concerns due to enormous amount of recent security and privacy breaches. Vendors provide connectivity as a value-added feature to their product to facilitate administration. For example, connected fridge, panel heater, oven, dish washer, air conditioner, smart TV, etc. enable users to administer their appliances and home remotely and efficiently. However, connected devices increase security and privacy risks, which can result in severe consequences, therefore data security and privacy are a big issue in current market such that user data can be stored, processed and exchanged.

The objectives of this deliverable are to address the market for secure, privacy-aware and trusted services and devices with the major focus on the home. We look into managed and monitored wirelesses, with the need for perceived Quality of Service (pQoS). Already today, lot's of wireless (WiFi) installations do not satisfy what they promise, and don't deliver even the capacity of the provided Internet link. By monitoring and managing the wireless network, we have the opportunity to add and separate wireless and create network slices in the home network and these network slices give us the opportunity to differentiate the services according to security, privacy, trust or the expected bandwidth as one of the Quality of Service (QoS) parameters.

3 WIRELESS TECHNOLOGY DEVELOPMENTS

Service differentiation, especially including security, privacy and trustability, is key for novel services and an increase user satisfaction. This chapter will introduce the major trends in Wireless and in Mobile Networks, pointing out the need for managed WiFi and building the basis for a market opportunities.

The chapter is structured as follows: First, developments in smart WiFi are discussed, followed by 5G and 6G developments. Thereafter, the need for managed wireless in industrial systems is expressed.

3.1 WiFi6 and Sensor Efficiency

WiFi is has traditionally got faster and faster, and faster internet is constantly in demand. The newest generation of WiFi connectivity, which is called WiFi6 is based on IEEE 802.11ax and brings faster speeds than previous technologies in the 2.4 GHz and 5 GHz bands. The other characteristics of WiFi6 are Increased range, better performance in environments where many devices are connected, and enhanced power efficiency for devices. WiFi6 will come to market by December 2019.

WAOO as a Danish Internet Service Provider, provides smart WiFi using MESH-technology. The main focus of them is to use managed WiFi to be able to provide the service with 300 Mbit/s speed (up and down). WAOO claims that customers get at least 100/100, 300/300 or 500/500 Mbit/s and they provides speed guarantee in delivering the bandwidth to the home. However, WAOO does not yet guarantee that WiFi will deliver these high speeds. That's why ongoing focus is on managed WiFi in order to ensure that the managed WiFi will live up to the required speeds in delivery to the home. One aspect on the WiFi standard in Wifi6 is the Dual-band Client Performance, that can reach 600 Mbps speed at 5 GHz wireless frequency.

As shown in Figure 1 the difference between the speed of Actual and Max Dual-Band clients at 5 GHz wireless frequency is significantly bigger and range from 500 Mbps to 600 Mbps in comparison with 2.4 GHz frequency which both perform about 100 Mbps. Reason is the availability of bandwidth in the 5 GHz domain, allowing for a much higher allocation of bandwidth for a dedicated service.
One of the world leaders in providing high-speed WiFi solutions is ZYXEL, addressing the following Wifi6 features for their novel product series:

- 10G WiFi: Theoretical top speed of 9.6 Gbps
- Larger Capacity: 4 x Capacity, and performance
- Dual Band: Operates in both 2.4 GHz and 5 GHz in a combined matter

WiFi6 is thus an excellent candidate for distributing the access speed from fibre-to-the-home to the various end devices. However, WiFi6 does not address interference and other effects on the communication channel. Thus, a communication speed of 500-600 Mbps is available in laboratory environments, but is far from being standard in realistic environments. As an example of factors limiting the available bandwidth are construction elements as well as interference. Regarding construction elements, even a traditional wall can reduce the 5 GHz communication by more than 20 dBm, thus reducing substantially the Signal-to-Noise ration and by that the capacity. Interference may come from other WiFi communication or from other sources, the best known is the microwave

oven radiation in the same frequency range as the WiFi. Though, given the large amount of electronics using digital circuits, these circuits also emit radiation in the WiFi bands.

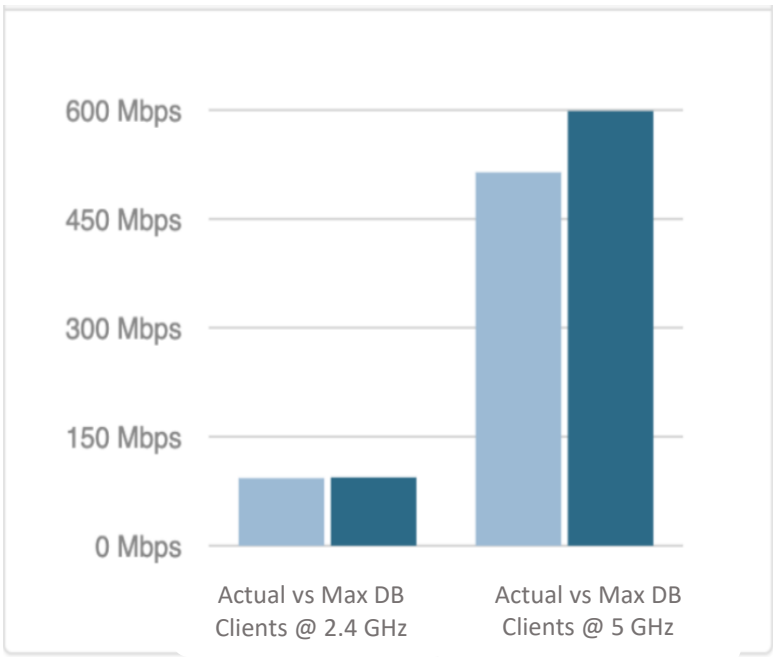

Figure 1 Dual-band Client Performance [3]

Given the interference and competing services in the ISM band, we need a continuous monitoring of devices and communications in the buildings to guarantee high throughput and an excellent perceived Quality of Service (pQoS).

Figure 2 Increase Overall Network Throughput from 802.11ac to 802.11ax [4]

Achievements in Wireless

Similar to mobile networks, also WiFi networks evolve continuously. Though device manufacturers promise certain service quality, e.g. 1800 Mbit/s WiFi capacity, reality is quite different. The announced capacity is often the capacity given optimum signal-to-noise ratio, and combining 2.4 and 5 GHz bands. Knowing that communication using high frequencies such as 5 GHz have severe restrictions due to attenuation of e.g. walls & floors, customers will observe the 1800 Mbit/s only in the 2-5 m surrounding of the WiFi access point.

New technologies like Multi-MIMO try to overcome the restrictions, using the new 802.11ax standard. As shown in the left part of the Figure 2, 802.11ax increases the bandwidth by about 50% as compared to 802.11ac. The increase is mainly due to the Multi-MIMO implementation, allowing each device to be served through a specific beam. As can be seen from the right part of the Figure 2, the increase is marginally (typically 20-40%) in the downlink, and essentially (up to 200-300%) in the uplink. For high signal to noise rations, the adaptation of 256 QAM and even 1024 QAM[1] is foreseen to achieve the increase in bandwidth in the uplink. It should be noted that an increase of 2 bits per symbol will result in a 6 dB reduced SNR, which is ¼ of the power. As a result, 16-QAM requires SNR of 18dB, 64-QAM requires SNR of 24dB, 256 QAM requires SNR of 30dB, and 1024 QAM requires SNR of 36 dB. Given the need for 256 or 1024 QAM and a signal-to-noise ratio of more than 30 dB, it typically means sitting in the same room as the WiFi access point. Furthermore, the high modulation is sensitive to other impairments, such as phase noise and interference[2].

While certification for 802.11ax is achieved, and first chip-sets are on the market, the market dominance is expected to be reached by early 2022 (see Figure 3). Current work in SCOTT (WP8) contributes with performance measures in mixed traffic environments.

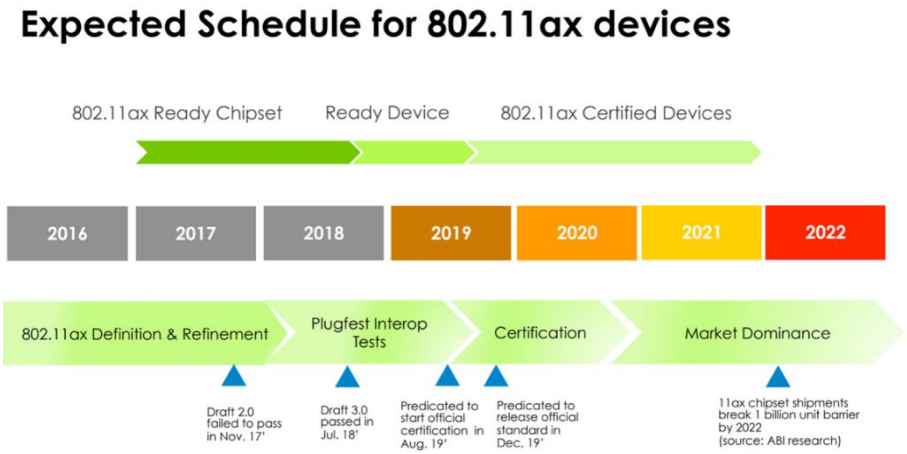

Figure 3 Schedules for WiFi 802.11ax [4]

Figure 3 shows that the work on WiFi6 (802.11ax) has started since 2016, the draft failed in 2017 and passed in 2018. Certification started in August 2019 and first chip-set were released in December 2019. It is expected that 11ax chipset shipments break 1 billion unit barrier by 2022.

WiFi6 for interoperability with 5G and sensor connectivity

What is even more important than the usage of the 11ax chipset in WiFi is the novel capability for sensor applications. So far, WiFi focusses solely on bandwidth and high communication capabilities. With WiFi6 the second focus is on integration of battery-driven devices. WiFi6 introduces Target Wake Time (TWT), that allows the access point and the client to negotiate the timing, such that the client (a sensor) only needs to wake up and be operable for a very short moment.

These low-power advances will, in addition to sensors, affect smartphones, tablets and notebooks. Today, these devices have to wait all the time to get known when they are allowed to transmit. In WiFi6, the scheduled operation will allow for a drastically reduced battery consumption. Longer periods on standby mean less frequent transmissions and thus less power consumption, so saving

[1] https://lancomwire.com/wi-fi-6-faster-and-energy-efficient-thanks-to-qam-and-twt/

[2] http://educypedia.karadimov.info/library/QAM.pdf

energy and also reducing interference on the densely populated radio frequencies. One application is voice over WiFi, which today needs that WiFi is listening all the time for an incoming call. With WiFi6, the mobile can get a short status say every 2 seconds to listen to an incoming call.

Regarding SCOTT, the most interesting advances in WiFi6 are the capabilities for extended range and lower battery power, as well as interworking with 5G usage.

3.2 Mobile Networks

The mobile networks have developed to new generation (5G). 5G provides mobile broadband network with higher capacity. The difference between the 5G network and previous generations is that the 5G is designed to provide networks and services to various industrial and community-powered devices, as well as the services and networks of the smartphone. It is claimed that 5G offer connections that are multitudes faster than current connections, with average download speeds of around 1 Gbps [5].

In addition to mobile broadband, 5G is offered as a fixed broadband access to households and businesses in areas without fibre networks. It is also arranged for broadcasting of radio and TV.

5G is extending the current capability in three dimensions. services that 5G will support include eMBB (*Enhanced Mobile Broadband*) that supply high bandwidth internet access for wireless connectivity, large-scale video streaming, and virtual reality, and mMTC (*Massive Machine Type Communication*) which supports internet access for sensing, metering, and monitoring devices. The third area which is addressed is URLLC (*Ultra Reliable Low Latency Communication*) which is allowing the mobile network to enter the industrial communication area.

Enhanced mobile broad band (eMBB) is one of three primary 5G New Radio (NR) use cases defined by the 3GPP as part of its SMARTER (Study on New Services and Markets Technology Enablers) project. The objective behind SMARTER is to develop high level use cases and identify what features and functionality 5G would need to deliver to enable them. eMBB is bringing higher access rate up to 10 Gbps, pick rates are typically around 1 Gbps or has claimed 100 Mbps into the mobile network whenever it is needed.

Massive Machine Type Communication (mMTC) focus on providing connectivity to many devices in a small area and transmit a low amount of traffic that may only send data sporadically, such as Internet of Things (IoT) use cases.

Ultra Reliable and Low Latency Communications (URLLC) is the other type of use cases supported by the 5G New Radio standard which targets wireless connections with stringent requirements on both latency and reliability. See the Figure 4 for application areas of 5G.

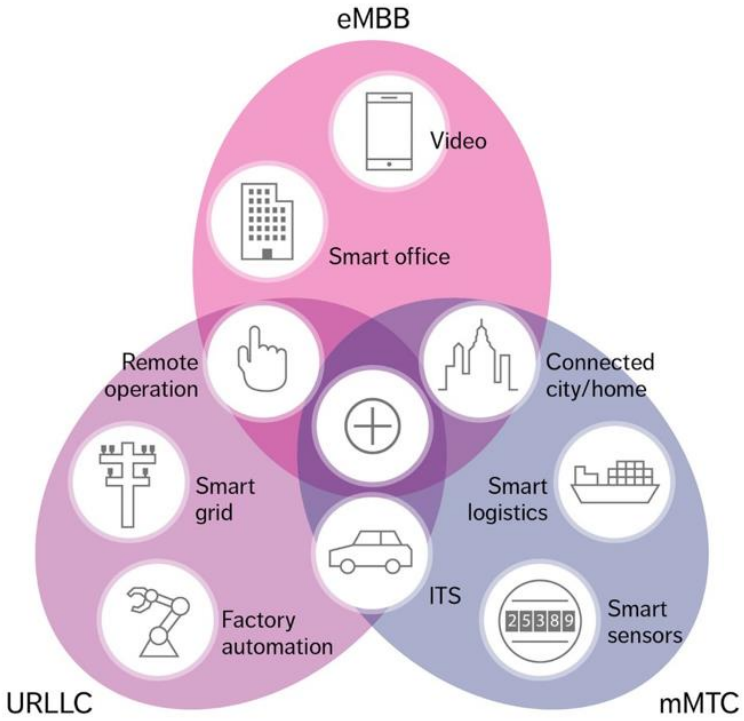

Figure 4 Three main 5G use cases and examples of associated applications [6]

Given the use of higher frequencies in 5G, and thus shorter range and higher attenuation, a 5G network slice in home environments is needed. The outdoor to indoor attenuation using frequencies larger than 2.4 GHz is too high, and would perform to substantial degradation of mobile network capacity. Thus, we need to prepare the home network infrastructure to cope with the service demands of 5G, which can't be achieved with "best effort" WiFi currently provided.
Thus, what is required, is new interface between the home network and the 5G network in order to allow 5G services to be deployed at home. However, that again needs a new architecture for the current WiFi implementation. This is also a reason for the discussion of opening new bands for WiFi in the market, such as mentioned WiFi 6. In SCOTT, we contributed with demonstrating the 5G network slice in a home scenario.

Although 5G is very new in the market, research into the new generation (6G) is already underway[3]. What is lacking in 5G is to address both the impact on the society and the impact on the sustainable development goals of the agenda 2030 as well as digital inclusion and other factors. Kate Gilmore from the United Nations in Genève (UNOG) addressed that "Internet had the ability to dismantle the divide. But Internet failed miserably, the divide is bigger than ever" [7]. Reason for her statement is the digital divide, which is not only an information divide, but getting more and more a technology and industrial divide. Given sensor-driven operations in highly industrialized environments, more and more processes are performed in an automatic manner. Such automotive processes allow a cost efficient automated production, and thus reduce the need for non-specialized people. At the end, those societies without automation and with a large number of hand-made jobs will suffer from the ongoing digitization in industry.

[3] The 6G flagship project is centred around the city of Oulu, and attracted a total of 251 Million EUR in budget, see http://6genesis.com

5G focuses on the industrial sector, addressing both massive IoT and process automation, but lacks on digital inclusion. As a part of the future vision of SCOTT we have discussed on IoT security, cyber security and societal security and identified the need for societal impacts of mobile communication. Therefore, 6G is underway and got the slogan is ”6G for humanity and sustainability” (See Figure 5).

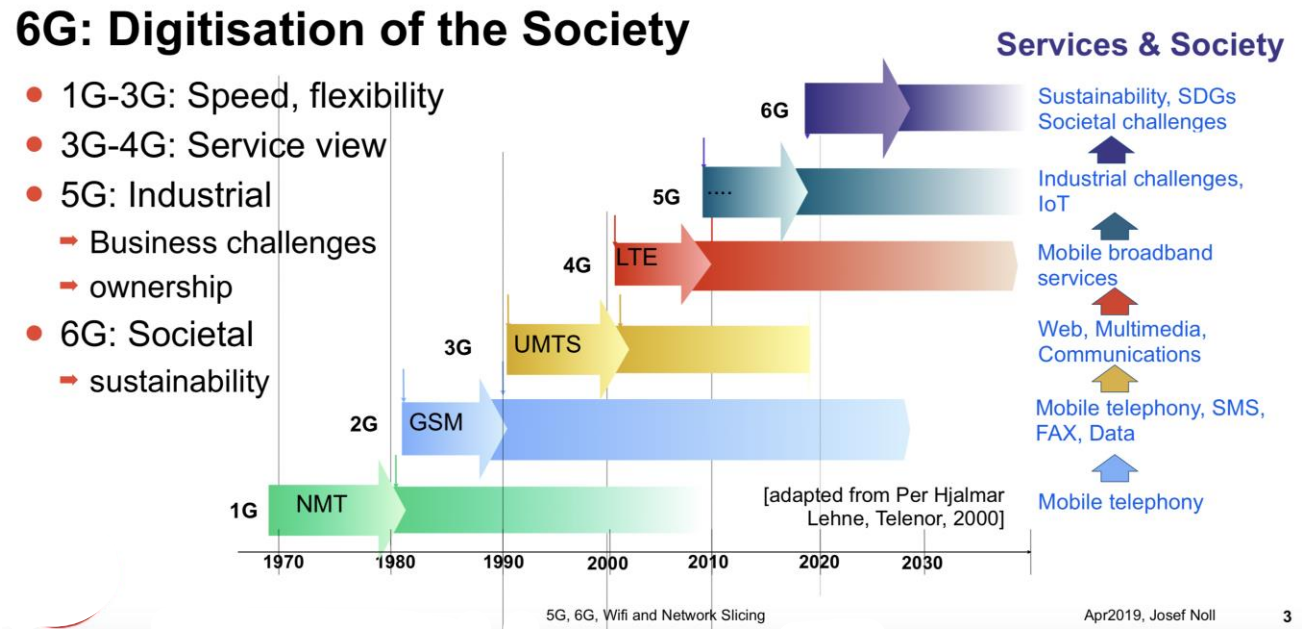

Figure 5 Service Developments by 1G to 6G

Figure 5 shows the development of mobile services, indication the roughly 10 years of development before the market entry. The figure also points out the change in services from 1G to 6G; while 1G and 2G was about Mobile telephony, 3G and 4G tailored data services, while 5G opened for industrial automation, and 6G addressing societal challenges, e.g. contribution to sustainability and the SDGs. What is core is to bring the benefit of mobile networks for the individual person into the foreground by relating the environment to the needs of the person, making information being both transparent and adapted to the context and the personal preferences of the user. As an example, novel services which are allowing information to reach the user on artificial surfaces or holograms, will include situation awareness like taking care on how and when the user is going to be disturbed during the attack.

On the sustainability, the main focus is on building an infrastructure that allows every single person to become part of digital society. Requirements include both the coverage of mobile networks, the inclusion of low-cost wireless interfaces, such as WiFi in the mobile networks, as well as a change of the regulatory framework. The 6G network needs both private-public collaboration in building community networks in areas where commercial operation is not viable. In addition, introducing edge knowledge with computing capabilities at the edge of the network, e.g. in local information spots, at home or in the office, are essential to create service and applications of value to the end customer.

3.3 Conclusions and Demands for Industrial Wireless

History has shown that bandwidth is going to be used, and that the demand on wireless, both for WiFi and for mobile networks, is only increasing. Thus, given the need of “wireless everywhere”, we need novel models for providing seamless services both within a building and outside. However, we

need the transition from “best-effort” wireless to managed wireless, allowing to have “wireless on demand”, both for extreme broadband at data rates beyond 1 Gbit/s and for sensor application.
As an example of using wireless for in-door applications, connected buildings are setting the following demands:

- Every building is different, with different connectivity capabilities. Securing and deploying IoT equipment can be challenging in the various environments, if the radio characteristics and the wireless coverage in the building are not adequately managed.
- Sales teams traditionally selling physical equipment can be confused by new products which contain data services with certain QoS demands.
- Even though data analysis can yield useful information, ensuring data is handled correctly according to GDPR (General Data Protection Regulation) can be challenging. Big data analysis can recapture personal information through profiling, e.g. connecting movement profiles with access profiles.

In SCOTT, Tyco has focussed on Integrating technology choices and architecture choices to become safe and secure. Up until now, the focus in SCOTT has been on to how to contribute to the use case to solve problems posed for secure, connected facility management. Solutions are evolving as separate pieces of functionality which target various aspects of the use case. While these advancements are hugely beneficial by enhancing JCIs capacity for innovation, problem solving with a view to next generation of products, our SCOTT project planning must also include resource allocation for our integration strategy. The strength of the innovation lies in the sum of each functional piece, so adequate preparation must be made for the integration and coupling of overall solution fragments.

Other intended goals are that the integrated solution should effectively permit free flow of use case event data in real time while securely transmitting data. All physical connections and attack vectors should be considered in a vulnerability assessment.

Further ambitions include adopting FIWARE into our integration strategy. This offers the opportunity to share data to project partners which could potentially broaden the scope of the research effort and promote smart city / smart solutions.

Challenges to be faced will be integrating new and legacy systems in a way that provides stability, is easily repeatable and cost effective. Secure integration is of primary importance for acceptance within existing sales divisions and customers. Integration platform must offer the usual standards of quality and reliability while be able to demonstrate what is the differentiator. This further provides input for evaluation cycles and feedback.

In conclusion, the demand for wireless has changed drastically, from a best-effort network to a network being flexible, robust and able to deliver both high-bandwidth as well as include battery-driven devices. These demands can only be answered by monitored and managed wireless, knowing at any point of time the network characteristics and being able to handle the fluctuations in the network.

4 SCOTT SOLUTIONS

The SCOTT solutions include focusing on:

- Wireless systems by considering the security, privacy and trustability: to enable cooperation of secured and trustable wireless systems with the required privacy across the industrial domain
- European leadership and market opportunities: to address European societal challenges
- Smart sensors and actuators: to foster interoperability, scalability, and reusability

4.1 Wireless systems by considering the security, privacy and trustability

The solution of Wireless systems by considering the security, privacy and trustability targets to enable cooperation of secured and trustable wireless systems with the required privacy across the industrial domain.

The work in SCOTT on monitored and managed wireless is first initiated for the WiFi domain though by using the standards, the work can easily be transferred to monitored IoT. Wireless will be the driving force for connectivity in the industrial sector, mainly because of simplicity. The challenge is about reliability and attack which are the main issues by a monitored and managed wireless.

Though it is expected that IoT manufacturer take security and privacy risk seriously, most of IoT devices are designed and manufactures having the focus on a cost-efficient design and implementation. Thus, the majority of IoT devices does not satisfy security and privacy by design. However, the challenge of unsecured and non-GDPR compliant devices has reached the attention of both data protection authorities and industries.

Regarding security, the latest examples from both Mærsk and Hydro on ransomware encrypting both personal computers and those controlling industrial operations increased the awareness of unsecured infrastructures. Following the presentation from F-Secure on the “Shared Insights 2019” workshop from Eye Networks, the threat potential from IoT devices had increased from 6 family threats in 2016, including Remaiten, Mirai, Hajime and Leet to 35 family’s threats in 2018 (See also Figure 6).

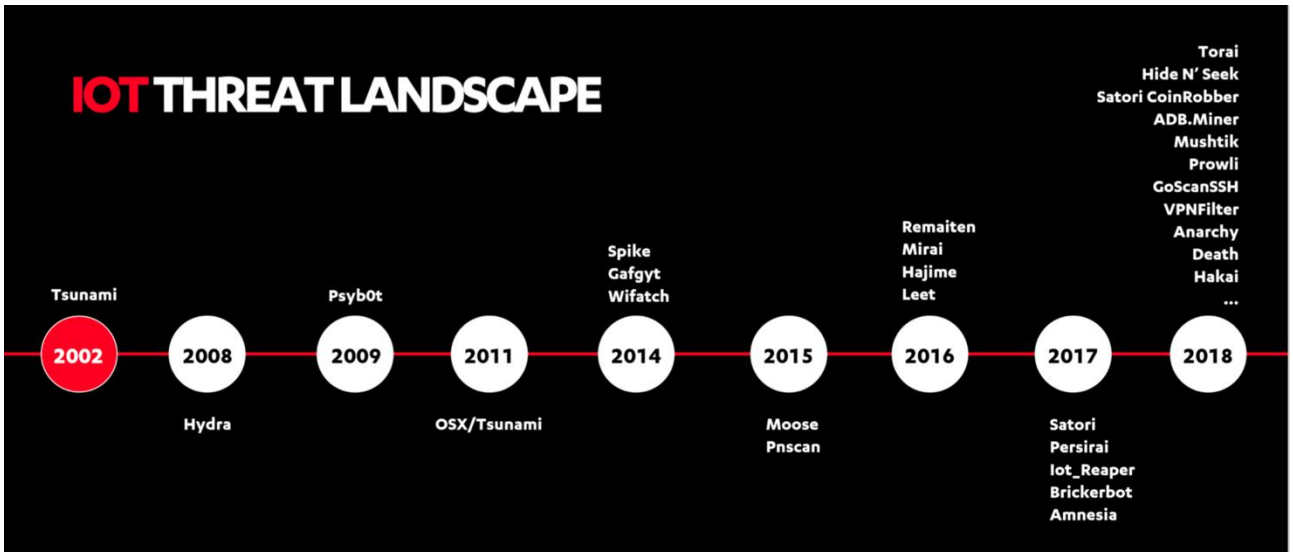

Figure 6 IoT Threat Landscape [8]

Figure 6 shows a drastic increase in IoT threats from 2002 to 2018 which does not only address new variants, but even more new threats addressing different functionalities of IoT. This means that manufacturer should perform risk and threat analysis assessments from very early stage of product design process. One of the major steps to implement security and privacy by design is to manufacture IoT products with reasonably updated software that does not contain sever or known vulnerabilities. Meantime, IoT product should have an automated secure update mechanism to be resilient against upcoming attacks.

On the other hand, envisaged market should encourage standardization to improve interoperability and reusability IoT product and services. Thus, it can enhance monitoring compliance of IoT products and services and risk assessment process to mitigate security and privacy concerns.

In SCOTT, new technologies and services will be developed with security and privacy consideration in mind. For example, WP8 with the title of *Managed Wireless for Smart Infrastructure* presents remote configuration for smart infrastructure in which it enables remote configuration of wireless access points in homes. The remote configuration enables operators to manage many devices simultaneously without the need for technicians in preemies. In addition, remote configuration can be accounted as security measure to respond to zero-day attacks quickly by patching vulnerabilities in many devices simultaneously. Meantime, remote configuration system encrypts monitoring and management communication between remote device and auto-configuration server in order hinder eavesdropping by malicious parties. Besides, remote configuration mechanism only monitors and manages wireless parameters of WiFi access points in homes.

Eye Networks leads the work in WP8 and based on the results from SCOTT work, it has established a cloud-managed service for monitoring and management of WiFi installations. The service, called EyeSaaS Carat, is designed for Internet Service Providers that quantifies and improves WiFi quality of experience (QoE) for consumers. The service is cloud-based and supported by artificial intelligence (AI), thus it is scalable and applicable to other service areas.

While scientific analysis tends to analyze the impact of each parameter, the focus on the Carat service is providing the resulting insights in a simple, actionable way are the keys to QoE

improvement. Carat collects performance data from home gateways and uses machine learning and data analytics to proactively detect and resolve wireless connectivity problems.

EyeSaaS Carat supplies actionable insights that inform and enable services across departments. The outcome is reduction in support costs, increased customer satisfaction, and a reduction in subscriber churn.

The Carat data gathering agent is a script that allows the ISP full visibility of the source code and control of the entire process. All data and commands are sent in human-readable formats. Server communication is encrypted when supported by the CPE.

The service providers try to do not see a home as a black box and the main change that are on the way is the change from *"I don't know what is going on in your home"* to actually say *"yes we can identify the devices which are in faulty or trouble, we can identify your network problems and we can help you fixing your network problems"* (See Figure 7).

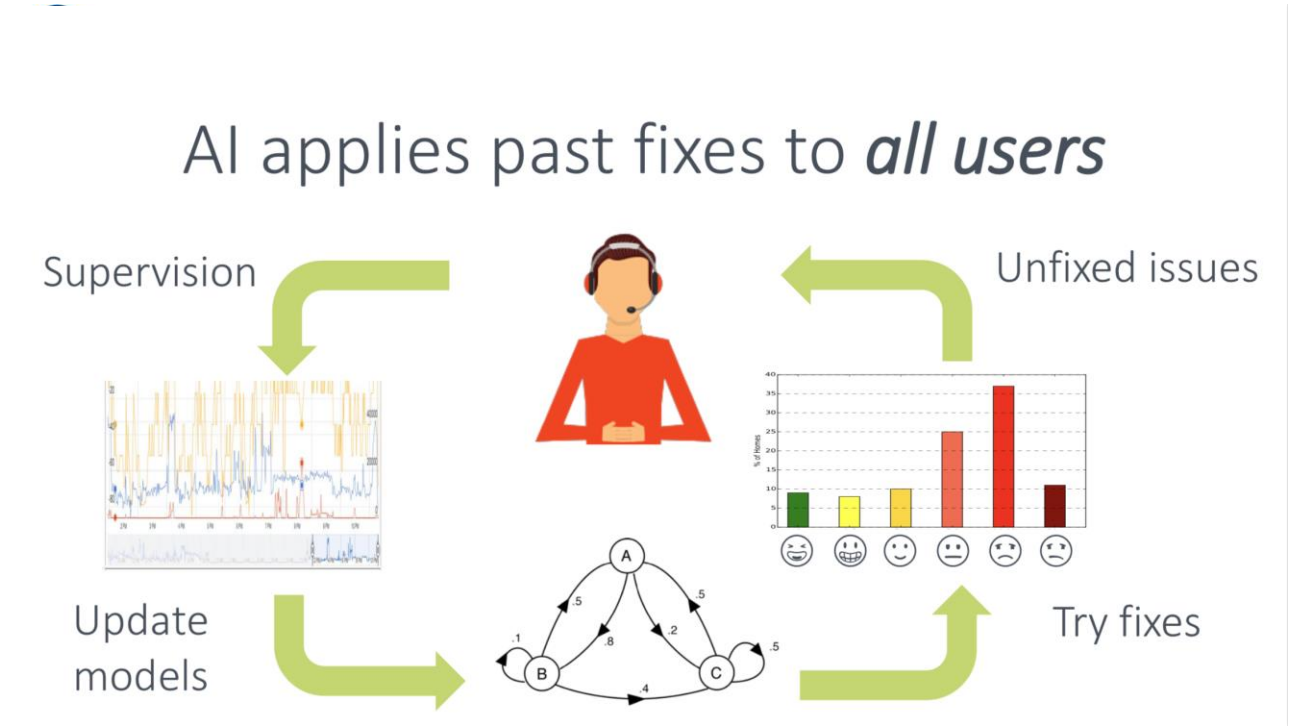

Figure 7 The AI cycle for supervised error fixing [9]

Figure 7 shows the AI cycle for supervised error fixing, based supervision of the real network traffic, then creating state models do match the network traffic to the potential sources of error, and providing suggestions for solution. A typical example is a bad WiFi coverage in a home, which is characterised through low capacity (2 or 5 Mbit/s) data rates, low energy of the receive signal (RSSI), large retransmissions due to bit errors, and an overall low cell capacity of the wireless. While some of the characteristics, e.g. low capacity communication, might be a result of limited device capability, the combination of the indicators give a clear picture of "what to fix". As an example, bad WiFi coverage can often be solved through Mesh networks, where multiple access points (APs) talk to each other and allow clients to roam to the AP with the best connectivity.
The task of identifying network issues is not based on roughly

EyeNetworks has co-developed and implemented “Carat”, which, in addition to the monitoring, provides automation options including:

- Setting WiFi parameters via the agent or an ACS integration
- Event-based service provisioning
- Correcting misconfigured devices

Apart from the wireless management, we focus in SCOTT on security and privacy work, including the understanding of what a security class is, what a privacy level is and how we can bring this understanding of security and privacy out to the society. So far, the multimetric framework was finalized and builds the frame for measurable security, privacy and Trustability.

The multimetric framework addresses both components of network layers and system layers in achieving a dedicated criticality or security for the parts in question which means it allows us to not only get an overall assessment of the security, privacy and trustability but also a detailed assessment of which components are the critical components in security value chain, ranging for example from an embedded system over a communication link into a vacant system and from there into the headset of a user

The current state of the art is that the multimetric system is applied in variety of projects as a part of the hackathon activities in WP30 and is also part of an industrial applicability.

Where the main challenges are to

A) Bring the understanding of measurable security into an industrial context
B) Define the security classes which needs to be evaluated

As one of the application examples, the Norwegian government has now introduced security classes CIL1, CIL2, CIL3 for the operation of the smart grid.

Both in the transport and in the distribution networks we are amongst the collaborating with our partners on how we can make the compliments to this security classes. The process of getting measurable security into the understanding of the public and the involved businesses has been more complicated and is taking more time than expected. The reason is that the term of measurable security is still not a part of common understanding of how security assessment is done, because security assessment is seen as a response to an attack in most of the industrial areas. Thus, the thinking in security classes and how functionalities will supply the security classes can only be exemplified for the certain domain.

Recognizing and collecting security functionalities to find all security aspects is helpful to consider a different set of metrics together and finally assess security in a system. To do so, we have investigated and studied the well-known security standards, and added the standards to the security ontology as specified in Figure 8.

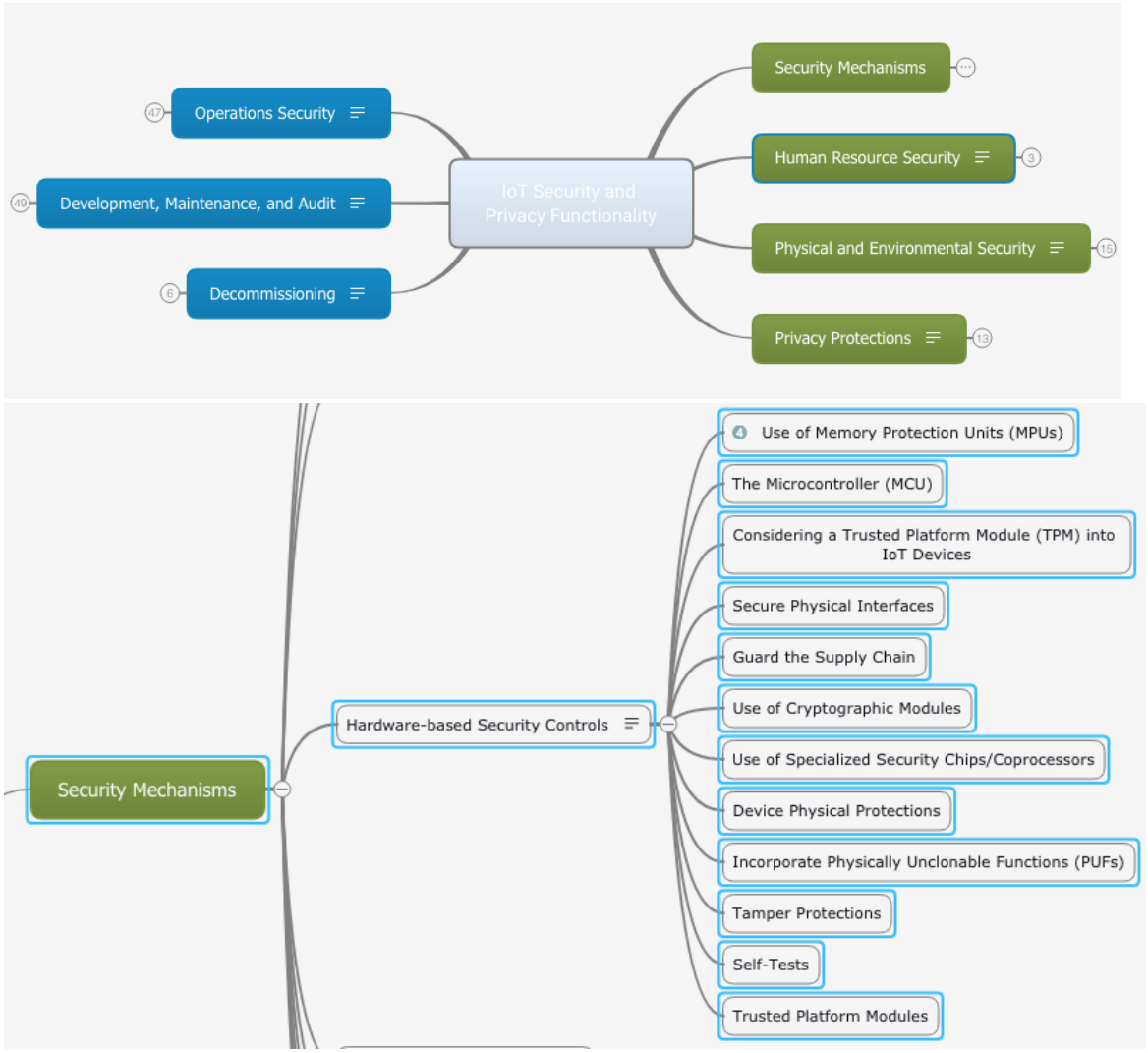

Figure 8 Security functionalities for life-cycle assessment of IoT devices [10]

Based on the security functionality, we have established a novel model for defining security classes (see Table 4. 1). While a traditional risk assessment uses likelihood/frequency and impact as the two axes in the table, such an argumentation does not hold for IoT systems. Reason is that the vulnerability of IoT systems can't be judged out from the frequency of attacks, but rather from the exposure to sources of attack. Such sources of attack include both physical and IT-based exposure of the IoT (sub-) system.

Catastrophic	Class A	Class D	Class E	Class F	Class F
Major	Class A	Class B	Class D	Class E	Class F
Moderate	Class A	Class B	Class C	Class E	Class E
Minor	Class A	Class B	Class B	Class C	Class D
Insignificant	Class A	Class A	Class A	Class B	Class C
Impact/Exposure	1	2	3	4	5

Table 1 Smart Grid Security Classes [11]

Table 4.1 presents the novel approach for IoT security classes, where impact is considered along the line of insignificant, catastrophic, and exposure which is expelled based on both physical and IT-exposure.

Security class A represents a system with the best security (highest security class) and F represents the worst (lowest security class) one.

The current work is to bring security functionalities and IoT security classes together and apply the methodologies on the SCOTT use cases. Specifically, our work focusses on the security functionality (Figure 8) to be applied for the specific security classes. As an example, the highest security class (Class A) needs minimum exposure. In addition to physical exposure, a Class A device needs also security functionality to reduce the IT-exposure, e.g. firewall, port control, white listing.

The security classes can be applied in WP8 to use for future home applications where we clearly see that the current trend of all wireless traffic joining in one router and being handled simultaneously creates an extremely open attack surface for all kind of security attacks being out there. Thus, our focus in measurable security is first, to increase the awareness with industry, second, to convince suppliers that we need even in the home domain applications specific routing and third, to define the security classes which are needed for the different kind of applications and the routing profile going together with it.

In fact, we are working on having security classes on the appliances and then put the functionality which is needed for those security classes either as part of the routing or as part of the separation that we say all the services in that class have their own slice and they are by that one physically separated from other slices. For example, when a guest interred to a smart home, he can only have password to general items not a health information of the host. In the smart home you may have difference between controlling the lights and opening the door which are completely different scenarios and of course to open the door, we need higher security and higher monitoring, etc. In terms of security classes, we say for example, the alarm services, door opening and maybe health services are class A, then car charging and that energy control are class B or C, etc.

In addition to the mentioned point, what has reached the attention is the need for free access to information as being the lowest layer in an information society where we amongst others pick up the draft recommendations from the United Nations high level panel on digital collaboration pointing out on inclusiveness, trust and capacity building as the core blocks for enhancing digital cooperation. We discuss with partners on how SCOTT can contribute A) with the security profile on separating the applications and B) Making the capacity building on security related to digital systems to be available for all.

4.2 European Leadership and Market Opportunities

European leadership and market opportunities are introduced to address European societal challenges.

4.2.1 European Adaptation to Digitisation and Societal Challenges

Europe has been slow in adapting digitalization in industry. Though the industry 4.0 was stated as being the leader in the transition process towards digital industries, the applicability of the digital is

still dominated by platform industry mainly sitting outside of Europe. Thus, the focus in SCOTT is on ensuring the security and privacy awareness of solutions in the connectivity. Our experiences show that Europe has a tremendous impact on the world regulation when it comes to security and privacy. As an example, the GDPR regulations resulted in that Canada, California and Australia have adapted the principles and put them into their laws. Furthermore, GDPR has changed even big businesses. Microsoft has announced that all the portfolio is going to be GDPR compliant and that they don't make differences for any products around the world. Meaning at the end of the day, an introduction of European standards preserving on privacy and ensuring security will get an impact on the world. In the society the trust in digital has decreased in the last year. For example, Facebook-Cambridge Analytica data scandal as a major political scandal in early 2018 have made a complex to regain confidence of the European society. Through SCOTT we want to lift up the awareness of the members of the society by putting measures on it. Measures both in terms of security (security classes) and measures with respect to privacy, in terms of privacy labels. The public awareness of the different grades of security and privacy will help both customers to get empowered in digital society and help industry to bring new products in the market which guarantee even more privacy than what is demanded by GDPR.

We consider three types of security in SCOTT, namely, the IoT Security, the Cyber Security and the Societal Security. Both of IoT Security and the Cyber Security are immediately getting an impact on what we call the Social Security, but it can also have an impact on the trust in business (See the Figure 9).

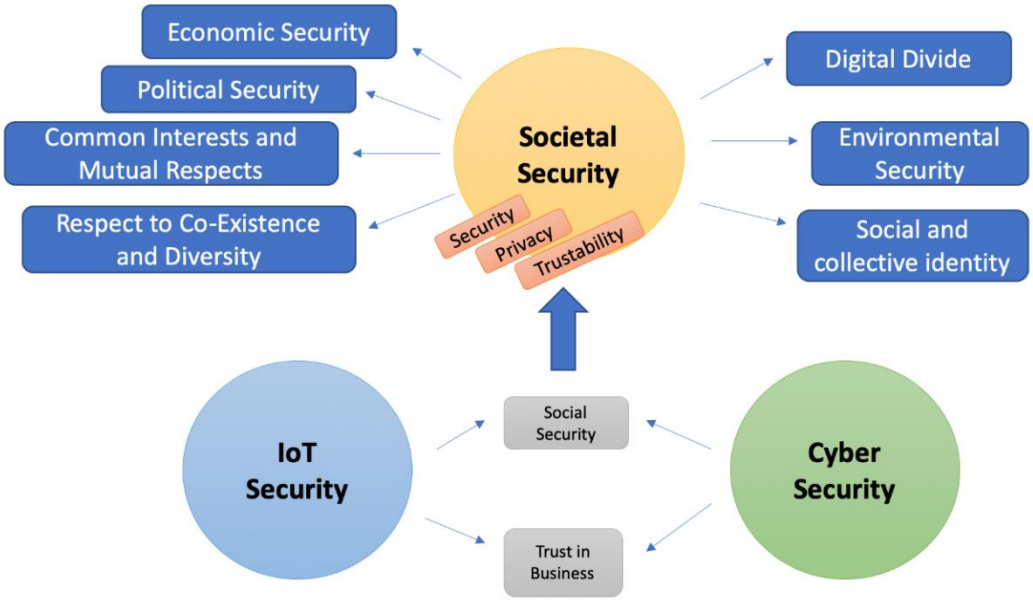

Figure 9 From IoT- and Cyber-Security to Societal Security

From the three security aspects that are shown in Figure 9, we mainly focus on Societal Security and we are not addressing the Cyber Security and the threats on IoT. The main focus in Societal Security is the ability of a society to persist in its essential character. In addition, providing the societal

security for all in the world can be considered as a global goal. Figure 9 also shows the basic components of Societal Security. A part of SCOTT is working on the Digital Inequality or the Digital Divide, so here we focus a bit on Digital Divide.

Digital Divide refers to the gap between demographics and regions that have access to modern information and communications technology, and those that don't or have restricted access. This technology can include the telephone, television, personal computers and the Internet. If people don't understand the digital, then people get afraid, they will loose the trust and they will not adapt the digital society.

In the other hand, in Social Security, the aim is to protect the society by putting counter attacks in protections, firewalls, etc. to do not let external things getting into the inner circle, so it is about protection mechanisms which are not directly focused by SCOTT but if the Social Security is threatened then it has a direct implication on the Societal Security, because in the Societal Security you have this things as trust in the society, you have things as feeling well, not feeling insecure and it is about the perception. If for example, the people´s perception are that their state can handle, organize, and ensure jobs then everyone are on the Societal Security. If the state misses the capabilities for providing the trust, then people lose the confidence and when people lose the confidence, then the state loses the power of getting something down because everyone just put question on.

4.2.2 Related initiatives for Societal Security

Nordic Centre of Excellence for Security Technologies and Societal Values (https://cast.ku.dk/nordsteva/) has the objective to map and critically analyze the relationship between security technologies and societal values. There is also a program called Nordic Societal Security Program (http://cast.ku.dk/nordsteva/) which targets to develop new knowledge about and solutions for the many aspects of societal security affecting the Nordic countries.

In addition, European Societal Security Research Group (http://www.societalsecurity.eu/wp/) exists and their main objective is to use empirically-driven analysis and theory innovation to generate new insights into how EU cooperation is contributing to the security and safety of individuals.

SCOTT focusses on technologies which are linked to sensors and communications for the next level of systems. As such, SCOTT does not address the societal implications directly. However, the introduction of measurable security, security classes, trust frameworks and privacy labels are the contribution to a security- and privacy-aware society.

4.2.3 Privacy beyond GDPR

As mentioned before, beside the security discussion, we have worked on privacy awareness in SCOTT and started to discuss about GDPR. General Data Protection Regulation (GDPR) is a new set of rules designed to give EU citizens more control over their personal data. It aims to simplify the regulatory environment for business so both citizens and businesses in the European Union can fully benefit from the digital economy.

"The digital future of Europe can only be built on trust. With solid common standards for data protection, people can be sure they are in control of their personal information," said Andrus Ansip, vice-president for the Digital Single Market.

It is an essential principle of the law throughout many nations of the world that an individual has the main right to his/her personal property. The right to exclude people from using one's property. This property should include data and information as well.

That lack of legal authority concerning ownership of personal information has changed significantly with the recent enactment of the (GDPR) in the European Union (EU). In a broad sense, the GDPR has given EU residents power over their personal information. The GDPR bill, which was passed in 2016 and took effect in May of 2018, grants EU residents substantial rights regarding their personal information. Those rights include:

- Right to be forgotten
- Right to access
- Right to data portability

Those rights listed above afford EU residents the ability to have their personal information erased, disclosed, or transferred by a company who possesses, has control, or otherwise processes that information. The GDPR also places a heavy burden on companies engaged in the collection, maintenance, and use of personal information.

Under the GDPR, companies must operate on a new level of transparency with EU consumers. The GDPR requires a company to receive consent for purposes of what information it will collect and what it will do with that information after collecting it. A company must also provide all its policies (Privacy Policy, Terms of Usage, etc.) in clear and plain English absent of legalese. In addition, companies must appoint a Data Protection Officer ("DPO"), who must map and classify the personal information of EU residents, provide oversight of data security, and correspond with the Data Protection Authority (the "DPA"). Failure to comply with the GDPR is costly, and fines of up to 4% of annual turnover or $23.4 Million can result under its penalty provisions. [12]

To ensure GDPR compliance, Data Loss Prevention (DLP) is necessary. DLP is a strategy to make sure that the end users do not send sensitive or critical information outside the corporate network. It is also used to describe software products to control what data end users can transfer by helping a network administrator.

The benefits of DLP can be categorized as below [13]:

- Improve visibility into their enterprise's data loss risk, deliver measurable risk reduction, and stay ahead of emerging threats and new technologies.
- Educate and protect well-meaning employees and third parties from accidentally leaking or losing confidential data.
- Enables rapid implementation, delivers predictable costs, and reduces total cost of ownership.

Therefore, DLP needs to be considered by the systems to work efficiently in terms of privacy.
Finally, the third solution of SCOTT, addressing smart sensors, is described as below.

4.3 Smart sensors and actuators

Smart sensors and actuators are required to foster interoperability, scalability, and reusability.

European sensor industry has been strong in providing solutions. Amongst others at the mobile network is an excellent example of how technologies have been adapted and with the currently already existing 4G IoT and other IoT standards, Europe has still dominant position in using mobile network capabilities for industrial processes. 5G goes even one step beyond and it is focusing dedicatedly on two aspects related to the smart sensors and the actuators by introducing the massive IoT with interoperable standards to connect and by focusing on the Ultra Low Latency Communication used in industrial automation systems.

Through SCOTT we have addressed wireless sensors and the ecosystem for wireless and mobile communications, as outlined in the use cases and technology building blocks mentioned in Chapter 5. The IoT ecosystem consists of technology for sensors, communication within networks as well as to outside servers, and certainly addressing trust as driver for societal acceptance. By addressing this ecosystem in a holistic approach, we ensure the adoption in Europe, and thus contributed to European leadership.

5 USE CASES AND BUILDING BLOCKS CONTRIBUTIONS

5.1 Use Cases Contributions

Managed wireless is mainly reflected in WP7 (Air Quality Monitoring for Healthy Indoor Environments) and WP8 (Managed Wireless for Smart Infrastructure). These are the core work packages of having the idea of managed wireless, though what we have seen is that the control of wireless communications is essential for most of the use cases in SCOTT. As an example, we will use WP21 (Assisted living and Community Care) handles wireless in the context of healthcare.

5.1.1 WP7 Air Quality Monitoring

WP7 focuses on integration of various sensors using mainly wireless interfaces to enable advanced services in buildings. Air quality monitoring is one of the examples of taking variety of sensors which is not only being direct air quality but also being door sensors and other sensors contributing to the knowledge of people in the domain.

In WP7 the developed monitoring solution is aimed to be integrated into the cloud and have the data available for creating new types of services and for supporting and enhancing existing ones. The backend solution also acts as the platform for the data fusion and data analytics components. These components provide the processed information to be utilized by different services and users such as building maintenance and management personnel. The utilization of external data sources to enrich the analytics, such as weather information will also be explored. The data need to pre-process to allow privacy protection (e.g. humidity and temperature increase in the bedroom can probably regarded are very personal information), but on the other hand the abstract data analytics should be able to process the information in such a way, that a general building management is still possible.

5.1.2 WP8 Managed Wireless

WP8 has introduced, standardized protocols and has built monitoring system for the quality of wireless which is amongst the European champions in managing wireless. The expertise of Europe's leading security company, F-Secure, in IoT security has resulted in the formulation of managed and monitored wireless, especially with the respect to security and privacy monitoring. In a collaboration between SCOTT partners, Eye Networks and F-Secure, discussions are ongoing to build a software development kit (SDK) for enabling ISPs to both managed and monitored wireless and IoT networks (That is the core message for WP8). Thanks to SCOTT both Eye Networks and F-Secure in their positions as expertise and domain leaders in managed and monitored wireless. Through the combination of the expertise of the partners, with F-Secure adding the big-data measures on security of IoT, and EyeNetworks adding the deep insight into the wireless networks, we have paved the way towards trusted wireless networks, being monitored and managed to answer the demands of the novel applications such as eHealth, alarm and energy control or other home automation tasks.

5.1.3 WP21 Assisted Living and Community Care

WP21 is about fall sensor and fall alarm of elderly which is then coupled to the home system in order to open a door in case of someone falls and then people from outside can be awarded that the person inside can't open the door, so it needs to be a secured method of involving people in other places and letting them open the door.

The current implementation scenario is rather limited. The one which we extended was this context aware and person life service. So, we can say that an extended WP21 scenario is where we profile the user based on electricity and water consumption monitoring, in addition to the fall sensor, as the person may need help even without the fall sensor, we can then establish a probability of that something has happened to the person. Now depending on the probability and the grade of what eventually might have happened we then have a matching with the help care which could be neighbours, family members, normal health workers or emergency services. So, what we have in total are these three blocks of anomaly detection, grade of incident (if possible) and the social in public network (the social network of the person) then it is semantic decision making to what is happening. Now what is all involved are huge degrees of capabilities on the home network to measure electricity and water consumption as very intrusive and privacy technology which then needs to be implemented in privacy aware node on the edge of the network, meaning in the router of the home.

A home monitoring service as an example of a privacy aware service, using the current infrastructure, additional services envisaged by using the same technologies may actually link to the electrical system being in the home when it comes to security, alarms and proactive maintenance. As an example, the failure of electrical instruments (for example white goods) are often given with some pre-warnings such by using big data analysis, one can from the high frequency electricity metering. One can establish profiles of A) the infrastructure within the home and B) giving warnings if the fridge door is open or if the fridge is completely iced and uses much more power than it usually would need and for that one there are already existing studies showing the capability of EG TV channel identification based on high frequency meter data. What is new in SCOTT is the privacy aware of monitoring of the electricity consumption as an Edge service which can be the edge of the network and not in the centralized cloud, thus what we use in SCOTT is a distributed cloud where we have an instance in the centralized cloud. So, it is the distributed cloud with an instance at the edge allowing privacy aware of processing of privacy sensitive data.

5.2 Building Blocks Contributions

The technology building blocks in SCOTT had dedicated goals, first of all in the development of technology needed to address the trust, security and privacy challenges of the future. All building blocks are implemented in at least one use case, and their impact is described for other use cases. As this report focusses on the market impact of wireless, only those building blocks related to wireless are listed.

5.2.1 BB23.A Dependable Wireless Sensor Network

The BB23.A addresses the security issues in the WSNs, attending other relevant aspects of the performance which are Quality of Service and Autonomy. The BB will analyse the design space exploration of different solutions for a given application, trying to optimize the quality of the solutions. The BB will be mainly used and tested in the railway UCs.

5.2.2 BB23.B End-to-end assured QoE

The BB23.B provides traffic classification and prioritization capabilities covering a wide range of QoS profiles including those that fits in critical mission applications where minimum delay and maximum priority must be assured. This BB adapts to the particular behaviour of the M2M IP traffic where

packets to be sent are sporadic and low bitrate. Finally, it also provides mechanisms to adapt to mobility scenarios where coverage loss events may occur dynamically and also the adaptation to sudden changes of the capacity of the selected WAN interface is critical for a proper QoS prioritization.

5.2.3 BB23.J Reliable Wireless Multi-hop Communications

The BB23.J defines mechanisms and algorithms to add basic QoS features to the communication between nodes inside the WSN. This is achieved thanks to the deterministic medium access, and a traffic periodization protocol for adding packets to different queues and buffers according to type and priority flags. This ensures, on one hand, that critical data is received with less delay and with delivery guarantee; and on the other hand, that the rest of the traffic is routed successfully with minimal losses. Furthermore, quality metrics are used as input for path and route selection and as feedback for the network managers and deployment tools, enhancing the stability and lifetime of the network and the user experience when using a WSN.

5.2.4 BB23.K Reliable Wireless PHY and MAC

The BB23.K provides a reliable wireless physical layer to be used in the wireless sensor network. The reliable PHY will provide a fault tolerant wireless transmission between sensors and data concentrator. The data concentrator will receive the information from the application level using a Ethernet or a common interface. The concentrator will translate the information from a wired interface to the wireless sensor system. The reliable wireless system could be used to send critical control data to sensors and actuators replacing the wired system. The use of reliable wireless system to send or receive critical data replacing wired communications will increase the safety of the system, decreasing the complexity of a wired system. With this system, wireless sensors could be located in harsh environments. The BB is related with "safety" because the wireless PHY proposed in this BB will be used to send and receive critical control data from/to a sensor.

5.2.5 BB23.L Routing and scheduling in real-time WSN

The BB23.L is providing routing and scheduling algorithms, supporting dynamic adaptation, based on sensor data (from WSN or a gateway level). It is expected that the designed algorithms will be able to manage events from sensors with high acquisition rate, performance test will be conducted once developed and deployed.

5.2.6 BB23.Q Towards a Safe Virtual Coupling

The BB23.Q aims at a Smart Train Composition Coupling Application (STCC Application) to support the virtual coupling between trains in the low-speed manoeuvring mode and the corresponding vehicle-to-vehicle (V2V) communication support.

Currently two compositions, where a composition is a sequence of railroad carriages that form a unit, are joined by pneumatic, mechanical and electrical connections, doing the operation procedures with trains very difficult, expending a lot of time and personnel. At the same time, the current connections imply an interoperable restrictions, because the compositions to be joined must be the same model or at least compatible. Self-configuring adaptive solutions providing plug-and-play features such as Virtual Coupling may solve this issue. In a Virtual Coupling, the compositions run together, as

coupled, but without any physical connection, thus trains manufactured by different companies and with different interfaces could be virtually coupled, driven together by the leading cabin and sharing the same traffic slot. In this scenario, Virtual Composition solutions shall require a functional layer where the required business logic to allow different compositions to understand each other will be implemented. All this functional layer will also require V2V Communication support.

5.2.7 BB24.A Remote Configuration of Infrastructure

The BB24.A provides the remote monitoring and management capability toward the managed wireless concept. Hence, the main objective of BB24.A is to provide remote monitoring and management mechanisms in wireless networks, particularly remote monitoring and management of WiFi access points using open standard protocols. Indeed, BB24.A will develop a software component for remote configuration of wireless devices using open standard protocols such as TR-069 and TR-098. Therefore, BB24.A will result in establishing a cloud instance of open standards and infrastructure management standardization approaches.

5.2.8 BB24.B Addressing and Mobility Management of Devices

The BB24.B defines addressing of security and privacy requirements for SCOTT sensors/actuators, including potential mobility management mechanisms.
Addressing of sensors and actuators in SCOTT in a non-trivial issue given the fact that different access networks may be used, and sensors/actuators should be movable from one network to another. Existing limitations of current access networks (e.g. private IPv4 addresses, limited IPv6 availability, CGNAT in mobile networks, enterprise networks with tight security, non-IP networks) make it difficult to identify nodes. SCOTT nodes should be flexible to deal with these issues in order to be used in as many networks as possible.

5.2.9 BB24.G Mobile Edge Computing

WSN applications with relaxed real-time requirements may perform well with a centralized cloud in the Internet. In such a case, the physical location of a cloud server may in the worst case also be located on another continent. Other WSN applications however, do require lower round trip times and therefore need a distributed cloud, i.e. cloud servers located close to the physical location of the WSN (Mobile Edge Computing, Fog Computing). The edge computing provides also the possibility to filter and pre-process too sensitive data.
The main output is analysis of applicable solutions for mobile edge computing and potentially prototype implementation to be used in SCOTT use cases.

5.2.10 BB24.J Wireless Vehicle Interface

The objective of the BB24.J is to develop and demonstrate an automotive remote diagnostic and update system with secure device interfaces relying on NFC-technology and cloud-based services in the backend. Realized solution shall provide access to in-car network and V2X connectivity.

5.2.11 BB24.L Adaptable network slicing

The BB24.L experiments the network slice concept, which allows the next 5G mobile network to support a variety of IoT applications ranging from massive Machine Type Communication to Ultra

Reliable Low Latency ones. Network Slicing combined with the ubiquitous presence of the mobile network will enable the connection of many devices, static or mobile to the Internet in a trustable way.

5.2.12 BB26.A Autonomous Wireless Network

The BB26.A remains linked to intelligent transport systems applications considering the existing baseline for trackside networks within the rail domain. The existing ones rely on cables between wayside cabinets to deliver communications, which considerably increase the cost of the infrastructure (both CAPEX and OPEX). This fact often causes problems as a consequence of the weak established link on the trackside infrastructure, which can be damaged by vandalism acts or simply by unfavourable weather conditions.
The proposed reference architecture will provide a transportation layer across the complete infrastructure to the cloud/centralized system. This will be used to distribute all the necessary data sensor/actuator/other to/from the infrastructure (including vehicles) to/from the cloud/centralized system. Moreover, cabling communication systems are particularly difficult within the rail domain, as trains are composed by several moving parts. Those are some of the reasons why BB26.A propose a reference architecture for an autonomous wireless communication infrastructure that will provide mobility and connectivity to both ontrack and onboard elements.

6 CONCLUSIONS

Future home and business buildings will see a variety of devices, all predominately providing services using wireless networks. Regarding the devices, they will run from very primitive ones with limited energy and processing power to very powerful ones having access to continuous power supply. Needless to say, it is not only the energy consumption, devices will also vary in the provision of security for the services they are offering. A resource-constrained device will not be able to achieve the same level of security as compared to a powerful device. Thus, mixing both device types in one network will reduce the security of all communications to the security of the device having the lowest security level. Novel concepts including the separation of communication, as well as management and monitoring of wireless infrastructure, need to be implemented. As an example, monitoring misbehaviour of devices will allow to isolate them and not let them infect other devices, services or the communication network.

To achieve successful services, it is not only a question of responding to technology and service challenges, it is also a question of how to bring the necessary infrastructure into the customer's home. The operators are ideally positioned to integrate the services and bring the infrastructure into the homes. However, current return-on-investment requirements for operators prevent them from rolling out complex and thus expensive infrastructure.

Low cost gateways, allowing the free access to information, are seen as a feature for digital inclusion of everyone. On top of that comes a service portfolio, answering the specific need of a user.

SCOTT contribution to the future of WiFi and wireless networks by addressing all three aspects:
1) security and privacy needs of services,
2) monitoring of wireless networks to identify failures and deficiencies, and
3) management of networks including reallocation of devices and isolation of malicious services.
Driver of our work were the industrial demands from ISPs, offering high-bandwidth services (100 – 1000 Mbit/s) to the home, which are often hampered by WiFi networks not delivering the requested capacity. Interference is often a limiting factor, as well as bad coverage, together with other wireless failures contributing to more than 75% of all calls to customer service at ISPs.
Furthermore, addressing security in the wireless networks requires monitoring and management of devices, and identification of erroneous behaviour. Through the European collaboration including EyeNetworks, F-Secure, TYCO and others we have addressed solutions for more secure and trusted operations of wireless services.

In addition, this report provides an outlook on standards for both wireless and mobile networks, being WiFi6 and 5G mobile technologies. Both technologies harmonise well with each other, and commonly prepare for both high-bandwidth services, as well as the introduction of energy-saving technologies for battery driven sensors and devices.

7 REFERENCES

[1] S. Jose, “Cisco visual networking index (VNI) global mobile data traffic forecast update, 2017-2022", Cisco white paper, 2019.

[2] GSMA, "The Impact of the Internet of Things, 2015 The Connected Home.”

[3] Martin Jürgensen, “How to Deliver Wi-Fi as a Service", Eye Networks shared Insight, Apr 2019, https://eyenetworks.no/en/shared-insights-2019-trust/

[4] Tore Richard Andreassen, “11ax Technology and Portfolio Introduction", Eye Networks shared Insight, Apr 2019 https://eyenetworks.no/en/shared-insights-2019-trust/

[5] https://www.techradar.com/news/what-is-5g-everything-you-need-to-know .

[6] https://www.ericsson.com/en/ericsson-technology-review/archive/2017/evolving-lte-to-fit-the-5g-future

[7] Kate Gilmore, UN Panel discussion, November 2017.

[8] Tom Gaffney, “Can We Trust Smart Things?", Eye Networks shared Insight, Apr 2019 https://eyenetworks.no/en/shared-insights-2019-trust/

[9] Eren Soyak, “Three Pillars of Clear Home Wi-Fi", Eye Networks shared Insight, Apr 2019 https://eyenetworks.no/en/shared-insights-2019-trust/

[10] Elahe Fazeldehkordi, Olaf Owe, Josef Noll, “Security and Privacy Functionalities of Internet of Things", 17th International Conference on Privacy, Security and Trust (PST), 2019

[11] Manish Shrestha , Christian Johansen , Josef Noll, “Security Classification for Smart Grid Infrastructures", Research report 476, December 2017, ISBN 978-82-7368-441-7 , ISSN 0806-3036. Department of Informatics, University of Oslo.

[12] https://www.cpomagazine.com/data-protection/the-future-of-data-privacy-corporate-compliance-in-a-post-gdpr-global-market/

[13] https://www.virusrescuers.com/our-solutions/data-loss-prevention/

A. ABBREVIATIONS AND DEFINITIONS

Term	Definition
AP	Access Points
eMBB	Enhanced Mobile Broadband
SGNAT	Carrier-grade NAT
DPA	Data Protection Authority
DLP	Data Loss Prevention
DPO	Data Protection Officer
EU	European Union
GDPR	General Data Protection Regulation
UNOG	United Nations in Genève
IoT	Internet of Things
ISP	Internet Service Provider
mMTC	Massive Machine Type Communication
NFC	Near Field Communication
NR	New Radio
pQoS	perceived Quality of Service
QAM	Quadrature Amplitude Modulation
QoE	Quality of Experience
QoS	Quality of Service
SDK	Software Development Kit
SMARTER	Study on New Services and Markets Technology Enablers
SNR	Signal to Noise Ratio
STCCA	Smart Train Composition Coupling Application
URLLC	Ultra Reliable Low Latency Communication
WSN	Wireless Sensor Network