The document reflects only the author's view and the commission is not responsible for any use that may be made of the information it contains.

SCOTT:
Secure COnnected Trustable Things

Market Innovation

Document Type	Deliverable
Document Number	D22.4
Primary Author(s)	Josef Noll | UiO Maunya Doroudi Moghadam | UiO
Document Version / Status	1.0 | 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
Peter Priller	AVL	Carlo Alberto Boano	TUG
Christoph Pilz	VIF	Ramiro Robles	ISEP
Frank van de Laar	PRE	Mateusz Mul	VEMCO
Salva Santonja Climent	ITI	Jose Luis Buron	ACCIONA - INDRA
Jani Koivusaari	VTT	Javier Uceda	UMP
Przemyslaw Kwapisiewicz	GUT		

FORMAL REVIEWERS

Name	Organization	Date
Ramiro Robles	ISEP	2020-09-08
Johanna Kallio	VTT	2020-09-10

DOCUMENT HISTORY

Revision	Date	Author / Organization	Description
V0.1	2020-04-15	Josef Noll	Inputs
V0.2	2020-06-01	Maunya Doroudi Moghadam	Inputs
V0.3	2020-08-28	Christian Johansen	Inputs and Overview
V1.0	2020-08-30	Maunya Doroudi Moghadam	Inputs and Overview

TABLE OF CONTENTS

TABLE OF FIGURES

LIST OF TABLES

1 EXECUTIVE SUMMARY

In this deliverable, UiO has provided the solutions that have been developed by SCOTT partners as the market perspectives. The partners' contributions to this deliverable include the works that they have done in the SCOTT Work Packages and Building Blocks which contain the objectives, achievements through SCOTT and what they have for the market. Some of the solutions are ready to be commercialized and some others have already been commenced in existing commercial or market roadmaps of the involved companies.

Total of 18 work packages and building blocks' leaders of SCOTT have provided their contributions. Work packages are namely, Managed Wireless for Smart Infrastructure, Secure Connected Facilities Management, Secure Cloud Services for Novel Connected Mobility Applications, Trustable Wireless in Vehicle Communication Network, Safe Freight, Traffic Management in Intermodal Logistic Hubs, Autonomous Wireless Network for Rail Logistic, Smart Train Composition Coupling, Trustable Warning System for Critical Areas, Assisted Living and Community Care, Security and Safety and Reference Architecture. The building blocks are namely, Trustworthiness Indicator, Vehicle-as-a-Sensor within Smart Infrastructure, Reliable Wireless Multi-Hop Communications, Big Data Analytics, Cross-Technology Synchronization, System Level Availability and Aeronautics.

Key words: managed wireless, market innovation, commercial solutions

2 INTRODUCTION

Throughout the work of SCOTT many partners have developed solutions that either are ready to be commercialized or have already been taken up in existing commercial or market roadmaps of partner companies. We list the most prominent and promising of these in the subsection of Section 3. It is always very important to connect the research achievements to market requirements.

We would like to give here a flavor of the diversity of solutions by shortly listing that we have picked from the text below, without claiming a particular rule for our picks.

TUG has developed and patented an award winning, generic and modular cross-technology communication framework named X-Burst for use in heterogeneous wireless environments like smart homes and is currently approaching several companies, including ARM Holdings and Nordic Semiconductors to investigate how to increase the marketability of the solution (see Section 3.15 below).

Through the managed wireless platform developed in SCOTT and its application within the operations of the company, EyeNetworks has become the de-facto market leader in WiFi knowledge in Norway (see Section 3.1 below).

GUT has signed preliminary cooperation agreements with the Port of Gdansk and one of the hospitals in Gdansk (Poland) for the multimodal positioning system developed during SCOTT (see Section 3.2).

CIT has filed a patent application with the Intellectual Property Office of the United Kingdom covering the online learning approach to uplink data rate estimation, aiming to offer this solution to interested parties under suitable licensing terms or further partnership with one of the SCOTT partners for commercialization and exploitation (see Section 3.8 below).

Indra, together with others like UPM, has develop an innovative railway system involving smart train coupling and wireless sensor network for rail that is breaking with the current paradigm, aiming to provide to the market segment a new solution that solves important problems faced by this industry (see Sections 3.9 and 3.10).

Besides such concrete commercialization activities and results, many good connections have been created between SCOTT partners that will continue after the project and foster new commercial endeavors. Moreover, SCOTT as a project has offered the partners an arena for presenting their various commercial solutions to the other partners, as well as to external actors through our several industry meetings. Due to its visibility, the SCOTT project has allowed our partners to have a strong promoting factor when showcasing their technologies in various show-forums outside the project, bringing them more credibility for their technological offers.

Several of the models or ideas which were not directly implemented are now part of standardization efforts and will thus be available to the market within the next few years. The respective SCOTT partners are managing such efforts. For those technologies and ideas where research papers have been published, this offers even more credibility in the viability of those results. Many SCOTT partners and results have been parted in such research publications, all of which have had a technological and/or implementation aspect.

3 SCOTT INNOVATION TO THE MARKET

In this section, we will highlight the Market Innovation coming from both use cases and technology developments. For each technology item, the contribution is structured into:

1) Objectives of the work
2) Achievements through SCOTT
3) Market innovation and perspective

3.1 Managed Wireless for Smart Infrastructure

3.1.1 Objectives

Managed WiFi was demonstrated in WP8 and developed through BB24.A in SCOTT. Managed Wireless for Smart Infrastructure use case is seen as an example of smart infrastructure developments. While current infrastructures are limited in terms of (remote) configurability and service differentiation, smart infrastructures will use a service-oriented view. This is a novel view where services, devices and systems will interconnect to provide added value or functionality, e.g. trusted connections in case of medical data, or secure and reliable communications in case of an alarm. Wireless communication has opened up a whole new dimension with IoT connectivity for cooperating cyber physical systems. We assume that there are already numerous different wireless sensors and actuator networks (“legacy networks”) from different providers and different administrative domains, which have to be connected to each other in order to provide added value and new services and applications.

However, these networks and systems are generally not homogenous and hardly are able to interact with each other. The main objective of this work package was to enhance the concept of interconnected bubbles significantly, by introducing interoperability, security/privacy functionality, remote management, and dedicated service-quality. This will include the following concrete objectives:

- Move from homogeneous controlled environments to heterogeneous environments with secured interaction between networks.
- Manage the wireless bubbles to make them secure and trustable
- Extend and connect bubbles and integrate distributed bubbles into the Cloud
- Extend the established multi-domain high-level architecture concerning security, trustability and cloud integration
- Go the last mile to market implementation

3.1.2 Achievements through SCOTT

Following the main objective of managed wireless, managed wireless incorporates security/privacy measures with technological implementations in order to improve trustability, quality of service and interoperability in the heterogeneous wireless environment. The demonstrator of WP8 incorporates various functionalities in the managed wireless platform including, monitoring, factory reset, reboot, change Wi-Fi SSID and firmware update. Each functionality attempts to realize WP8 and SCOTT objectives. EyeSaaS managed wireless platform enables remote monitoring and configuration of Wi-Fi access points (APs) and Internet gateways in home and buildings. The cloud platform connects and integrates networks or bubbles in order to perform unified management across different bubbles. In addition, managed wireless platform incorporates security and privacy measures such as remote software update mechanism with technical implementation such as quality monitoring in order to enhance trustability of wireless networks in homes and buildings. Finally, cloud implementation of the managed wireless platform improves quality of service and last-mile delivery of service providers.

Wireless components and services need to be secure and trustable to enhance the concept of smart infrastructure. However, current wireless networks follow the best effort approach such that wireless networks are good as long as they operate as intended, and service providers have no insight into the network to investigate whether the network can handle user expectation regarding quality of service (QoS) and quality of experience (QoE). Lack of insight can increase operational expenditure by increased technician roll out to the premises and number of support requests as well as customer churn. Remote monitoring and management are effective strategies to gain insight and accordingly improve QoS and QoE.

Therefore, WP8 presents a managed wireless concept by implementing remote monitoring and management of Wi-Fi access points and Internet gateways in order to enhance performance, security and trustability of wireless services in homes and buildings. The remote monitoring functionality provided insight into wireless networks by collecting network performance metrics such as wireless frequency bands, channel selection, bandwidth, signal strength, number of bytes sent and received, etc. In addition, monitoring network performance metrics enables operators to assess QoS in wireless network and accordingly evaluate whether the network can handle novel services in smart infrastructure. Then, operators require functionalities in order to configure remote devices to improve performance and security. Therefore, the WP8 demonstrator implemented a set of remote management functionalities such that operators can manage Wi-Fi access points and Internet gateways efficiently. The WP8 demonstrator implemented the following functionality in the managed wireless platform:

1) Monitor QoS in the home network,
2) Rebooting the router,
3) Change Wi-Fi setting of the Mesh network,
4) Reset to factory default configuration, and
5) Firmwares upgrade functionalities.

Rebooting functionality enables operators to reboot the remote device while changing Wi-Fi provides a capability to change SSID and password on customer demand. Operators often require resetting the running configuration to factory default in order to eliminate any misconfiguration while firmware upgrade enables operators to apply the latest performance improvements and security fixes on remote devices.

The BB24.A provides a cloud-based platform, with which operators can monitor and manage remote devices in a simple dashboard. In effect, functionalities and simple user interface of the platform enhance acceptability, performance and trustability of wireless services in smart infrastructure. Thus, Internet service providers and third-party service providers can use this platform to monitor QoS and manage their devices or services for improving user satisfaction and security measures while reducing their operational costs. In addition, the managed wireless concept can accelerate user readiness for novel services that require carrier-grade quality in smart infrastructure.

3.1.3 Market Innovation and Perspective

Through SCOTT, EyeNetworks has become the de-facto market leader in WiFi knowledge in Norway. Furthermore, through the international collaboration EyeNetworks has built a cloud management platform for managed WiFi devices being unique in Europe.

Through this platform, broadband network operators and Internet service providers (ISPs) have received a tool to handle customer requests in a much more satisfying matter. Traditionally, up to 75% of calls were related to WiFi, and the first line agent could only address the challenges by asking standard questions, like

- Did you reboot your device?
- Have you tested the speed by cable?

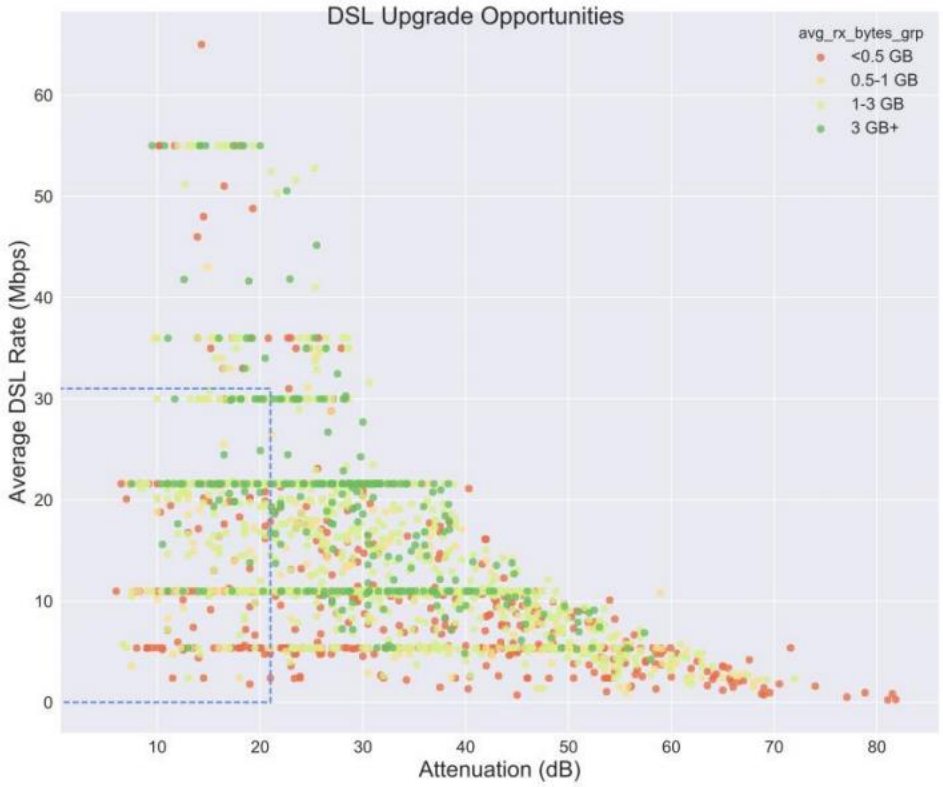


Figure 1. EyeNetworks analysis solution (by Carat) - here applied for DSL upgrade opportunity

The conversation between customer care and the customer was highly unsatisfactory, and often ended in “We will send you a new gateway”. Moreover, the gateways received in return, more than 80% of them were fully functionable.

Through the new analysis tool, the following achievements have been reached:

1) Analysis has been drastically improved. The employees at the ISPs got a tool at hand immediately being able to identify potential problems, including hardware failures of the modem.
2) Work of the employees has become much more meaningful and satisfactory. From previously talking “out of the blue” and being frustrated in not being able to solve the challenges, the employees now see the problem, and can suggest specific solutions.
3) Sales has increased, as the analysis shows that (i) more bandwidth can be sold “have you thought about upgrading to 30 Mbit/s – we have a specific offer for you”, as well as (ii) achieving a better WiFi coverage “I see that you have some devices with bad coverage. My recommendation is to extend the coverage by adding our premium package for the WiFi mesh”.
4) Remote configurability has been added, allowing interference avoidance through reconfiguration.

Thus, thanks to SCOTT, EyeNetwork has become the de-facto knowledge leader in wireless, and have increased sales substantially. Through the “Shared Insight” meetings, webinars and knowledge sites, a pro-active approach has been introduced to share the knowledge on connectivity.

3.2 Secure Connected Facilities Management

3.2.1 Objectives

Ensuring a high level of user comfort and simultaneously safety and security in facility areas, e.g. in buildings and infrastructure objects, is one of the most challenging and ambitious directions of development in situation awareness systems. Modern buildings are strongly focused on providing user-oriented services to increase human comfort and safety within the facility. It is hard to reconcile it with keeping high safety and security level at the same time due to the necessity of following the cumbersome security procedures. This use case goal is to increase safety and security keeping high users' comfort level. The main challenges are related to detection, identification and localization of different objects and their behaviour within facilities or areas of critical infrastructure. The other issue is extending the access control in physically separated locations with virtually defined areas with locally defined rules, e.g. customized area and behaviour definition, virtual fences.

3.2.2 Achievements through SCOTT

One of the main achievements of WP9 is developing and demonstrating the Multimodal Positioning System (MPS), a part of TBB23.P. The MPS addresses localization of assets and people indoors, which is one of the key WP9 objectives. Although there are a few solutions on the market providing Bluetooth-Low-Energy-based indoor positioning, most of them suffer from the same problem – they require a lot of BLE devices to achieve coverage. This is one of the biggest challenges in the adoption of the existing BLE-based indoor positioning systems. To address this issue, GUT designed a dedicated antenna and prepared localization algorithms leveraging it. As for April 2020, the GUT's MPS needs only one device requiring a mains power supply and 3 to 4 simple battery-powered BLE beacons to provide coverage of a room. The most popular system available on the market needs 3 to 4 devices requiring a mains power supply to do the same. Moreover, the first tests show that the MPS might not need these battery-powered beacons at all to provide a quality localization data. The BLE-Wi-Fi gateway equipped with the ESPAR antenna designed by GUT will suffice.

The real impact of the localization data provided by GUT's MPS on the safety and security of the facilities can be shown when it is combined with other systems and services, e.g. for authorization and authentication purposes. This allows for scenarios like:

- Detecting when an unauthorized person takes a valuable asset from a certain area.
- Preventing unauthorized people to enter a room in the presence of a valuable asset and let them in otherwise.
- Detecting when a person enters a potentially dangerous area and informing them about the risk.

These and many more scenarios possible when the localization data is available, require defining both physically separated zones as well as virtual ones, defined by geofences. Moreover, a very flexible approach to the management of access rules is required. In SCOTT, Vemco prepared and demonstrated a prototype of the Access Control System (ACS), a part of TBB23.P, which incorporates all of the mentioned characteristics.

To sum up, in WP9, GUT and Vemco prepared two systems designed to work together, i.e. Multimodal Positioning System and Access Control System. They allow for the definition of fine-grained, localization-focused access rules. This, together with UCC's algorithms for dynamic changing statuses of virtual zones, can have a significant impact on the safety and security of facilities. The main MPS differentiator, i.e. the reduced number of devices required to obtain the localization data, is expected to support the adoption of the technology.

Some of the videos presenting some of the achievements of WP9 are the following (published on YouTube):

- SCOTT WP9 promo video – Inviting guests to facilities made simple (link)

- Spatial-based authorization and authentication (link)

3.2.3 Market Innovation and Perspective

The major market innovation introduced by the Multimodal Positioning System stems from its novel approach to the objects' localization. Instead of using trilateration requiring the use of many BLE devices, the MPS uses one device equipped with a dedicated antenna and direction-of-signal-arrival algorithms. For the customer, fewer nodes translate into lower costs and easier system deployment. Moreover, the MPS' BLE-Wi-Fi gateway can be mounted on the ceiling, in the same way as a smoke detector.

GUT actively pitches the MPS. Preliminary cooperation agreements have already been signed with the Port of Gdansk and one of the hospitals in Gdansk (Poland). Moreover, Gdansk Lech Wałęsa Airport is interested in using the MPS as well. Some of these parties consider deploying the MPS as a standalone solution or in the ACS-MPS tandem, whereas others plan integrations with 3rd party smart building systems. In one of the exemplary cases, the MPS is used for improving the energy efficiency of buildings.

Vemco has a well-established customer base in Poland and abroad. The exemplary facilities using accardMP, a current version of the Vemco Access Control System, are refineries, energy plants, factories and warehouses. Two major customers of Vemco are interested in applying the solution for managing visits of guests at their facilities. Moreover, Vemco is planning further development of the Access Control System developed in SCOTT to make it production-grade and replace accardMP as the main system in the Vemco's offer. Some of the Vemco's customers have already shown their interest in improvements that Access Control System and Multimodal Positioning System combined can bring. Moreover, the new version will help Vemco to acquire new customers.

3.3 Secure Cloud Services for Novel Connected Mobility Applications

3.3.1 Objectives

Due to the long lifetime of a vehicle, software updates will be necessary. For instance, if after the release of a vehicle errors in safety functionality (such as malfunctions of the ESP) or security flaws in the software get detected. Security is of extraordinary importance for the aforementioned use cases, because the communication link can be subject to Man-in-the-Middle attacks. If secure communication protocols such as TLS are not properly implemented and configured, an attacker may attack the weakest link, for example, in the OTA update process and inject malicious software into the update. Without proper verification mechanism, the malicious updates will be installed which modify the correct functions (for example, safety functions) of a vehicle. Another example is that cryptographic keys or functions get compromised and need to be updated or changed. Also, new regulations by law could make updates necessary.

Vehicles are becoming increasingly connected with each other (V2V) and a connection to the internet is becoming standard. However, this "connectivity" makes it interesting for hackers to attack vehicles, because this technology allows them to remotely attack fleets of cars, which could lead to privacy issues and in the worst case even to safety issues. Unfortunately, this issue is not a theoretical issue anymore. To name a concrete example, a remote hack that takes control of a Jeep has been publicized few years ago (Miller and Valasek 2015). Hackers were capable of remotely locking and unlocking doors or starting the engine. Another example in the press was that hackers were capable of remotely opening BMW, Mini and Rolls-Royce vehicles in minutes by finding security flaws in BMW's ConnectedDrive service. These cyber-security incidents damaged users' trust in such digital services.

However, it is important that users accept new digital technologies, such as ADAS or BMW's ConnectedDrive service, and that a certain level of trust and reliance to such systems is achieved in order that users are willing to pay for it.

3.3.2 Achievements through SCOTT

The application scenario "Secure Over the Air Software Update (flashing Electronic Control Unit)" consists of three main components: AVL SSH (Secure In-Vehicle Gateway), MQTT Broker, and the Smart Service Framework.
The Frontend (car) and the Backend (cloud) communicate via a concentrator service over the internet, which serves as bi-directional messaging queue for both ends and temporarily stores the data during the exchange in an encrypted and authentic manner.
The concentrator module collects data from both the Frontend and the Backend and manages the distribution of the data between both ends over a secure and authentic channel. It is implemented as an MQTT broker and both the Frontend and the Backend act as MQTT clients (publishers and subscribers) and, in doing so, interact bidirectionally while using only outbound connections. The data in general and the security-relevant data appear on both the Frontend and the Backend are stored in a database located at the AVL, but will be outsourced in near future to the SCOTT cloud infrastructure hosted by SICS. However, in the first demonstration the AVL infrastructure will be used (See figure 2).

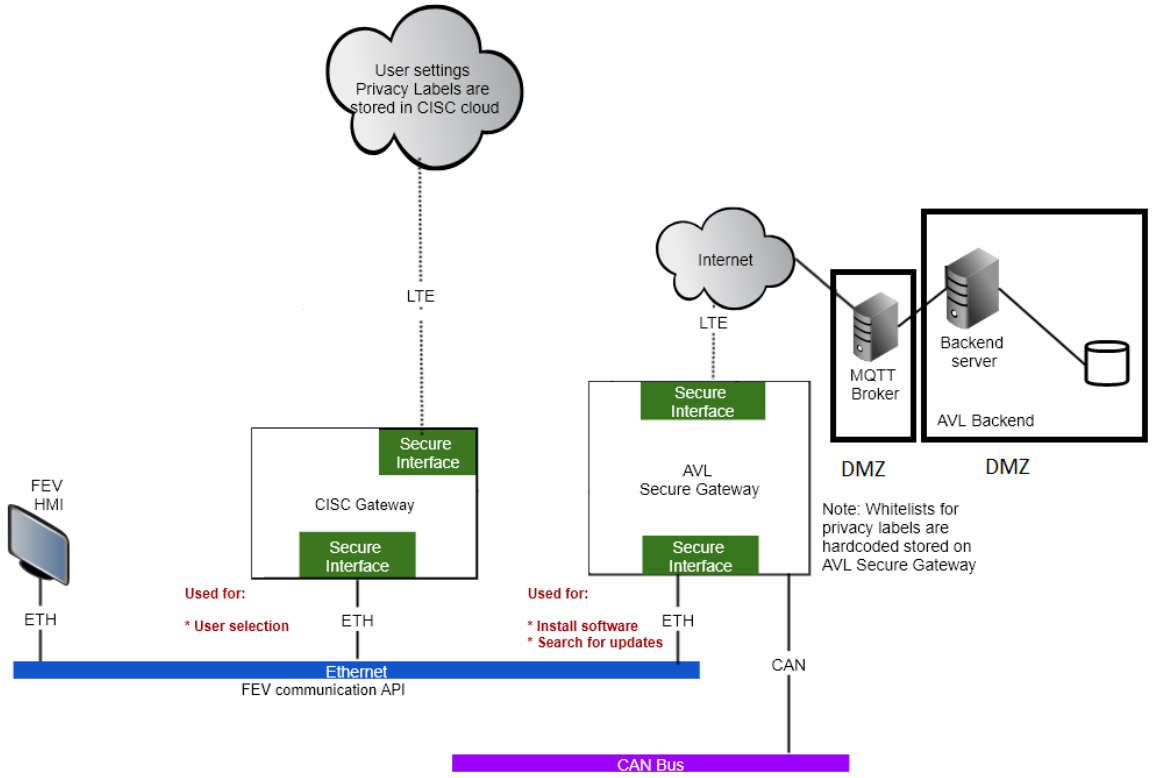


Figure 2. Secure Over the Air Software Update

- Concentrator (MQTT Broker)

The concentrator is a server that acts as a mediator between the Frontend and the Backend (Cloud). This server uses the MQTT protocol, which is based on the publish-subscribe messaging protocol.

- Smart Service Framework

The Smart Service Framework is a cloud-based solution on the backend aiming to connect and remotely access vehicles, to decrypt data sent from the vehicle to the cloud and to encrypt software update packages sent from the Backend to the car.

3.3.3 Market Innovation and Perspective

Instead of calling back fleets of cars in order to be able to update the software, which causes high costs for the OEM (e.g. VW recently had to recall many vehicles for updating their firmware software), a secure software update over the air is the cheaper way for the OEM and is more comfortable for the customer who does not need to bring the car back. With the development of a device which makes secure over the air updates possible we can demonstrate to OEMs that we can construct such security concepts and provide the hardware and software for the backend and frontend. Furthermore, we are not only limited to software updates; we will also be able to provide more services like secure, and privacy-aware transmission of maintenance data over this device. The privacy aspect in this use case is of special interest for users. According to an actual survey (Habeck et al. 2014), many users want to have full control over their private data sent over the internet and want that their private data is well protected, otherwise they do not want to use such functionality and therefore do not pay for it.

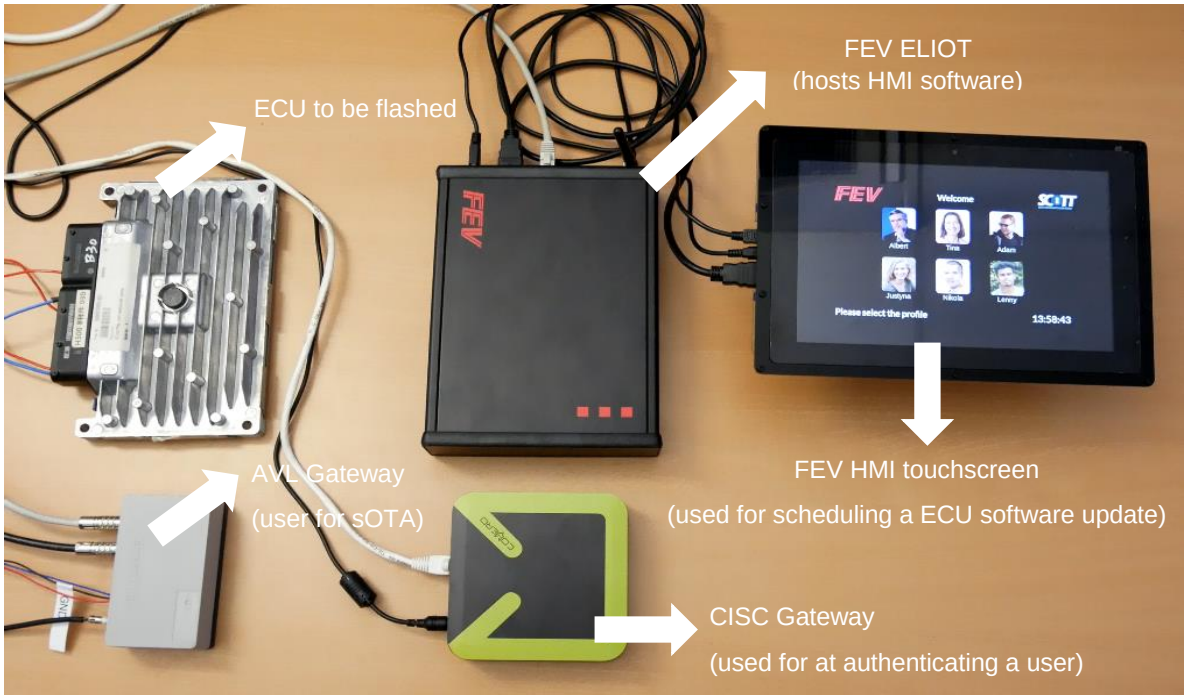


Figure 3. Devices to secure over the air

3.4 Trustable Wireless in Vehicle Communication Network

3.4.1 Objectives

Within WP13 we developed a technique called Pair&Trust. The objective of Pair&Trust is to provide a method of pairing which automatically leads to trusted equipment. When pairing devices, you do not always have the devices beside each other. Even more, someone might run a man-in-the-middle (MITM) attack on you. Therefore, Bluetooth devices usually require you to use personal identification numbers (PINs) for authentication.

Within SCOTT, we presented a novel method, which uses NFC to trigger pairing. With this approach, you have a close physical proximity. That way you “touch” what you scan, which means you know it can only be that device. This can then mitigate MITM attacks.

3.4.2 Achievements through SCOTT

At first, development showed several issues with this approach. We also found some of these issues within literature. However, we are certain that future implementations of our software will fix these issues. Certainty comes hereby also from literature, where active NFC devices were tested in medical industry, with Pair&Trust like features. In difference to this active version, our approach is passive and does not require active internet connection.

3.4.3 Market Innovation and Perspective

With our technology we found a niche market. The Pair&Trust method grants the ability to authenticate devices without active internet connection. Good examples are low energy devices that are not equipped with WiFi or mobile network chips. The biggest issue for commercial appliances is yet the stated lack of mass-affordable hardware, as stated in WP13.

3.5 Trustworthiness Indicator

3.5.1 Objectives

The Trustworthiness Indicator (TWI) was designed and developed in WP13. The TWI’s purpose is to indicate the trust of data, i.e. it analyses the stream of data for key factors that make data trustworthy. More specifically, the TWI in its basic version:

1) checks the integrity of data, such as signatures;
2) checks the connectivity values, such as timing and packet loss; and
3) also checks the data itself, for example, if measured temperatures are plausible.

The TWI has three states:

(i) green, everything okay, all data can be trusted,
(ii) yellow, there may be a problem with the data, i.e. one wrong temperature measurement in the last minute, which might indicate a future sensor failure but the overall data can still be trusted, or fading battery, which might indicate a future failure, and
(iii) red, measurements are flawed. This may be the case if a sensor is damaged and delivers not correctible data, i.e. the data cannot be trusted.

3.5.2 Achievements through SCOTT

Industry does currently not inform the user if data can be trusted or not. Especially in business use-cases this can be a problem. Engineers have to check the raw data, which is error prone, as small data flaws are rapidly overlooked. WP13 solved this problem with the TWI. The engineer can see at one glance if data can be trusted, if it can be corrected, or if it is flawed.

3.5.3 Market Innovation and Perspective

We see a general gap in the market for consumer products. At least Apple showed that users do not want to deal with necessary overhead information. The principle: “as long as it works” is prevalent in users. However, with the overwhelmingly positive reactions we got from the engineers reviewing the TWI for normal data streams (Feedback from reviews within SCOTT, from VIF, AVL and TUG), we also see huge potential for the consumer market. For example during video calls, a thin green border or no border (as of now) could show that everything is OK; a thin yellow border could indicate

something like packet loss, low battery, or slow connection; finally, a red border can show an approaching disconnect (similar to the red banners you get when for example YouTube disconnects).

We see Blue Ocean potential on usability side for the TWI. While this does not mean revenue per se – as few people might pay for that feature – the technology using these indicators have potential to stand out from competition.

3.6 Vehicle-as-a-Sensor within Smart Infrastructure

3.6.1 Objectives

The main work is focused on the development of comprehensive solutions related to vehicle-as-a-sensor within Smart infrastructure. It covers the following aspects:

1) vehicle-to-infrastructure communication,
2) autonomous driving and authentication, and
3) authorization of vehicles and drivers.

The main objectives are to ensure safety and security in broadly understood Vehicle-to-anything (V2X) communication - room the authorization and authentication of a user in an autonomous car to secure data exchange between the car and the infrastructure. The main objectives related to this use case are:

1. Ensure communication between car and infrastructure in order to increase the level of safety and security.

2. Implement the trustable “car as a sensor” approach in order to highly increase situational awareness and enable flexible access rights management in a challenging area.

3. Develop intelligent mechanisms to increase the efficiency of safety & security systems.

4. Develop a data integration model, which allows for the utilization of various types of data.

3.6.2 Achievements through SCOTT

Partners involved in the use case have been working on scenarios that cover three aspects:

1) Authentication and authorization of a driver and his vehicle at the facility gate. This process can be done in the mobile application by scanning the QR code presented on the car's screen. If the authorization is correct, the messages containing basic information about the driver and the car can be sent in a reliable way and the entry barrier is automatically opened so that the driver can enter the facility. A novel method has been proposed as an additional level of security on the physical layer that is achieved by using the reconfigurable ESPAR (Electronically Steerable Parasitic Array Radiator) antenna together with a dedicated localization algorithm allowing determining the spatial position of the vehicle. An ESPAR antenna also enables to change the radiation pattern automatically to improve connectivity and reduce the influence of jamming (intended interference) in V2X (vehicle to anything) communication.

2) Autonomous driving within the facility. The autonomous car takes the user to the selected destination. The user authorizes himself in a dedicated system and the car arrives at the indicated address. The car moves along the optimal route. This leads to amplify security in private facilities. Guests, who have to be authenticated and authorized, are safely driven to a destination place.

3) Automatic access to a parking lot, where the user can authenticate and authorize himself in the mobile application and also redeem tickets (online and offline) at the parking gate. The payment process is triggered when leaving the parking lot and closing the parking session.

3.6.3 Market innovation and perspective

During the SCOTT project many market aspects have been declared, discussed, or started to be implemented. Within WP15 several system prototypes were created and have the market potential.

GUT plans to create a Smart Infrastructure and expand the V2X (vehicle-to-anything) coverage at the university campus. This will allow GUT to conduct advanced tests in the physical layer security aspects in V2X communication. This infrastructure will consist of IoT devices and sensors that will transfer data between each other and vehicles.

Such a dedicated infrastructure will be also a test space, where future development of SCOTT related system can take place. This will have an influence on TRL level of the products – dedicated test space may be valuable for product improvement and also serve as a showroom for potential customers.

VIF generally develops its autonomous driving algorithms across various funded projects, such as AutoDrive (ECSEL) (https://autodrive-project.eu/.), and together with industrial partners, such as ZF (https://www.v2c2.at/gtc2018.). VIF did not have much effort planned within WP15, but despite that fact VIF got a huge benefit from a realistic use-case scenario that was developed together with the WP15 partners. While testing this special use-case, VIF discovered several challenges in the fields of usability, security, and safety that would have gone unnoticed. Just to mention a few, for each:

- Usability
  - The way, how the AD functionality was started, is too complicated for the general ease of use
  - The user has to be informed about the current state of the AD system, i.e. is it off, is it starting, is it running, has it failed

- Security
  - New policies towards accessing the vehicle via software: the software on research vehicles may not be accessed via wireless networks. Even though the system can be secured, it is hard to tell what colleagues are currently doing with the vehicle.

- Safety
  - There have to be methods to ensure that the vehicle is only moving, when all passengers are belted in, …
  - What to do, when the path is blocked, in a level 4 scenario of autonomous driving.

3.7 Safe Freight and Traffic Management in Intermodal Logistic Hubs

3.7.1 Objectives

The use case developed within WP17 targets a scenario of logistics management in the railway domain, with the aim of increasing the interoperability, capacity and efficiency of shunting yards. In this scenario, the rolling stock is recombined in a vast variety of dynamic train compositions, which are created and set to travel daily. The entry of these compositions into the main line for travelling to the targeted yard/depot may be delayed due to different reasons (e.g. delayed cargo, clogged tracks, etc.), thus affecting to the capacity, punctuality and efficiency of the rolling stock and of the infrastructure.

In order to address this issue, the use case has developed a Real Time Management Network (RTMN), integrating a wide variety of wireless infrastructure and communication elements, including WSNs (Wireless Sensor Networks), GNSS (Global Navigation Satellite System) location, cargo identification, and backhauling via satellite communications. The use case makes use of a wide range of technology building blocks developed within SCOTT project, addressing topics such as security & safety, distributed cloud integration, and energy efficiency and autonomy of wireless devices.

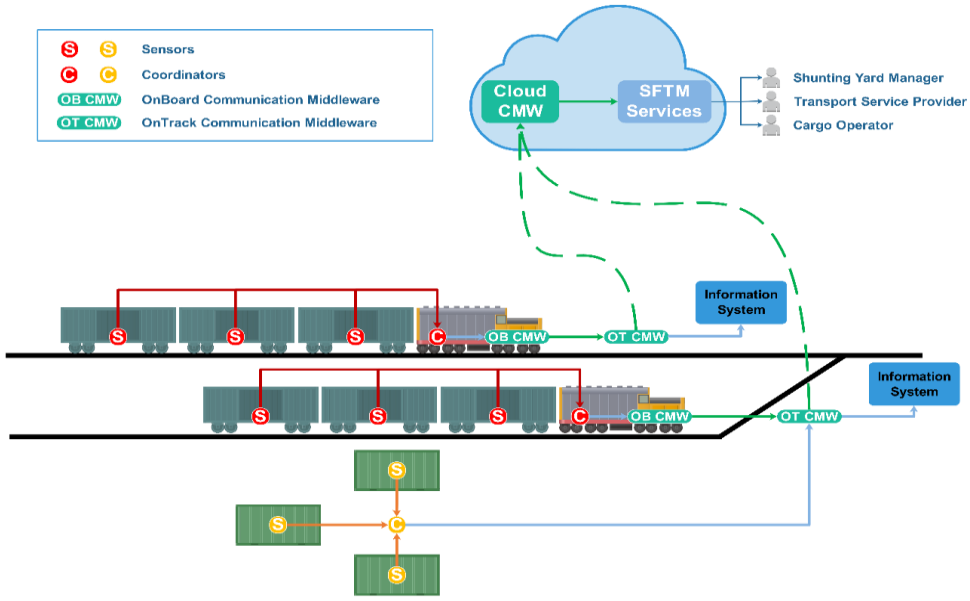


Figure 4. Safe Freight and Traffic Management System

For the development of the RTMN, *one of the main challenges* of the use case is to achieve an optimal trade-off between the availability of accurate enough asset localization information, and the cost-efficiency of the infrastructure needed for this purpose, considering that the networks operate in dynamic and changing environments.

Another key challenge is the complexity of multi-modal logistics planning, which stems from underlying uncertainties, such as vehicle malfunctions, multi-modal and yard service delays and disruptions, and inherent risk situations.

This use case contributes to the realization of SCOTT project objectives through:

- The integration of wireless technologies to optimize the management of logistic hubs, thus contributing to achieve the full potential of the Internet of Things (IoT).
- The use of WSN for the identification and location of the cargo, thus fostering the adoption of this technology in the mobility domain, while addressing at the same time a relevant European societal challenge.
- The consideration of security, privacy, safety, and trustability issues, in order to increase the social acceptance of wireless solutions.

3.7.2 Achievements through SCOTT

According to the objectives initially defined, the main result provided by the use case is a Real Time Management Network for safe freight and traffic management in the context of a railway shunting yard, mainly based on wireless technologies. This network contributes to the reduction of delays, the

increase of the railway infrastructure capacity, and the efficient management of the rolling stock. More specifically, the *main benefits* provided by this network are:

- Provision of interoperable information (e.g. details about train compositions travelling between the shunting yard and the rest of target yards, continuous freight tracking data, etc.) covering the needs of the different actors in the multi-modal supply chain, namely: multi-modal logistics operator, railway company, shunting yard operator, etc.
- Optimization of shunting operations within the yard, in terms of number of shunting operations and resource allocation, while ensuring fixed delivery times and complying with the safety constraints of freight management.
- Reduction of the costs of Infrastructure-to-Infrastructure (I2I) communications thanks to the replacement of traditional wired solutions with the proposed wireless technologies.

One of the main achievements of this use case for the market is that it proposes a cross-domain solution, encompassing both logistics and railway operational environments. In fact, logistics, transport, scheduling and rolling stock management are usually segregated, and the use case addresses this situation through the provision of a gateway that connects heterogeneous data sources and sensors, unify formats in a way compliant with the Sensor Network Reference Architecture and existing common data-models, and integrates with a cloud-based centralized monitoring system.
Furthermore, the use case contributes to the development of smart multimodal infrastructures, by exploring new IoT-based methods to improve the capability of planning, management and optimization of logistics infrastructures; while in the railway domain, the use case allows the centralization of rail infrastructure information from both track and rolling stock, thus opening new opportunities in both rail and logistics markets.
Lastly, some technical building blocks integrated into the use case can be applied to other market domains, such as the energy harvesting building blocks (BB25.C and BB25.E), which can be used in the healthcare sector.

3.7.3 Market innovation and perspective

The ongoing liberalization of the European railway market, based on the open access to railway capacity for any railway company, poses a set of challenges, among which the optimization of the capacity allocation is a key issue for the emerging new ecosystem.

The solution proposed for the current Use Case shows a connection between the internal capacity management inside a shunting yard with the network slot coordination. This link between both systems achieves a better answer to possible modification on the original plan, providing more flexibility to the system.

The application of the AI on this UC can also enhance the efficiency of the procedures of the internal management on the shunting yard, where the order of the wagons and cargo load needs to be carefully scheduled.

On the other hand, the use of a sensor network on the internal shunting yard management will show a reduction on the time spent on the rolling stock and cargo identification when they arrive to the logistic facilities. The matching of this information with the plan avoids possible human errors and provides an internal tracking of all the goods moved inside the shunting yard. The data gathered by the sensor network is uploaded to the cloud, where can be used on several application such confirmation to the operators, statistics or to coordinate multimodal freight.

To achieve this goal, the needs of the different actors of the multi-modal supply chain (e.g. the multi-modal logistics operator, the railway company and eventually, the shunting yard operator) shall be considered. Furthermore, the optimization of the rolling stock and shunting yard management, the

provision of interoperable information among agents, and the availability of continuous freight tracking are key aspects for the success of new emerging business models.

3.8 Autonomous Wireless Network for Rail Logistic

3.8.1 Objectives

The development of the autonomous wireless network on railway tracks as well as on trains were treated in the Work Package (WP) 18 and BB26.A "*Autonomous Wireless Network*".

Nowadays, in the railway domain, the infrastructure for managing the rolling stock is expensive to install and maintain due to it requires long wired installations, which increase costs. In fact, the current communication networks often rely on cables between coaches becoming a weak link in the infrastructure, as it can be targeted by vandalism due to the economic value. Moreover, most of the logistics and maintenance procedures in the rail industry are based on the human supervision as the wagon identification, the confirmation of the composition or the maintenance needs. Furthermore, the current data obtained are only limited to the rail operator without using any cloud solution, which could reduce the expenses.
In this context, the main objective is to digitalize the railway domain through an autonomous network that enhances the currently constraints on the rail services, as the logistics or the signalling. In order to achieve this goal, the following challenges were proposed:

- Implementation of On Track wireless communications.
- Improvement of the On Board equipment communications.
- Increase of the safety with the predictive maintenance.
- Reduction of the wired installations, with less costs.
- More efficiency on the management due to the cargo and rolling stock monitoring, available on an application.

To accomplish the main objectives, a wireless communication system allowing establishing between the vehicles and the infrastructure (V2X) has been developed. The reliable V2X communication requires knowledge about the availability and the Quality of Service (QoS). To address this, the available 3G and 4G connections are monitoring, estimating the available data rate on those connections and switch between them based on these data rate estimations in order to maintain a reliable cellular uplink for the V2X communication.
Concerning the maintenance issues, they are improved using sensors avoiding the human error and adding more efficiency. The developments carried out avoid the need of an operator for the identification and composition of the train, providing all the information and management. In addition all these data will be available at the cloud for the logistic companies in order to track the cargo through an app which provides location and current state, given from the wireless sensors installed, in real time.

3.8.2 Achievements through SCOTT

To solve the currently constraints in the rail domain as the increase the cost of the infrastructure or the safety and security deficiencies in the services, the Autonomous Wireless Network (AWN) solution has been developed in order to provide service to all the railway needs. For that purpose, the solution digitalizes the railway infrastructure enhancing the current and future services as the Logistics and Maintenance or the signalling.
The Autonomous Wireless Network (AWN) solution develops a meshed backbone network in order to control and monitor every device of the infrastructure which need access. In addition, V2X and I2I wireless communication capabilities have been integrated in order to provide service to the Logistics and Maintenance (L&M) sensorization network. However, these capabilities can be applied to every

signaling and sensorization network, which architecture has been defined with flexibility in order to develop more capabilities in the future.
The developed solution follows the architecture defined in the SCOTT project ensuring the security, safety, trustworthiness and privacy of the involved IoT systems. In addition, the architecture has been designed following the regulations and standards below:

- ISO/IEC 29182. The defined ontology and data model to interconnect the elements belonging to the distributed architecture are fully compliant with this regulation.
- OSI standard. The ontology is based on this standard.
- CENELEC EN50155. The data is secured at the node level following this regulation.
- CENELEC EN50159. To assure the message transmission in the network, the reliable communication follows this rule.

Based on the previous regulations, the IoT network developed on the current solution is divided into the following components:

- The **edge devices** are the Wireless Sensor Network and its coordinator. The network is composed by smart devices of sensors and actuators in charge of collect and generate Logistics and Maintenance data under the WSN coordinator. This sensors can be allocated on the trains (On-Board) or on the rail track (On Track). The solution used for the AWN has implemented a Trusted Platform Module (TPM), which includes several cryptographic algorithms and creates an isolated environment to improve the security and trustability of the IoT sensors.
- The **WSN Adapter** is the responsible of managing data messages coming from WSN Coordinators and distributing to the CMW in a safety and secure way. The support was rationalised using advanced mechanisms between the WSN Adapter and CMW over secure channels adding upgraded policies to improve the performance as setting different limits to the message and avoiding possible loops amongst interconnected agents. Also, a dockerized version of the WSN Adapter has been designed and deployed in order to get the best portability of the system and aiding support to the cluster formation with the CMW adding more scalability support to the architecture.
- The **CMW** is in charge of validating, processing and distributing the data send by WSN Coordinators and WSN Adapter. Each WSN Coordinator can only communicate with its related CMW using MQTT protocol. In turns, each CMW can communicate with its related WSN Coordinators and with all the CMW across the system using AMQP protocol. This communication is based on OSI layer protocol. The access of the WSN coordinators to CMW is secured with Radius implementation to authenticate the user passwords making use of PEAP protocol.

The cloud infrastructure performed in the SCOTT project is a hybrid solution that implies the use of the public and private cloud in order to enhance the functionality, allow greater flexibility and enable multiply data deployment options. This solution provides common services to the different elements of the system with a lower latency and managing the messaging in an efficiency way. The cloud is secure with extra capabilities as centralized user authentication system (LDAP) that is the responsible of revoking the user and isolating the area in which that anomaly or deviation was found in the expected traffic, if necessary or the Network Time Protocol Server (NTP) and Domain Name Server (DNS).
Regarding the wireless communications, the UC18 has developed methods and algorithms to manage multiple 3G and 4G modems in a V2I gateway, implemented on the TRX-R6 hardware platform.

The main achievements accomplished with these methods and algorithms are in the areas of data rate estimation and interface selection, resulting on a reward-based machine learning that assess each interface based on the expected reward it offers. This way, the system can handle and adjust to situations where the data rate estimation differs from what is actually available, which may occur

for example if there is heavy load on the cell. This adds another layer of reliability to the overall solution.
In comparison to pre-trained offline estimation methods, this greatly enhances the adaptability to changing conditions and to unknown environments. Further, the actually achieved data rate in case of ongoing transmissions is also taken into account to further improve the estimation accuracy. Most current methods to determine the available data rate rely on active transmissions. So in the absence of user data traffic, they either cannot determine the data rate or have to generate traffic for measurement purposes. New approach overcomes these problems by not relying on active transmissions, but instead exploiting parameters that are available anyway. This makes the communication solution attractive in cases where the environment is changing rapidly, e.g. in high speed scenarios, and where unnecessary transmissions should be avoided for cost or congestion reasons.

The final demonstrator of the UC18 validates the AWN solution in a real scenario. The selected location for the testing activities has been a regular tourist operation track operated by NÖVOG in Austria. The demonstrator consists in a composition of five wagons and a locomotive, where the IoT network for logistics and maintenance as well as the communication devices are installed. The train will traverse along the available route, around 40 kilometres. During all the route, the sensors will collect and send the information to the coordinators and CMW in order to transmit all the information to the cloud platform.
Therefore, the UC18 demonstrator validates the following functionalities in the Autonomous Wireless Network system:

- Collect and report maintenance information from the wireless sensor network:
    - Vibration data from the rolling stock
    - Impact data from the rolling stock
    - Humidity data from the rolling stock
    - Pressure data from the rolling stock
    - Temperature of the cargo
    - Power consumption
    - Acceleration
    - RSSI
- Collect and report the position of each node:
    - Accelerometer data
    - GNSS data
    - RSSI data
- Collect and report the distance between nodes:
    - Distance data
- Secure wireless communications Vehicle-to-everything (V2X)
- Secure wireless communications Infrastructure to Infrastructure (I2I)
- Processing and storage the logistics and maintenance data in the cloud platform
- Display real-time logistics and maintenance information on a mobile application

3.8.3 Market innovation and perspective

INDRA is leader on the Internet of Things (IoT) technology implementation on railway domain through the design and development of a secure platform for the integration of the rail services performed in the SCOTT project. The platform covers all edge data collection, wireless communication systems, and Cloud services accomplishing with the security and requirements established by the regulations.

The modernization of the railway market demands the use of new technologies to provide new rail services. The future tendencies that are planned into the autonomous wireless network are aligned with the shifts that all the IoT systems will follow:

- 5G Technology. The high potential of the new wireless technology is meant to low latency, high speed and data transmission in real time capacity. These improvements on the communications empower the IoT networks providing more efficient services and high interconnectivity. Therefore, the 5G will allow to enhance the current autonomous wireless networks due to its competitive advantages.
- Artificial Intelligent (AI). The powerful of the AI tools permits to analyse and make decisions with the huge amount of information gathered for example by the IoT devices. This technology improves the Cloud platform as well as the services developed in the UC18 allowing the spreading of control and supervision to the entire infrastructure.

The solution of the uplink data rate estimation developed by Cork Institute of Technology (CIT) is considered the one with most market potential. CIT, as an academic institution, is not aiming to bring it to the market by itself, but rather aims to exploit it through licensing. Consequently, CIT has filed a patent application with the Intellectual Property Office of the United Kingdom, covering the online learning approach to uplink data rate estimation. CIT considers the approach described in this patent application as applicable in setups where it is required to have client-side knowledge about the current and immediate future quality of the uplink from a mobile network end device to online services. This knowledge can be useful in a number of applications, for example:

- Network interface selection: If multiple interfaces are available, the invention can assist in selecting the interface that offers the most reliable link quality – an example would be the UC18 scenario with a V2I gateway on a moving train.
- Traffic flow distribution: If multiple data traffic flows have to be allocated to multiple interfaces, accurate estimations of available data rates can be used as a basis for matching the demands of the traffic flows with the offered capabilities of the interfaces.

CIT will offer this solution to interested parties under suitable licensing terms. Commercial exploitation by one of the SCOTT partners is regarded as a preferred route for exploitation.

Moreover, the developments are focused on providing a solution for train digitalisation, providing a wireless communication backbone for developing on-board services. In this context, these works are aligned with Shift2Rail IP5 concerning the development of a wagon On-Board Unit able to able to provide seamless on-board communications services for sensors, actuators and telematics applications installed on rolling stock and wagons of train compositions. Furthermore, the developments are also aligned with Shift2Rail IP2 for the development of a safe and secure solution for train composition determination and train integrity monitoring.

3.9 Smart Train Composition Coupling

3.9.1 Objectives

The development of the coupling system was treated in the Work Package (WP) 19 and BB23.Q "*Towards a Safe Virtual Coupling*".

The current coupling system available in the railway industry is based on a mechanical and physical joint between two or more compositions. One of the main problems of this system is the need of time without operation for the works and the slow manoeuvres, with On Track operator in some cases to assist the operation. The consequences of these disadvantages are the inefficient of the rolling stock services, due to the need of facilities such a station or shunting yard for the movement, and less workers' safety. Furthermore, the railway industry has also another constraint related with the current coupling system that involves the efficiency of the tracks. Nowadays, the tracks are limited by the minimum distance between trains that can be safety handled by a signalling, control and train protection systems, as European Train Control System (ETCS) in Europe.

To improve these constraints, the virtual coupling developed in the UC19 ensures a safety manoeuvre avoiding the physical joint between the trains but with one of the train assuming the control of both compositions, without the need of the operators between both compositions and the possible risks of the manoeuvres. In addition, the solution also enables the communication between the trains (V2V communications), allowing them to automatically accelerate and brake together as well as manage them to follow each other at a closer distance. This means an improvement in the line capacity, which nowadays is limited, as a result on the reduction of the distance between compositions.

Therefore, the UC19 includes the following concrete objectives:

- Establish the safety V2V communication specification as well as implement and validate some approaches based on 802.11 standards.
- Evaluate WSN solutions to assure distance between compositions.
- Design and implement safety control solutions to the signalling future.
- Improve the line capacity reducing the distance between trains.
- Reduce the operating time suppressing the conventional coupling and decoupling manoeuvres with operators.
- Interoperability between different compositions, as currently only compositions from same manufacturer can be coupled.
- Establish a safety communication protocol between gateways in order to secure the data transmission between compositions.

3.9.2 Achievements through SCOTT

According to DG Move (Mobility and Transport Department), the climate change means a larger environmental threat. For this reason, SCOTT developments carried out in the railway domain are focused on protecting our environments. The enhancing energy efficiency of current railway systems improves the quality of life of European citizens and reaches the goals set by the Paris Agreement due to the low-emission. Two of the main points on which the Smart Train Composition Coupling WP is based are:

- Improve the coupling manoeuvre in order to increase the capacity and efficiency on the railway lines with the aim of reduce the emissions.
- Improve the rail infrastructure efficiency by Increasing the capacity of the lines, reallocating the Rail Authorities and adding flexibility for the operation of several routes at the same time.

Following the main objectives of the use case 'Smart train composition coupling (STCC)' is about managing manoeuvres to allow to join multiple compositions into a unique virtual composition and split the virtual compositions based on the journey planned for each composition taking into account all safety conditions of this type of market segment. To validate the overall STCC system in the integration tests, a Train-Track simulator has been developed that allows train control based on train position, traction capabilities and local distance measurements through the different subsystems using the defined interfaces, as well as the defined messaging protocol.

The final demonstrator of WP19 allows testing the overall STCC system in a real scenario, the chosen placement for these activities is located in the north of Austria and it is operated by NÖVOG.

To allow the control of virtual compositions as well as the coupling or uncoupling manoeuvres a V2V communications between compositions is needed. The works performed about V2V channel testing along the project illustrated a high TX rate with a small link error rate, a good user experience of video-streaming performance and a small jitter of UDP traffic. Furthermore, the CPCE channel estimation technique has been implemented together with the midamble estimation technique (which is an alternative proposed in the NG-V2X standardization group) in the back solution for the V2X communication.

Therefore, the WP19 presents a railway concept that allows the wireless coupling or uncoupling of compositions from independent manufacturers decreasing time manoeuvres issues and improving the railway track capacity due to distance between compositions decrease. The WP19 demonstrator *validate the following functionalities* in the Smart train compositions coupling system:

- Coupling and uncoupling manoeuvres between different compositions.
- Establish T2T communications and secured it.
- Remote control between trains by train traction orders.
- Safety control of emergency cases (V2V communications loss, distance control between compositions or integrity loss in the compositions).
- Driver control by DMI.
- Local distance between compositions measurement.
- Distance measurement through two solid state LIDAR.
- Geolocation of the train and the wagons
- Inertial data measurement for position integration

3.9.3 Market Innovation and Perspective

This project adds new end-to-end secured, trustworthy and interoperable wireless capabilities between trains (V2V communications) to solve the hazardous situations relating to safety that can occurs in typical rail lines.

Nowadays, current implementations of train protection systems are based on the absolute braking distance between trains. These implementations presents limitations to the potential headway of the line due to absolute braking distance supervision in which each train takes into account its own braking characteristics to determine the speed allowed. For these reason distance between trains is unnecessarily high, compared with the current capabilities of the protections functions.

Current systems have been optimized with the objective of maximize the capacity of the tracks based on this paradigm, but the railway technology is reaching a limit where the cost and complexity of adding one vehicle on a congested link raises exponentially.

Modifying this paradigm to a cooperative system view allows breaking with the limitations of the currents railway systems in terms of track capability and centralized architecture.

Therefore, through SCOTT, Indra has develop an innovative railway system able to break with the current paradigm and able to provide to the market segment a new solution with a new point of view. In addition, the solution relies on the wireless sensor network for rail application developed by the top institution in this field, the Universidad Politecnica de Madrid (UPM).

These developments are in alignment with the S2R VCTS system definition that is currently being designed and in which Indra is involved. The tests carried out allow the evaluation the system based on SoA as a first approach to detect improvements and to enhance the system that will be launched in the market in the future, and that Indra has in its roadmap.

3.10 Trustable Warning System for Critical Areas

3.10.1 Objectives

The reinforcement of the critical areas in the railway domain was treated in the Work Package (WP) 20 and BB23.I "*Reinforcement of the safety in Critical Areas of Traffic Infrastructure*".

Over the last years, the number of accidents along the European railway lines have increased due to safety deficiencies. A high number of these incidents are focused on the level crossing and working areas, which are classified as critical scenarios. The current analogical system is based on a trigger located on the track, mechanical or electronic, which activate the barriers and signals indicating the approaching of the train and it avoids the occupation of the track by vehicles or pedestrians. This mechanism is limited, due to its incompatibilities with other technologies and its non-flexibility to adapt it to other critical areas.

In order to enhance the security and safety in the railway domain, the UC20 is focused on developing a wireless Trustable Warning System for critical areas (TWS). The system performed will be able to detect possible obstacles, which are on or near the track, using a Wireless Sensor Network for object detection in a railway level crossing. In railway scenario, there are critical areas talking about safety where human lives must be protected. This Wireless Sensor Network integrates a 3D Lidar, as the sensor for point cloud getting and objet detection though edge processing. The WSN node with the Lidar is connected to a centralized cloud for decision making, within the Internet of Things paradigm. Furthermore, the system will broadcast the relevant warning information to the vehicles in the vicinity and the train, in case of an emergency maneuver is required by the last one.

However, this system could not be performed with the current wired installations due to its limitations as the time of response or the coverage. In addition, this kind of installations are susceptible to mechanical problems and vandalism that can cause issues in the railways service. For this reason, the UC20 also develops a wireless communication system between the vehicle and the infrastructure (V2X). This communication is in both directions; therefore, the critical area provides data about the possible track obstacle and the train dynamic information. Taking this data, the system provides safety answer for each situation. On the other hand, the use of wireless connectivity allows its integration with other domains, such the automotive one.

Therefore, the UC20 includes the following concrete objectives:

- Increase the safety conditions in critical areas.
- Ensure the interoperability between different domains, as the automotive.
- Improve the compatibility with the current and future systems.
- Provide a scalable architecture.
- Object detection and classification.
- Protection of safety critical areas.

3.10.2 Achievements through SCOTT

The main objective to be fulfilled by the TWS WP20 Use Case defined is the early alert to a critical rail area users about the trains approaching to that area. This objective is achieved providing a system that it is divided in two related but differentiated parts: an On Board embedded system and an On Track installation. In order to generate a general model for the "critical rail area" term, a set of regions around the critical area are defined with different actions to deal with the critical area situation. These set of regions' actions goes from establishing the connection and the handshake between the On Track and the On Board installation to the control of the train to be adapted to the critical area situation. These actions are under the supervision of some conditions: the area evaluation using a wireless sensor network that, throw AI algorithms, providing insight to evaluate

the critical area situation and the communication loop between the On Board and On Track part with a variable, as user desired, range, and the safety and security rail regulations.

To validate the overall TWS system in the integration tests, a Train-Track simulator has been developed that allows train control based on train position, traction capabilities, critical are conditions simulation, and local distance measurements through the different subsystems using the defined interfaces, as well as the defined messaging protocol. The final demonstrator of WP20 allows testing the overall TWS system in a real scenario, the chosen placement for these activities is located in the north of Austria and it is operated by NÖVOG.

Therefore, the WP20 presents a railway concept that allows the wireless evaluation of a critical area and report it to the trains that are approaching to that mentioned area. Moreover, it incorporates functionality to detect and classify different types objects. The objective is to carry out SCOTT WP20 objectives.

The entire train trip constrains are managed to reduce the impact of the critical circumstances into the train trip in a safe and secured manner increasing the train railway track capacity. Moreover, both passengers/personnel and critical area actors security is enabled. The WP20 demonstrator validate the following functionalities in the Trustable Warning System for critical areas system:

- Train and critical areas management.
- Establish T2I communications and secured it.
- Remote control of trains by train traction orders based on critical area conditions.
- Safety control of emergency cases (V2I communications loss, distance control between On Track and On Board systems or integrity loss in the compositions).
- Driver control by DMI.
- Local distance between On Track and On Board systems measurement.
- Objet detection and classification in level crossing for railways.
- Safety critical area protection
- The WSN nodes include security enhance by hardware to increase trustability of the system.

3.10.3 Market Innovation and Perspective

This project adds new end-to-end secured, trustworthy and interoperable wireless capabilities between On Track and On Board infrastructures (V2I communications) to solve the hazardous situations relating to safety that can occurs in typical rail lines.

The current systems are based on wired connections that introduce generate high CAPEX and OPEX and limitations into the critical area management range. In addition the TWS system introduces the opportunity to integrate future systems that may appear thanks to a safety and secure designed architecture and messaging system solutions.

- Provision of a non-limit coverage range thanks to the V2I communication technologies owned.
- Provision of a system that establishes a communication link between the trains and the On Track infrastructure to manage the critical area Safety conditions.
- Provision of a system that, based on the critical area Safety conditions management, interacts with the signalling and security systems to improve the Safety a conditions.
- Provision of flexibility and decision time to the driver and the rail operator to manage a critical area in safe manner.

Current systems have been optimized with the objective of maximize the capacity of the tracks based on this paradigm, but the railway technology is reaching a limit where the cost and complexity of adding one vehicle on a congested link raises exponentially.

Modifying this paradigm to a cooperative system view allows breaking with the limitations of the currents railway systems in terms of track capability and centralized architecture.

Therefore, through SCOTT, Indra has develop an innovative railway system able to break with the current paradigm and able to provide to the market segment of a new point of view. Addtionally, UPM has become a top institution in the field of Wireless Sensor Networks for railway applications. Though UPM hardware, it is possible to add objet detection and classification capabilities, without using cameras, and using embedded resources. This is a great improvement in cost/performance, without decreasing reliability.

3.11 Assisted Living and Community Care

3.11.1 Objectives

The WP21 initial objectives as described in the SCOTT Description of Work are:

- Provide solution for secure **trust-based delegation** in assisted living and community care. This involves the actual delegation, how this is modelled and executed using a set-of protocols on the one hand and the trust computation plus context evaluation that underpins the decisions on the other hand.
- Provide solution for automated **context derivation for resident as well as potential responders**. This involves wirelessly connected sensors to monitor the resident's home, as well as his/her vital signs to assess personal health, wellbeing and trustable system operation. It also involves reliable and secure geolocation (enables spatial-based authentication) to help finding the most appropriate responder.
- **Realize a demonstrator** integrating the abovementioned trust-based delegation and automated context derivation functionalities, which showcases the combined functionality supporting the use case and therefore enabling validation of the concept from an end-user perspective. For the latter, stakeholder (e.g. focus group) involvement is needed throughout the process to continuously improve the demonstrator with the end-user in mind.

At the end of the 3rd iteration of WP21 all these objectives have been met in the following way:

- The secure trust based delegation solution has been achieved by using an architectural model in which elderly or patient data are kept on-premise and separated from caregiver data in the cloud. Only in the case when really needed (for example an emergency event) the required data are provided to the selected caregiver(s). The trust-based delegation system forms the core decision logic of the ALCCS as it collects, processes and fuses information from multiple sensors for reliable fall detection. The context Detection and Trust Modelling are described in detail in the D21.7 deliverable.
- An (on premise) elderly context deviation (ECD) block has been designed and included in the use-case demonstrator. Sensors connected to it are used for fall detection, presence detection, localization and blood glucose level monitoring (diabetes type II) services. An Attribute Based Access Control (ABAC) control system in a secured cloud environment provides a context based solution for potential responders. A Semantics based ABAC (SABAC) demonstrator has been made in the 3rd iteration.
- An ALCCS demonstrator has been designed and implemented in the 1st iteration, further improved and extended in the 2nd iteration and completed as planned in the 3rd iteration of the project. It includes the trust-based delegation and automated context derivation functionalities, has been mapped on the WP26 reference architecture and is using various building blocks as defined in WP23 and WP24. Also the ALCCS demonstrator has been used as a reference test case for trust assurance (WP28) and security analysis (BB26F).

3.11.2 Achievements through SCOTT

Following is a list of main WP21 achievements over the past 3 years:

- Successfully implemented the ALCCS demonstrator as described in the previous section.
- Extension of the ALCCS demo with a diabetes monitoring sub-system, producing alerts on low blood glucose.
- A common RabbitMQ message broker deployment for secure data exchange.
- Development and application of (Xetal) ceiling presence detection sensor.
- Development of a Multimodal Positioning System (MPS) using a gateway with ESPAR antenna.
- Investigation and secure application of suitable low power wide area network (LPWAN) technologies for IoT devices.
- Development of a reasoning engine framework based on trust modelling for fusing multiple sources of weak information about an environment to generate a consistent and robust decision outcome.
- Improvements to state-of-the-art automated context detection systems for human activity recognition (HAR) using, among others, multi-sensor augmentation strategies and federated learning with self-supervision.
- Smartphone demonstrator showing large scale IoT device commissioning and patient linking as required for healthcare IoT deployment, using FHIR observation resources.
- Demonstrator to recognize daily activities from sensory data of a smartphone using the TensorflowLite transfer learning library.
- Standalone demonstrator for a secure and efficient SABAC to show advantages over ABAC (as used in the ALCCS) in heterogeneous distributed environments (including a formal language for the specification of access control policies).
- Specifying and evaluating a network slice for healthcare in 5G cellular networks.
- Various papers published as described in deliverables D21.1-D21.6.

Part of these activities have a follow-up in the InSecTT and the 5G heart projects.

3.11.3 Market Innovation and Perspective

The ALCCS demonstrator has shown how to develop a (elderly) care system in a secure and trustable manner. Concepts applied in this demonstrator (i.e. trust modelling, context derivation, SABAC, device localization, device commissioning, diabetes monitoring, cellular network slicing) can be deployed in next generation healthcare systems by industrial partners.

Moreover, the demonstrator has functioned as a test case for evaluating and improving methods and tools for trust assurance, privacy labelling and security analysis.

The (Xetal/Yugen) presence sensor and the MPS have been evaluated and improved in such a way that they are ready for large scale deployment. This also applies to the ElderlyUI's IoT device commissioning and patient linking capabilities.

Various university studies have resulted in conference papers and provide further insight in trust modelling, context derivation and attribute based control systems that may be deployed in next generation smart IoT devices for healthcare devices. Some of these activities will be continued in the InSecTT project.

3.12 Security and Safety

3.12.1 Objectives

WP23 Safety and Security (technology Line) consist of a number of Building Blocks that address different aspects of safety and security. SCOTT Building Blocks are deployed in different domains and Use Cases since the interoperable nature of BBs is one of the key focus in the SCOTT Project.

3.12.2 Achievements through SCOTT

Each Building Block has a contribution to the specific Use Case. The key achievements of the WP23 are highlighted within the particular Work Package.

WP9: The main solution in WP9 is the indoor localization of assets and people, called *Multimodal Positioning System* (MPS), a part of TBB23.P. Thanks to the dedicated antenna designed by GUT, the MPS complexity is significantly reduced compared to the other systems.

In SCOTT, Vemco and GUT prepared and demonstrated a prototype of the Access Control System (ACS) that incorporates:

- Detecting when an unauthorized person takes a valuable asset from a given area;
- Preventing unauthorized people to enter a room in the presence of a valuable asset and let them in otherwise;
- Detecting when a person enters a potentially dangerous area and informing them about the risk.

In order to implement the whole Work Package work, following TBBs was utilized (SCOTT WP9 contributors, Deliverable D9.5 2020):

TBB number	TBB Name	TBB Owner in UC	TBB Contributors
23.B_INDRA	End-to-end secured quality of experience (QoE)	Vemco	Vemco
23.D_NOKIA	Integrated Safety and Security Development	Vemco	Vemco
23.F_LCM	Out of Band Security	Vemco	GUT, Vemco
23.G_JKU	PHY Layer Security	GUT	GUT
23.H_UCC	Real-time configuration	UCC	GUT, UCC, Vemco
23.P_GUT	Spatial-based authorization and authentication	GUT	GUT, UCC, Vemco
23.R_VIF	Trust Anchor for ES smart sensors	GUT	GUT

Table 1. TBB overview D9.5

WP15: The main work in WP15 is focused on the development of comprehensive solutions related to vehicle-as-a-sensor within Smart infrastructure. It covers the following aspects: vehicle-to-infrastructure communication, autonomous driving and authentication, and authorization of vehicles and drivers.

In order to implement the whole Work Package work, following TBBs was utilized (SCOTT WP15 contributors, Deliverable D15.5 2020):

TBB number	TBB Name	TBB Owner in UC	TBB Contributors
23.B_INDRA	End-to-end secured quality of experience (QoE)	Vemco	Vemco
23.D_NOKIA	Integrated Safety and Security Development	Vemco	Vemco
23.F_LCM	Out of Band Security	Vemco	GUT, Vemco
23.G_JKU	PHY Layer Security	GUT	GUT
23.H_UCC	Real-time configuration	UCC	GUT, UCC, Vemco
23.N_VIF	SCOTT Security Lib	GUT	ViF
23.O_NOKIA	Security Core	CISC	CISC
23.P_GUT	Spatial-based authorization and authentication	GUT	GUT, UCC, Vemco
23.R_VIF	Trust Anchor for ES smart sensors	GUT	GUT, ViF

Table 2. TBB overview D9.5

3.12.3 Market innovation and perspective

GUT actively pitches the MPS. Preliminary cooperation agreements have already been signed the Port of Gdansk and one of the hospitals in Gdansk (Poland). Moreover, Gdansk Lech Wałęsa Airport interested in using the MPS as well.

GUT plans to create a Smart Infrastructure and expand the V2X (vehicle-to-anything) coverage at the university campus. This will allow GUT to conduct advanced tests in the physical layer security aspects in V2X communication. This infrastructure will consist of IoT devices and sensors that will transfer data between each other and vehicles. Such a dedicated infrastructure will be also a test space, where future development of SCOTT related system can take place. This will have an influence on TRL level of the products – dedicated test space may be valuable for product improvement and also serve as a showroom for potential customers.

Vemco has a well-established customer base in Poland and abroad. The exemplary facilities using accardMP, a current version of the Vemcos' access control system, are refineries, energy plants, factories, or warehouses.

3.13 Reliable Wireless Multi-hop Communications

3.13.1 Objectives

Reliable Wireless Multi-hop Communications is developed in WP18-19 and BB23.J in SCOTT. Starting from Wireless Sensor Networks with capability to form mesh networks, the BB23J defines mechanisms and algorithms to add QoS features to the communication between nodes inside the WSN bubble.
This is achieved thanks to the deterministic medium access, and a traffic prioritization 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. On the other hand, 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.

- Manage the wireless sensor network bubbles to make them trustable
- Extend the area covered by sensors by supporting multi-hop
- Enhance the quality of connection dynamically
- Extending lifetime of the network

3.13.2 Achievements through SCOTT

The technology provided by BB23J has proved robust and efficient according even in the harsh environment and restrictive requirements of WP18 and 19; this is, in the Rail Domain. Not only is trustable because it complies with QoS parameters set by applications, such as delay or the newly developed Quality of connection for multi-hop networks, but it also ensures privacy and security of data through channel encryption.
This allows the WSN based on BB23J not only to protect data, but also to restrict unauthorized access to wireless nodes at MAC level. Nodes that do not have valid keys cannot join the network. Even if nodes can listen to the channel, data is encrypted, and they cannot transmit (inject malicious data) because they are not synchronized with the network and the rest of valid devices. This feature is even more meaningful, because it allows user to isolate their WSNs without problems of coexistence (for example, WSNs in trains that cross their paths).
The reactive scheduling algorithm based on the network topology, which is changing according to quality parameters, ensures that during the operation of the network, it can achieve > 99% PDR (packet delivery ratio) even without retries.
Furthermore, the BB23J WSN used for WP18-20, and for demonstrator purposes, packs a toolset that takes away the complexity of deployment from the user.

With onsite guidance, assistant User Interface, and NFC secure activation mechanism, it is easy to configure and run without previous planification or expertise.
Other interesting features integrated into the WSN are the safety gateway backup, which means that data coming from WSN nodes is locally persisted and can be downloaded and restored off site, after connection losses. Wireless nodes also implement safety modes, in order to prevent data loss when running out of battery or connection is lost due to unexpected situations.

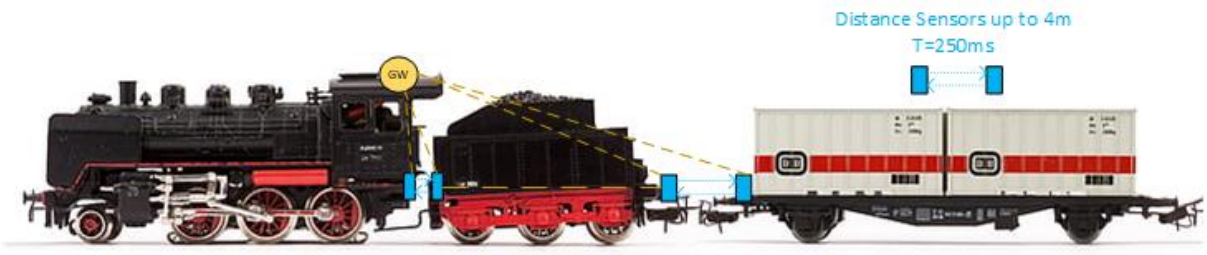
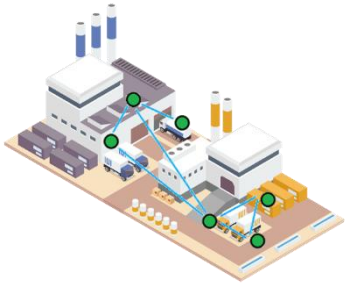


Figure 5. Example of BB23J WSN in Rail Integrity Application

BB23J WSNs have been tested in WP18 and 19, collecting different types of data and integrating with the Rail Demonstrator: logistics and maintenance (temperature, humidity, pressure, impact and vibrations), and integrity (based on distance between cars).

3.13.3 Market Innovation and Perspective



ITI, as DIH and a research and technology organization, has established an exploitation strategy based on technology transfer to the market. ITI focuses on being a regional leader and international representative agent in components and services that serve to the engineering process of complex and robust communication systems. Through SCOTT, ITI has developed an innovative communication technology in the field of wireless sensor networks. This positions ITI as an important ICT provider that supports the expansion and reception of this kind of technology in the always-demanding industrial market.

The state of the art technology achieved thanks to SCOTT allows ITI to be a key partner in the field of digitalization, where BB23J can help clients (companies, SMEs) to impulse their degree of sensorization. The BB23J Wireless Sensor Network adds value:

- Flexibility to the deployment of sensors
- Allows achieving wider number of devices monitored
- Reduced infrastructure costs
- Improved wireless communication in harsh environments

The direct client of these results will be an IT or Industrial Engineering company that can integrate the components and technologies into its portfolio and address the deployment of applications for industry and transport, such as digital twins, on demand production, V2I communications, or reduction of costs in intravehicular communications.

3.14 Big Data Analytics

3.14.1 Objectives

Big Data Analytics has been tackled in BB24.D and applied to WP7, WP9, WP10, WP11, and WP15.

Each involved partner has worked independently on its own analytics platform, and applied it to different use cases. The aim of the building block has been the development of their platforms, and the collection of their experiences when tackling big data analytics in SCOTT project, addressing the project's main topics (trustability, security, privacy, usability and safety) when analysing data from IoT wireless sensors in a big data environment.

3.14.2 Achievements through SCOTT

All partners implemented similar big data analytics pipelines following three main steps:
1) data collection,
2) data processing and
3) data storage/visualization.

Although the specific technologies for each module differed from one partner to another, most of them were open source, scalable, portable and supported by a wide community of users, thus making them highly suitable to address SCOTT project. Additionally, the most used analytics techniques in all use cases were exploratory data analysis, data cleansing, anomaly detection and data prediction (regression or classification), all of them developed on programming languages like Python. Moreover, these analytics techniques were carried out over similar data sources, all being composed of environmental measurements. Finally, the common goal of all use cases was similar: enhancing the efficiency / performance of systems, in order to improve the human life quality.

BB24.D has been a core building block for WP7. There, two main partners (VTT and ITI) have applied their platforms for indoor air quality (IAQ) analytics, while other partners (such as Centria) have played the role of data providers and participated on the use case analysis.

One of the goals of IAQ monitoring for the use case was related to analyze the monitored data and its produced information/knowledge. The aims were anomaly detection and prediction of IAQ conditions, as well as finding correlations between IAQ information and specific events or actions within the building. Moreover, datasets from partners such as Centria and Qplox were analyzed. Additionally, ITI helped Nokia to assess safety and security on data by performing a set of anonymization processes over a certain group of datasets provided by VTT.

On the other hand, the main goal of VTT in WP7 has been the development of a real-time system that continuously measures IAQ/IEQ (Indoor Air Quality / Indoor Environmental Quality) parameters and their level evolution along the day. For demonstrating the benefits of the monitoring system, VTT has utilized mainly the data collected by the monitoring system to control HVAC appliances, while user feedback has been also taken into account.

3.14.3 Market Innovation and Perspective

According to a report recently published by FORBES[1], 94% of the companies affirm that data analytics is important for their business growing; while 65% of them are spending more money on analytics during 2020; and 47% of the analytics platforms are cloud-based.

Although current technologies and solutions allow SMEs their access to massive data analytics, the existing complexity for technology configuration, deployment and management is hindering their adoption, in addition to the lack of qualified personnel and the high prices of the market solutions.

In addition, another point that shows the interest of the European Union on these topics is the fact that, as stated in the Mentoring Report 2018[2], the Big Data Value cPPP is receiving 534 million euros between 2016 and 2020, while it has already moved more than 1570 million euros coming from private investments.

In this context, through SCOTT, BB24.D partners have improved their analytics platforms, and proved their suitability to tackle heterogeneous use cases, such those proposed in the project. Thus, the resulting platforms could be easily applied to future projects. The experiences of SCOTT have also been useful to establish a verified methodology in terms of analytics pipelines, contributing to the consolidation of a set of techniques in order to extract insight from the available data.

[1] https://www.forbes.com/sites/louiscolumbus/2019/10/21/the-global-state-of-enterprise-analytics-2020/#15b85383562d
[2] http://www.bdva.eu/sites/default/files/MR2018_BDV_cPPP_Main%20Report_and_Annex%201_V1.0.pdf

Whereas most of the partners have applied existing third-party solutions, ITI has worked on its own big data as a service platform. In this case, SCOTT has been essential for the development and improvement of several components based on open-source technologies, meeting scalability, security, elasticity, recovery, resilience, responsiveness, flexibility, and interoperability requirements. Moreover, ITI has taken into account the above-mentioned SMEs needs, by designing a platform which reduces both time, costs and effort in order to apply analytics.

Thus, thanks to SCOTT, ITI and the rest of BB24.D partners have validated the suitability of analytics platforms, consolidating a promising ground for future projects in both public and private sectors.

Now, ITI, as DIH and a research and technology organization, has to put in practice its established exploitation strategy based on technology transfer to the market. ITI focuses on being a regional leader and international representative agent in tools and infrastructures that help Software companies to be more competitive. In this sense, ITI will transfer the knowledge and tools to the IT sector and will provide services around them to create a rich and innovative ecosystem around the center.

3.15 Cross-Technology Synchronization

3.15.1 Objectives

The technology building block BB24.F (cross-technology synchronization) deals with the run-time coordination and synchronization of heterogeneous wireless sensor networks (WSNs). Sensors employed in large-scale industrial data acquisition systems are often designed by different vendors and make use of different wireless technologies (e.g., IEEE 802.15.4, Wi-Fi, or Bluetooth Low Energy). When these heterogeneous WSNs are used to measure the performance of the same system or to observe the same phenomenon, it is necessary to allow a seamless communication between the heterogeneous devices and to synchronize the different measurements in order to give sense to the collected data.

Towards this goal, the objectives of BB24.F are twofold. On the one hand, BB24.F investigates how to allow a seamless coexistence using cross-technology communication (CTC), a novel paradigm that aims to directly convey information among heterogeneous wireless devices with incompatible physical layer without the need of intermediaries. CTC allows, for example, an IEEE 802.15.4 network to talk to another IEEE 802.15.4 network, to a Bluetooth Low Energy (BLE), or to a Wi-Fi network without the need of an expensive multi-radio gateway. Therefore, CTC functionality can be used, for example, to let two devices sharing the same ISM band directly exchange information about the used frequency channels and proactively avoid interfering each other. On the other hand, BB24.F leverages CTC for synchronization purposes and contributes solutions to synchronize low-power wireless devices making use of heterogeneous technologies without the need of a dedicated gateway. Specifically, BB24.F investigates the design of a cross-technology time synchronization primitive that allows to seamlessly exchanging timestamps between IEEE 802.15.4 and BLE devices.

3.15.2 Achievements through SCOTT

With respect to the aforementioned objectives, within BB24.F we have firstly completed the design and implementation of a generic and modular cross-technology communication framework named X-Burst (Hofmann, Boano, and Römer 2019). The latter allows off-the-shelf IEEE 802.15.4, Bluetooth Low Energy, and Wi-Fi devices to directly exchange broadcast packets in a seamless way despite their incompatible physical layer. Thanks to its generality and modularity, X-Burst allows reducing the complexity of CTC implementations, to increase the code portability, as well as to simplify the development of new functionality. X-Burst further enables a simpler customization of the

employed CTC scheme, for example by means of different encoding or decoding strategies (Hofmann, Boano, and Römer 2019). We have presented X-Burst's design and implementation at the 16th IEEE International Conference on Sensing, Communication and Networking (SECON) and won the **best paper award** (Hofmann, Boano, and Römer 2019).

X-Burst has been implemented, among others, using the Contiki operating system and evaluated on four off-the-shelf Internet of Things (IoT) platforms (i.e., the TI CC2650 LaunchPad, the Zolertia Firefly, the TelosB mote, and the Raspberry Pi 3B+). Experimental evaluations have shown the ability to carry out a cross-technology broadcast communication among IEEE 802.15.4, BLE, and Wi-Fi devices at data rates above 1 kB/s (Brunner et al. 2020). The implemented demonstrator, which showcases X-Burst's ability to carry out a cross-technology broadcast communication among four off-the-shelf IoT devices has been presented at the 17th International Conference on Embedded Wireless Systems and Networks (EWSN) and won the **best demo award** (Brunner et al. 2020).

Furthermore, within BB24.F, we have developed a cross-technology time synchronization primitive, called X-Sync (Grubmair et al. 2020), which allows to seamlessly exchanging timestamps between IEEE 802.15.4 and BLE devices in a bidirectional fashion. To build X-Sync, we have adapted and extended X-Burst (Hofmann, Boano, and Römer 2019) to allow medium access control layer based timestamping, as well as to include transmission delay compensation and skew rate estimation algorithms.
X-Sync has been implemented using the Contiki-NG operating system and evaluated on three off-the-shelf IoT platforms (i.e., the TI CC2650 LaunchPad, the Zolertia Firefly, and the TelosB mote). Experimental evaluations have shown that X-Sync can achieve sub-µs-level accuracy when using a synchronization interval of 10 seconds and when measuring the error as the maximum deviation over a time of 1000 s at a rate of 1 Hz (Grubmair et al. 2020). We have presented the preliminary design and implementation of X-Sync at the 17th International Conference on Embedded Wireless Systems and Networks (EWSN) (Grubmair et al. 2020).

3.15.3 Market Innovation and Perspective

The developed cross-technology communication coordination and synchronization schemes within BB24.F offer several advantages to both IoT application developers and end-users. On the one hand, developers and providers of IoT applications can avoid the need to fabricate and include expensive multi-radio gateways in their solutions. On the other hand, end-users can benefit from cheaper IoT systems requiring less installation effort.

Such multi-radio gateways, indeed, are currently one of the main hampering factors to the widespread adoption of IoT technology, as they are often significantly more expensive to fabricate than sensing/actuating units. Consider, for example, smart home (home automation) applications, where the light, the temperature, and the air quality of different rooms is monitored and controlled via the users' smartphones. As IoT devices use a plethora of different wireless technologies that may not be supported by the user's smartphones, multi-radio gateways are required. Even worse, several gateways are often necessary to build up a smart home, as sensors/actuators from different manufacturers may use a specific wireless technology. This is not only annoying and cumbersome for the end-users (installing and setting up the devices), but also very inconvenient for the application providers (as gateways constitute an additional non-negligible cost item). The concepts and solutions designed within SCOTT's BB24.F allow a direct communication and synchronization among wireless devices with incompatible physical layers, thereby addressing the aforementioned problems and allowing the development of cheaper and more sustainable IoT applications.

Furthermore, by enabling communication across wireless devices with incompatible physical layers, cross-technology communication provides a side channel that can be used by legacy devices to still communicate when the wireless technology for which they were originally designed is no longer supported or obsolete. This practically prolongs the lifetime of an IoT device and thus helps saving

resources and reducing the amount of electronic waste – an important observation as billions of IoT devices will be deployed and commercialized in the coming years.

Thus, thanks to SCOTT, a potentially disruptive technology for the development of cheaper and more sustainable IoT applications, i.e., the use of cross-technology communication and synchronization without dedicated multi-radio gateways, has been designed and prototyped. Specifically, the cross-technology communication scheme developed within SCOTT was patented by TUG (EU patent application no. 18212281.2-1213, “Method and system for transmitting a cross protocol message”; by R. Hofmann, C.A. Boano, and K. Roemer), who plans to market or license it to companies – especially those in the home automation sector. TUG is currently approaching several companies, including ARM Holdings and Nordic Semiconductors to investigate how to increase the marketability of the solution, to further improve the developed CTC concepts, and to set up future collaborations.

3.16 System Level Availability

3.16.1 Objectives

The basic idea of Fault Injection Techniques is to emulate (is in fact imitate) both hardware and software to better predict the final product quality and reliability. To make models of the hardware, a good representation of the actual hardware is needed. In many cases, emulation can be used to evaluate the software components without the (final version of the) hardware. To create those models, the software requires the following:

- Representation of hardware models in transfer functions, derived from hardware simulation tools, physics of failure knowledge, Design of Experiments (DoE), or by using the transfer function from previous hardware versions.
- Models for functional parts of the hardware, to be able to test specific parts only.
- Descriptions of interactions between models (dependency/relation).

In SCOTT PhLi has investigated to what level fault injection can contribute to a fast release of large and complex systems. The approach by itself is quite straightforward, as indicated in the figure below. Where traditional stress testing adds elevated loadings to the system or product, under fault injection methods the system is tested under the conditions of having a (minor) fault inside. How the system reacts under such a condition can give information on it’s availability under normal use.

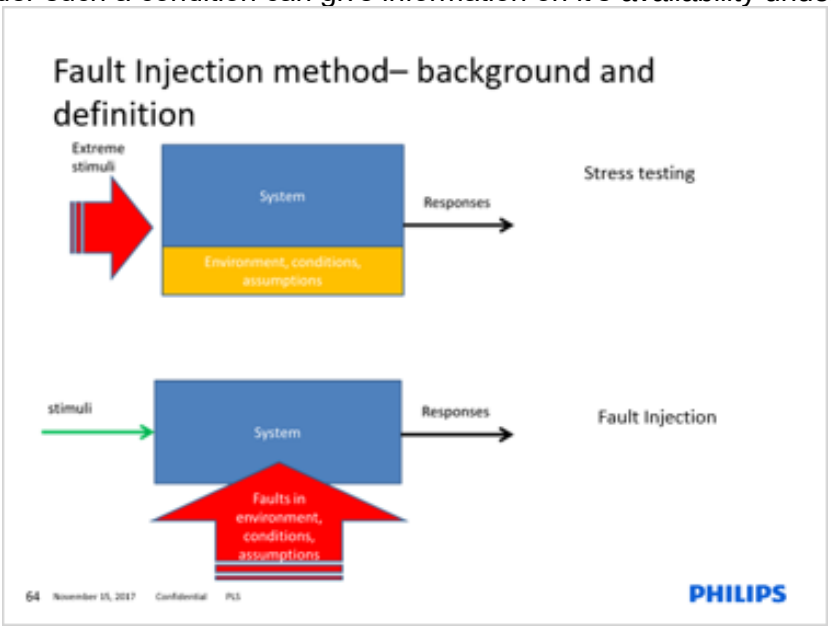


Figure 6. Approach of fault injection; traditional stress testing (top), faults injection (bottom).

3.16.2 Achievements through SCOTT

The system to demonstrate the technique was connected office or interact office. InterAct Office provides a complete LED retrofit system and up to 70% energy savings, without upfront capital investment. Hassle free installation leverages the existing lighting infrastructure, while easy operation saves time and provides peace of mind. You gain crucial insights into your lighting's energy consumption and occupancy patterns across your portfolio. These insights, supported by data, allow you to make decisions on portfolio optimization and bring stakeholders on board with facts. InterAct Office is scaled across all properties in your real estate portfolio, and grows with your needs, enabling unlimited expansion of connected sites and data management. As it uses cloud technology, InterAct Office's intuitive cloud-based analytics dashboard is accessible anytime, anywhere to provide detailed, real-time real estate energy use information. A test bed is available for the investigations, see Figure below.

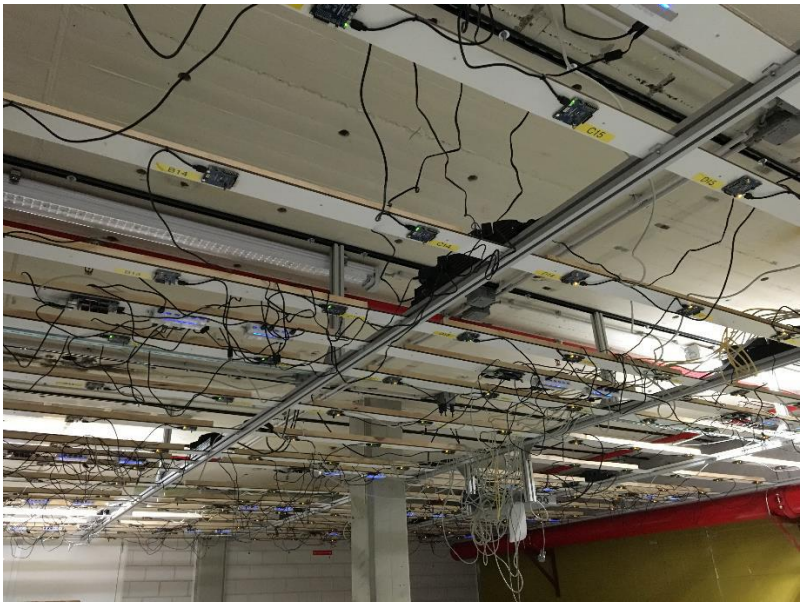


Figure 7. Test bed connected office lighting.

The testing approach is listed in the figure below. A reference test is compared towards the test with the fault injection in order to check the system recovery under the worsened conditions.

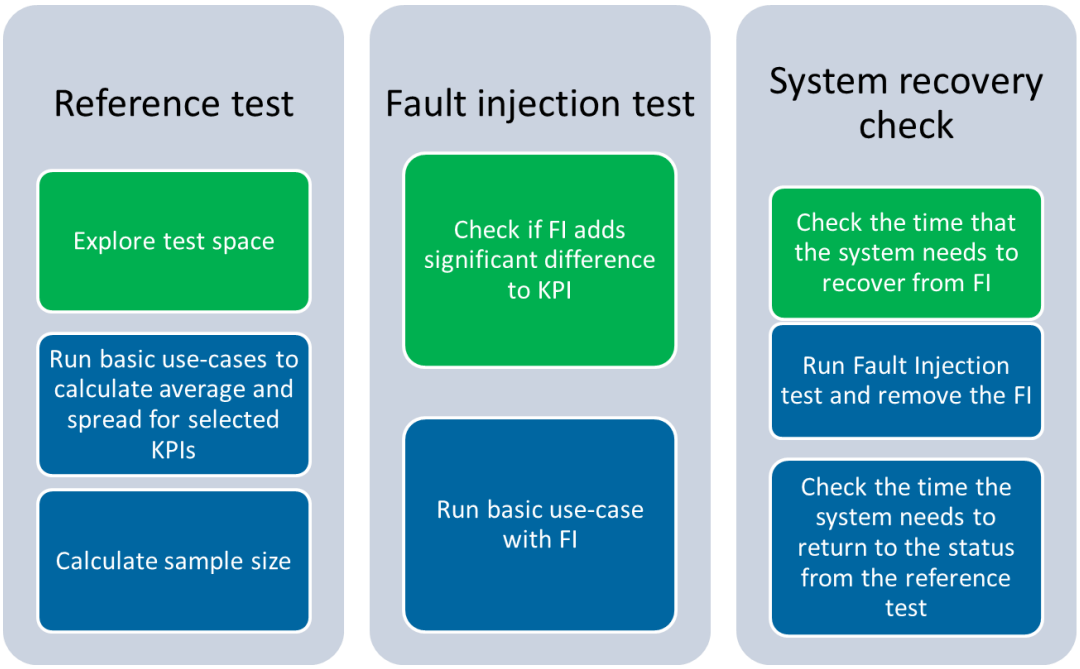


Figure 8. Test description – proposed FI test strategy.

Main achievements are listed as:

- Testbed is up and running.
    - SPLUNK is used as analyser and all test data is logged into traffic data
- Fault injection is performed, nodes in the corridors are silenced
- We have set-up minimum efforts for application level fault injection, recoverability and fault tolerant scenarios, these are applicable for UCs:
    - Ubiquitous Testing of Automotive Systems
    - Air Quality Monitoring for healthy indoor environments
- Fault injection techniques has become a vital part for the release of the PhLi connected product portfolio.
- Fault injection will enable us to faster release complex systems w/o hampering the quality levels

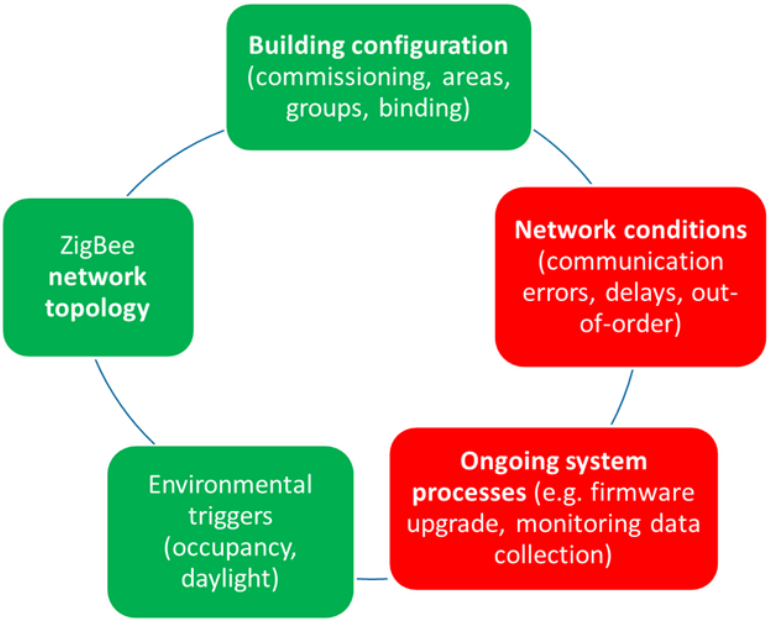


Figure 9. FI test strategy for complex lighting systems.

3.16.3 Market Innovation and Perspective

The work from this technology building block is contributing to the use case *Ubiquitous Testing*. Other use cases originally also were in scope, e.g. *air quality monitoring for healthy indoor environments* and *trustable wireless in-vehicle communication network*. As the fault injection technique is quite general for any complex system, other use cases in the project may also benefit from this work. For that reason PhLi has made connections to the standardisation bodies. SCOTT has made it possible to develop the testing method and make it the de-facto standard way of system release at PhLi.

3.17 Reference Architecture / Reference Implementations

3.17.1 Objectives

The objective of the reference architecture was to produce a set of building blocks and network components that enable the communication between all the objects and entities of the bubble infrastructure inside each industrial use case (intra- and extra-bubble communications) , as well as across different use cases (inter-bubble communications). In addition to this, the activities also focused on infrastructure evaluation, security metrics, functionality management and overall trustworthiness assessment.

3.17.2 Achievements through SCOTT

The reference architecture of SCOTT has been adapted to support a variety of building blocks related to state-of-the-art security, dependability, safety and trustworthiness of IoT solutions. This architecture has also been analysed and implemented for interoperability with existing industrial solutions such as Fiware, Microsoft Azure, IBM red, and it has been also aligned with industrial standards for Edge computing, blockchain, IEEE reference architecture, as well as the ISO and ITU reference architectures. Additionally, the use of functionalities such as network virtualization and network slicing positions our architecture solution in combination with 5G industrial standards and architectures. We have also upgraded the concept of bubble to be adapted to a wide number of

industrial use cases and provided a trustworthiness perspective to help in the design and robustness analysis of use cases for different industrial domains.

3.17.2.1 Interoperability

The concept of Bubble for interoperability solution was improved in the project. While it has no purpose of commercial implementation as it was perhaps initially intended during the conception of the initial proposal, the bubble has been proved useful as a tool to analyse interoperability between heterogeneous commercial solutions. In addition, the bubble has been used to include concepts such as edge computing, network slicing, network virtualization, and block chain. Therefore, the bubble can be used as a method to create improved connectivity, trusted communications, and enhanced trustworthiness evaluation between cyber entities. This has a clear consequence on standardization, certification and regulation of future IoT services and objects.

3.17.2.2 Semantics

Regarding the semantics proposal of the project we have proposed final recommendations for the adoption of modified semantics that support trustworthiness metrics for communications between bubbles. The project did not propose a unique semantics solution for all use cases, but instead each use case and domain have chosen their unique semantic solution adapted to their needs. The proposal was to find extensions of those already defined semantics to support added security, trusted communications, domain modelling and bubble infrastructure identification. This means that we foresee a heterogeneous landscape of multiple semantics protocols, which can be extended or modified to be able to support SCOTT services with trusted communications.

3.17.2.3 Trusted bubble communications

Together with our partners for trust framework and security metrics we have proposed the use of trustworthiness metrics for Bubble communications. A vector of trustworthiness metrics that can be grouped in classes is used to evaluate each bubble and its components in the cyberspace. These trustworthiness metrics are used by the different third-party entities or other bubbles to modify the communication and security enhancing technologies to communicate with such Bubble. The framework is based on a detailed functionality model of the reference architecture and several techniques to evaluate trustworthiness metrics inside and outside the bubble. All the technology building blocks of the project have been mapped to the functionality and vulnerability (threat) models used for this trustworthiness evaluation of communications between bubbles. This contribution aims to analyse how to implement trust aspects in future IoT architectures. We foresee a future market of IoT cyberspace solutions with multiple methods to evaluate trust of other entities (potentially conducted by trusted third parties), and thus adapt their content and protocol communications accordingly.

3.17.3 Market Innovation and Perspective

We foresee a heterogenous and dense market of IoT architectures and interoperability between multiple protocols with different trustworthiness and security metrics related with safety issues in different use cases and contexts. Therefore, SCOTT innovations target a complex landscape of interacting cyber entities using the bubble as the basis of analysis of interoperability, security, dependability and trust. The bubble is not mandatory to be implemented, and therefore is useful mainly as guideline for industrial connectivity and infrastructure design. We expect the future market to take benefit from the conclusions and recommendations obtained from bubble infrastructure organization, trust analysis, and modified reference architecture. In other words, we expect that the concept of bubble could be used not only as implementation technology, but also as a useful infrastructure organization guideline and base for trust and security analysis. The conclusions of the bubble design are being considered in several standardization bodies, which means they would be available to end commercial products in the following years.

3.18 Aeronautics

3.18.1 Objectives

The objective of the aeronautics domain was to introduce security and trust concepts in the design of wireless avionics intra-communications (WAICs). The associated objective was to bring the concept of the Bubble for secure IoT applications on board any type of aircraft, particularly commercial passenger airplanes. Another objective was to continue the development of the turbulence compensation schemes based on dense wireless sensor and actuator networks. The turbulence compensation scheme has a low TRL, but it is useful to analyze the different types of threats on board commercial aircraft and the safety issues of running a sensor and actuation mechanism on a commercial aircraft.

3.18.2 Achievements through SCOTT for the Market

The aeronautics domain, particularly for wireless solutions on-board aircraft, is perhaps the most limited in terms of commercial testing and market perspectives. This is due to the inherent safety cautionary perspective of the industrial players. We have confirmed in our development and evaluations, that there was potentially a strategic marketing mistake made by the early proposals of WAICS regarding the feature of wireless links seen as the replacement of cabling structures in an aircraft. This, while one of the main attractive solutions of wireless in avionics, has created a lack of trust in the conservative members of the aeronautics industry. The conclusion of our work on trust is that the approach recommended is to highlight wireless solutions in non-critical applications for the aircraft, or as a redundant feature to the cable infrastructures. This is the recommendation for strategy of introduction of wireless solutions based on trust and experience of the project. Eventually, the feature of replacement of cables can be introduced once the basic non-critical and redundant applications have been commercially tested and have proved to be trustworthy. Another option is to do tests of fly-by-wireless on unmanned aerial vehicles and draw the conclusions for passenger planes. This is another conclusion of our strategy. As observed in the success contest won by our partners TU Delft for passive switches on board aircraft, the non-critical wireless avionics services represent an important door for commercial implementation and market viability of wireless avionics intra-communications and SCOTT security solutions. We expect that these recommendations lead to a faster market adoption of wireless solutions for aircraft management.

Regarding the proposal for turbulence compensation, the developments are still with low TRL. However, the concept has been evolving to target a wider potential market audience. The patch of sensors and actuators would be made completely of a printed ink technology circuit. The patch would use high frequency antennas to receive and harvest electromagnetic energy. The same waves would be used for channel estimation and turbulence measurement. The energy stored can be used for enabling a set of electric actuators based on electromagnetic barrier discharge. This solution, still not analysed in terms of viability, would be ideal for commercialization, due to the flexibility of the patch, the low cost of printed electronics technologies, the low cost in terms of energy consumption, as well as the flexibility of a patch that can be stuck to the surface of an airplane with all the functionalities of a SCOTT bubble in constrained devices.

4 CONCLUSIONS

The companies and universities that have been the partners of the SCOTT project such as TUG, GUT, UiO, CIT, Indra, Philips, Vemco, AVl, ISEP, Eyenetworks, UMP, ACCIONA, etc. had a variety of solutions and perspectives to the market as it has always been essential to use the research achievements for market requirements.

The SCOTT partners had concrete commercialization activities and results and also many good connections were established between SCOTT partners that will continue after the project and foster new commercial endeavors. Moreover, SCOTT as a project offered the partners an arena for presenting their various commercial solutions to the other partners, as well as to external actors. Due to its visibility, the SCOTT project allowed the partners to have a strong promoting factor when showcasing their technologies in various show-forums outside the project, bringing them more credibility for their technological offers. In addition, several of the models or ideas which were not directly implemented are now part of standardization efforts and will thus be available to the market within the next few years.

A. REFERENCES

[1] Miller, C., & Valasek, C. (2015). Remote exploitation of an unaltered passenger vehicle. *Black Hat USA*, *2015*, 91.

[2] Habeck, A., Newman, J., Bertoncello, M., Kässer, M., Weig, F., Hehensteiger, M., ... & Yan, Z. (2014). Connected car, automotive value chain unbound. *McKinsey & Company, Report*.

[3] https://autodrive-project.eu/ [online, last accessed 2020-09-12]

[4] https://www.v2c2.at/gtc2018 [online, last accessed 2020-09-12]

[5] SCOTT Deliverable D9.5 “Use Case "Secure Connected Facilities Management" Demonstrator Description and Evaluation”, v1.0, 2020-05-05

[6] SCOTT Deliverable D15.5 “Use Case “Vehicle-as-a-sensor-within Smart Infrastructure” Demonstrator specification and evaluation”, v1.0, 2020-05-15

[7] Hofmann, R., Boano, C. A., & Römer, K. (2019, June). X-Burst: Enabling Multi-Platform Cross-Technology Communication between Constrained IoT Devices. In *2019 16th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)* (pp. 1-9). IEEE.

[8] Brunner, H., Hofmann, R., Schuß, M., Link, J., Hollick, M., Boano, C. A., & Römer, K. (2020, February). Cross-Technology Broadcast Communication between Off-The-Shelf Wi-Fi, BLE, and IEEE 802.15. 4 Devices. In *EWSN* (pp. 176-177).

[9] Grubmair, D., Hofmann, R., Boano, C. A., & Römer, K. (2020, February). Poster: Accurate Cross-Technology Clock Synchronization Among Off-the-Shelf Wireless Devices. In *EWSN* (pp. 162-163).

B. ABBREVIATIONS AND DEFINITIONS

Term	Definition
ABAC	Attribute Based Access Control
ACS	Access Control System
AI	Artificial Intelligent
ALCCS	Assisted Living Community Care
AWN	Autonomous Wireless Network
BB	Building Block
BLE	Bluetooth Low Energy
CIT	Cork Institute of Technology
CMW	Communication Middle Ware
CTC	cross-technology communication
DoE	Design of Experiments
DNS	Domain Name Server
DMI	Driver Machine Interface
ECD	elderly context deviation
ETCS	European Train Control System
ESPR	Electronically Steerable Parasitic Array Radiator
GNSS	Global Navigation Satellite System
HAR	human activity recognition
IAQ	Indoor Air Quality
IEQ	Indoor Environmental Quality
I2I	Infrastructure-to-Infrastructure
IoT	Internet of Things
LDAC	Lightweight Directory Access Protocol
LIDAR	Light Detection and Ranging
MPS	Multimodal Positioning System
MQTT	Message Queuing Telemetry Transport
NTP	Network Time Protocol
PEAP	Protected Extensible Authentication Protocol
QoS	Quality of Service
QoE	quality of experience
QR	Quick Response
RTMN	Real Time Management Network
SABAC	Semantics based ABAC
STCC	Smart train composition coupling
TPM	Trusted Platform Module
TWI	Trustworthiness Indicator
TWS	Trustable Warning System
UC	Use Case
UPM	Universidad Politecnica de Madrid
V2V	Vehicle to Vehicle
VCTS	Vertical Case Transport System
WAICs	wireless avionics intra-communications

WP	Work Package
WSN	Wireless Sensor Network