SCOTT:
Secure COnnected Trustable Things

Demonstrator Generation 1

Document Type	Deliverable
Document Number	D12.2
Primary Author(s)	Przemysław Popowicz | GUT
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 the latest version of Annex I against which the assessment will be made	2018-07-11

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
Przemysław Popowicz	GUT	Peter Priller	AVL
Carlo Alberto Boano Rainer Hofmann	TUG	Hans-Peter Bernhard	JKU
Leander Hörmann	LCM	Andreas Springer	JKU

FORMAL REVIEWERS

Name	Organization	Date
Rocío Gómez, Francisco Parrilla	INDRA	2018-06-27
Ramiro Samano Robles	ISEP	2018-07-18

DOCUMENT HISTORY

Revision	Date	Author / Organization	Description
0.1	2018-05-10	Przemysław Popowicz/GUT	Initial template with GUT example
0.2	2018-05-29	Przemysław Popowicz/GUT	Template after Peter Priller review
0.3	2018-06-11	Carlo A. Boano/TUG Rainer Hofmann/TUG	Added CTC demonstrator
0.4	2018-06-14	Przemysław Popowicz/GUT	Added paragraph about demonstrator public output
0.5	2018-06-21	Leander Hörmann/LCM	Added OOB communication demonstrator
0.6	2018-06-22	Peter Priller/AVL	Added Vehicle Conditioning (SOAK) demonstrator
0.7	2018-06-23	Hans-Peter Bernhard/JKU and Andreas Springer/JKU	Demonstrator Energy Efficient Secure Communications added
1.0	2018-07-01	Przemysław Popowicz/GUT	Fixes after INDRA review

TABLE OF CONTENTS

1 EXECUTIVE SUMMARY 7

2 OBJECTIVES 8

2.1 Requirements fulfilment 8

2.1.1 Demonstrator MPS – GUT 8
2.1.2 Demonstrator CTC – TUG 9
2.1.1 Demonstrator OOB Communication – LCM 9
2.1.2 Vehicle Conditioning (SOAK) Demonstrator - AVL 10
2.1.3 Demonstrator Energy Efficient Secure Communications – JKU 11

3 DESCRIPTION OF WORK 12

3.1 Demonstrators link to Use Case Scenarios 12
3.2 Demonstrators description 13

3.2.1 Demonstrator Vehicle Conditioning (SOAK) demonstrator - AVL 13

3.2.1.1 Link to technology lines 14
3.2.1.2 Demonstrator public output 15

3.2.2 Demonstrator MPS – GUT 16

3.2.2.1 Link to technology lines 17
3.2.2.2 Demonstrator public output 17

3.2.3 Demonstrator CTC – TUG 18

3.2.3.1 Link to technology lines 18
3.2.3.2 Demonstrator public output 18

3.2.4 Demonstrator OOB Communication – LCM 19

3.2.4.1 Link to technology lines 19
3.2.4.2 Demonstrator public output 19

3.2.5 Demonstrator Energy Efficient Secure Communications – JKU 20

3.2.5.1 Link to technology lines 21
3.2.5.2 Demonstrator public output 21

3.2.6 Demonstrator Security Threat Analysis - SBA 22

3.2.6.1 Link to technology lines 22
3.2.6.2 Demonstrator public output 22

4 DISSEMINATION, EXPLOITATION AND STANDARDISATION 23

5 LINK TO TECHNOLOGY LINES 24

6 CONCLUSIONS 25

7 REFERENCES 26

A. ABBREVIATIONS AND DEFINITIONS 27

LIST OF FIGURES

Figure 1. Example Soak Room (1) [2] 13
Figure 2. Example Soak Room (2) [3] 13
Figure 3. Architecture Overview - Integration with PUMA Open 14
Figure 4. MPS camera with the embedded processing architecture 16
Figure 5. Developed by the GUT cheap camera with embedded processing encapsulated in a 3D-printed housing 16
Figure 6. The result of LED detection 17
Figure 7. Setup of the CTC Demonstrator. 18
Figure 8. Out-of-Band Communication Demonstrator Overview 19
Figure 9. Typical timing measurements for evaluating synchronization in case the communication link is not disturbed 20
Figure 10. Secure communication links between nodes and base station and automation system 21

LIST OF TABLES

Table 1. MPS – fulfilment of requirements. 8
Table 2. CTC – fulfilment of requirements. 9
Table 3. Vehicle Conditioning demonstrator – fulfilment of requirements. 10
Table 4. Energy Efficient Secure Communications – fulfilment of requirements. 11
Table 5. Use Case Scenarios link to Demonstrators 12
Table 6. Technology lines link. 24

1 EXECUTIVE SUMMARY

The main objective of this deliverable is to describe the first iteration of a demonstrator implemented for WP12 in the 1st year of the SCOTT project. It summarizes the results of works of the partners involved in the Ubiquitous Testing in the 1st year of the SCOTT Project. This document, as the second deliverable of WP12, provides the link to the requirements, technical building blocks and scenarios defined previously.

Keywords: WP12, demonstrator, Y1, SOAK, MPS, CTC, OOB Communication, Energy Efficient Secure Communications, Ubiquitous Testing, instrumentation of automotive testing, test bed, test vehicle, WSN, trust indicator.

2 OBJECTIVES

The objectives of this deliverable are:

- Define the scope of the SCOTT WP12 Y1 demonstrator
- Provide a description of each partner demonstrator
- Link the demonstrators with requirements and technology building blocks

The list of SCOTT objectives and their fulfilment was described in the SCOTT D12.1 [1]. The fulfilment of those objectives will be demonstrated by the demonstrators described in next chapters.

2.1 Requirements fulfilment

This chapter describes how requirements are fulfilled by each demonstrator.

2.1.1 Demonstrator MPS – GUT

ID	BB	Short_name	Fulfilment
390	23.P	Object localization and position	Implemented detection of blinking LED by the camera for positioning with high accuracy. The calibration procedure for 3D localization under development.
391	23.P	Localization_method	Distributed system architecture was planned and cheap cameras with embedded processing for vision localization was developed.
557	23.P	Different_detecion_accuracy	The Demonstrator in this UC uses high accuracy vision localization. Further test and improvements of algorithm needed.
679	23.P	Location Based Security	Not implemented in the Y1 demonstrator

Table 1. MPS – fulfilment of requirements.

2.1.2 Demonstrator CTC – TUG

ID	BB	Short_name	Fulfilment
627	24.F	Co-existing networks	Developed a cross-technology communication (CTC) scheme that allows data exchange between wireless devices making use of IEEE 802.15.4 (ZigBee) and Bluetooth Low Energy (BLE) without the need of a dedicated gateway. Based on this CTC scheme, a management system that coordinates the used frequency channels among heterogeneous wireless devices will be developed, so to reduce cross-technology interference and maximize coexistence.
628	24.F	Cross-technology-sync	Not implemented in Y1 demonstrator. Based on the aforementioned CTC scheme, a mechanism to synchronize the clocks of heterogeneous devices at a microseconds-scale will be developed and demonstrated in the next iteration.

Table 2. CTC – fulfilment of requirements.

2.1.1 Demonstrator OOB Communication – LCM

ID	BB	Short_name	Fulfilment
522	23.F	Out_of_band_communication	Communication using a physical channel different to radio-communication. This will be demonstrated using Near Field Communication (NFC) communication using the nRF52832 IC and an embedded computer exchanging wireless network configuration data.
523	23.F	Localized_communcition	The Out-of-band (OOB) communication is only possible in a very reduced space. This will be demonstrated as above using NFC communication.
525	23.F	Energy_efficiency_OOBCom	The OOB communication should be implemented in an energy efficient way. This will be shown by a measurement of the power consumption.

Table 3. OOB - fulfilment of requirements.

2.1.2 Vehicle Conditioning (SOAK) Demonstrator - AVL

ID	BB	Short_name	Fulfilment
416	23.G	Physical_layer_parameters	In order to implement a first version of trust indicator, the base station of the Wireless Sensors Network (WSN) shall be able to provide information about the conditions of the physical layer (e.g. strength of the signal, SNR), state of the communication channel.
532	25.F	Sensor_node_assignment	Within vehicle conditioning facilities (“soak area”), nodes must be uniquely identified (sensor nodes must be assigned to test vehicles).
658	Demo	Robust WSN	WSN system needs to demonstrate robust communication in industrial environments, as well as operate reliably under respective environmental conditions (temperature, vibration, humidity etc.).
671	BB25.B	Low power design	To allow autarkic operation of WSN nodes, ultralow power design of all parts of the node, including data acquisition, processing, communication, and security mechanisms is required.
672	BB24.B	Unambiguous bubble assignment	Co-existence of multiple wireless test systems must be supported, e.g. by intelligent management in time and frequency domain. Appropriate methods must be provided so nodes join/unjoin correct network in a fast, secure, and verifiable manner.
676	Demo	Multi-sensor node	Multiple types of sensors (in this iteration: temperature sensors Pt100, Pt1000, Thermocouple) shall be supported by WSN.
677	Demo	WSN node usability	Node state must be clearly recognizable to user (e.g. with LED, or a diagnostic connector etc.)
678	Demo	System usability	System shall report info about network state and conditions to the user, e.g. number and type of connected nodes, bandwidths, signal strengths, etc.) upon user request.

Table 3. Vehicle Conditioning demonstrator – fulfilment of requirements.

2.1.3 Demonstrator Energy Efficient Secure Communications – JKU

ID	BB	Short_name	Fulfilment
499	25.A	Secure operation cycle	Partly implemented based on the work described in section 3.2.6, but testing not yet finalized.
500	25.A	Secure disruptions	This requirement is not yet fulfilled and will be targeted in the Y2 and Y3 versions.
501	25.A	Out-of-band security	Work on this requirement has been started (see section Demonstrator Energy Efficient Secure Communications – JKU) but no final decision on the key exchange mechanism has been made.
502	25.A	Energy efficiency	In the current version of the demonstrator this requirement is fulfilled.
504	25.A	Latency(2)	In the current version of the demonstrator this requirement is fulfilled.

Table 4. Energy Efficient Secure Communications – fulfilment of requirements.

3 DESCRIPTION OF WORK

The Y1 demonstrator consist of many sub-demonstrators that are used in different Use Case (UC) Scenarios specified in SCOTT D12.1 [1]. NXP AT and NXP NL did not make a formal contribution to first iteration of demonstrator described in this deliverable.

3.1 Demonstrators link to Use Case Scenarios

Relation to scenarios described in SCOTT D12.1 [1].

Scenario No.	Scenario Name	Demonstrator Name	Organization
1	Instrumentation and hot testing of an Unit under test (UUT)	Vehicle Conditioning (SOAK) demonstrator	AVL
2	Localization of Sensors and automatic deduction of context	Multimodal Positioning System (MPS)	GUT
3	Mount UUT into a test bed (or vehicle) and check setup	OOB Communication	LCM
4	Run tests (operate and monitor UUT, test bed/vehicle and measurement system)	Vehicle Conditioning (SOAK) demonstrator Energy Efficient Secure Communications	AVL JKU
5	Define, manage and evaluate test	[will be part of next generation demonstrator]	
6	Configure, check and run a **distributed** test setup, combining two or more parts of a UUT	CTC	TUG
7	Check, maintain and calibrate measurement system	[will be part of next generation demonstrator]	
8	Produce and maintain measurement system	[will be part of next generation demonstrator]	

Table 5. Use Case Scenarios link to Demonstrators

3.2 Demonstrators description

3.2.1 Demonstrator Vehicle Conditioning (SOAK) demonstrator - AVL

The European emission legislation for vehicles (Euro 6c) allows certain emission test and certifications runs to be executed on chassis dyno test beds. However, in order to prove the fulfilment of side conditions (e.g. environmental temperature, humidity, etc.), it requires exact measurement and documentation of temperature values (time series) during the conditioning of vehicles to be tested. This is usually done in a specialized, air-conditioned room called soak area. This might be a large room (or multiple rooms, or a “vehicle stacker”) from 1 up to 10 or 30 cars.

Example pictures for such facilities:

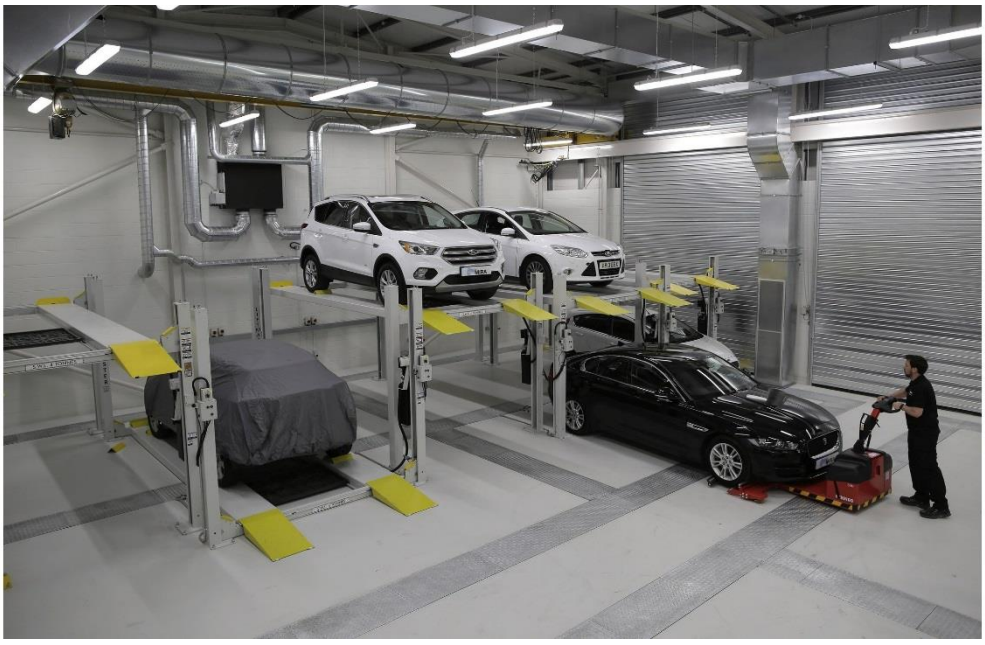

Figure 1. Example Soak Room (1) [2]

Figure 2. Example Soak Room (2) [3]

The duration for such “soak process” may vary between 6 and12 hours. During soaking the area is typically dark, which excludes existing energy harvesting solutions like photovoltaic cells for the WSN nodes. This is why it was decided to go with (special long life) batteries for this first prototype. Battery life shall exceed 1500h, in other words 62 days of operation time. The battery state needs to be reported wirelessly to the base station.

During soaking the vehicle engine is off.

Soak-temperatures depend on testing conditions, and might be:

- room temperature (20 - 30 °C)
- 14 Degree C soak
- -7 degree C
- Or anywhere between -30 and +45 °C

Temperature measurements must be done with 1Hz during the full soak process. Temperature sensors (Pt100 or Thermocouple) are mounted in car (e.g. at the cooler), with a short cable (like 25 cm) to the electronics (ADC, communication etc.), which might be partly outside of the vehicle, e.g. mounted on front grill of the car. That part needs to withstand potential test drives on the road as well (there should be no need to dismount these parts during test drive)

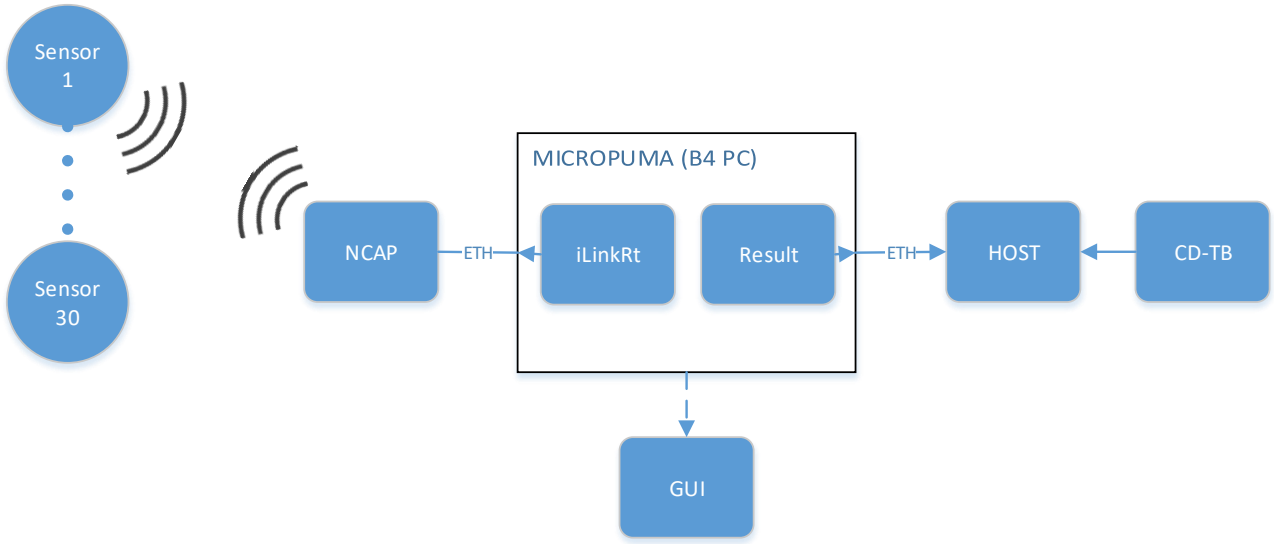

Figure 3. Architecture Overview - Integration with PUMA Open

3.2.1.1 Link to technology lines

As defined in the table above, and based on the existing prototype of WSN (node + base) developed in DEWI; this SOAK demonstrator will focus on:

- BB23.G Physical_layer_parameters In order to implement a **first version of trust indicator**, the base station of the WSN shall be able to provide information about the conditions of the physical layer (e.g. strength of the signal, SNR), state of the communication channel.
- BB25.F Sensor_node_assignment Within vehicle conditioning facilities (“soak area”), nodes must be **uniquely identified** (sensor nodes must be assigned to test vehicles).

- BB25.B: Low power design: To allow autarkic operation of WSN nodes, ultralow power design of all parts of the node, including data acquisition, processing, communication, and security mechanisms is required.
- BB24.B: Unambiguous bubble assignment: Co-existence of multiple wireless test systems must be supported, e.g. by intelligent management in time and frequency domain. Appropriate methods must be provided so nodes join/unjoin correct network in a fast, secure, and verifiable manner.

3.2.1.2 Demonstrator public output

As the SOAK UC is a very new opportunity for applying WSN in automotive testing, AVL can provide only information about its generic architecture and protocol used (EPHESOS via BT) for this first demonstrator. More details are expected to be publicly available in Y2.

3.2.2 Demonstrator MPS – GUT

MPS is responsible in WP12 for localization of wireless nodes mounted on an engine in the test bed. In the demonstrator, GUT will show detection of a blinking LED with use of a camera developed by GUT.

GUT use a COTS lens, an image sensor, and a RaspberryPi 3 with CSI2 (Camera Serial Interface). Image from the sensor is recorded in RAM and processed by algorithm working on RaspberryPi. The simplified architecture is shown in the figure below.

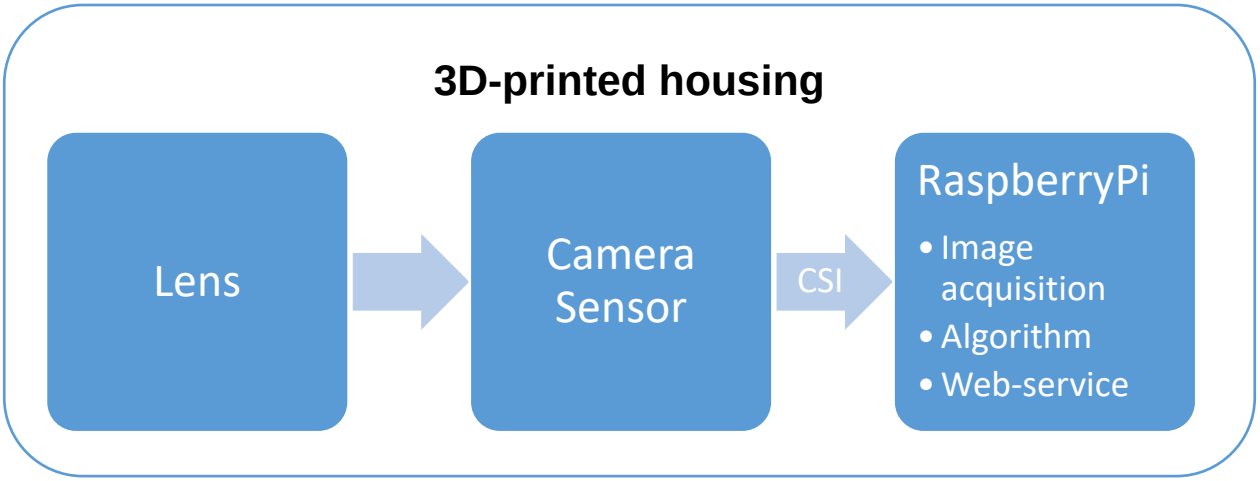

Figure 4. MPS camera with the embedded processing architecture

This approach allows for distributed image processing in case of many cameras used in the target solution. GUT created a 3D-printed housing for the camera with the lens mounting brackets. It is shown in the photo below.

Figure 5. Developed by the GUT cheap camera with embedded processing encapsulated in a 3D-printed housing

The result of the algorithm is a position (x,y) of the LED on the camera matrix. An exemplary result of the algorithm is shown in the picture below.

Figure 6. The result of LED detection

For visualisation purposes, GUT developed a simple web service which is able to display image from the camera with marked detected positions.

In the future works, GUT will improve the detection algorithm and use the information from at least 2 cameras for 3D positioning. Also, tests of accuracy will be carried out.

In the target solution, the system will be integrated with AVL NCAP and JKU nodes.

3.2.2.1 Link to technology lines

The MPS component is related to BB23.P and uses high precision vision localization method with distributed processing. The RabbitMQ and Wireless Sensors Network described as a part of BB23.P in SCOTT D23.1 [4] is not used in this UC.

In the next iteration, BB23.G will be used for improving the security.

3.2.2.2 Demonstrator public output

Video of the localization process presenting the result of an embedded processing algorithm with use of 1 camera and 4 blinking LEDs in laboratory conditions.

3.2.3 Demonstrator CTC – TUG

CTC is a key component of WP12 that allows heterogeneous wireless devices to exchange data among each other without the need for a dedicated gateway.

In this demonstrator, TUG will show how two off-the-shelf Internet of Things (IoT) devices making use of IEEE 802.15.4 and BLE technology, respectively, can communicate bi-directionally without the need of a third dedicated device acting as a gateway. The demo consists of a Texas Instrument CC2650 Launchpad (Cortex M3 microcontroller and TI CC2650 radio) as BLE device and an Advanticsys MTM5000-MSP sensor node (MSP430 microcontroller and TI CC2420 radio) as IEEE 802.15.4 device. Both devices are running the Contiki operating system.

Interacting with the user buttons of one platform will toggle the LEDs of the other platforms accordingly thanks to the developed CTC communication scheme. Furthermore, additional data is embedded in the CTC messages being exchanged by the two devices (e.g., sensor readings). Both IoT devices are connected to a laptop via USB, in order to display the received messages on a terminal. To show the working principle of the CTC communication scheme, a picoscope displays the ongoing communication between the two devices in detail. Figure 7. Setup of the CTC Demonstrator. summarizes the setup of the CTC demonstrator.

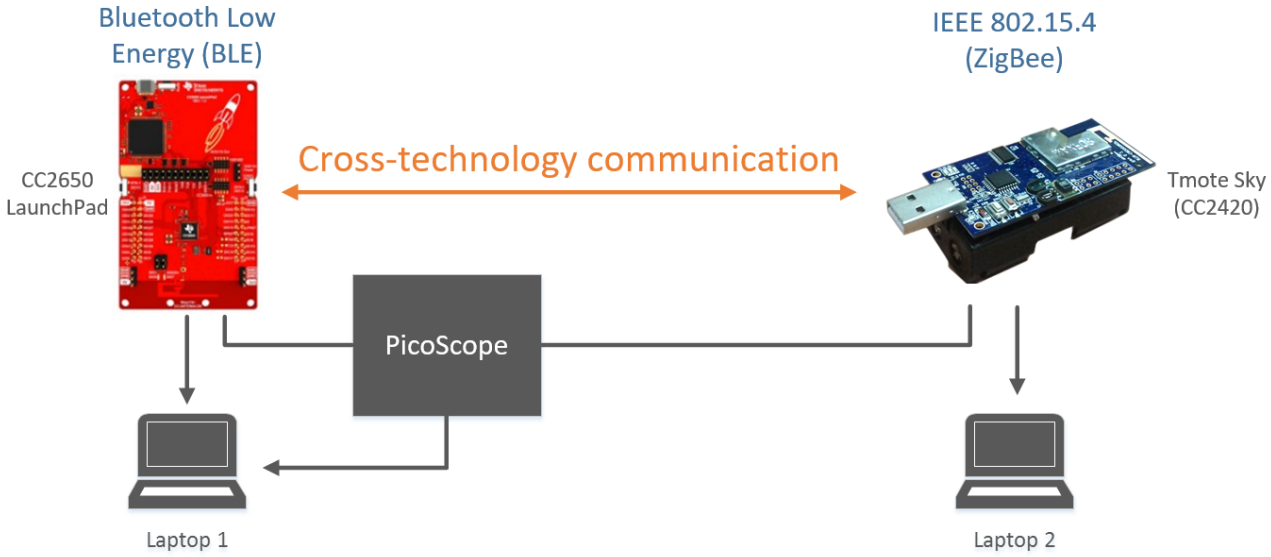

Figure 7. Setup of the CTC Demonstrator.

3.2.3.1 Link to technology lines

The CTC component is related to BB24.F (cross-technology communication), as it allows wireless devices using heterogeneous technologies (e.g., IEEE 802.15.4 and BLE) to exchange data in both directions.

In the next iterations, the CTC component will be used to (i) coordinate the used frequency channels among heterogeneous wireless devices in order to maximize coexistence, and to (ii) synchronize the clocks of heterogeneous wireless devices at a microseconds-scale.

3.2.3.2 Demonstrator public output

Video demonstrating the communication between the CC2650 Launchpad as BLE device and an Advanticsys MTM5000-MSP sensor node (IEEE 802.15.4 device).

3.2.4 Demonstrator OOB Communication – LCM

OOB security enhances the overall security of a communication system by adding a special communication channel with certain properties. These properties typically include a short and well-known communication range and different physical layer than the main communication channel. The additional channel is used to exchange secret information for example a cryptographic key. This enables an encrypted communication over the public accessible network without the possibility of a man-in-the-middle attack. Figure 8 shows an overview of the OOB communication demonstrator.

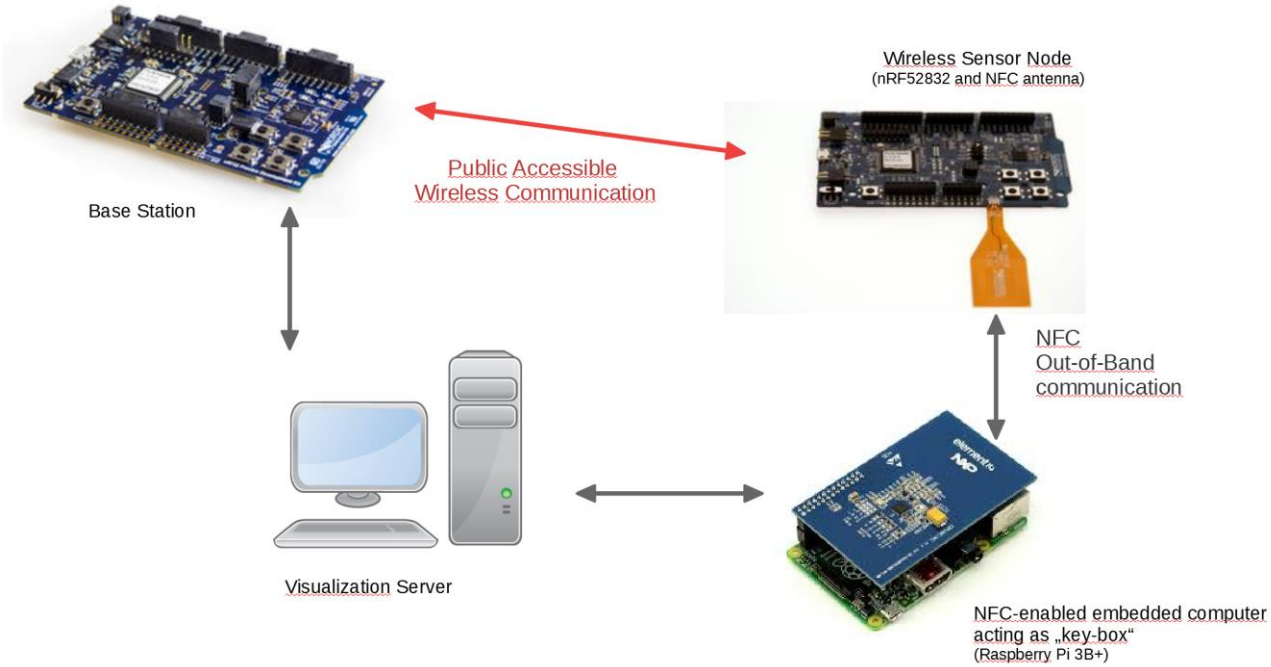

Figure 8. Out-of-Band Communication Demonstrator Overview

We will show the secure communication between a NFC-enabled embedded computer and a wireless sensor node with a NFC antenna. This communication will be integrated into an existing sensor network. The purpose of the OOB communication is to securely read the node ID of the sensor node and add it to the network. Thus, only specifically selected node can be added to the network. This procedure will be visualized using textual output on a PC and using the internal LEDs of the sensor node. Energy efficiency is very important to operate the wireless sensor nodes as long as possible. Thus, we will demonstrate the energy efficiency of the used OOB communication by measuring the power consumption of the sensor node during the communication activity.

Future Work will target the exchange of cryptographic keys between the sensor network controller and the sensor nodes and integrate the security concepts into the industrial use case.

3.2.4.1 Link to technology lines

The demonstrated OOB communication setup is related to BB23.F (OOB communication) and will be integrated in WP12 and in different setup in WP09.

3.2.4.2 Demonstrator public output

Video demonstrating the joining of a new sensor node to the sensor network.

3.2.5 Demonstrator Energy Efficient Secure Communications – JKU

Based on the WSN prototype for automotive verification and validation from the predecessor project DEWI, this demonstrator aims for providing security mechanisms for efficient, dependable and energy autonomous WSN systems for local instrumentation of UUT's. In the final version, the demonstrator should at least include the possibility for authentication and data encryption. The goal is to implement hardware encryption for all communication tasks between the nodes and the base station in a way that the tight energy budget, resulting from the requirement for powering the nodes only from solar panels, is kept. The selection of the encryption mechanism is statically implemented. Data are sent from the nodes to the base station in an encrypted form. The base station is decrypting all data and is sending the resulting data stream to the console or to the automation system e.g. PUMA of AVL.

Following security measures are evaluated or presented:

- Retransmission Rate: The retransmission rate indicates the quality of the connection and the validity of the end to end encryption.
- Synchronicity: Monitoring of the synchronisation allows to derive a security relevant parameter and pass it to the automation system.

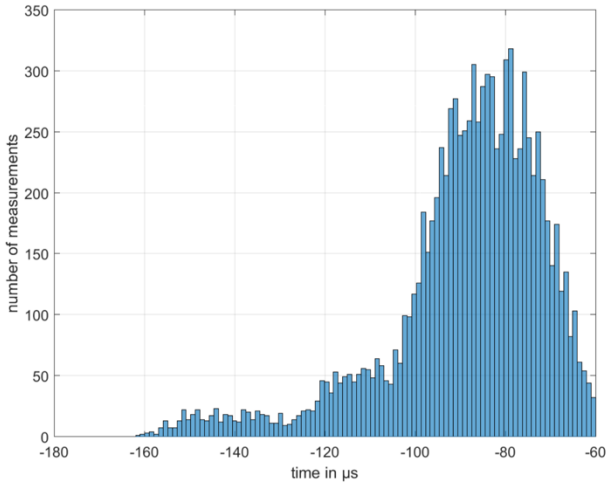

Figure 9. Typical timing measurements for evaluating synchronization in case the communication link is not disturbed

- Encryption:
    - Node to base station encryption for administrative monitoring and protocol specific communication
    - End to end encryption between node and PLC or automation system.

Encryption has to be applied to secure the communication between the nodes and the base station. The nodes and the base station exchange parameters relevant for the communication such as channel timing, which should be kept secret to increase the security level (represented by the grey arrows in Figure 10). End to end security has to be guaranteed to protect the measurement data sent to the PLC from being eavesdropped, altered or disturbed. The base station can be a transparent hop for the data or data have to be repacked in a newly secured communication line to the automation system (represented by the grey arrows in Figure 10).

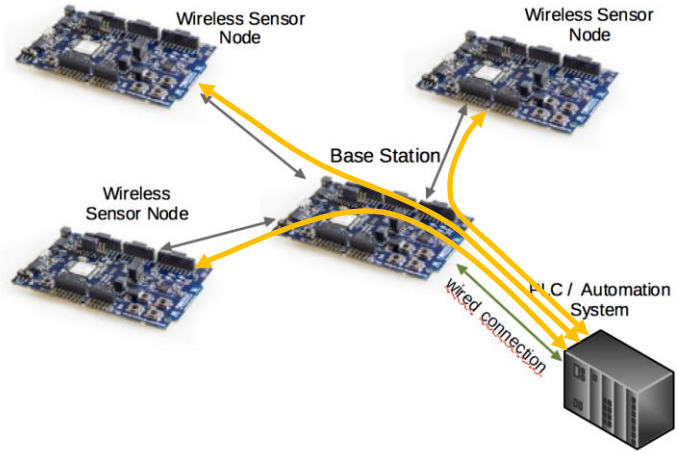

Figure 10. Secure communication links between nodes and base station and automation system

3.2.5.1 Link to technology lines

The Energy Efficient Secure Communications demonstrator is based on BB 25.A: Energy efficient security implementation in WSNs.

3.2.5.2 Demonstrator public output

Video demonstrating security parameter measurement including packet transmission from node to base station and automation system.

3.2.6 Demonstrator Security Threat Analysis - SBA

For the demonstrator, SBA's contribution is twofold:

First, we provide a threat model of the EPHESOS protocol that has been developed in cooperation with JKU and LCM. The model covers both modes of the EPHESOS protocol (EPHESOS-C and EPHESOS-S) as well as all six phases, namely (1) pairing, (2) storage, (3) rigging, (4) idling, (5) measuring and (6) unmounting. The model has been developed according to the STRIDE methodology, a threat classification model initially developed by Microsoft that is used in computer science. It groups threats into the following six groups of threats:

1. Spoofing identity
2. Tampering with datator
3. Repudiation
4. Information disclosure
5. Denial-of-service
6. Elevation of privilege

Following this methodology, we found 24 threats encompassing among others jamming and tampering of sensors eventually resulting in denial-of-service attacks and data tampering. In the course of this work package, the EPHESOS protocol should be enhanced to withstand the threats identified this way.

Second, we will verify the current level of implementation of the EPHESOS protocol against the previously described threat model. This will result in a report on the current level of security of the EPHESOS protocol. It will especially emphasize the threats that have already been tackled by the implementation, and futher identify these that require additional security mechanisms for adequate protection.

Both parts of the demonstrator will be provided in the form of a report.

3.2.6.1 Link to technology lines

The demonstrator is related to BB26.D (Infrastructure Design and Security Threat Analysis) and will be integrated in WP12.

3.2.6.2 Demonstrator public output

As our demonstrator is neither stand-alone nor tangible, we do not see any option for public output in the form of a video or similar.

4 DISSEMINATION, EXPLOITATION AND STANDARDISATION

The Y1 demonstrator of WP12 consists of sub-demonstrators described above in the section 3 which will be used to create a public video illustrating the operation of each sub-demonstrator. This video will be then uploaded to a video-sharing website (such as e.g. YouTube) for a dissemination purpose.

Dissemination, exploitation and standardisation actions carried out within WP12 was described in detail in SCOTT D12.1 [1].

5 LINK TO TECHNOLOGY LINES

This part of the deliverable describes how the UC work described in this deliverable is linked to the Technology Lines and their Technical Building Blocks (TBB).

TBB \ Demonstrator relation	SOAK_AVL	MPS_GUT	SEC JKU	CTC_TUG	SBA
BB23.F_LCM					
BB23.P_GUT		X[1]			
BB25.A_JKU			X[1]		
BB25.B_NXP-NL					
BB26.A_INDRA					
BB23.G_JKU	X[2]	X[2]	X[2]		
BB24.B_VIF	X[2]				
BB24.F_AVL				X[1]	X[1]
BB25.B_NXP-NL	X[2]				
BB25.C_ACCIONA					
BB25.E_ACCIONA					
BB26.D_ISEP					
BB23.C_VIF					
BB23.K_MGEP					
BB23.L_TECNALIA					
BB23.N_VIF					
BB23.O_NOKIA					
BB23.R_VIF					
BB24.K_VIF					
BB25.F_LCM	X[2]				

Table 6. Technology lines link.

[11] Presented in the Y1 demonstrator

[2] It will be presented in the next iteration of the demonstrator

6 CONCLUSIONS

This document presented demonstrators prepared for SCOTT Y1 review. Each partner proposed an own demonstrator. In the next iteration of the demonstrator, actions will be undertaken to partially integrate the partner's work.

The scope of requirements covered by each demonstrator in WP12 was explained and the link to technological building blocks was provided. As a public output for dissemination purposes, a public video will be prepared and released.

In the first year of the SCOTT project, all partners involved in WP12 started their work within this work package. The partners focused not only on gathering requirements and determining architecture but also on the development of simple prototypes. Some of the prototypes will be shown in the first review meeting (09.2018).

AVL will provide information about SOAK and possibilities of applying WSN network in automotive testing with proposed architecture and protocols.

GUT will present a developed camera with embedded vision processing algorithm for detecting blinking LEDs on WSN nodes.

TUG will demonstrate communication between BLE and 802.15.4 device.

LCM will show the secure wireless communication through NFC used to join a new sensor node to the WSN in protected way.

JKU will present security parameter measurement of the energy efficient secure communication in WSN.

SBA will provide a report about threat model in WSN and EPHESOS protocol in cooperation with LCM and JKU.

Further work is already defined and will be presented in the second iteration of the demonstrator.

7 REFERENCES

[1] SCOTT Deliverable D12.1 “Use Case Specification – Ubiquitous Testing of Automotive Systems”, v1.0, 2017-12-21

[2] Horiba Mira (2017). *HORIBA MIRA Opens £8m Advanced Emissions Test Centre*. Figure 1. Recovered from https://www.prnewswire.com/news-releases/horiba-mira-opens-8m-advanced-emissions-test-centre-632608583.html

[3] Weisstechnik (2018). *Soak Room*. Figure 2. Recovered from http://weiss-uk.com/products/automotive-testing/soak-rooms

[4] SCOTT Deliverable D23.1 “Dependable communication and safety building blocks – Iteration 1”, v1.0, 2018-05-08

A. ABBREVIATIONS AND DEFINITIONS

Term	Definition
BLE	Bluetooth Low Energy
CSI	Camera Serial Interface
CTC	Cross-technology communication
IoT	Internet of Things
MPS	Multimodal Positioning System
NFC	Near Field Communication
OOB	Out-of-band
SOAK	Vehicle Conditioning
TBB	Technical Building Block
UC	Use Case
UUT	Unit under test
WSN	Wireless Sensor Network