Industrial IoT Security Concept with Extended ISO/IEC/IEEE 21450 TEDS

Tobias Mitterer[1], Leander B. Hörmann[2], Hans-Peter Bernhard[3], Peter Priller[4] and Hubert Zangl[1]
[1]Institute for Smart Systems Technologies, Universität Klagenfurt, Austria, {tobias.mitterer, hubert.zangl}@aau.at
[2]Sensors and Communication, Linz Center of Mechatronics GmbH, Linz, Austria, leander.hoermann@lcm.at
[3]Silicon Austria Labs GmbH and Institute for Communications and RF-Systems,
Johannes Kepler University, Linz, Austria, h.p.bernhard@ieee.org
[4]AVL List GmbH, Graz, Austria, peter.priller@avl.com

***Abstract*—Electronic data-sheets that are stored within and provided by a transducer such as ISO/IEC/IEEE 21450 Transducer Electronic Data-sheets are currently intended to ease the utilization of transducers. This is achieved as the data-sheets provide information about sensing and actuation as well as communication capabilities, data formats, calibration information and more. However, so far it can not be ensured that the provided information is trustworthy. Consequently, we propose a concept based on ISO/IEC/IEEE 21450 Transducer Electronic Data-sheets in which signatures and secure elements are used to validate the information in the data-sheets, the manufacturer and calibration labs. Furthermore, this information can be utilised for secure key exchange mechanisms and permission management. This approach ensures that the low-power consumption expected of transducers is still met while providing security and trust.**

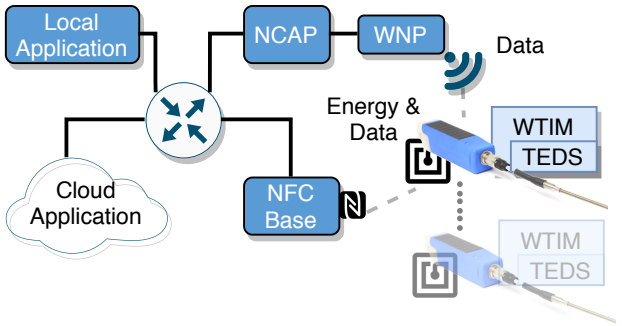

Fig. 1: Network setup.

I. Introduction

Current trends in data acquisition point in a direction where many small autarkic, i.e., self-sustained sensor platforms are positioned and connected via low-power wireless or other networks. In such applications, the connections are frequently not secured and can thus easily be eavesdropped or manipulated or the process to ensure security is rather complex and prohibitive. For many situations e.g., in industrial networks, security is of utmost importance to circumvent industrial espionage or tampering. Nonetheless, many current industrial Wireless Sensor Networks (WSNs) still lack security.

Electronic data-sheets can be used for fast integration and recognition of sensor nodes in a system. One such electronic data-sheet format is provided by the ISO/IEC/IEEE 21450 Transducer Electronic Data Sheet (TEDS) standard [1]. TEDS are electronic data-sheets, which can be stored in machine-readable form on the flash or Electrically Erasable Programmable Read Only Memory (EEPROM) medium of intelligent transducers (sensors or actuator nodes). Such transducers offer functionality to write and read TEDS and to access their sensor or actuator channels. TEDS comprise meta information about the transducer, like the number of sensors and actuators as well as channel information about every sensor and actuator channel, like the adopted data encoding schema. Additionally, calibration information, information about the physical properties of the transducer and other information is provided in a TEDS.

Security aspects for WSNs have been subject of extensive research. An example approach for security in industrial WSNs can be seen in [2], where a protocol called FlexiCast is used to check the integrity of the software on sensor nodes. Another approach for security in WSNs has been proposed by [3], where a random key management system is developed. An overview of the potential security risks in industrial WSNs is shown in [4]. An approach to include security information in the TEDS standard is discussed in [5], where a Management Information Base (MiB) is used in conjunction with TEDS.

In this paper a concept is proposed to include security aspects in the TEDS that allows for distributed utilization and does not require a central database or an Internet connection. As an extension of a previous work described in [6], additional roles in the life cycle of a device are considered. The concept results in a workflow starting from the production of a node until its end of life. While the approach is not restricted to such devices, a focus is on nodes that are autarkic low-power wireless nodes that also support Near Field Communication (NFC) for data transmission.

II. Workflow and Roles

The sensor network depicted in Figure 1 shows a setting with wireless sensor nodes utilizing an ISO/IEC/IEEE 21450 implementation. According to the smart transducers standards family IEEE-1451, the Network Capable Application Processor (NCAP) is connecting the sensor nodes to the user network e.g., LAN or WLAN. The wireless connection to communi-

cate with the sensor nodes is based on Energy and Power Efficient SynchrOnous Sensor network (EPHESOS) [7] which allows autarkical environmentally-powered sensor nodes [8]. Additionally, an alternative wireless communication path via a NFC exists to connect to a NFC base station. Therefore, it is possible to support two wireless communication channels for, as an example, two factor authentication. Moreover, the base station can provide energy to the node by Wireless Charging (WLC) in addition to the pure communication task. The WLC supports higher power consumption for the initial node and security setup or to recharge the backup battery of environmentally-powered sensors. The TEDS is stored on the Wireless Transducer Interface Module (WTIM). Additionally, the communication path to the Cloud and local application allows to align the digital twin with the real world sensor attached to a specific NCAP.

III. TEDS Security Extension

To support the need of Industry 4.0 (I4.0) security requirements, we propose an extension of the ISO/IEC/IEEE 21450 TEDS standard (Table I). The fields 1 to 4 in this extension are standard which can be combined with manufacturer-specific fields.

TABLE I: Proposed IEEE 21450 Security TEDS Extension.

Id	Field	Description	Type
1	UsedEncAlg	Enc. Algorithm	UInt8
2	UsedHashAlg	Hashing Algorithm	UInt8
3	CA	Certificate Authority	String
4	LastModified	Last Modified	TimeInstance
100	Signature	Signature	String
101	NodePublicKey	Node Pub Key	String
102	SigNodePublicKey	Signature Node	String
103	ManufPublicKey	Manuf. Pub Key	String
104	SigManufPublicKey	Signature Manuf.	String
105	CalibrationPublicKey	Calib. Pub Key	String
106	CAPublicKey	CA Pub Key	String
107-255	reserved	reserved	-

In detail, Field 1 determines the used encryption algorithm for the signature exchange, cf. I. Field 2 determines the hashing algorithm used by the encryption algorithm. Field 3 is defined as a string which denotes the name and possibly the Domain Name Service (DNS) of the root of trust in the network. Field 4 denotes the date at which the security TEDS has been updated last. The extension in Table I shows the standard and manufacturer-specific fields as used in this specific workflow. The manufacturer-specific fields, as described in Section II, range from 100 to 106. Field 100 is the certificate computed over the whole TEDS. Field 101 is the public key of the node itself. Field 102 is the signature of the public key of the node created by the manufacturer. Field 103 is the public key of the manufacturer and Field 104 is the signature of the manufacturer public key done by the root of trust. Field 105 is the public key of the trusted calibration lab and Field 106 is the public key of the root of trust.

The proposed security extension is an optional TEDS, as not all transducer nodes are expected to have a security concept implemented. An overview of the security TEDS as implemented can be seen in Figure 2.

```
<security>
    <LastModified>28.01.2020:10:00:00</LastModified>
    <Signature>placeholder</Signature>
    <UsedEncAlg>0</UsedEncAlg>
    <UsedHashAlg>0</UsedHashAlg>
    <CA>testserverca.local</CA>
    <NodePublicKey>placeholder</NodePublicKey>
    <ManufPublicKey>placeholder</ManufPublicKey>
    <CalibrationPublicKey>placeholder</CalibrationPublicKey>
    <SigNodePublicKey>placeholder</SigNodePublicKey>
    <CAPublicKey>placeholder</CAPublicKey>
    <SigManufPublicKey>placeholder</SigManufPublicKey>
</security>
```

Fig. 2: Template of security TEDS in Extensible Markup Language (XML) form.

Tables II and III include security algorithms commonly used for encryption and hashing. As not all viable algorithms are included, they can be added to the reserved fields in the future. The security domain in Industrial Internet of Things (IIoT) is rapidly developing and we encounter this by reserved for future expansion fields in the TEDS.

TABLE II: Options for field ”used encryption algorithm” as proposed in [6].

Id	Field	Description
0	RSA	Rivest, Shamir and Adleman
1	DSA	Digital Signature Algorithm
2	ECDSA	Elliptic Curve Digital Signature
3	ElGamal	ElGamal Signature Scheme
4–128	Reserved	
129–255	Manufacturer reserved	

TABLE III: Options for field ”used hashing algorithm” as proposed in [6].

Id	Field	Description
0	MD5	Message Digest Algorithm 5
1	SHA-256	Secure Hash Algorithm 2-256
2	SHA-512	Secure Hash Algorithm 2-512
3–128	Reserved	
129–255	Manufacturer reserved	

The signatures and keys within the TEDS template have a default string value of ’placeholder’. The placeholders are substituted by the keys and signatures according to the step-by-step signing process. In the initial boot-up of the transducer node, only the public key of the transducer node, ’intpk’, and the public key of the root of trust, ’CAPublicKey’, is filled. The placeholder values get replaced during the set-up of the node. During the configuration step, when the first NCAP system retrieves the initial security information and writes the complete TEDS into the transducer node, the remaining fields are filled with the corresponding keys and signatures, cf. Section IV.

IV. Roll out of TEDS Security to sensor nodes

Figure 3 shows an overview of a typical workflow for sensor nodes, cf. [9], from their production, during its productive use

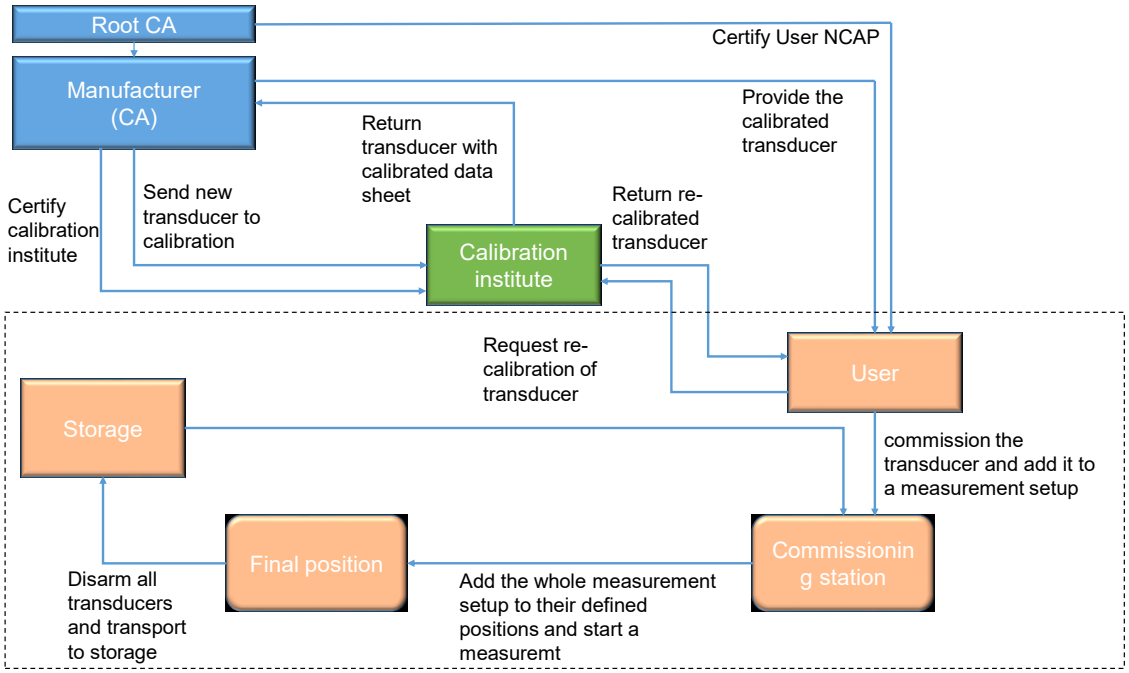

Fig. 3: Flowgraph depicting the lifecycle of a fresh sensor node coming from production, being used in a measurement task and finally being put into storage.

in a measurement setup and the return into a storage. In this workflow, a manufacturer may serve as Certification Authority (CA) providing the root of trust, or another party acts as CA that confirms trustworthiness of the manufacturer. All devices include Secure Elements (SEs), which are hardware components that are capable to generate and securely store key pairs and to validate signatures that are generated using the public part of the key pair, while the private key never leaves the secure element. By including this public key into the TEDS and signing the TEDS, the manufacturer confirms that the specific device containing this specific hardware secure element is genuine.

During the design of the sensor node, a TEDS is adapted and assigned to the node. When the sensor node is manufactured, it first needs a boot-loader, then a firmware and after that the finished sensor node needs to be configured, calibrated and supplied with a TEDS before being delivered or stored in a storage facility. The setup for the configuration step is visualized in Figure 6. First, the boot-loader is flashed on the node to securely install the firmware, which is shown in Figure 4. After the new node is started, it connects via NCAP to a manufacturer base station, which could also be called Secure Production Computer (SecProdPc). Then, the SecProdPc retrieves a Manufacturer Key Pair (MKPair) key pair for its secure production environment from the Manufacturer Hardware Secure Module (ManufacturerHSM). This key pair is then signed by the root of trust (RootCA) and the Root of Trust Public Key (RTKPublic) is retrieved. With this preparation the SecProdPc then retrieves the sensor node hardware identifier from the sensor node to further personalize the boot-loader. After the boot-loader is compiled with the retrieved information, it is flashed onto the sensor node and the RTKPublic is also stored on the sensor node. The secure boot-loader verifies that only trusted firmware and firmware updates are being flashed onto the node. After the secure boot-loader is flashed onto the node, the firmware has to be installed on the node. The process of creating firmware where the security and other aspects are tailored to the specific node is conceptually shown in Figure 5. In this process, the firmware itself is receiving a signature from the manufacturer before compiling. The signature is needed for the secure boot-loader to verify if the firmware is trusted and can be flashed onto the node.

Executing the new firmware the sensor node is going through its first boot-up, it communicates with the on-board Secure Element (SE) and creates a key pair which is stored in the SE. The public key of this key pair is retrieved from the SE and is used to create an initial security TEDS. The SecProdPc then retrieves the initial security TEDS. Then the RTKPublic is added to the security TEDS. The manufacturer retrieves the TEDS which has been created for the node and adds the security TEDS. This TEDS is then signed by the manufacturer and the signature is added to the security TEDS section. The updated TEDS is then written to the node. On the node, the TEDS is verified via the signatures in the security TEDS with the RTKPublic which was copied to the node during the flashing of the secure boot-loader.

The configured node is moved to a trusted calibration lab, which is either directly certified by the root of trust or by a sub CA, which can also be the manufacturer. The calibration

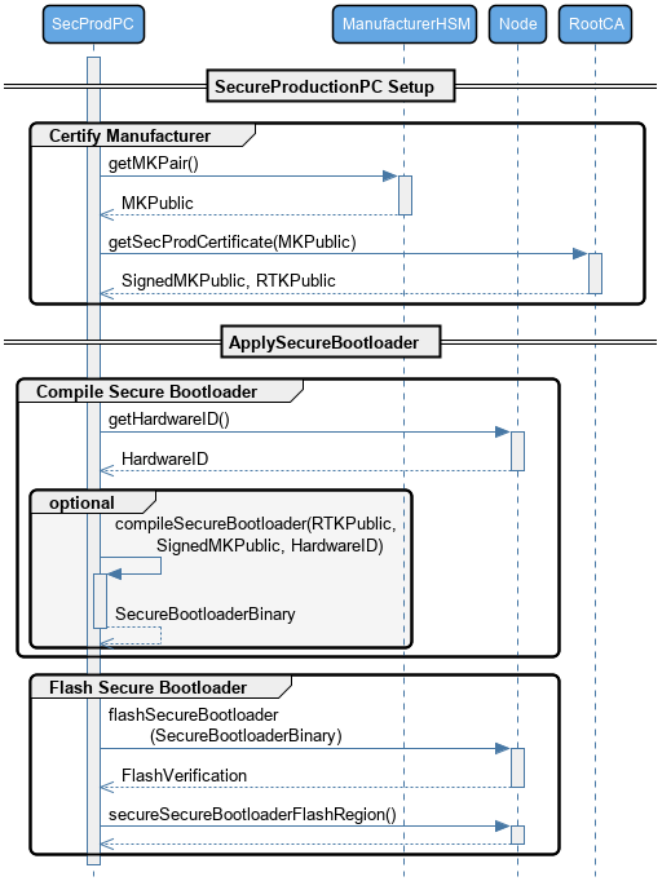

Fig. 4: Sequence diagram of compiling and flashing the secure boot-loader.

lab operates a NCAP system which has its own key pair. This public key has been signed by the root of trust. The calibration lab then retrieves the channel TEDS stored on the node and creates calibration data for the sensor channels on the node. Then a calibration TEDS is created by the lab and signed with the calibration lab's key. The calibration TEDS, its signature, the calibration labs public key and its signature are then written back to the node. After the node receives the calibration TEDS, it first ensures that it came indeed from a trusted calibration lab by testing the calibration lab's public key signature with the RTKPublic. Then the calibration TEDS signature is checked with the calibration lab public key. After trust is ensured between the node, the calibration lab, and the received calibration TEDS, the calibration TEDS is added to the on-board TEDS of the node. The calibrated node is then returned to the manufacturer. The calibration setup is shown in Figure 7.

The end user tests the functionality of the calibrated node by commissioning it and adding it to a measurement setup. The commissioning of nodes has to be done to link the transducers to the base station and finalize the security measures to be taken during measurements. The commissioning of the node is done by connecting the node to a commissioning NCAP via NFC. The commissioning NCAP itself has also been certified by the root of trust and owns a signed key pair.

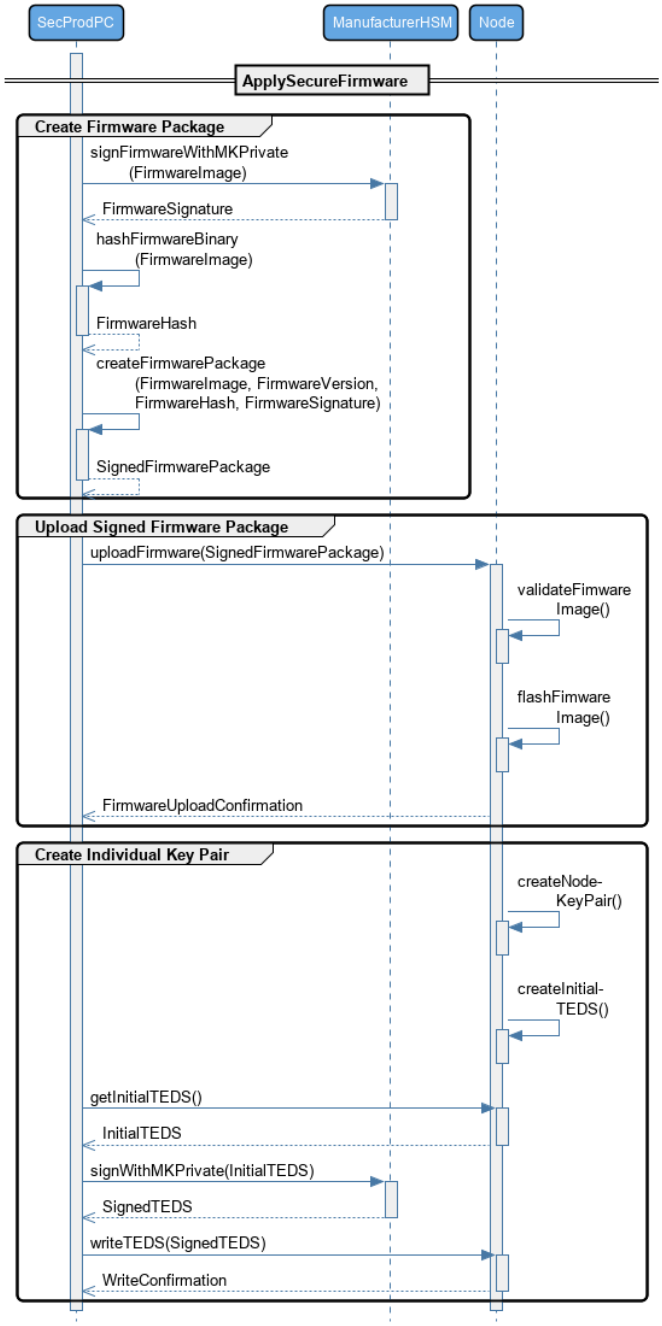

Fig. 5: Sequence diagram showing the process of adapting Firmware to node and flashing the Firmware using a secure process.

The node is then added to a measurement group identified by its Universally Unique Identifier (UUID). The UUID is retrieved via the NFC connection. With a combination of the key pair of the commissioning NCAP and a signature done by the root of trust, a verification request is sent to the node. If the node verifies that the commissioning NCAP is trustworthy, it replies with its TEDS, which contains a signature by its own key pair which, in turn, is verified by the root of trust. The commissioning NCAP verifies the TEDS of the node and the node itself with the received information. Thus, a

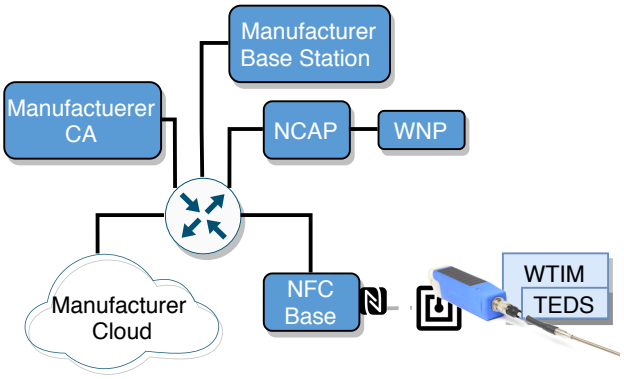

Fig. 6: Overview of the setup for the node configuration after the finished sensor product leaves the production line.

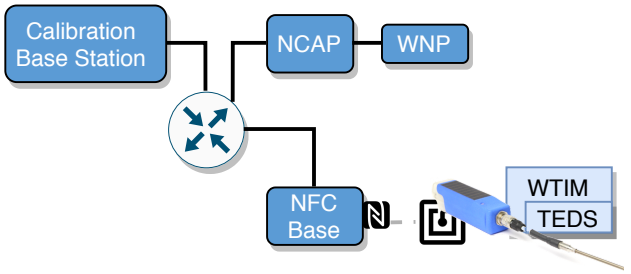

Fig. 7: Overview of the setup for the node calibration after the node is sent to a trusted calibration lab.

mutual trust between commissioning NCAP and sensor node is established. By using the exchanged key information of both parties, a symmetric key can be calculated by using for example the Elliptic Curve Diffie Hellman (ECDH) approach. This symmetric key is then stored in a list of keys at the commissioning NCAP. If needed at this step, an updated firmware can also be flashed onto the node using the NFC interface, where the new firmware is checked for validity by the secure boot-loader on the node. The verification process and optional firmware updating process via NFC is shown in Figure 8.

The measurement list, the symmetric key list for the node and optionally the TEDS of each node is transferred to the measurement NCAP. Then, the node is moved to its position in the measurement setup. As the node is no longer in the vicinity of the NFC gateway, it connects to a NCAP using a Wireless Network Processor (WNP) which controls the wireless interface. The measurement NCAP also receives the measurement list and the list containing the keys for each node, which are used for the uplink of measurement data retrieved from the nodes. To ensure secure communication via the wireless interface, the WNP connected to the measurement NCAP creates a beacon session key which is used as a shared secret between the WNP and all connected and assigned sensor nodes. This ensures, that only trusted sensor nodes receive the commands from the WNP and that the received commands can be trusted. Additionally, it is ensured that broadcast commands can only be read by trusted nodes. The reason why a different symmetric uplink key for each sensor is used, is that when

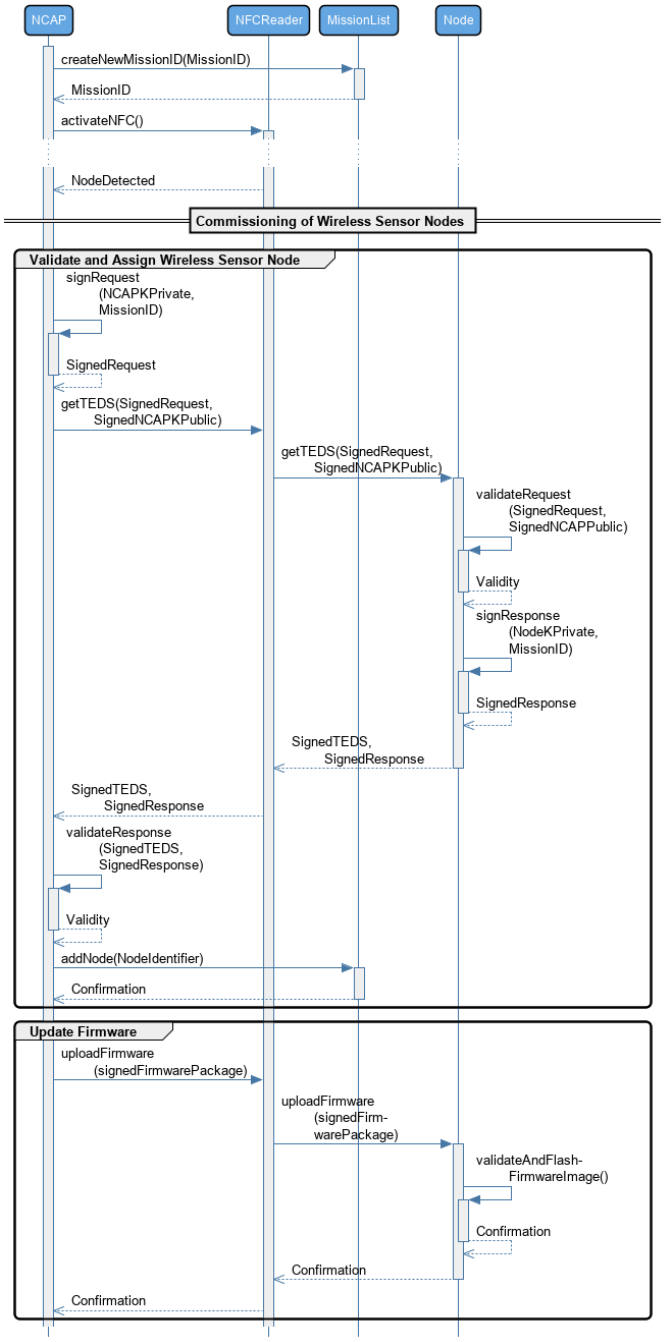

Fig. 8: Overview of the verification and optional firmware update process during commissioning of the nodes.

one key is no longer secure, the other nodes are not affected.

If this setup with all nodes is positioned and connected, the NCAP checks their availability and retrieves their TEDS if not already cached on the NCAP. Then the NCAP changes the transmission mode of the connected nodes to a measurement mode, in which they stream their data encrypted with their corresponding Advanced Encryption Standard (AES) key, to the NCAP. To ensure a continued trust of the received sensor data over time, a hash value is computed by the nodes over their sensor data. After a given time, the hashes get signed

by the node and sent to the NCAP, which then verifies the signatures. The measurement setup is shown in Figure 9.

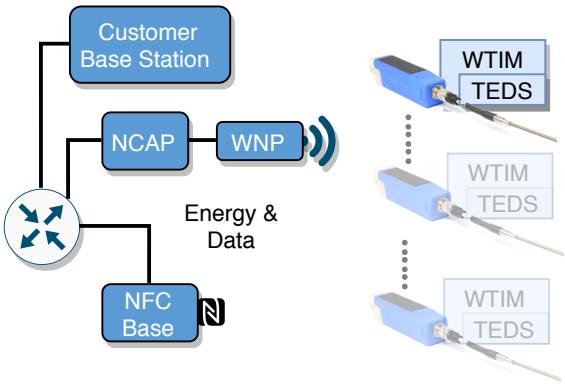

Fig. 9: Overview of an established measurement setup for new nodes.

V. Simulation

The workflow described in Section III-IV has been implemented as a simulation, i.e., the simulated nodes are used together with a real NCAP, which connects to a simulated node via a simulated wireless connections. This was done as a first test to study the applicability of the workflow as proposed and it was done in a way, that the simulated parts can be easily exchanged by the real counterparts once the hardware becomes available. An overview over the simulated environment is given in Figure 10. A video displaying the testing of the workflow in the simulation is also available at [10].

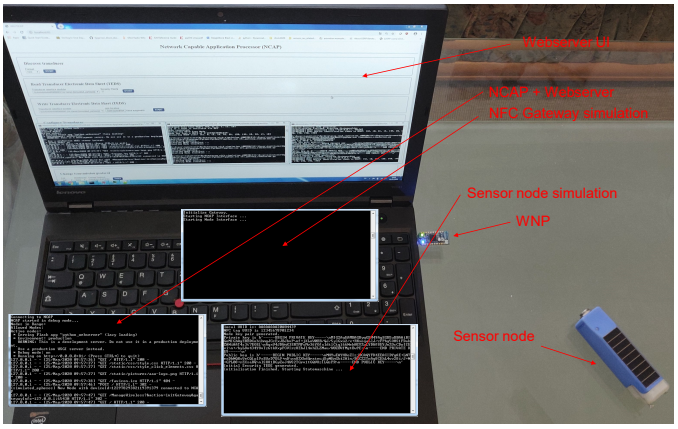

Fig. 10: Measurement setup of the simulation.

VI. Conclusion

In this paper, an extension for the ISO/IEC/IEEE 21450 TEDS standard for security purposes is proposed. By adding a signature to the TEDS by the manufacturer and calibration labs, the information provided by the TEDS is secured against manipulation. In addition, the TEDS also includes a public key that is uniquely paired to a secure element within the sensor node. Consequently, it is not possible to transfer the TEDS to another node because the coupling of TEDS and the device can be validated. Furthermore, the approach can also be used to exchange symmetric keys for power-efficient encrypted communication during the measurement process. The workflow has been studied and validated within a simulation environment and corresponding hardware implementations are currently ongoing.

Acknowledgement

The project was partially funded by the Carinthian Economic Promotion Fund (KWF), the Government of Styria (Section 8 Health, Healthcare and Science) and the Styrian Business Promotion Agency (SFG) within the 2017 Call Silicon!Alps–the call for R&D projects in the field of microelectronics in Carinthia and Styria and has been supported in part by the COMET-K2 Center of the Linz Center of Mechatronics (LCM) funded by the Austrian federal government and the federal state of Upper Austria and the InSecTT project. InSecTT has received funding from the Electronic Component Systems for European Leadership Joint Undertaking under grant agreement No 876038. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme and Austria, Spain, Finland, France, Ireland, Sweden, Germany, Italy, Poland, Portugal, Netherlands, Belgium, Norway.

References

[1] "ISO/IEC/IEEE information technology – smart transducer interface for sensors and actuators – common functions, communication protocols, and transducer electronic data sheet (TEDS) formats," *ISO/IEC/IEEE 21450:2010(E)*, pp. 1–350, May 2010.

[2] J. Lee, L. Kim, and T. Kwon, "Flexicast: Energy-efficient software integrity checks to build secure industrial wireless active sensor networks," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 1, pp. 6–14, Feb 2016.

[3] L. Zhu and Z. Zhan, "A random key management scheme for heterogeneous wireless sensor network," in *2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC)*, Aug 2015, pp. 1–5.

[4] L. Liang, Y. Liu, Y. Yao, T. Yang, Y. Hu, and C. Ling, "Security challenges and risk evaluation framework for industrial wireless sensor networks," in *2017 4th International Conference on Control, Decision and Information Technologies (CoDIT)*, April 2017, pp. 0904–0907.

[5] X. Feng, J. Wu, J. Li, and S. Wang, "Efficient secure access to ieee 21451 based wireless iiot using optimized teds and mib," in *IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society*, Oct 2018, pp. 5221–5227.

[6] T. Mitterer, H. Gietler, L.-M. Faller, and H. Zangl, "Artificial landmarks for trusted localization of autonomous vehicles based on magnetic sensors," *Sensors*, vol. 19, no. 4, 2019. [Online]. Available: https://www.mdpi.com/1424-8220/19/4/813

[7] H.-P. Bernhard, A. Springer, A. Berger, and P. Priller, "Life cycle of wireless sensor nodes in industrial environments," in *13th IEEE Int. Workshop Factory Commun. Sys.*, Trondheim, Norway, May 2017.

[8] A. Berger, T. Hölzl, L. B. Hörmann, H.-P. Bernhard, A. Springer, and P. Priller, "An environmentally powered wireless sensor node for high precision temperature measurements," in *2017 IEEE Sensors Applications Symposium (SAS)*, March 2017, pp. 1–6.

[9] L. Hörmann, C. Kastl, H. P. Bernhard, P. Priller, and A. Springer, "Lifetime security concept for industrial wireless sensor networks," in *16th IEEE International Conference on Factory Communication Systems (WFCS 2020)*, Portugal, Porto, 4 2020, PAPREFCONF, pp. 1–8.

[10] "Video showing implemented simulation of workflow," https://seafile.aau.at/f/9055e154eda144cd9047/, accessed: 2020-05-26.