LoRaWAN with HSM as a Security Improvement for Agriculture Applications - Evaluation

Reinhard Kloibhofer[1], Erwin Kristen[1], Afshin Ameri E.[2]

[1] AIT Austrian Institute of Technology GmbH, Giefinggasse 4, 1210 Vienna, Austria
reinhard.kloibhofer@ait.ac.at, erwin.kristen@ait.ac.at
[2] MDH Mälardalen University, Högskoleplan 1, 722 20 Västerås, Sweden
afshin.ameri@mdh.se

Abstract.

The future of agriculture is digital and the move towards it has already started. Comparable to modern industrial automation control systems (IACS), today's smart agriculture makes use of smart sensors, sensor networks, intelligent field devices, cloud-based data storage, and intelligent decision-making systems. These agriculture automation control systems (AACS) require equivalent, but adapted, security protection measures. Last year, the agriculture-related security theme was addressed in a presentation [1] on DECSoS '20 workshop of the SAFECOMP 2020 conference. In the workshop a simple soil sensor prototype with wireless communication system was presented. The sensor was used to demonstrate the improvements to operational security of field devices through employing cyber security protection techniques. As a continuation of the last year contribution, this paper presents the evaluation of the technologies presented in real-life deployment of AACS. It also describes operational scenarios and experiences with the implementation of security measures for AACS, e.g.: the implementation of a four-layer cyber security architecture, the signalling concept of alarms and notifications in the event of a cyber-attack, the assessment of security measures, the costs of security, and an outlook of upcoming future security requirements for wireless IoT devices which are specified by the European Commission through the European Radio Equipment Directive (RED).

Keywords: Agriculture Automation Control Systems (AACS), Hardware Security Module (HSM), Internet of Things (IoT), Cyber-Physical Systems (CPS), Safety & Security, Agriculture, LoRaWAN, European Radio Equipment Directive (RED)

1 Introduction

Digitalization is making a rapid progress in agriculture. Ground vehicles are becoming more and more intelligent with integrated control electronics that support the farmer in doing their daily work in a more precise and simple manner. The vehicles themselves are constantly generating operational and environmental data that can be

used for future maintenance and mission decisions. Some of this data is stored on removable data storage media, which are manually transferred to a data repository after completion of the task. However, often such data are transferred directly through a wireless connection to an online cloud-based data center.

Agricultural companies, such as fertilizer and pesticide suppliers and the machinery manufacturers also benefit from the continuous data collection. In such cases, all production data is recorded during task execution, which enables cooperation with the machinery supplier and/or other agriculture companies for task optimization. This in turn can lead to an increase in product output and quality.

While machinery suppliers exchange data, for example, via DataConnect (used by John Deere, Claas, CNH, New Holland and Steyr), the farmers collaborate on platforms, like 356FarmNet [2] and Agrirouter [3].

Using different deep learning approaches and statistical evaluations, the information gathered can be used to discover connections between various data sets. Such approaches can result in recommendations for process improvements in the agriculture farm. They will help to reduce the use of energy resources, especially the fossil fuels and water and to reduce the emission of environmentally harmful greenhouse gases such as carbon dioxide.

Apart from ground vehicles and machinery, other hardware involved in agriculture (i.e. ground sensors, drones, aircrafts, etc.) can also produce data sets. All together they span a dense data collecting sensor network over the agricultural operation area.

Despite all these new and fascinating digitalization technologies, data security and security of ensuring the trustworthiness of the data must never be forgotten in design and system architecture considerations.

The authors of this paper presented a data security approach in the paper “LoRaWAN with HSM as a Security Improvement for Agriculture Applications” [1] at the SAFECOMP - DECSoS workshop 2020. In this paper, a Long Range Wide Area Network (LoRaWAN) end node, built around a soil sensor, was presented, which was connected to the cloud data repository by a LoRaWAN [4] network. While the LoRaWAN data communication standard already offers a high level of data security measures, the sensor prototype used has been expanded with additional security improvements to provide protection against tampering, theft, misuse and malicious use. In last year’s paper, the focus was on the technology behind the integration of a so-called Hardware Secure Module (HSM). The sensor with this HSM is part of the Security Evaluation Demonstrator (SED). This year, as a continuation, the evaluation of the implemented security features and the lessons learned during the installation will be presented.

This paper is divided into the following parts: a brief overview of the functions of the HSM, which are described in detail in the document mentioned above [1]. A layer structure of the security improvement features is also presented. The next chapter shows the alarm and notification properties. Security improvement features realized on the SED, will be presented in their own sub-chapter with an explanation of the evaluation steps, lesson(s) learned, and experiences gained during the implementation.

The paper is closed by conclusions, where the costs of extended security and the higher power requirements of future field devices are discussed. In the outlook, the expected upcoming European Radio Equipment Directive (RED) [5] will be presented. The RED describes what must be provided by product manufacturers and product integrators in the future for wireless network IoT devices.

2 Security features provided by an HSM

A Hardware Security Module (HSM) is a module with a security controller and a cryptographic processor that can be added to a system to generate, manage, and securely store cryptographic keys. See [1] for more details. For this demonstrator, a HSM from Zymkey [6] is used. It offers the following security and general features:

- Multi Device ID and Authentication.
- Data Integrity, Encryption & Signing.
- Key Security, Generation & Storage.
- Physical Tamper Detection.
- Real Time Clock (RTC).
- Ultra-Low Power Operation.
- Secure Element Hardware Root of Trust.

In combination with further securing methods and system condition supervision mechanisms, the HSM allows a multi-layered active cyber security protection architecture (CSPA). As shown in Fig. 1, the CPSA of the SED implementation consists of four layers.

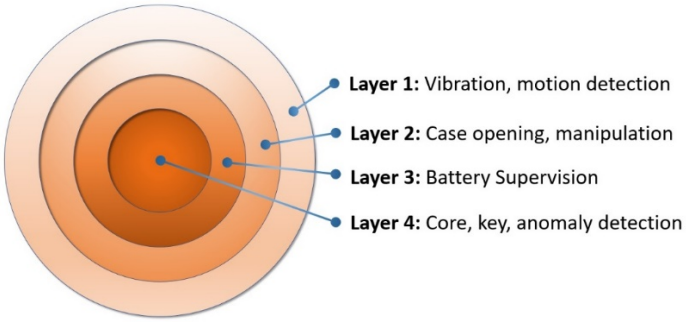

Fig. 1. Four-layer cyber security architecture

Layer 1 defines the outmost protection mechanism. It detects unusual vibrations caused by forcibly removing and tilting the sensor from its location. This event triggers the build-in Global Positioning System (GPS) tracker, which begins to continuously send the current geographical position to the system supervision. Also, the sensor sends an alarm message to the Alarm Processing & Reporter (APR), a functionality in the cloud-based middleware of the system control center. From there the alarm

will be visualised in the main Mission Management Tool (MMT), a graphic screen equipped control center. It informs the operator about the event and notifies them that something irregular is happening to the sensor. Additionally, a Short Message Service (SMS) message is generated and warns a selected person in the field about the situation. The person in the field can get more detailed information on his mobile MMT, which could be a tablet or the information screen in a field vehicle. With this information, the first steps can be taken to prevent theft by quickly intervening. Layer 1 is the first barrier, which can help with theft attempts on field devices. If Layer 1 security measure fails, Layer 2 provides a further break-in barrier. It detects the physical intrusion by an unauthorised person who tries to open the device case. The HSM provides alarm wires which are embedded in the housing material. These wires will be broken if the housing is opened improperly. In such cases, the HSM can, if activated, destroy the device firmware to prevent reverse-engineering of the device firmware software and its reuse.

These first two layers are mechanical security protection measures. The next layer, Layer 3, provides the battery supervision function. This is an immensely important function to ensure correct functioning of the device components with a good energy supply. The battery monitor reports the current battery level and initiates charging or replacement of the battery before the battery power falls below a defined power level.

Finally, Layer 4 provides the core security functions, such as software encryption, and key storage, which cannot be read out or manipulated. The HSM allows, when activated, the destroying of the main security key to prevent code manipulation and reverse engineering of the code. This last layer is the software-related security function and represents the last possibility to prevent device abuse. The onion-like security architecture, by means of a coordinated layer structure, represents the so-called Super Security Solution Protection (S^3P).

3 Event signalisation: Alarms and Notifications

A field device performs in diverse operational modes. These are, for example, the normal, the update and the emergency modes of operation. In the normal mode of operation, the field device both receives commands from a control instance or transmits data to a gateway located nearby, which transfers the data to a data center. In the update mode of operation, the field device enters an operation condition in which, the on-board firmware can be overwritten by a new software version. In the emergency operating mode, the field device enters a self-protecting operating state if an abnormal operating condition or an anomaly in the data communication has been detected. These events trigger the generation of alarm messages that are send to the control center to inform the operator of the condition. Another type of message, which includes the status of the field device, is the notification message. In contrast to the alarm message, this message type can be generated in all three of the operating modes mentioned above. A good example is the low battery message, which informs the operator to charge or replace the battery in the field device.

Alarms are used in the SED to notify the operator of various abnormal operating conditions caused by illegal acts and handling of the field device. The supported security protection measures are described in detail in the next chapter.

When an alarm is triggered, a SMS message is generated to inform a predetermined person about the emergency condition. The SMS is provided by the on-field edge node for a fast and immediate reaction. The alarm message is handled and acknowledged at the operator center. A hand-held device, such as a tablet or mobile phone provides the person on site with more details and the selected countermeasures to fix the alarm situation.

Mission Management Tool (MMT) is the software responsible for receiving and visualizing the alarms and notifications to the operator. MMT also is used to provide visualizations of different sensor readings on the farm. Apart from that, MMT can be used to plan, execute and supervise different missions on the farm involving tractors, drones and other systems. MMT's planning, execution and supervision features have been demonstrated earlier in underwater scenarios [7].

In this work, MMT is run at the command and control center and also on handheld devices. This way, MMT's planning functionalities can be used at the command and control center, while the operators on the field can use it for visualization of required sensor values and receiving alarms and notifications. Sensor alarms and notifications are presented on MMT's panels in two different ways: (1) through the "Alarms" panel which lists all the alarms and notifications received and (2) on the map. In the latter cases, if a sensor reports a notification or raises an alarm, this sensor is marked with red colour on the map and hovering the mouse over the marker shows extra information regarding the received alarm/notification (Fig. 2).

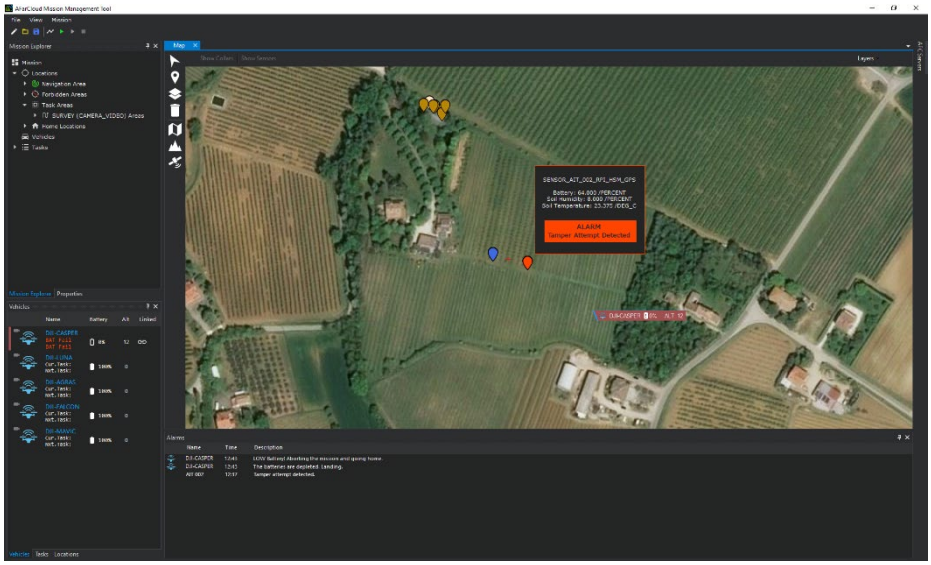

Fig. 2. MMT displaying a tamper attempt alarm on the map and the alarm panel.

4 SED Evaluation of security measures

In last year's DECSoS workshop paper [1], the implemented security mechanism of SED architecture was presented and described. In short, SED consists of the battery-powered sensor, which is located in the field. This sensor is part of the SED and includes the HSM. Components like the data gateway, edge computer, interface to the cloud environment and MMT are part of the SED, as well. In this paper, the successful integration of all SED components, especially the HSM and an advanced battery supervision in the sensor are described. Since the SAFECOMP conference last year, the following evolution of the correct functioning of the security mechanisms were done and shall be documented in this chapter. The following security mechanisms are implemented to improve the protection of IoT devices against cyber security attacks:

- Detection of unauthorised moving of the sensor.
- Ensuring the physical integrity of the sensor.
- Inhibit unauthorised reuse of manipulated sensors.
- Prevent manipulation of the sensor communication data.

These mechanisms are implemented and evaluated because they give a broad coverage of security features from theft to manipulation. Further security features can be added at any time. Each of these cyber security functions is explained using an application example and the personal experiences, learned during the implementation work.

4.1 Detection of unauthorised moving of the sensor

Security application: External manipulation. The sensor is placed in the field, self-powered with a built-in battery, and transfers the measurement sensor data over a wireless LoRaWAN communication link to the LoRaWAN gateway. The gateway collects the data from several LoRaWAN IoT devices and transmits it to a cloud-connected edge computer. A built-in shock sensor detects the theft of the IoT device by a series of strong shock events and sets the IoT node in the emergency mode. In this mode, a GPS receiver is started to determine the current geographical position, which is continuously sent to the gateway. The edge node incorporates a Long Term Evolution (LTE) interface, which sends a SMS alarm to a designated person. Sensor movement is reported in the MMT. The MMT can also run on a mobile device like a tablet or a light version of MMT on a mobile phone for persons working on the field to receives GPS position updates from the sensor through the cloud infrastructure.
Event signalisation: ALARM (theft), pre-information with an emergency SMS, GPS position.
Evaluation steps:

- Place the sensor in the field. The sensor automatically determines the reference position and starts normal operation. This is the initial state.
- The sensor is removed from its place.
- The sensor enters the emergency state.
- The sensor generates an alarm message.
- The edge computer sends a SMS message.

- If the sensor leaves the non-alarm area, the theft is confirmed.
- The GPS receiver starts to continuously transmit the current position.
- The SMS is received by the designated person.
- The movement of the sensor is displayed on the MMT.

Implementation experience: Challenges to setup a GPS module for an application.
To get geographical position data, a GPS module is needed. There are many GPS modules on the market. Standard modules either have a Universal Asynchronous Receiver Transmitter (UART) interface or a provide UART through a Universal Serial Bus (USB) interface. The standard configuration of these modules is to send a data packet each second via a NMEA (National Marine Electronics Association) standard. For using this data, the UART interface can be polled or read out via interrupts. Reading and processing the UART data is time consuming. A better solution in Linux-based systems is to use a so-called GPS demon (GPSD), all data access work is done in the background. Once the GPSD is configured, the GPS position data can be retrieved via a port access and a time out.

However, use of GPS modules can lead to some problems. On the LoRaWAN/GPS module used in our field demonstrator, there is a GPS implementation based on the Mediatek MT3339 [8]. The data can be read from the controller via UART in standard mode. If the GPS antenna is stationary small variations in measured GPS position are expected. This is due to variations in radio wave propagation conditions of the different tracks between GPS satellite and GPS antenna. But data read from the GPS module appears frozen, even if GPS time is changed as expected. The reason for this behaviour is that the module is set up in a so called “tracking mode”. This means that GPS position data is only changed if the measured speed of the module is higher than a certain threshold. For car navigation this mode is helpful because the displayed position seems to be constant for low speed. In the case of sensor tracking, where the position varies with low speed, this function is a problem. This “tracking mode” of the module can be switched off with a command from the microcontroller to the GPS module. For the demonstrator, a USB module with a LEA-6S GPS-chip from the company “u-blox” [9] is used. This module has an active antenna which is very sensitive.

The accuracy of GPS position data varies due to many parameters. These are the most important errors for GPS reception:

- Atmospheric effects: changes in ionosphere and troposphere.
- Timing errors of GPS satellites.
- Multipath effects of the received signal.
- Number of GPS satellites received.
- Dilution of precision due to satellite position.

From a user aspect, buildings and trees surrounding the GPS receiver are important. The receive condition is lower if the receiver is placed in a street canyon and worse if trees are shadowing some GPS satellites. Cloudy weather, fog, rain and snow attenuate the signal and influence the accuracy of the measured position. Moving objects near the receiver such as vehicles driving on the street change the multipath situation and therefore the accuracy. To estimate the practical computed accuracy some measurements were done in different situations. In Fig 3 measurements are

shown in an unfavourable situation (high buildings and trees near the receiver, cloudy weather) and in a good receiving situation (free view, cloudless weather).

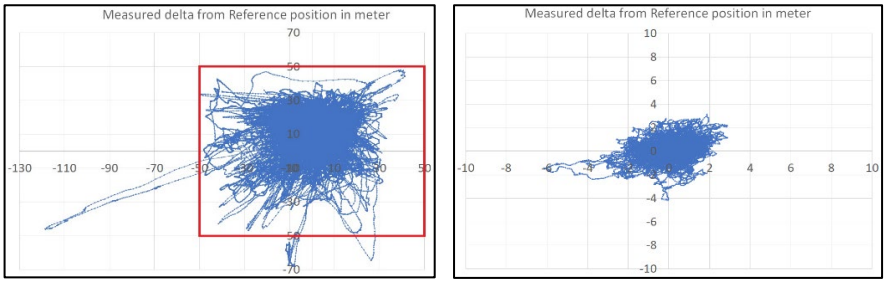

Fig 3. GPS accuracy (a) unfavourable and (b) good receiving situation

It can be concluded that the position error most of the time is lower than ± 50 m from the reference point also in the case of unfavourable receiving situation. If the position drifts out of this area it is only for a short time and can be eliminated by a rule that the measurements are out of the area for a specific time. Only in this case a movement of the reference position is detected.

To determine the reference position, hundreds of measurements are taken, and the average is used.

For higher accuracy differential GPS can be used. The component cost would be higher, and the power consumption would increase. For a theft detection normal GPS is sufficient.

4.2 Ensuring the physical integrity of the sensor

Security application: External manipulation. The electronics of the SED are protected by a safe housing. Violent and unauthorized opening of the housing interrupts tamper detection wires and activates alarm switches. This is detected by the HSM and an unauthorised opening, an intrusion, is assumed. This event will be notified to the control center by an alarm message. The housing alarm can be activated by a dedicated magnetically activated switch or via software by an activation command. The activation is acknowledged by a blinking light-emitting diode (LED). Deactivation is done with a magnet.

Event signalisation: ALARM (Tamper detection), pre-information with an emergency SMS.

Evaluation steps:

- The sensor housing is opened without prior authentication.
- The tamper detection wires get broken, the HSM detects this.
- The sensor enters the emergency state.
- The sensor generates an alarm message.
- The edge computer sends a SMS message.
- The alarm message is received and displayed on MMT.

Implementation experience: For the demonstration, the broken wires are emulated by plugs and sockets, which interrupt the tamper detection wires.

4.3 Inhibit unauthorised reuse of manipulated sensors

Security application: Internal manipulation. The firmware is protected against unauthorized reading and updating through encryption. The encryption keys are stored in the HSM and cannot be changed or read out. An unauthorised access attempt is detected by wrong credentials. After a predefined number of tries the access interface is blocked for a given time period and after another unsuccessful attempt, access is completely locked.
Event signalisation: ALARM (unauthorised access), pre-information with an emergency SMS.
Evaluation steps:

- The attacker connects a terminal to the access interface.
  - The sensor asks for authentication.
  - For each wrong credential the sensor generates a notification message.
  - After a predefined number of access attempts with wrong credentials, the sensor blocks the access interface.
- The sensor enters the emergency state.
- The sensor generates an alarm message.
- The edge computer sends a SMS message.
- The alarm message is received and displayed on MMT.
- Reading out the firmware from external memory for reverse engineering and manipulation does not make sense because the firmware is encrypted.

Implementation experience: The HSM must be handled carefully. There are two types of activation of the security mechanism of the HSM. Development mode and permanent mode. If the permanent mode is activated, it cannot be cleared again. The module can no longer be removed without losing the software.

4.4 Prevent manipulation of the sensor communication data

Security application: Internal manipulation. The field device protects the stored communication keys in such a way that these keys cannot be read out by an unauthorised person and used in a different device for (manipulated) data communication in the agriculture sensor network.
Event signalisation: ALARM, pre-information with an emergency SMS.
Evaluation steps:

- Connect the sensor to the network normally.
- Try to read communication keys from ongoing communication with a sniffer → not possible.
- Try to read out the communication keys memorised in the HSM → not possible without successful authentication.
- If the sensor stops working and does not send any data to the cloud, the system center triggers an alarm that the sensor has been lost.

Implementation experience: In common implementations of LoRaWAN end nodes, the communication keys are stored in a memory which can be read out with much effort. With this prototype sensor, the keys are stored in the HSM and the keys cannot be read out even with great effort.

5 Cost of security

Improving security of sensors used in outdoor environments comes at its own cost. Part of these costs are on the development side in the form of time required for developing such solutions and the cost of the necessary hardware components. There are ongoing costs such as System Control Centre and maintenance. Another part of these costs lies on the sensor itself in the form of increased power consumption which is needed to run the extra security components.

For a prototype such as the SED prototype presented here, the development costs are not the essential factor. For industrial production the cost of development must be divided by the number of devices expected to be sold.

In the SED two special hardware components are used: the HSM and a GPS receiver with an external active antenna. Additionally, the case of the device must be constructed with a wire loop that is broken if the case is opened. The HSM costs about 40€ for single items, the GPS module about 40€ and the active antenna about 15€. The wire loop in the enclosure has no significant cost. The connection of these components to the sensor is not complex and in general plug and play. All components together can be purchased for less than 100€.

The running costs for these safety functions are also low, since the System Control Center is normally be used without these safety improvement functions and there are very low additional costs. Mobile devices such as cell phones or tablets are typically used for general maintenance of field devices and do not need to be purchased for these security functions.

As many sensors in the field are battery powered, the power consumption of the additional security components is of high importance. Especially LoRaWAN sensors are designed to work for up to several years from a built-in battery, related to the sensor component itself. The HSM used in our demonstrator has a coin cell as a power supply and can work for years. The wire loop in the enclosure also requires only very low current and is not significant for the overall power consumption. However, the power consumption of a GPS receiver with active antenna is much higher. It is in the range of 50 mA in receive mode with active antenna. To decrease this power consumption, the GPS receiver is in general in power down modus or shut off and only activated by a tilt or acceleration sensor. Standard acceleration sensors such as the ones in mobile phones consume very low current. With the use of a passive antenna, the power consumption can be lowered as well. A GPS receiver with a passive antenna has a lower performance but it is suitable for many outdoor environments.

In general, the additional cost for the security features comes mainly from the additional GPS module and its greater power supply requirements.

6 Conclusions

For the demonstration of cyber security protection improvements on field devices an implementation for a soil sensor was selected. Such a sensor represents one of the smallest field devices used in the agriculture domain. Regardless of the size, these field devices need the same cyber security measures as large field devices, such as tractors and field operation machines. In the future, field devices will become more and more powerful, equipped with a powerful 32-bit microcontroller, with large firmware and large data memories as well as with a wireless broadband communication interface such as 4G or 5G. These devices will become part of the multitude of IoT devices in our future digital world. But the increasing distributed computing power of these devices, which are spread across the region, will also awaken the interest of cyber criminals. For example, the Mirai [10] IoT Botnet attack has shown what criminals are able to establish, when the cyber security protection of IoT devices is very weak. In 2016, Mirai disturbed several high-profile services via massive DDoS (Distributed Denial of Service) attacks with a data bandwidth of 1 Tbps (Tera bits per second), by compromising IoT devices such as routers and edge nodes.

Today it is not so simple to integrate both an HSM, a 4G / 5G data modem and a GPS receiver of small size into one sensor and at low unit costs. But these functions will become available together in one small system module for the mass market in near future.

The evaluation of the SED showed that the security measures are working efficiently. The cost for components is not very high and the power consumption can be trimmed to a good level.

7 Outlook

Securing networked IoT devices against cyber-attacks and unauthorized use is becoming increasingly important. Modern electronics, the basis of digitalization, must not be operated unprotected. The technology offers a highly interesting operating platform for cyber-attacks if strong security measures are not taken.

In the next few months, the European Commission will clarify Article 3.3 of the European Radio Equipment Directive (RED) [5]. Manufacturers and distributors of IoT devices that exchange data via wireless interfaces must fulfil security requirements that are very difficult to meet. These are the "Essential Requirements" - specifications that are binding but have not yet been implemented. For example, in Article 3.3 the following security requirements are relevant for future developments of wireless devices:

Radio equipment within certain categories or classes shall be so constructed that it complies with the following essential requirements:

- *e) radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected;*
- *f) radio equipment supports certain features ensuring protection from fraud;*

> *g)* ...
> *i)* *radio equipment supports certain features in order to ensure that software can only be loaded into the radio equipment where the compliance of the combination of the radio equipment and software has been demonstrated.*
>
> Excerpt from the EU-Guideline [5]

The distributors are obliged to integrate the necessary cyber security protection measures and to prove efficient function. There are security improvement efforts necessary in any domain of the digitalization, such as residential, automotive, industrial and agriculture technology.

Acknowledgments
This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No. 783221 (AFarCloud). The JU receives support from the European Union's Horizon 2020 research and innovation programme and Austria, Belgium, Czech Republic, Finland, Germany, Greece, Italy, Latvia, Norway, Poland, Portugal, Spain, Sweden.
Parts of this work were funded by the Austrian Research Promotion Agency (FFG) and BMK (Austrian Federal Ministry for Climate Action, Environment, Energy, Mobility, Innovation and Technology).

References

[1] Reinhard Kloibhofer, Erwin Kristen, Luca Davoli, LoRaWAN with HSM as a Security Improvement for Agriculture Applications, SAFECOMP 2020 - DECSoS '20 ("Dependable Smart Embedded and Cyber-Physical Systems and Systems-of-Systems"), https://zenodo.org/record/3999637#.YHv3mOgzbmE.
[2] Website of 365FarmNet platform: https://www.365farmnet.com/en.
[3] Website of Agrirouter platform: https://my-agrirouter.com/en/.
[4] LoRa Alliance. LoRaWAN 1.1 Specification. Accessed on 2020-05-02. http://lora-alliance.org/lorawan-for-developers.
[5] DIRECTIVE 2014/53/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 16 April 2014, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32014L0053.
[6] https://community.zymbit.com/c/zymkey/22.
[7] Ameri, E. Afshin, et al. "Planning and Supervising Autonomous Underwater Vehicles through the Mission Management Tool." *Global Oceans 2020: Singapore–US Gulf Coast*. IEEE, 2020.
[8] https://www.mediatek.com/products/locationintelligence/mt3339, https://community.zymbit.com/c/zymkey/22.
[9] https://www.u-blox.com/en/product/lea-6-series?lang=de

[10] Inside the infamous Mirai IoT Botnet: A Retrospective Analysis,14.12.2017, https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/.