applied sciences

Article

Security Assessment of Agriculture IoT (AIoT) Applications

Erwin Kristen [1,*], Reinhard Kloibhofer [1], Vicente Hernández Díaz [2] and Pedro Castillejo [2]

[1] Austrian Institute of Technologies AIT GmbH, 1210 Vienna, Austria; reinhard.kloibhofer@ait.ac.at
[2] Departamento de Ingeniería Telemática y Electrónica (DTE), Universidad Politécnica de Madrid (UPM), C/Nikola Tesla, s/n, 28031 Madrid, Spain; vicente.hernandez@upm.es (V.H.D.); pedro.castillejo@upm.es (P.C.)
* Correspondence: erwin.kristen@ait.ac.at

Abstract: Cybersecurity is an important field in our digital world. It protects computer systems and communication networks against theft or sabotage of information to guarantee trouble-free operation in a trustworthy working environment. This article gives an overview of a cybersecurity assessment process and an appropriate Cybersecurity Management (CSM) implementation for future digital agriculture applications. The cybersecurity assessment follows the IEC 62443 cybersecurity standard for Industrial Automation Control Systems (IACS), adapted to Agriculture Automation Control Systems (AACS). However, the research results showed application differences; thus, an expansion of the standard is necessary to fill the existing open security gaps in agriculture. Agriculture differs from industrial control systems because of the outdoor located field area, which requires other forms of security. An appropriate cybersecurity standard for the agriculture domain is not currently available. However, such a standard will be necessary to define generally applicable procedures to protect agricultural assets against cyberattacks. The cybersecurity standards and regulations existing today (2021) are not sufficient for securing the agriculture domain against new and domain-specific cyberattacks. This article describes some of the cyber vulnerabilities identified and provides initial recommendations for addressing them.

Keywords: cybersecurity; agriculture; Information Technology (IT); Operation Technology (OT); Internet of Things (IoT)

check for updates

Citation: Kristen, E.; Kloibhofer, R.; Díaz, V.H.; Castillejo, P. Security Assessment of Agriculture IoT (AIoT) Applications. *Appl. Sci.* **2021**, *11*, 5841. https://doi.org/10.3390/app11135841

Academic Editor: José Machado

Received: 26 May 2021
Accepted: 17 June 2021
Published: 23 June 2021

1. Introduction

Today, all major product suppliers in the agriculture vehicle and machinery manufacturing domain support their products with a set of sensors to gather all available functional and vital data from the machines for maintenance analysis. These data are collected via USB-sticks in the workshop during periodic maintenance phases or, increasingly commonly, initiated via in-time data transfer from the machine to the manufacturer via cellular radio communications. These technologies allow preventive maintenance to shorten the service (nonoperating) time and the collection of highly informative real-time data for the further development and improvement of the machines.

The agricultural companies also benefit from continuous data collection using modern network technology. In this case, all production data are recorded during execution. It enables cooperation with the machinery supplier and the cooperation with other agriculture companies for task optimization and improving product 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 365farmNet (https://www.365farmnet.com/en, last access on 10 June 2021) and Agrirouter (https://my-agrirouter.com/en/, last access on 10 June 2021). The DataConnect interface was originally developed by Claas, 365FarmNet, and John Deere.

The increasing digitalization in agriculture and the associated networking of machines and production systems increases the risk of cyberattacks. Security describes the protection of production plants and all the related components against deliberately or unintentionally caused errors externally introduced to the farm. In the early days of automation, only the Information Technology (IT) sector was affected by security threats. The Operational Technology (OT) domain was isolated from the outside world and was technically set up very simple. Today, the IT domain is seamlessly connected with the OT domain, and cybersecurity measures are necessary for both domains. By widely distributed production facilities (field level), which are typically for agriculture, new points of attack were added, making it easier for attackers to penetrate the production facility, manipulate it, and even impair safety (machine safety). Nowadays, employees who are not IT experts also have to deal with potential security threats. Therefore, it is necessary to carry out a comprehensive security risk assessment of the entire agriculture production system, both from IT and from OT, to ensure an adequate security level. Also, the involved employees must be trained according to existing and new security threats in periodic intervals so they can react quickly and purposefully.

Most importantly, an extensive security program both for the IT and the OT layer must be established to ensure smooth and trustworthy operation. For new agriculture production system designs, cybersecurity is part of the system architectural design (Security-by-Design). For pre-existing legacy agriculture production systems, a security assessment exposes the necessary cybersecurity improvements to guarantee a defined, sufficient security level.

This article gives an overview of the cybersecurity work and the research outputs of the European research project "AFarCloud" (http://www.afarcloud.eu/, last access on 10 June 2021), with a focus on Cybersecurity Management (CSM) methods research in agriculture. The AFarCloud project deals with the aspects of the current ongoing and future digitalization in the agriculture domain. AFarCloud defines a general architectural structure of a data driven agriculture architecture divided into four function levels, as shown in Figure 1.

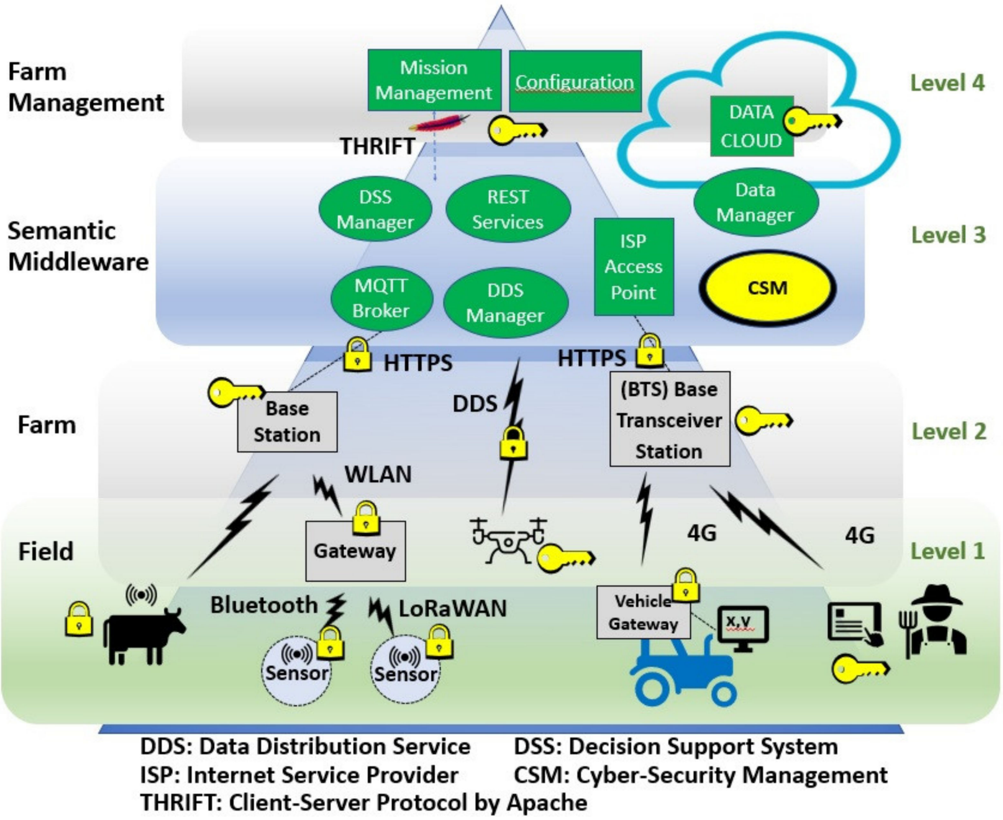


Figure 1. AFarCloud architecture of a future agriculture architecture.

Starting from the cloud level (Level 4), the system connects with the Farm Management System (FMS) and external data repositories, then to the middleware function layer (Layer 3), and finally, down to the farm level functions (Level2) and the field level (Level 1) devices. In this architecture, CSM is embedded as a cross-layer service, both for the FMS, the semantic middleware, which includes the cloud-based data processing, the decision making and the data repository functionalities, and finally, for the hardware elements at the field level, such as sensors, vehicles, and actuators. Figure 1 will be described in more detail later in Section 2.

Cybersecurity is a very important issue in modern agriculture, according to system security and data confidentiality. Today's agriculture production plants are equipped with a huge number of interconnected computers and modern electronic equipment. These components and the data communication between them must be considered in a cybersecurity risk assessment. The use cases and applications, where all system components are involved must be added to the system description, and all involved stakeholder's roles complete the overall system description for the cybersecurity assessment.

1.1. Security Standards Overview

The following overview of well-known safety and security standards shows that the main initiatives to create security standards come from the industrial automation and mobility (vehicles, railway, avionics) domains.

Security standards for agriculture mainly handle the area of food and nutrition security, while no dedicated standards are defined for the agriculture IT/OT security domains at the present. But in this case, today's well-established industrial control security standards are a perfectly good source for agriculture applications too.

The following overview lists some cybersecurity standards from the IT/OT domain:

- ISO/IEC 15408 establishes the general principles of IT security evaluation;
- ISO/IEC 27000 overviews the Information Security Management Systems;
- ISO/IEC 27001 specifies a management system for information security;
- ISO/IEC 27002 describes guidelines for organizational information security and information security management practices;
- ISO/IEC 27005 brings guidelines for information security risk management;
- ISO/IEC 62443 Industrial Communication Networks—Network and System Security series.

Food Security concerns the availability and sufficient access to food. Food security is ensured by using new agricultural technologies and by establishing good product quality.

The focus of safety standards for agriculture are in safety regulations: to prevent illnesses and injuries from agriculture work by pesticide handling and to guarantee a safe use of heavy machines and safe work with animals.

Food Safety concerns the production of wholesome food products. A lot of safety standards and legal regulations for food safety are defined.

Animal welfare regulations ensure animal-friendly treatment of livestock.

To provide cybersecurity requirements, a successful approach could be the adaptation of the cybersecurity standard IEC 62443 as a basis to assess the security vulnerabilities in the agriculture domain. The standard describes a security analysis flow and recommendations for the system development and the assessment of existing systems. Adapting a cybersecurity standard for Industrial Automation Control System (IACS) makes sense because the hardware and software architecture is similar in these two domains and the vulnerabilities are of the same types, except for the extensive differences at the field level. Both system architectures have a similar structure: field area, edge processing area (middleware), and administration and planning area (farm management, data repository). On the industrial control side, in most cases, the field elements are enclosed in industrial control buildings and are, by this circumstance, easy to protect and to supervise. In the agriculture domain, the field elements may be installed and located far away from the farm buildings and these elements are more likely to be endangered by manipulations, destruction, and risk of theft.

There are many reasons why cybersecurity attacks will be performed. The following must be considered for a cybersecurity analysis.

1.2. Cybersecurity Attack Motivation

There are three groups of attack motivation types identified: espionage, destruction, and sabotage, as described by examples in the following list.

1.2.1. Espionage

- Unauthorized data access
- Data leakage
- Loss of know-how (IP) and production data
- Phishing
- Trojans
- IP Theft
- Spyware

1.2.2. Destruction and Exaction

- Causing physical damage to farming equipment
- Deterioration of product quality
- Ransomware
- Data manipulation
- Data destruction

1.2.3. Sabotage and Misusage

- Loss of farming equipment availability
- Loss of production
- Deterioration of product quality
- Botnets
- Distributed Denial of Service (DDoS) attacks
- Man-in-the-Middle (MITM) attacks

To limit possible cyberattack risks in agriculture applications, a cybersecurity management process must be installed to identify the system vulnerabilities with the possible attack vectors, and to propose suitable countermeasures.

1.3. Cybersecurity Considerations

Cybersecurity examines various aspects and points based on the following four considerations:

1.3.1. Technical Considerations

Cybersecurity in agriculture is different in contrast to security in industrial production, but both system architectures have, as already mentioned, a similar structure: field area, edge processing area (middleware), administration and planning area (farm management with Mission Management Tool (MMT), Decision Support System (DSS), and system configuration for agriculture), and cloud service/storage area.

Relevant components: software applications, embedded devices, host devices, network devices, etc.

1.3.2. Vulnerability Considerations

There are multiple reasons why an attacker performs a cyberattack on vulnerable Internet of Things (IoT) systems. One of the most common reasons is stealing or leaking of information. A secondary reason is the manipulation and sabotage of smooth operation of the agriculture processes to disrupt the correct operation.

The given attack vectors are, as already mentioned above, more extended in agriculture because of the wide, not gapless monitoring, field area. Also, there are attack vectors in the communication links and (cloud based) managing and planning area (farm management and system configuration).

Relevant: type of attackers, attack vectors, etc.

1.3.3. Economic Considerations

This viewpoint considers the aspect of the security options available for small (S), mid-sized (M), and large (L) agriculture companies (AC). In general, a L-AC has more economic options for security measures in the company compared to that of S- and M-ACs; it is possible that an L-AC could employ security experts in-house full-time. What are the possible threats and vulnerabilities for such ACs, and what are suitable solutions for external support if needed by the S- and M-AC?

Relevant: farm size, IT/OT experience at the AC, etc.

1.3.4. Privacy Considerations → Data Privacy

This view handles the question of data security and gamification. The future agricultural IoT landscape produces Masses of Data (MOD). The MOD has a value and each farmer must receive the possibility to sell it similarly to agriculture goods. Here, data security is a very important topic. Who is storing the data in the cloud and where? How reliable are the security measures of the internet, the cloud, and the digital service provider? Is this answerable by S- and M-AC without external assistance?

Relevant: who is the owner of the digital data produced; who ensures data security; who handles the intellectual properties, etc.

2. Materials and Methods

To perform a cybersecurity assessment, a standardized process brings the best results when security statuses are compared, the ongoing improvements are assessed, and the work carried out is certified.

In this chapter, the cybersecurity assessment of a given system, worked out in the AFarCloud project, is explained in more detail as a practical example. The assessment is carried out according to the cybersecurity standard IEC 62443. As a reference, this standard, a well-established work standard for IACS's, is used and adapted for agricultural applications.

2.1. Cybersecurity Management Methods

There are well-defined methods for cybersecurity analysis that define measures for a new design or how to implement such measures in an existing system. Monitoring and maintenance cybersecurity for a system is a mandatory continuous process to guarantee maximal cybersecurity situation for the whole life period of the given system. These four tasks are evident.

(a) Security Risk and Threat Analysis.
  - ○ Structured cybersecurity assessment process.
  - ○ Identify vulnerabilities and threats.
  - ○ Gapless security assessment documentation.

(b) Security-by-Design.
  - ○ Tool support for the system designer to implement security during the development phase to avoid security flaws.
  - ○ Threat modeling for the cybersecurity assessment.
  - ○ Model update for each system change.

(c) Security Monitoring.
  - ○ Continuous system supervision to detect security attacks, respond with counter measures, and perform postattack analysis.

(d) Security Maintenance.

- ○ Periodical system assessment to identify system security status and new attack vectors.

2.2. The System Operation States

One aspect of the cybersecurity assessment is the definition of all system operation states which the system will pass in their overall life cycle. Table 1 lists an example of four main cycles of a system life cycle: production, installation, operation, and decommissioning. Each of these operating states can be divided into substates to define the performed activities and consider the possible security vulnerabilities for the different operation conditions.

Table 1. System operation states.

Main-State (Activity)	Substates (Activity)
Production	Component selection Design (HW, SW) Manufacturing Firmware Installation Component testing
Installation	Software installation Component and system Integration Security key transfer and initialization System testing
Operation	Data reception Data processing Data transmission Renew security keys System backup
Decommissioning	System/component reset Disposal Complete data deletion (data management)

A security assessment is never fixed to only one of the system's life cycles, and furthermore, for a complete security assessment, all cycles must be rated and analyzed with the same level of care and precision. For example, an unsafe and undefined process in the "decommissioning" state is the disposal of old data storage devices, which can lead to a data breach. This could enable third parties to recover highly sensitive system information, using it for attacks in the "operation" state of the new devices. However, if all operating cycles are not considered during the safety assessment, this fact must be carefully recorded in the safety documentation.

2.2.1. Cybersecurity Assessment Key Questions

An assessment process should always follow the same procedures. This is important because a cybersecurity assessment must be repeated periodically to identify new types of vulnerabilities and to improve the system against new attack vectors. This enables successive evaluations to be compared.

- What is the System under Consideration (SuC)?
- Based on the SuC definition, what are the borders of the system?
- Which interfaces reach from the outside into the SuC?
- What are the assets of the system?
- Which assets are not part of the analysis?
- Which assets are outside of the SuC?
- What are the potential threats?
- What are the security leaks and vulnerabilities of these architectures?
- What are the existing hardware vulnerabilities?

- What are the existing software vulnerabilities?
- What are the existing network vulnerabilities?
- Which attack vectors must be assumed for the defined SuC?
- What are the impacts of security attacks for the different parties and situations (loss of values, loss of trust, and loss of reputation)?

2.2.2. The System Roles and Responsibilities

Further aspects in the cybersecurity process are the roles and responsibilities of all persons involved. The IEC 62443 security standard defines three different roles of competence and responsibility. The Asset Owner (AO) operates the Agriculture Automation and Control System (AACS), and the System Integrator (SI) integrates the functionalities and components in the AACS, instructed by the AO. The Product Supplier (PS) develops and validates the functionalities and components used and provides these with appropriate test certificates to the SI. All these roles must be considered in the CSM processes.

The cybersecurity process must be coordinated with the AO, who must agree and support the mandatory tasks to harden the system according to the actual possibilities in technology.

The CSM process consists of the four main cycles:

○ Security assessment and analysis.
○ Security measure installation.
○ Security guidance and training.
○ Security verification.

2.3. The Cybersecurity Assessment Process

The standardization of a cybersecurity assessment process was mainly driven by the initiative of the International Society for Automation (ISA) and the American National Standards Institute (ANSI) started in 2002. Originally named ANSI/ISO-99, it was later renamed as the ANSI/ISA-62443 standard series. In 2009, the European standardization committees utilized a fundamental concept from the original ANSI/ISA-62443 standard to introduce the IEC 62443 cybersecurity standard series [1–8].

The industrial security standard IEC 62443 specifies a security assessment process for the overall system domain, both from the system and component view. Different security aspects are relevant for the security assessment, and these aspects must be analyzed. The appropriated analysis results are documented in a security documentation and define the security determinations in a security plan.

The security assessment process flow defines five dedicated steps, as shown in Figure 2. Each step must be performed to carry out a standard cybersecurity assessment.

An assessment process should always follow the same procedures. This is important because a cybersecurity assessment must be repeated periodically to identify new types of vulnerabilities and improve the system against new attack vectors. This enables ongoing and comparable evaluations.

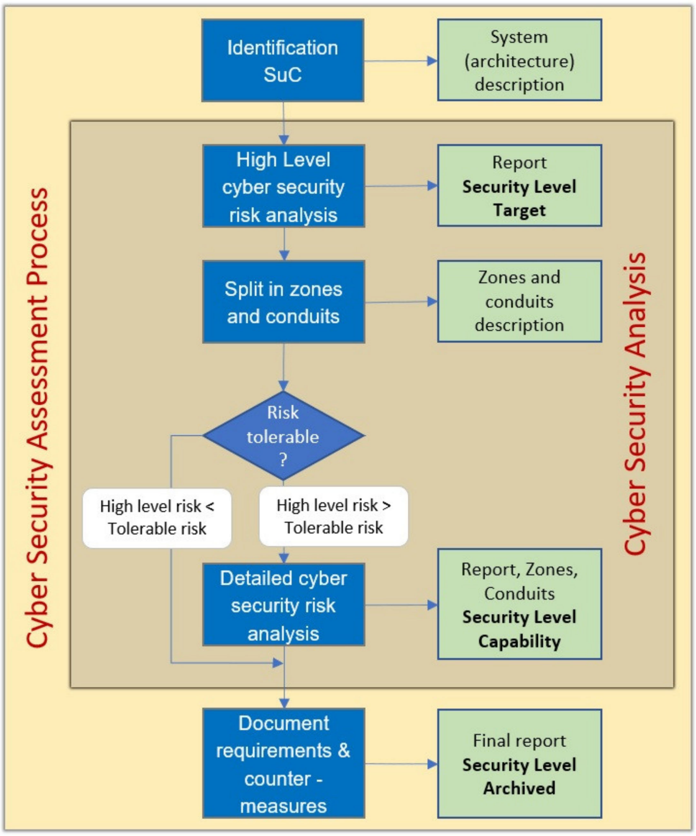

Cyber Security Assessment Process
Cyber Security Analysis
Identification SuC
System (architecture) description
High Level cyber security risk analysis
Report Security Level Target
Split in zones and conduits
Zones and conduits description
Risk tolerable ?
High level risk < Tolerable risk
High level risk > Tolerable risk
Detailed cyber security risk analysis
Report, Zones, Conduits Security Level Capability
Document requirements & counter - measures
Final report Security Level Archived

Figure 2. IEC 62443 cybersecurity process steps.

The process defines five main activity steps and one decision and assessment step.

The following overview of the process steps gives a short introduction. In the following chapter, the steps and the necessary activities are explained in detail.

- SuC Identification:

Activity: accurately describe the SuC for which the security assessment shall take place. It is important to define the borders of the system to define what is and is not part of the SuC.

- High-level cybersecurity risk analysis

Perform a high-level security risk analysis of the system defined by the SuC description. Determine the Target Security Level (SL-T). This is the minimum cybersecurity level the system must have.

- Split into zones and conduits

Split the SuC into zones (system areas with similar criticality) and define the communication paths (conduits) which connect the zones. This activity prepares the system for the detail cybersecurity assessment.

- Detail cybersecurity risk analysis

Perform for each zone and conduit a detailed risk analysis. The analysis determines existing threats and vulnerabilities. The standard IEC 62443 provides seven Foundational Requirement (FR) groups to support the analysis. By the definition of a suitable SL the standard provides a set of requirements that must be fulfilled and well-ordered in the seven FR groups. Each group specifies a set of sub-requirements, depending on the selected SL.

- Tolerable risk assessment

Repeat the detailed risk analysis in a loop manner until the SL-T matches the Capability SL (SL-C). The system or component capability level describes the maximal realizable SL by implementation. When no match can be targeted, the system does not provide the necessary SL. In this case, a possible solution may be to embed the entire system in a safe, enveloping operating environment.

- Document requirements and countermeasures

Document all the security implementations, security requirements and any security artefacts to create a final cybersecurity report. The actual security implementation documents the Archived SL (SL-A).

2.4. Process Step: SuC Identification

The cybersecurity assessment process starts with the exact and careful definition of the system which shall be assessed. An appropriate system description of the SuC must first include a general description of the system use and all planned applications. These descriptions are important for a general vulnerability and security threat estimation. A list of the hardware and software components (assets) involved defines the level of available and necessary security features. Next, a detailed system overview, in the form of a block diagram, shows all the components in a sector of identical criticality and the interconnections between the sectors, where data are transmitted. Finally, the definitions of the system borders are significant. An incomplete system description or an inaccurate system border definition will lead to an inconsistent safety assessment. This can have the consequence that the security assessment delivers wrong results or calls for unnecessary measures, thus leading to undesirably higher implementation costs. It is very important that the system to be assessed is described completely with a sufficient level of detail. Defining the system in an inadequate way implies the hazard that important system security issues may be overseen, whereas too large a system definition may lead to unnecessary security risk analysis efforts, which usually do not help improve the security of the system.

The output of this step is a detailed system description, which is the basis for the next assessment steps. This document is part of the overall security assessment documentation and describes the actual system state. This is an important input to identify changes when performing a periodical security reassessment in the future.

2.4.1. SuC Identification Key Questions

System relevant questions:

(a) What is the SuC?
(b) Based on the SuC definition, what are the borders of the system?
(c) Which parts of the system are not part of the SuC?

Asset relevant questions:

(d) What are the assets of the system?
(e) Which assets are not part of the analysis?
(f) Which assets are outside of the SuC?

Interface relevant questions:

(g) Which data communication interfaces reach from the outside into the SuC?
(h) Which protocols are used by the interfaces?

When the SuC is carefully defined and documented, an imported step is done to know the assets, which must be protected against cybersecurity attacks.

In the IACS domain, IEC 62264 defines an edition of functional hierarchies of the industrial automation process (IAP) [9], as shown in Figure 3.

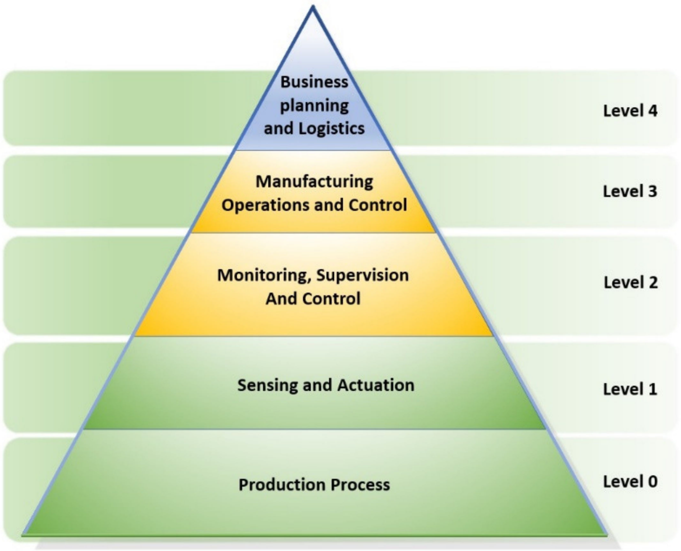

Business planning and Logistics
Level 4
Manufacturing Operations and Control
Level 3
Monitoring, Supervision And Control
Level 2
Sensing and Actuation
Level 1
Production Process
Level 0

Figure 3. Industrial production functional hierarchies, according to IEC 62264.

The "Sensing and Actuation" segment is located at the bottom of the pyramid, with the sensors and the actuators (IAP: Level 1). On top of the pyramid is the "Business Planning and Logistics" segment (IAP: Level 4). Between these segments, both the "Monitoring, Supervision and Control" segment and the "Manufacturing Operations and Controls" segments are arranged (IAP: Level 3 and Level 2). In most cases, Level 0, Level 1, and Level 2 are found at a single geographical location, generally in a company building. Level 3 and Level 4 could be located far away from the building, possibly anywhere worldwide. The top levels can operate by using cloud-based services and can be partially outsourced to third-party companies. These decentralized system architectures are becoming more and more general for both large and medium-sized companies.

In AFarCloud, a comparable system architecture for agriculture applications was defined and developed as shown in Figure 1. It is divided into four main-segments. On the bottom, in the "Field" segment, there are the sensors and the actuators for the livestock and crop process activities. On the top "Farm Management" segment, functions, such as mission management and configuration, are provided. Also, the data repositories are installed in the top segment level by using cloud-based services. The "Semantic Middleware" segment provides services to collect and distribute data and to perform decision finding by processing actual and historical data. In this segment, the CSM services are installed to support the overall system with security processes. The "Farm" segment provides the OT functionalities for data collecting and distributing, and acts as the fog or edge computing layer.

In Figure 1, all communication interfaces established between the segments are illustrated. While, in the field segment, numerous different communication protocols are in use, adapted for a special use and application, the higher segments are only supported by some selected communication paths and protocols to improve the data and cybersecurity. The yellow key and lock symbols give a rough overview of implemented cybersecurity measures.

The following overview lists all assets of the system architecture. Only a short excerpt of the available hardware and software and the communication protocols in use are given. In a real cybersecurity assessment, the system documentation is performed in more detail. Each detail of interest is important to find the appropriate security protection level and to identify potential security vulnerabilities.

Field segment:

Hardware/software assets:

- Livestock collar sensors
- Temperature, humidity sensors (soil and air)
- Air quality sensors
- Light spectral sensors
- Cameras
- Vehicles
- Drones
- In-vehicle data display monitors
- Outdoor data display monitors
- Cellular phones
- Data gateways

Communication protocols:

- Cellular phone protocol LTE and 4G
- Bluetooth
- LoRaWAN
- WLAN
- Sigfox

The drones link directly via cellular communication to the Data Distribution Service (DDS) manger in the semantic middleware using the DDS protocol.

Farm segment:

Hardware/software assets:

- WLAN base station
- Gateways (collects the data from the field sensors)
- Base Transceiver Station (BTS), supported by the telephone provider
- Business computer (not shown in Figure 1)
- Internet router (not shown in Figure 1)

Communication protocols:

- HTTPS/SSL/TLS/MQTTS

Semantic Middleware:

Hardware/software assets:

- DDS manager service
- Decision support system (DSS) manager service
- Internet service provider (ISP) access point service
- Data manager service
- MQTT Broker service
- REST service manager service
- Data storage service

Communication protocols:

- HTTPS/SSL/TLS/MQTTS

Farm Management:

Hardware/software assets:

- Mission management service
- Configuration management service
- Data storage repository service

Communication protocols:

- HTTPS/SSL/TLS/MQTTS
- Apache THRIFT [10] binary communication protocol

The hardware and software assets of the "Semantic Middleware" and the "Farm Management" segments are denoted as "services". This means that the services are executed on one or on different computing units by the appropriate service provider.

In the architecture segments Levels 1 and 2, the asset owner has full control over the installed security measures to harden the system against cybersecurity attacks. For Levels 3 and 4, the asset owner can only perform a very accurate provider selection and must trust that the defined security specifications are fulfilled. The asset owner has little or no influence upon the security conditions of these services. He/she can only request security certificates and must trust the service provider on compliance with the duty of caution. Unfortunately, from time to time, one hears about cyberattacks against service providers in which private customer data was stolen. Further points of discussion in security and privacy are the questions of where the data are stored by active service providers operating worldwide with remotely located cloud-based data repositories and service farms.

Continuous security monitoring is the only activity the asset owner can perform to increase confidence. This is a requirement which may be performed by medium and large farm companies. Small farm companies need support and consultation from their professional associations to reach a level of security and privacy such that the company can work trouble-free.

2.4.2. Components (Assets) Location

To perform a cybersecurity assessment, the location of the components of the architecture must be first considered. In Figure 1, the associated components (assets) of the AFarCloud architecture are shown and categorized in three criticality groups:

(a) Components located outside in the field or outside a farm outbuilding:

- Level 1: Field segment
  OT hardware/software infrastructure:
  Sensors and actuators, vehicles, drones, mobile data terminals, etc.
  Criticality: Under the control of the farm company.
  Accessible to anyone when placed on the field.
  Not always monitorable by farm personnel.

(b) Components located in-house:

- Level 2: Farm level
- IT hardware/software infrastructure
- Criticality: Under the control of the farm company.
  Accessible only to persons which have access to the farm building.
  Easily monitorable by farm personnel.

(c) Components provided by third party service provider companies:

- Level 3: Semantic middleware
- Level 4: Farm management
- IT hardware/software infrastructure
- Criticality: Not under the control of the farm company
  Use of services based on trust to the service provider
  Use based on valid certificates

2.4.3. Sub-SUC

If the overall SuC is very complex, a good approach is to divide the overall system into sub-SuCs, where each individual sub-SuC receives its own cybersecurity assessment.

The overall SuC in Figure 1 will be divided into the following sub-SuCs:

- Livestock SuC (SuC-A) Livestock with sensors (Field)—Farm—Middleware—Farm management
- Soil-sensor SuC (SuC-B) Soil sensors (Field)—Farm—Middleware—Farm Management → see Figure 1
- Drone SuC (SuC-C) Drone with spectral sensors (Field)—Farm—Middleware—Farm management
- Vehicle SuC (SuC-D) Tractor with sensors and actuators (Field)—Farm—Middleware—Farm management

- Data SuC (SuC-E) Farm management—Middleware—Farm—Personal With tablet (Field)

The documentation of all five sub-SuCs would go beyond the scope of this document. In this case, only "Soil-sensor SuC" is used as an example (see Figure 4) to document the cybersecurity assessment process further on. Furthermore, in this paper, the cybersecurity assessment focuses on field sensor security in segment 1 (Field) and segment 2 (Farm). This reduces the scope of the work and the size of the paper and gives a sufficiently detailed overview of the cybersecurity assessment process. On the other hand, segment 1 (Field) and segment 2 (Farm) are of great interest to the farm staff, as these are their areas of responsibility.

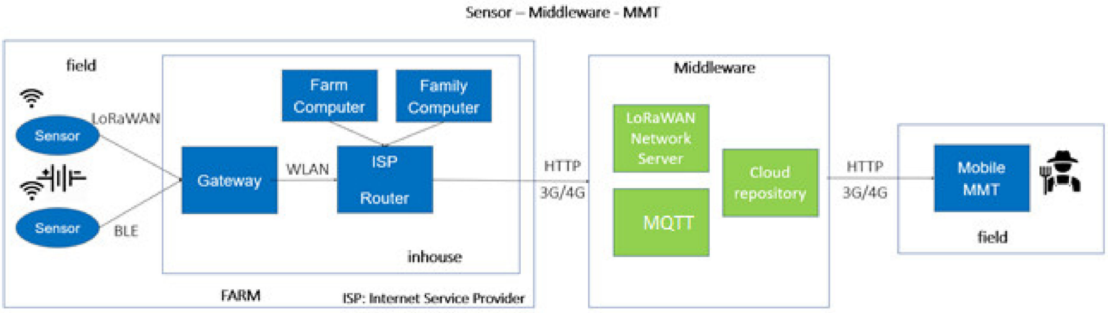


Figure 4. Sub-SuC for Sensor—Middleware—MMT.

The sub-SuC "Soil-sensor SuC" defines the architecture, the components and the sensor communications data flows of a soil sensor application. It defines the sensor to the middleware and the middleware to the mobile MMT data communication. It provides a set of sensors in the field zone which transfer sensor data via Long Range Wide Area Network (LoRaWAN) or by using the Bluetooth Low Energy (BLE) transmission protocol to the cloud repository in the middleware. The farmer on the field side can request postprocessed environmental data via a telecommunication link on a mobile MMT device (smart mobile phone, tablet with 3G/4G functionality).

Asset List:

Field (Environment Sensor: LoRaWAN communication protocol, Soil sensor: BLE communication protocol, Mobile MMT: Tablet Computer—Data/Mission Display), Farm house (LoRaWAN/BLE Gateway, Router, Farm Computer, Family Computer), Middleware (LoRaWAN Network server, Cloud repository, DDS).

Data communication links:

LoRaWAN, BLE, WLAN, 3G, 4G.

2.5. Process Step: High Level Cybersecurity Risk Analysis

When the SuC, or the sub-SuC, is clearly defined, the maximal allowable cybersecurity risk shall be fixed at a high-level view. The output of this assessment process step is the definition of the minimal acceptable SL of the target SuC. This fixed SL is also named SL-T and represents a reference point in the further assessment process.

2.5.1. Cyber SL's

The standard defines four SL for the protection classes. Each class defines the protection capability necessary to protect the system again potential attacks, as listed in Table 2.

Table 2. Cyber SL definitions.

SL-0	No specific requirements or security protection necessary
SL-1	Protection against casual or coincidental violation
SL-2	Protection against intentional violation using simple means with low resources, generic skills, and low motivation
SL-3	Protection against intentional violation using sophisticated means with moderate resources, IACS specific skills, and moderate motivation
SL-4	Protection against intentional violation using sophisticated means with extended resources, IT specific skills, and high motivation

The SL-1 and SL-2 will be sufficient for small and medium agriculture enterprises to ensure a general cybersecurity protection against many of the known cyberattacks. The necessary cybersecurity countermeasures can be managed by the farm staff itself. It is important that general and mostly recommended precautionary measures are observed and implemented.

The SL-3 and especially SL-4 require advanced knowledge and precautions, which in special cases can only be achieved by well-equipped and educated experts. If necessary, this knowledge can be requested from cybersecurity service providers.

For example, the Component Requirement (CR) 2.1 (Authorization enforcement) requires the establishment of access regulations for each user regarding certain actions (e.g., access control, read/write/execute). For SL-2, this requirement is mandatory for all users (humans, software processes and devices), not only for humans, and it requires that the access rights are mapped to roles. SL-3 additionally requires that in the event of emergencies or other serious events a supervisor allows an operator to quickly react to unusual conditions by overruling the access control. SL-4 requires a dual approval for actions which can have a serious impact. These requirement enhancements are required for most of the base requirements by the IEC 62443 cybersecurity standard.

2.5.2. Security Aspects

In the following paragraphs, the security aspects are discussed in detail and supported by values to determine the SL with a defined valuation method.

To define the minimum acceptable security level, various security aspects must be considered and assessed, such as:

(A) Device category: (which components and devices are used in the SuC in general?)

Software Application
Embedded Devices
Host Devices
Network devices

(B) Security vulnerabilities: (which vulnerabilities are to assume for the (sub-)SuC?)
(C) Security threats: (which cyberattacks on the system are to be assumed?)
(D) Attack Potential (AP) Factors: (which cyberattack strengths are to be assumed?)

2.5.3. Security Aspect: Device Category

According to IEC 62443-4-2, the following component categories are defined: each category needs different, component-specific security requirements.

The following definitions are an extract from the standard description.

- Software Application—IEC 62443-4-2/3.1.41 Software applications consist of one or more software programs and their dependencies that are used to interface with the process or the control system itself (for example, configuration software and history database). Note 1: Software applications typically execute on host devices or embedded devices. Note 2: Dependencies are any software programs that are necessary for the software application to function, such as database packages, reporting tools, or any third party or open source software. Examples: MMT applications, Middleware functions, etc.

- Embedded Device—IEC 62443-4-2/3.1.**18** An embedded device is a special purpose device designed to directly monitor or control an industrial process. Examples include Programmable Logic Controllers (PLCs), agriculture automation controller, wired or wireless field sensor devices, wired or wireless field actuator devices, safety instrumented system (SIS) controllers, and Distributed Control System (DCS) controllers. Note 1: Typical attributes are limited storage, a limited number of exposed services, programmed through an external interface, embedded operating systems (OSs) or firmware equivalent, real-time scheduler, may have an attached control panel, and may have a communications interface. Examples: Smart sensors, IoT devices, drone controllers, small robots.
- Host Device—IEC 62443-4-2/3.1.23 A host device is a general-purpose device running an operating system (for example Microsoft Windows OS or Linux) capable of hosting one or more software applications, data stores, or functions from one or more suppliers. Note 1: typical attributes include filesystem(s), programmable services, no real-time scheduler, and full HMI (keyboard, mouse, etc.). Examples: farm computers, Tractors MMTs with integrated computer, MMT computer, tablet computer (mobile MMT).
- Network device—IEC 62443-4-2/3.1.31 A network device is a device that facilitates data flow between devices or restricts the flow of data, but may not directly interact with a control process. Note 1: typical attributes include embedded OS or firmware, no HMI, no real-time scheduler, and configured through an external interface. Examples: wireless Sensor Networks (WSNs), data communication links.

2.5.4. Security Aspect: Security Vulnerabilities

During the high-level cybersecurity risk analysis, possible system vulnerabilities are identified.

Definition of system vulnerability: the vulnerability describes the disability of a system to withstand an attack both from inside or outside. This system weakness allows actors to gain unauthorized access to the system for (i.) espionage, (ii.) damage, (iii.) sabotage, or (iv.) misusage. During the security risk assessment, the severity (impact) of possible vulnerabilities are determined and defined.

The security risk assessment distinguishes between different types of security vulnerabilities, as listed in Table 3.

Table 3. Cybersecurity: security vulnerabilities.

Vulnerability	Explanation
Espionage	This vulnerability type focus on collecting data from the cyberattack victim. The data is used to gain secret knowledge or to obtain information to prepare further attacks. • Unauthorized data access • Data leakage • Loss of know-how (IP) and production data • IP Theft
Damage and Destruction	This vulnerability allows manipulation of data or causing system damage and deterioration of product quality • Data manipulation • Data destruction • Data replay attack • Partial or complete data deletion
Sabotage	This vulnerability enables the reduction of performing a correct system operation. • Limiting or loss of farming equipment availability • Limiting or loss of production • Deterioration of product quality
Mis-usage	This vulnerability allows the unauthorized use of the system equipment to perform criminal actions. • Botnets • Computers kidnapping • DDoS

This cybersecurity analysis task requires a good knowledge of possible risks and actual vulnerabilities for the individual system type. A list of possible risks and vulnerabilities examples, prepared and maintained by cybersecurity experts, will be a good support to perform the task. Recommended sources of such lists are collected in Table 4; most of them are accessible on the Internet.

Table 4. Cybersecurity risks and vulnerabilities list.

Process Flow Step	Description
NVD—NIST I-CAT vulnerability database [11]	The National Vulnerability Database (NVD) is the U.S. government repository of standards-based vulnerability management data Link: https://nvd.nist.gov/, accessed on 10 June 2021
SANS CIS [12]	The CIS Critical Security Controls recommends cyber defense measures Link: https://www.sans.org/critical-security-controls/, accessed on 10 June 2021
OWASP Top 10 [13]	The Open Web Application Security Project® (OWASP) provides recommendations to improve software security. Link: https://owasp.org/www-project-proactive-controls/, accessed on 10 June 2021
NIST I-CAT [14]	Vulnerability database of the National Institute of Standards and Technology (NIST) Link: https://nvd.nist.gov/general, accessed on 10 June 2021

The identified vulnerabilities must be documented in the cybersecurity assessment documentation. This expresses the detected weak points of the system architecture and represents the security analysis focus during the assessment process.

2.5.5. Security Aspect—Security Threats

During the high-level cybersecurity risk analysis, possible system threats are identified in contrast to operation environment and system architecture.

Definition of system threats:

A threat is the danger that system security can be reduced by exploiting a system vulnerability to produce system harm and system damage.

Definition from the standard IEC 62443-4-2/Chapter 3.1.43:

Security threats are sets of circumstances and associated sequences of events with the potential to adversely affect operations (including mission, functions, image, or reputation), assets, control systems or individuals via unauthorized access, destruction, disclosure, modification of data, and/or denial of service.

Table 5 lists well-known security threats discussed in the literature [15–23].

Table 5. Cybersecurity: security threats.

Threat	Explanation
Computer virus, malware	A computer virus will change the OS or other parts of operating software (malicious function). This can lead to improper system operation or system damage. Computer viruses affect system security and count as malware.
Rogue security software	This type of software mimics the presence of a computer virus to lead the user to pay money for virus removal software.
Trojan horse	A "Trojan horse" refers to tricking someone into inviting an attacker into a securely protected area.
Adware and spyware	Adware will track data from the computer use to get information of the user. In the most cases, adware is added to the computer by downloading software in consensus with the user. Spyware is added to the computer without consent or knowledge of the user. This can happen by malicious downloads from unsecure domains.
Ransomware	Ransomware is a type of malware which encrypts the user data to blackmail the user into paying money.

Table 5. *Cont.*

Threat	Explanation
Computer worm	A computer worm is a malicious program with the ability to replicate itself once it is run. The more and more powerful microcontroller performances used in the field and edge domain are rewarding targets for computer worms.
DoS and DDoS attack	These threat variants summarize network attacks to overload network resources to reduce operability: Denial of Service (DoS): attack from one computer to overload a target device by flooding this device with request packages in a high frequency. DDoS same as DoS, but the attack is performed by a synchronized cluster of computers. These clusters of computers and the high computing power are provided by manipulated kidnapped computers.
Phishing	This threat type obtains other people's personal data (e.g., password, credit card data) by using fake emails or websites.
Rootkit	A rootkit is a collection of software tools that are installed on the compromised system after breaking into a software system to prepare it for future undetectable access and to hide processes and files.
SQL injection attack	A vulnerability of SQL data bases, where an unauthorized person performs data and control manipulations in the case of weak access authentication and weak access checks and monitoring.
Man-in-the-middle attacks	This attack eavesdrops on the communication between two targets and may be used for several purposes: • Domain Name System (DNS) spoofing • HTTP Secure (HTTPS) spoofing • Internet Protocol (IP) spoofing • Secure Sockets Layer (SSL) hijacking • Wi-Fi hacking

2.5.6. Security Aspect: AP Factors

After the identification of possible system relevant security vulnerabilities and the possible cybersecurity threats, a combination of different attack potential factors will be determined to define the minimal necessary SL-T. The SL defines the rigor of the requirements and defines how robust the system is against attacks.

The following attack potential factors (Tables 6–11) are combined to define the security compromise level, which determines the minimal necessary SC-T. These are:

Table 6. Attack potential factor: motivation.

Range	Value	Description
Mistake	1	Causal or coincidental violations. Violation done by mistake
Low	2	Low violation motivation
Moderate	4	Moderate result target motivation
High	8	High result target motivation

Table 7. Attack potential factor: elapsed time.

Range	Value	Description
Months	1	The attack needs lots of time for preparation. The system provides a high protection level.
Weeks	2	
Days	4	
Hours	8	No or little time is necessary to get access to the system. The system provides a low protection level.

Table 8. Attack Potential Factor: Expertise/Skills.

Range	Value	Description
Ordinary person	1	Attacker has no special attack skills
Cybercrime, hacker, Competitors, malicious insider	2	Attacker has generic attack skills
Terrorist, professional thieves, Cybercriminals	4	Attacker has control system specific skills
Groups/nation-states, governmental organization	8	Attacker has control system specific skills and uses bespoken mechanisms

Table 9. Attack potential factor: expertise/skills.

Range	Value	Description
Public	1	Full public knowledge of specific target is available to perform the attack. Necessary skills are documented publicly.
Restricted	2	
Sensitive	4	
Critical	8	Extensive, nonpublic target knowledge and expertise are necessary to carry out the attack.

Table 10. Attack potential factor: access.

Range	Value	Description
Unlimited	1	Unlimited access to system, no security measures
Easy	2	
Moderate	4	
Difficult	8	Access to the system is very difficult due to security measures

Table 11. Attack potential factors: equipment.

Range	Value	Description
Standard	1	Only standard attack tools available to exploit vulnerabilities and to prepare attack
Adapted	2	Adapted standard attack tools available to exploit vulnerabilities and to prepare attack
Specialized	4	Specialized attack tools available to exploit vulnerabilities and to prepare attack
Bespoken	8	Bespoken attack mechanisms and tools are used to exploit vulnerabilities and to prepare attack

Motivation (MO)

The motivation factor states that an attack occurs coincidental by less motivation or is planned with a high successful result target.

Question: what level of motivation must be assumed for an attack to be carried out?

Elapsed Time (ET)

The amount of time required for an attacker to identify a specific potential vulnerability, develop an attack method, and maintain the effort required to perform the attack on the target. This factor states that the faster an attacker finds a vulnerability, the lower the protection is.

Question: how much time is required to get access to the system?

Expertise/Skills (ES)

Knowledge of the underlying principles or methods of a suitable attack.

Question: which expertise or skills does the attacker have?

Target Knowledge (TK)

Level of target technologies and knowledge needed to carry out the attack. But to perform an attack, the necessary tools are also needed.

Question: which target knowledge and tools does the attacker have?

Access (AC)

Access level of the target needed to carry out the attack.

Question: which access restrictions does the target system offer?

Equipment (EQ)

Knowledge and equipment to identify or exploit the vulnerability to prepare an attack. Question: which tools does the attacker have to perform the attack?

The sum of all attack potential values (AP value) gives a first cybersecurity assessment value which is used to determine the related SL, according to the IEC 62443 standard. In this assessment, the value ranges from 6–48. Table 12 gives the definition of the necessary protection and espionage requirements.

Table 12. Cybersecurity: AP value overview.

MO	ET	ES	TK	AC	EQ	AP Value
1	1	1	1	1	1	**AP sum = 1 . . . 6** Protection: only base security protection required.
2	2	2	2	2	2	**AP sum = 7 . . . 12** Protection against casual or coincidental violation. Espionage: prevent the unauthorized disclosure of information via eavesdropping.
3	3	3	3	3	3	**AP sum = 13 . . . 18** Protection against intentional violation using simple means, low resources, generic skills, and low motivation. Espionage: prevent the unauthorized disclosure of information to an entity actively searching for it using simple means with low resources, generic skills, and low motivation.
4	4	4	4	4	4	**AP sum = 19 . . . 24** Protection against intentional violation using sophisticated means, moderate resources, AACS specific skills, and moderate motivation. Espionage: prevent the unauthorized disclosure of information to an entity actively searching for it using sophisticated means with moderate resources, AACS specific skills, and moderate motivation.
8	8	8	8	8	8	**AP sum = 26 . . . 48** Protection against intentional violation using sophisticated means with extended resources, system specific skills, and high motivation. Espionage: prevent the unauthorized disclosure of information to an entity actively searching for it using sophisticated means with extended resources, AACS specific skills, and high motivation.

Attack Potential value overview

In a next step, the resulting AP value will be combined with the probability or likelihood that the attack will occur, which determines the severity of the attack risk.

2.5.7. Probability/Likelihood (PL)

The probability or likelihood value, which expresses if the attack occurs, is a further significant risk assessment factor for the security assessment process. Table 13 shows an example for a risk likelihood scale.

Table 13. Probability/likelihood of attack.

Range	Value	Description
Very high	11...12	Most likely to occur e.g., event occurred or is expected to occur within one to four months
High	9 . . . 10	Likely to occur e.g., event occurred or is expected to occur within 1 year
Moderate	6 . . . 8	Quite possible/not unusual e.g., event occurred or is expected to occur within 1 to 5 years
Low	3 . . . 5	Unusual/possible e.g., event occurred or is expected to occur within 5 to 10 years
Very Low	0 . . . 2	Conceivably possible but very unlikely to occur, e.g., event could occur at some time greater than 10 years

Questions: during which interval will an attack event occur?

2.5.8. Severity Level

The severity level defines the impact of a successfully performed attack on the system. Table 14 gives an example of a severity scaling.

Table 14. Severity levels.

Severity Level	Explanation
0/None	The attack has no impact
1/Low	A minor incident with low impact ● System operation interrupted but continues operation ● Incorrect operation by user
2/Medium	A minor incident with medium impact ● System operation interrupted and needs a manual restart and a system scan
3/High	A major incident with significant impact ● System operation failed ● Production data loss
4/Critical	A critical incident with very high impact ● Confidentiality or privacy is breached ● System operation failed, complete system recovery necessary

Questions: how serious is a successful attack on the system function?

2.5.9. Security Risk Matrix

Finally, the security risk matrix compares the risk severity with the attack probability/likelihood of an attack (as illustrated in Table 15).

Table 15. Cybersecurity: risk matrix.

Risk Value	**Probability/Likelihood of Attack (PL)**				
	Very Low 0...2	**Low 3 . . . 5**	**Moderate 6 . . . 8**	**High 9 . . . 10**	**Very High 11 . . . 12**
Severity					
0	0	0	0	0	0
1	≤2	≤5	≤8	≤10	≤12
2	≤4	≤10	≤16	≤20	≤24
3	≤6	≤15	≤24	≤30	≤36
4	≤8	≤20	≤32	≤40	≤48

Questions: how serious is a successful attack on the system function?

The table value is the product of the severity and the probability value.

The risk value is the product of the severity multiplied with the probability/likelihood.

$$Risk\ Value = Severity * PL \tag{1}$$

The AP value range 1–6 defines the tolerable risk, the risk where theoretically no protection is necessary. In this case, it is defined as the SL-0.

As already mentioned in Table 2, IEC 62443 defines five SLs, from SL-0 to SL-4, for different attack strengths and different protection requirements definitions.

In the high-level cybersecurity risk assessment phase, the resulting SL-T is defined. SL-T states the necessary SL to protect the underlaying SuC in a proper way.

To distribute the five SLs, SL-0 to SL-4, over the given attack potential range (AP values 0...48 from Table 12), the IEC 62443 standard defines the Cyber Risk Reduction Factor (CRRF) to support the mapping of the AP values to the SL values.

$$CRRF = \frac{\text{Risk}}{6} \tag{2}$$

The factor 6 denotes the value of the maximal tolerable risk (see the appointed green areas in Table 16).

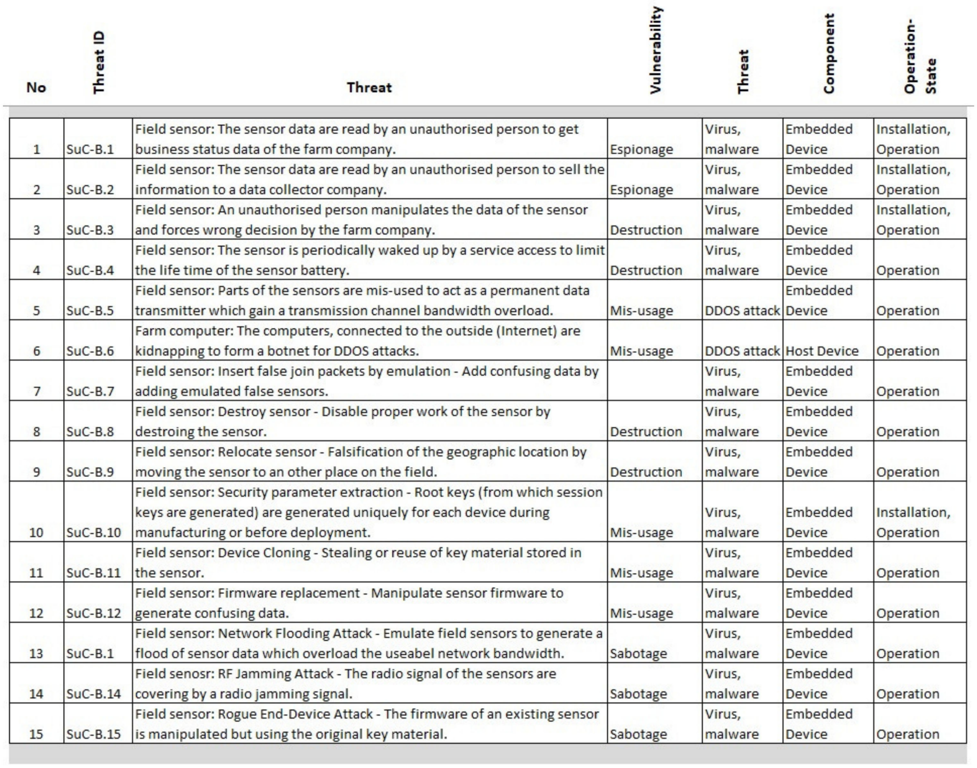
Table 16. Cybersecurity: AP value to SL mapping.

AP	CRRF	SL	AP	CRRF	SL	AP	CRRF	SL	AP	CRRF	SL
1	0.17	0	13	2.17	2	25	4.17	3	37	6.17	4
2	0.33	0	14	2.33	2	26	4.33	3	38	6.33	4
3	0.50	0	15	2.50	2	27	4.50	3	39	6.50	4
4	0.67	0	16	2.67	2	28	4.67	3	40	6.67	4
5	0.83	0	17	2.83	2	29	4.83	3	41	6.83	4
6	1.00	0	18	3.00	2	30	5.00	3	42	7.00	4
7	1.17	1	19	3.17	2	31	5.17	4	43	7.17	4
8	1.33	1	20	3.33	2	32	5.33	4	44	7.33	4
9	1.50	1	21	3.50	2	33	5.50	4	45	7.50	4
10	1.67	1	22	3.67	2	34	5.67	4	46	7.67	4
11	1.83	1	23	3.83	2	35	5.83	4	47	7.83	4
12	2.00	1	24	4.00	2	36	6.00	4	48	8.00	4

In this cybersecurity assessment example, 15 threats (as illustrated in Figures 5 and 6) are selected for the high-level risk analysis. In a real application, many more threats are dealt with, but here, only the process flow is shown, using examples with a reduced number.

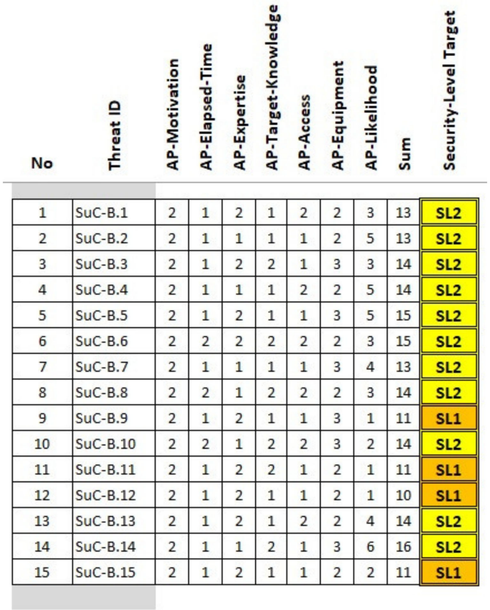
Gives an overview of 15 selected threat assessments according to the security aspects (A), (B), (C), and (D). The assessment ratings are drawn up in a voting round by security experts with appropriate experience. The sum of the assessment ratings of each threat defines the necessary SL (as illustrated in Table 2). The implementation and realization of the relevant security requirements enable the system to withstand cyberattacks in the estimated strength. The relevant security requirements are defined in IEC 62443 in seven requirements groups.

According to the results from the high-level cybersecurity assessment, the SL in the AFarCloud example is determined as SL-T = 2.



No	Threat ID	Threat	Vulnerability	Threat	Component	Operation-State
1	SuC-B.1	Field sensor: The sensor data are read by an unauthorised person to get business status data of the farm company.	Espionage	Virus, malware	Embedded Device	Installation, Operation
2	SuC-B.2	Field sensor: The sensor data are read by an unauthorised person to sell the information to a data collector company.	Espionage	Virus, malware	Embedded Device	Installation, Operation
3	SuC-B.3	Field sensor: An unauthorised person manipulates the data of the sensor and forces wrong decision by the farm company.	Destruction	Virus, malware	Embedded Device	Installation, Operation
4	SuC-B.4	Field sensor: The sensor is periodically waked up by a service access to limit the life time of the sensor battery.	Destruction	Virus, malware	Embedded Device	Operation
5	SuC-B.5	Field sensor: Parts of the sensors are mis-used to act as a permanent data transmitter which gain a transmission channel bandwidth overload.	Mis-usage	DDOS attack	Embedded Device	Operation
6	SuC-B.6	Farm computer: The computers, connected to the outside (Internet) are kidnapping to form a botnet for DDOS attacks.	Mis-usage	DDOS attack	Host Device	Operation
7	SuC-B.7	Field sensor: Insert false join packets by emulation - Add confusing data by adding emulated false sensors.		Virus, malware	Embedded Device	Operation
8	SuC-B.8	Field sensor: Destroy sensor - Disable proper work of the sensor by destroing the sensor.	Destruction	Virus, malware	Embedded Device	Operation
9	SuC-B.9	Field sensor: Relocate sensor - Falsification of the geographic location by moving the sensor to an other place on the field.	Destruction	Virus, malware	Embedded Device	Operation
10	SuC-B.10	Field sensor: Security parameter extraction - Root keys (from which session keys are generated) are generated uniquely for each device during manufacturing or before deployment.	Mis-usage	Virus, malware	Embedded Device	Installation, Operation
11	SuC-B.11	Field sensor: Device Cloning - Stealing or reuse of key material stored in the sensor.	Mis-usage	Virus, malware	Embedded Device	Operation
12	SuC-B.12	Field sensor: Firmware replacement - Manipulate sensor firmware to generate confusing data.	Mis-usage	Virus, malware	Embedded Device	Operation
13	SuC-B.1	Field sensor: Network Flooding Attack - Emulate field sensors to generate a flood of sensor data which overload the useabel network bandwidth.	Sabotage	Virus, malware	Embedded Device	Operation
14	SuC-B.14	Field senosr: RF Jamming Attack - The radio signal of the sensors are covering by a radio jamming signal.	Sabotage	Virus, malware	Embedded Device	Operation
15	SuC-B.15	Field sensor: Rogue End-Device Attack - The firmware of an existing sensor is manipulated but using the original key material.	Sabotage	Virus, malware	Embedded Device	Operation

Figure 5. Cybersecurity risk analysis table, Part A.



No	Threat ID	AP-Motivation	AP-Elapsed-Time	AP-Expertise	AP-Target-Knowledge	AP-Access	AP-Equipment	AP-Likelihood	Sum	Security-Level Target
1	SuC-B.1	2	1	2	1	2	2	3	13	SL2
2	SuC-B.2	2	1	1	1	1	2	5	13	SL2
3	SuC-B.3	2	1	2	2	1	3	3	14	SL2
4	SuC-B.4	2	1	1	1	2	2	5	14	SL2
5	SuC-B.5	2	1	2	1	1	3	5	15	SL2
6	SuC-B.6	2	2	2	2	2	2	3	15	SL2
7	SuC-B.7	2	1	1	1	1	3	4	13	SL2
8	SuC-B.8	2	2	1	2	2	2	3	14	SL2
9	SuC-B.9	2	1	2	1	1	3	1	11	SL1
10	SuC-B.10	2	2	1	2	2	3	2	14	SL2
11	SuC-B.11	2	1	2	2	1	2	1	11	SL1
12	SuC-B.12	2	1	2	1	1	2	1	10	SL1
13	SuC-B.13	2	1	2	1	2	2	4	14	SL2
14	SuC-B.14	2	1	1	2	1	3	6	16	SL2
15	SuC-B.15	2	1	2	1	1	2	2	11	SL1

Figure 6. Cybersecurity risk analysis table, Part B.

2.5.10. Impact Value

After the estimation of the SL, the severity and impact of an attack are quantified in the next step.

Tables 17–20 define the impact values for system safety, the financial situation, the operational behavior, and the system/components' effects in case a cybersecurity attack takes place. Table 21 lists the impact level ranges.

Table 17. Cybersecurity: severity (impact) value—safety.

Severity Level	Impact Level	Description	Impact Value
4	Destruction/ Catastrophic	A malfunction or a system failure leads to life-threatening injuries, fatal injuries, or extreme (catastrophic) environmental damage	2000
3	Severe/ Critical	Serious and life-threatening injuries or major environmental damage. Damage is critical for proper safe operation.	200
2	Damage/ Medium	Slight and moderate injuries or minor/medium environmental damage.	20
1	Save/ Insignificant	No injuries. Safety insignificantly lowered.	0

Table 18. Cybersecurity: severity (impact) value—financial.

Severity Level	Impact Level	Description	Impact Value
4	Destruction/ Catastrophic	Financial damages threatening existence and/or the incident will lead to legal proceedings against the company; a serious impact on the public image (reputation) of the company	1000
3	Severe/ Critical	Significant financial damages, but which do not threaten existence, and/or the incident can have a serious impact on the public image (reputation) of the company	100
2	Damage/ Medium	Unwanted financial damage and/or the incident may have an impact on the public image (reputation) of the company	10
1	Safe/ Insignificant	No financial or intolerable damage	0

Table 19. Cybersecurity: severity (impact)—operational.

Severity Level	Impact Level	Description	Impact Value
4	Destruction/ Catastrophic	Component (e.g., tractor, service) unusable; one or more fundamental functions are affected. The use of component is impractical.	1000
3	Severe/ Critical	Component (e.g., tractor, service) service or maintenance required; an important function is out of order. The component can only be used with restrictions.	100
2	Damage/ Medium	Component (e.g., tractor, service) comfort affected. The component can be used with certain restrictions	10
1	Safe/ Insignificant	No relevant effect, most of the time, an unimportant function is affected and the component (e.g., tractor, service) can be used without restrictions.	0

Table 20. Cybersecurity: severity (impact) value—system/component.

Severity Level	Impact Level	Description	Impact Value
4	Destruction/ Catastrophic	A strong impairment leads to a total failure of the system/function with a possible destruction of the system.	1000
3	Severe/ Critical	A strong impairment leads to a significant disturbing of the system/function operation with a partly possible destruction of the system.	100
2	Damage/ Medium	A system/function damage is detectable but will not influence the system/function operation. A low reduction of the system/function performance is noticeable.	10
1	Safe/ Insignificant	No damages of the system or the functions are noticeable or visible.	0

Table 21. Cybersecurity: impact levels.

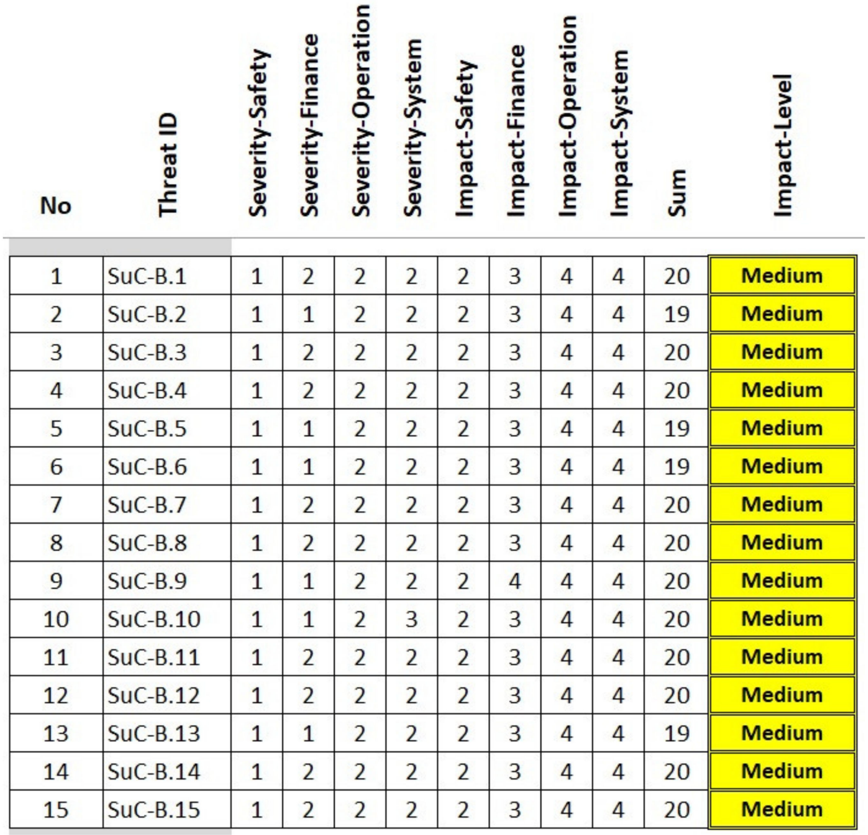
∑ Impact Values	Impact Level
>200	Catastrophic
31–200	Critical
6–30	Medium
0–5	Insignificant

$$\sum \text{ImpactValue} = \text{IV}(S) + \text{IV}(F) + \text{IV}(O) + \text{IV}(SY) \tag{3}$$

Legend: Impact Value = IV, Safety = (S), Financial = (F), Operational = (O), System = (SY)

To reduce the impact, a change of the system architecture can be adequate. As an example, reducing the number of external communication interfaces into the system or reducing the number of communication protocols used helps to strengthen the system against attacks. According to the risk matrix, all medium, critical, and catastrophic effects must be avoided by adding suitable cybersecurity measures, since the risk is unacceptable regardless of the probability value.

The following values were estimated for the example sub-SuC (as illustrated in Figure 7).



No	Threat ID	Severity-Safety	Severity-Finance	Severity-Operation	Severity-System	Impact-Safety	Impact-Finance	Impact-Operation	Impact-System	Sum	Impact-Level
1	SuC-B.1	1	2	2	2	2	3	4	4	20	Medium
2	SuC-B.2	1	1	2	2	2	3	4	4	19	Medium
3	SuC-B.3	1	2	2	2	2	3	4	4	20	Medium
4	SuC-B.4	1	2	2	2	2	3	4	4	20	Medium
5	SuC-B.5	1	1	2	2	2	3	4	4	19	Medium
6	SuC-B.6	1	1	2	2	2	3	4	4	19	Medium
7	SuC-B.7	1	2	2	2	2	3	4	4	20	Medium
8	SuC-B.8	1	2	2	2	2	3	4	4	20	Medium
9	SuC-B.9	1	1	2	2	2	4	4	4	20	Medium
10	SuC-B.10	1	1	2	3	2	3	4	4	20	Medium
11	SuC-B.11	1	2	2	2	2	3	4	4	20	Medium
12	SuC-B.12	1	2	2	2	2	3	4	4	20	Medium
13	SuC-B.13	1	1	2	2	2	3	4	4	19	Medium
14	SuC-B.14	1	2	2	2	2	3	4	4	20	Medium
15	SuC-B.15	1	2	2	2	2	3	4	4	20	Medium

Figure 7. Cybersecurity impact analysis table.

In this example, the impact analysis indicated "Damage/Medium" impact levels.

At the end of the "High level cybersecurity risk analysis" process step, the SL-T is defined. For the AFarCloud example, it is level 2 (SL-T = 2), and the impact level is set to "Damage/Medium". Cybersecurity risks are evident. It is strongly recommended to take appropriate security measures.

In the next process step, the SuC is prepared for a detailed cybersecurity analysis. For this task, the SuC is split in zones and conduits.

2.6. Process Step: Split in Zones and Conduits

IEC 62443 defines security zones as "groups of physical or logical assets that share common security requirements, which have clearly defined borders (physical or logical)". The zones are connected by so called conduits. A conduit includes necessary security measures to: (a) control the access to the conduit; (b) resist denial of service attacks; and, (c) prevent the spreading of any type of attacks. The conduit works as a shield for the succeeding zone and protects the integrity and confidentiality of communications.

Each zone implies an objective SL, derived from the SL-T. After a security analysis, the components of the zones and conduits must offer a SL-C. The SL-C must be equal or higher than the SL-T. If it is less, the detected security gap must be compensated for by including additional security measures. These improvements of the zones and the conduits are done until no security gap remains after the detailed cybersecurity risk analysis.

As shown in Figure 8, IEC 62443 gives hints on how to compensate the gap with extending the cybersecurity measures requirements. A conduit can be improved with appropriate security measures (e.g., a firewall), the SL-T of the subsequent zones, even when the SL-C of the desired zone has a lower value. In the above example, the farm zone is embedded by the conduits on the left and right side, which provide the SL-C with level 2. But this zone embedding must be performed with care because in a future zone extension, additional communication links are added (for example, by connecting unsecure wireless communication devices to the zone), and thus, a security weak point can be opened. Generally, it is always better to secure the system with a high level of security. The zone embedding can be usefully and appropriate in a SL-4 system to enable the use of components with a more or less SL or, on the other hand, this method can be used to protect old legacy systems, where an improvement or exchange of the existing devices will be not feasibly.

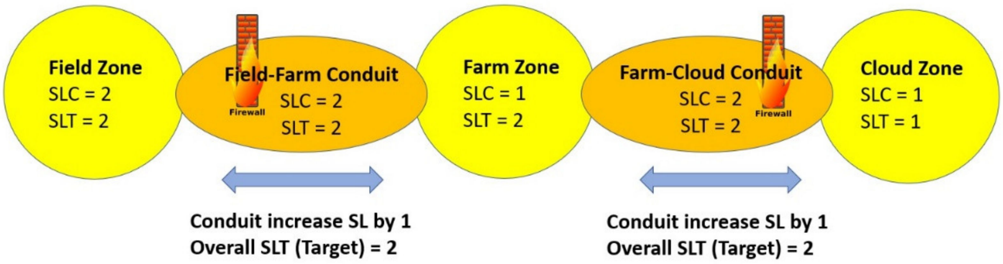


Figure 8. Zones and conduits concept with a zone embedding example.

Figure 9 shows the system split of the soil sensor sub-SuC. Zone embedding is not used in this example.

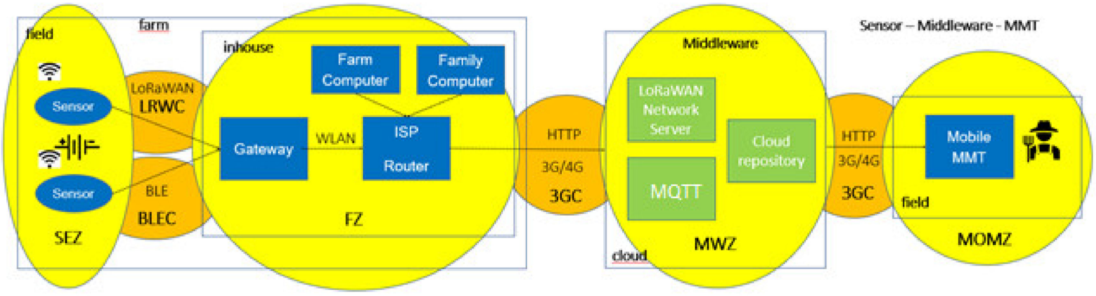


Figure 9. Zones and conduits of soil-sensor sub-SuC.

There are four zones with different security criticalities defined according to different threat types. The zones are aligned with the areas of the system architecture and are interconnected by four data communication links with different communication protocols.

A first approach to improve the security is to reduce the number of data communication links (conduits), but in this case it will not be possible. Table 22 summaries the designations and abbreviations of the zones and conduits.

Table 22. Sub-SuC: Zone/Conduit Overview.

Zone/Conduit	Description
SEZ	Sensor Zone
FZ	Farm Zone
MWZ	Middleware Zone
MOMZ	Mobile MMT Zone
LRWC	LoRaWAN Conduit
BLEC	Bluetooth Low Energy Conduit
3GC	3G Conduit

2.7. Process Step: Detailed Cyber Risk Analysis

Each zone and conduit are subject to a detailed analysis of the fulfilment of specified requirements given by the cybersecurity standard IEC 62443.

These requirements are grouped in seven foundational requirements, as listed in Table 23.

Table 23. Foundational requirements.

FR 1: Access Control (AC)	Identify and authenticate AACS (Agriculture Automation Control System) users by mechanisms which protect against intentional unauthorized access by entities using simple means • Password and user authentication requirements ➔ 13 system requirements/11 requirement enhancements
FR 2: Use Control (UC)	Restrict use of the system or assets according to specified privileges to protect against circumvention by entities using simple means. • Mapping of roles in the management process requirements • System use policy requirements ➔ 12 system requirements/12 requirement enhancements
FR 3: System Integrity (SI)	Protect the integrity of information in the system against manipulation by someone using simple means. • Session handling, cryptography, recognize changes requirements ➔ 9 system requirements/10 requirement enhancements
FR 4: Data Confidentiality (DC)	Prevent the dissemination of information to an entity actively searching for it using simple means. • Encryption requirements • End to end data encryption requirements ➔ 3 system requirements/3 requirement enhancements
FR 5: Restricted Data Flow (RDF)	Prevent the intended circumvention of zone and conduit segmentation systems by entities using simple means. • Less connectivity requirements • Network segmentation requirements ➔ 4 system requirements/7 requirement enhancements
FR 6: Timely Response to Events (TRE)	Monitor the operation of the system and respond to incidents when they are discovered by actively collecting forensic evidence from the system • Event/Action Logging requirements • Monitoring requirements • Anomaly/Inconstancy detection requirements ➔ 2 system requirements/1 requirement enhancements
FR 7: Resource Availability (RA)	Ensure that the system operates reliably under normal and abnormal production conditions and prevents denial-of-service situations by entities using simple means. • System backup requirements • System recovery requirements ➔ 8 system requirements/5 requirement enhancements

Each foundational requirement group consists of additional subrequirements. There are more than 50 system requirements with additional requirement enhancements defined by the IEC 62443 standard. The higher the SL, the more requirement enhancements are defined and must be implemented to satisfy the dedicated SL. Each system requirement must be fulfilled by the defined zones and the conduits of the SuC. A detailed security analysis is a very time-consuming task, especially for large systems.

Figure 10 gives a graphical overview of the numerous system requirements grouped around the foundational requirements. Moreover, it can also be used for a quick and clear PASSED/FAILED status display of a system element. For PASSED the appropriate cell is in green, for FAILED it is in red.

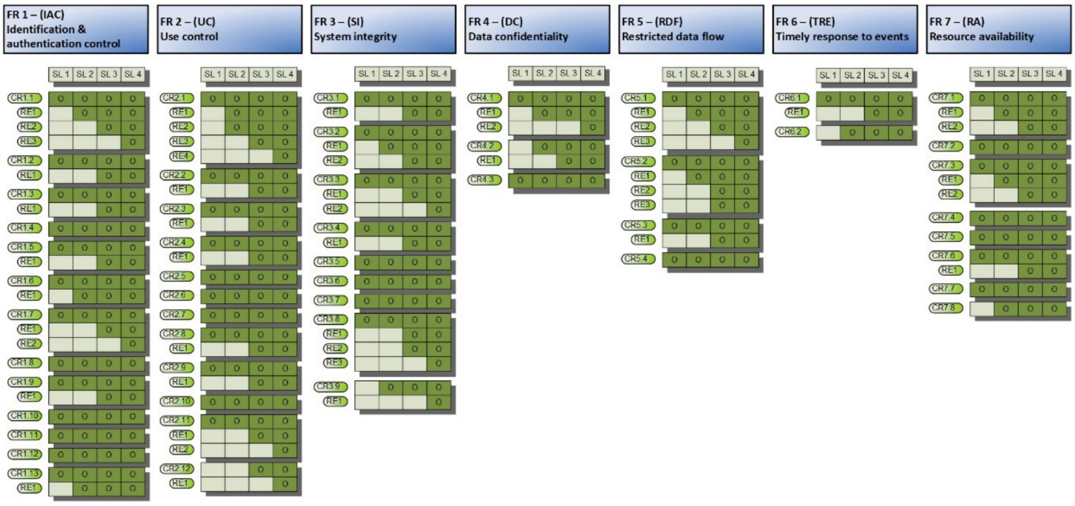

FR 1 – (IAC) Identification & authentication control
FR 2 – (UC) Use control
FR 3 – (SI) System integrity
FR 4 – (DC) Data confidentiality
FR 5 – (RDF) Restricted data flow
FR 6 – (TRE) Timely response to events
FR 7 – (RA) Resource availability
SL 1
SL 2
SL 3
SL 4

Figure 10. IEC 62443 system requirements overview.

2.8. *Process Decision: Tolerable Risk Estimation*

There are four SLs defined to classify risks, as shown in Table 2. The tolerable risk is expressed with the SL-T. Additionally, there are two further SL types defined, to document the result of the security assessment process. The SL types are explained in more detail in the following.

Cyber SL Types

To obtain a comparable result for the assessment, three types of SL are defined, which document the “Target”, “Capability”, and “Archived” levels (Source: IEC 62443-3-2):

- Security Level Target (SL-T) is the desired level of security for the identified SuC, usually determined by a risk assessment with the goal of identifying which security protection is needed to ensure correct system operation. This level is determined in the “high level cybersecurity risk analysis” phase of the cybersecurity assessment process.
- Security Level Achieved (SL-A) is the actual level of security for the SuC, which can be measured after the system concept and design are available. The purpose is to verify that the SL-A is identical to or higher than the SL-T.
- Security Level Capability (SL-C) is the presentation of the provided SLs by all system components when properly configured and integrated. SL-C expresses the need of cybersecurity improvements with additional compensating countermeasures to achieve the determined SL-T when SL-C < SL-T.

The SL-T to SL-A relationships can be figured out in graphical representations, as shown in Figures 11 and 12. These are two examples that express the relationship between two SL types in a fast and meaningful way to document the system security status.

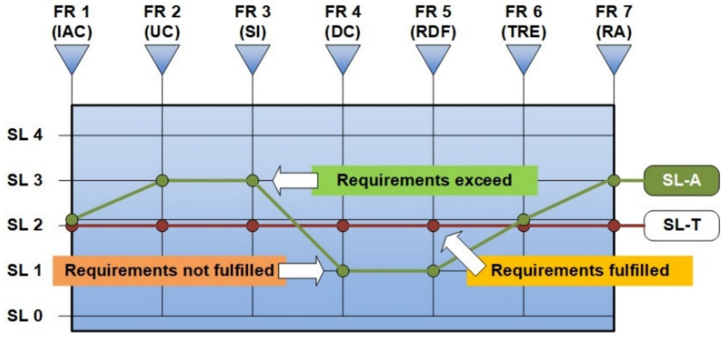


Figure 11. SL-T to SL-A relationship graph diagram.

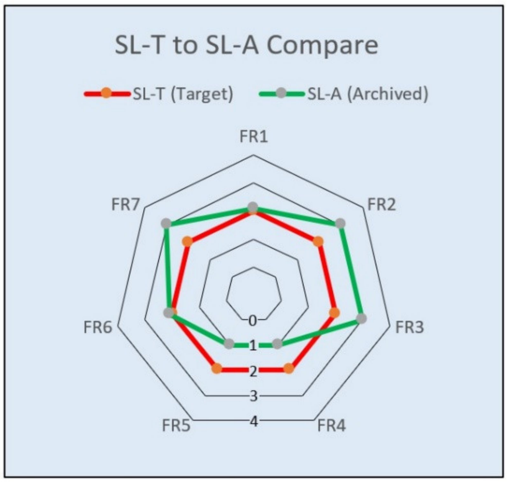


Figure 12. SL-T to SL-A relationship spider diagram.

The diagrams show briefly whether the expected target SL-T was met or whether additional improvements are necessary.

2.9. Process Step: Documentation, Requirements Fixing, Recommentations

2.9.1. Documentation

A cybersecurity certification needs good and complete cybersecurity assessment documentation. Some of the necessary documents are already created in the previous process steps. Finally, the following documents close the cybersecurity assessment documentation work: listing of all system relevant requirements (depending on the appointed SL), definition of test cases, test result documentation to verify the correct and complete requirements integration, list of necessary security countermeasures, and security recommendations which must be implemented.

2.9.2. Requirements

As an example, in the following paragraph an excerpt of three requirements definitions from the FR1 (Access Control AC) requirement group is shown. Note that the line "belongs to the zones/conduits" defines for which system elements the requirement is specified. The vulnerability was identified in the "high level cybersecurity risk analysis" phase.

- **(FR1-AC)**: The system shall provide functions to uniquely identify and authenticate all users, restricting access for unauthorized people.

Vulnerability	A system interface without user identification and authentication allows unrestricted access by anyone and from anywhere.					
Countermeasure	Use at least a single-factor authentication mechanism with username and password.					
System	The Farm Management System (FMS) access should require a user username/password. A MQTT broker should use a username/password protection mechanism					
Belongs to the zones/conduits	SEZ	FZ	MWZ	MOMZ	LRWC	BLEC

This requirement means that access to the system may only be possible with authentication via user name/password.

- **(FR 1-AC)**: The user credentials shall be restricted in format and length

Vulnerability	A simply structured password can be guessed by an attacker by trying.					
Countermeasure	Using a password setup check: a minimal length (8), a mix of letters, numbers, and special characters.					
System	Password length should be eight characters long, including lowercase & uppercase alphabetic characters, numbers, and symbols.					
Belongs to the zones/conduits	SEZ	FZ	MWZ	MOMZ	LRWC	BLEC

This requirement states that only a certain form of password must be used, and this must be checked.

- **(FR1-AC)**: The number of failed login attempts in a time period (e.g., 24 h) shall be limited to 3 tries.

Vulnerability	The attacker guesses the password with a brute force attack.					
Countermeasure	Using a login attempt statistic counter.					
System	After three wrong authentication attempts, the system should prohibit further inputs for a time of 24 h.					
Belongs to the zones/conduits	SEZ	FZ	MWZ	MOMZ	LRWC	BLEC

This requirement defines the use of a login attempt counter to prevent trying to guess the password.

An important part of the requirements definition work is also to design adequate and executable test cases to verify the requirements implementation. This part is often done as the last work in the full process life cycle, but this requires much additional time and must be prepared very carefully. The effort required is easily underestimated but note that these tests must be repeated in the event of a system change. Then, an existing and well-prepared test environment does the job with one mouse-click. Also, the cybersecurity reassessment for recertification is done quickly.

2.10. Recommendations

Finally, a few additional suggestions for the security implementation should be made.

- Network segmentations Isolate the business IT components from the privately used IT environment by using routers with activated firewalls.
- Using a business and a private cellular phone Consider using a separate business cellular phone with carefully selected and necessary business relevant apps only. This also protects your business partners if the private mobile phone has been spied on and compromised by an app.
- Zero trust
  Zero trust (ZT) defines a paradigm shift. Up to now, cybersecurity protection was done with a "perimeter-based" approach, where the protection was ensured to the company boundaries by applying network segmentation, intrusion detection, restricted network access, and so on. ZT is a purely "data-centric" security approach. Following the security principle "Do not trust anyone, verify everyone", the principle of ZT follows the granular approach of checking each individual data flow for trustworthiness. As an example: the MQTT (Message Queuing Telemetry Transport) protocol requires

data encryption with an asymmetrical keys and certificates and the transmission of user credentials for each data message. This gives this data transmission protocol a high level of data integrity and data security.

- Demilitarized Zone
  Another way to improve the local IT security is to define a so-called demilitarized zone (DMZ). The DMZ is isolated from the Internet (WAN) by a firewall and from the company internal network (Intranet, LAN) by an additional firewall. This isolation from both WAN and LAN provides a high level of protection and complete control over who can access the DMZ. As a result, a single vulnerability does not immediately compromise the DMZ. Ideally, the two firewalls are from different sources, since otherwise a single known vulnerability would be sufficient to overcome both firewalls.

3. Results

In the future, for modern agriculture, new types of IT tasks and new technology challenges await the farm company management and staff.

One significant challenge will be the responsibility for security measures. Refer to the agriculture architecture in Figure 1; for Levels 1 and 2, the asset owner has full control over the installed security measures to harden the system against cybersecurity attacks. For Levels 3 and 4, the asset owner can only perform an accurate provider selection and must trust that the defined security specifications are fulfilled.

The asset owner has no influence over the security conditions of the services; he can only request security certificates and must trust the service provider with compliance with the duty of caution. Unfortunately, from time-to-time, one hears about cyberattacks against service providers in which private customer data was stolen.

A further point of discussion in security and privacy are the questions of where data are stored by global active service providers operating remotely located, cloud-based data repositories and service farms.

Continuous security monitoring is the only measure the asset owner can perform to increase confidence. This is a requirement that is feasible and may be performed by large and medium-sized farm companies. If small farm companies are not able to perform security assessments by themselves, they need support and consultation from their professional associations to reach a level of security and privacy so that the company can work trouble-free. The external security service provider can support their customers with actual cybersecurity threats and appropriate security measures. Today, it is not feasible for small and maybe some medium-size farm companies to manage the necessary security monitoring in an increasingly digitalized agriculture world. Further research and adapted business structures must be developed to support and ensure secure operation.

Another significant challenge is the big difference between IACSs, as illustrated in Figure 3, and the agriculture architecture, illustrated in Figure 1. In an IACS environment, in the most cases, field components at level 1 are housed inside the factory buildings and are basically well-protected against direct physical access attacks. Malfunctions and manipulation can only be carried out if one breaks into the building to gain access, but that already shows high motivation and criminal intent. Also, direct supervision is easy installable in a factory building; however, in the agriculture domain, according to Figure 1, the field elements are mostly far away from the farm building, and the components are more vulnerable to manipulation, destruction, and risk of theft. Due to networking and widely distributed production facilities in modern agriculture environments, especially for Layer 1 and Layer 2, new points of attack were added, which make it easier for attackers to penetrate the production facility, manipulate it, and even impair machine safety.

Nowadays, employees who are not IT experts also have to deal with potential security threats. Therefore, it is necessary to carry out a comprehensive security risk assessment of the entire system, both from IT and from OT, to ensure an adequate SL.

4. Study Results

The above results mean that the components in Layer 1 and Layer 2 need additional protective measures. In the AFarCloud project, a conceptual prototype of an improved soil sensor protection concept is demonstrated to show solutions that manipulations are detected immediately, and the theft of field components is made pointless when they are not reusable outside of a defined area by a non-resettable protection measure.

The conceptual prototype, named SED (Security Evaluation Demonstrator) [24], is built around a standard soil sensor, which utilizes Long Range Wide Area Network (LoRaWAN) communication technology to transfer the field data wireless to a data gateway. From here the data are transported via an Internet connection by using the Message Queuing Telemetry Transport (MQTT) network protocol via the cloud-based AFarCloud Middleware (MW) to the cloud data repository.

Figure 4 shows the block diagram of the SED, which was built with real hardware to verify the implemented security improvements. If LoRaWAN and MQTT already bring a lot of data security features, the sensor has been upgraded with a Hardware Secure Module (HSM) and additional monitoring sensors, like GPS, which detects unauthorized movements of the device. The HSE is a non-manipulatable cryptographic device which manages cryptographic key storage and protects the sensor firmware. Figure 13 shows the SED sensor hardware without the case; such a sensor represents the most vulnerable part of an outdoor field device.

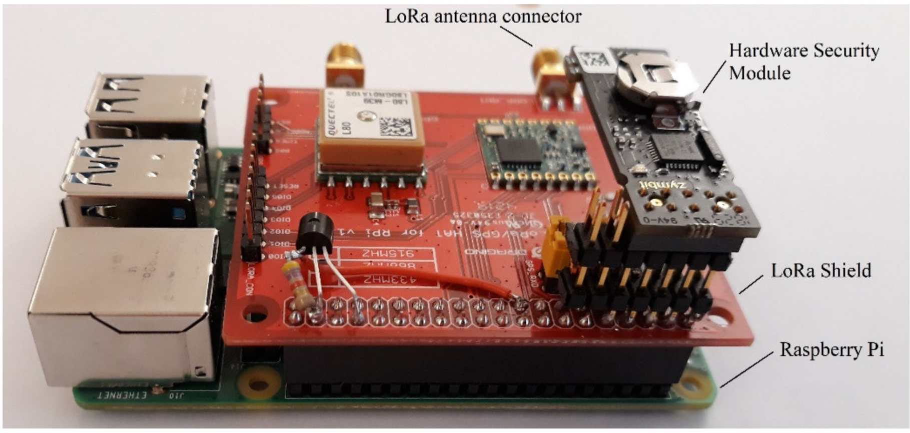


Figure 13. SED sensor hardware without case.

The SED prototype is based on a Raspberry-Pi single-board computer with an attached LoRa shield, which also carries the GPS receiver. The HSM is plugged into the expansion bus. In a commercial sensor all components are embedded on a single electronic board, ideally all integrated on a semiconductor chip. The environmental sensors (temperature, humidity, etc.) are also connected to the expansion bus.

The SED prototype demonstrates extended security functions for future outdoor field devices. It provides security measures for:

- Detect unauthorized moving of the sensor
- Ensure physical integrity of the sensor, e.g., open the case
- Inhibit unauthorized reuse of manipulated sensor, prevent firmware manipulation
- Prevent sensor communication data manipulation
- Notification on low battery

Each detected manipulation or irregular operation generates an alarm or a notification messages, which informs immediately selected users.

The verification results of the above listed security functions are descripted in detail in the [25].

Finally, all employees must be adequately trained in security issues when they operate with field elements which need security authentication for installation and maintenance.

5. Discussion

The following questions need to be discussed, and answers can be found by further research. Additional threat analysis work is necessary to identify existing and new vulnerabilities in agriculture.

What are the special vulnerabilities and cyber threats in agriculture that are not known and covered in this form by the IACS domain experience? The answer to this question defines (a) the need of a totally new cybersecurity standard for agriculture or (b) indicates that adaptions and extensions of already well-known cybersecurity standards will be sufficient. From our point of view, a dedicated cybersecurity standard for agriculture will be necessary, because of the totally different security conditions on the field segment and the farm segment in comparison to that of the security situation, provided by a well observable plant building.

The future problem is not the theft of a single field device and its subsequent manipulation for cybercriminal activities. Much more, there will be many IoT devices in the field in future installations which offer an attractive base for botnets. Because even the simplest sensor will contain a powerful processor with its own OS and extensive additional functions, these field IoT devices will require periodic software updates, which can be carried out using Over-the-Air (OTA) programming techniques.

Using Single Sign-On (SSO), Multi-Factor Authentication (MFA), and access broker structures to hide the real data storage location. An access broker reduces the attack surface to a very restricted system access port. A well-established approach of such a data access philosophy is provided by the MQTT protocol, which supports a publish-subscribe network protocol. The data exchange is only possible via an access broker, which authorizes the data traffic and monitors the data flow (intrusion detection).

6. Conclusions

After two years of project work and research in the field of cybersecurity for agriculture, the following insights were gained: nowadays, standardization in agriculture contains only a few standards and regulations to control the use of pesticides, to secure the use of heavy machinery without damage and injuries, and to require animal-friendly treatment of farm livestock.

One thing we learned from the first two years of the project is that the safety standards for agriculture mainly concern the area of food and nutrition safety, but so far, no specific IT/OT safety standards were defined for the agriculture specific architecture. In the Industrial Automation Control System (IACS) and in the automotive domain, there are cybersecurity standards that guide the system responsible to provide a safe operating condition. Some of these regulations can be applied (transferred) directly to agricultural electronic systems. In the communication area, there are some ETSI standards from the area of Machine-to-Machine (M2M) communication with expansions for interaction with agricultural machines, such as the ISOBUS [26].

There is a need to define cybersecurity guidelines for modern agriculture (Agriculture 4.0) in the European Union (EU), like those developed for industrial control systems. In the USA, the United States Department of Homeland Security (DHS) [27] carried out research during the last years to identify potential cybersecurity vulnerabilities for agriculture; in Europe, however, no similar investigation occurred. The document "European Cybersecurity Centres of Expertise Map—Definitions and Taxonomy" [28], focuses on many industries to show the risks and the need of monitoring support to ensure cybersecurity, but the modern agriculture domain is not included. Even in the EU publication entitled "Study on risk management in EU agriculture" [29], from Q4 2017, smart farming and cybersecurity are not mentioned.

7. Outlook

The work for cybersecurity in agriculture will continue in the last year of the project with a focus on a Security Evaluation Demonstrator (SED) to show the different security vulnerabilities and adequate improvements, achieved in both hardware and software, to demonstrate the security concept on a simple sensor node. The implementation examples avoid most cybersecurity vulnerabilities and provide a fast-responding sensor manipulation monitoring system.

A new proposal (NP) or a preliminary work item (PWI) is planned to start an initiative for a future agriculture cybersecurity standard.

Finally, the research results, cybersecurity assessment and analysis methodologies, requirements, and security recommendations will be collected in a publication, such as this one, which could be a useful cybersecurity guide for the agriculture domain.

8. Acronyms and Definitions

Acronym	Definition
AACS	Agriculture Automation Control Systems
AC	Access Control—an IEC 62443 term
ANSI	American National Standards Institute
AP	Attack Potential
AS	Asset Owner
BLE	Bluetooth Low Energy—Communication standard
BTS	Base Transceiver Station—Equipment of the telephone provider to establish a network
CRRF	Cyber Risk Reduction Factor
CNH	CNH Industrial N.V. is an Italian-American multinational company group
	Component Requirement—an IEC 62443 term
CSM	Cybersecurity Management
DC	Data Confidentiality—an IEC 62443 term
DCS	Distributed Control System
DDoS	Distributed Denial of Service—A type of a cybersecurity attack
DDS	Data Distribution Service—Function, which coordinates the data distribution in the middleware
DMZ	DeMilitarized Zone
DNS	Domain Name System
DoS	Denial of Service—A type of a cybersecurity attack
DSS	Decision Support System—Function, which derives decision by analyzing existing field data
FMS	Farm Management System
FR	Foundational Requirement—an IEC 62443 term
GPS	Global Positioning System
HSE	Hardware Secure Element
HMI	Human Machine Interface
HW	Hardware
HTTP(S)	Hypertext Transfer Protocol (Secure)—Communication protocol
IACS	Industrial Automation Control Systems
IAP	Industrial Automation Process
IEC	International Electrotechnical Commission
IoT	Internet of Things
IP	Intellectual Property
ISA	International Society for Automation
ISP	Internet Service Provider
IT	Information Technology
L-AC	Large Agriculture Company
LoRaWAN	Long Range Wide Area Network
M-AC	Medium Agriculture Company

Acronym	Definition
MITM	Man-in-the-Middle—A type of a cybersecurity attack
MMT	Mission Management Tool
MOD	Masses of Data
MQTT(S)	Message Queuing Telemetry Transport (Security)—Communication protocol
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database
OT	Operation Technology
OWASP	Open Web Application Security Project
PLC	Programmable Logic Controller
PS	Product Supplier
RA	Resource Availability—an IEC 62443 term
RDF	Restricted Data Flow—an IEC 62443 term
S-AC	Small Agriculture Company
SED	Security Evaluation Demonstrator
SI	System Integrator
SI	System Integrity—an IEC 62443 term
SIS	Safety Instrumented System
SL-A	Security Level—Archived
SL-C	Security Level—Capability
SL-T	Security Level—Archived
SSL	Secure Sockets Layer—Communication protocol
SW	Software Level—Target
SuC	System under Consideration—The system which is defined for the assessment and analysis
TL(S)	Transport Layer (Security)—Communication Protocol
TRE	Timely Response to Events—an IEC 62443 term
UC	Use Control—an IEC 62443 term
WAN	Wide Area Network
ZT	Zero trust

Author Contributions: Conceptualization, E.K. and R.K.; methodology, E.K. and R.K.; software, E.K.; validation, E.K., R.K., V.H.D. and P.C.; formal analysis, E.K.; investigation, E.K.; resources, E.K., R.K., V.H.D. and P.C.; data curation, E.K. and R.K.; writing—original draft preparation, E.K. and R.K.; writing—review and editing, V.H.D.; visualization, E.K. and R.K.; supervision, E.K., R.K., V.H.D. and P.C.; project administration, E.K., R.K., V.H.D. and P.C.; submission, E.K., R.K., V.H.D. and P.C.; funding acquisition, E.K., R.K., V.H.D. and P.C. All authors read and agreed to the published version of the manuscript.

Funding: This work received funding from AFarCloud, which is an ECSEL Joint Undertaking (JU) project under grant agreement No 783221. The JU receives support from the European Union's Horizon 2020 research and innovation program and Austria, Belgium, Czech Republic, Finland, Germany, Greece, Italy, Latvia, Norway, Poland, Portugal, Spain, and 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).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. International Electrotechnical Commission. *IEC 62443-1-1, Industrial Communication Networks–Network and System Security–Part 1-1: Terminology, Concepts and Models*; International Electrotechnical Commission: Geneva, Switzerland, 2009.

2. International Electrotechnical Commission. *IEC 62443-2-1, Industrial Communication Networks–Network and System Security–Part 2-1: Establishing an Industrial Automation and Control System Security Program*; International Electrotechnical Commission: Geneva, Switzerland, 2010.
3. International Electrotechnical Commission. *IEC 62443-2-3, Security for Industrial Automation and Control Systems-Part 2-3: Patch Management in the IACS Environment*; International Electrotechnical Commission: Geneva, Switzerland, 2015.
4. International Electrotechnical Commission. *IEC 62443-2-4, Security for Industrial Automation and Control Systems-Part 2-4: Security Program Requirements for IACS Service Providers*; International Electrotechnical Commission: Geneva, Switzerland, 2017.
5. International Electrotechnical Commission. *IEC 62443-3, Security for Industrial Process Measurement and Control-Network and System Security*; International Electrotechnical Commission: Geneva, Switzerland, 2020.
6. International Electrotechnical Commission. *IEC 62443-3-1, Industrial Communication Networks–Network and System Security–Part 3-1: Security Technologies for Industrial Automation and Control Systems*; International Electrotechnical Commission: Geneva, Switzerland, 2009.
7. International Electrotechnical Commission. *IEC 62443-3-3, Industrial Communication Networks–Network and System Security–Part 3-3: System Security Requirements and Security Levels*; International Electrotechnical Commission: Geneva, Switzerland, 2013.
8. International Electrotechnical Commission. *IEC 62443-4-1, Security for Industrial Automation and Control Systems–Part 4-1: Secure Product Development Lifecycle Requirements*; International Electrotechnical Commission: Geneva, Switzerland, 2018.
9. International Electrotechnical Commission. *IEC 62264-3 Enterprise-Control System Integration—Part 3: Activity Models of Manufacturing Operations Management*; International Electrotechnical Commission: Geneva, Switzerland, 2007.
10. Apache TriftTM. A Software Framework, for Scalable Cross-Language Services Development. Available online: https://thrift.apache.org/ (accessed on 10 June 2021).
11. NVD-NIST I-CAT Vulnerability Database. The NVD (National Vulnerability Database) is the U.S. Government Repository of Standards-Based Vulnerability Management Data. Available online: https://nvd.nist.gov/ (accessed on 10 June 2021).
12. SANS CIS. Critical Security Controls (CIS) Recommends Cyber Defence Measures. Available online: https://www.sans.org/critical-security-controls/ (accessed on 10 June 2021).
13. OWASP Top 10. The Open Web Application Security Project® (OWASP) Provides Recommendations to Improve the Software Security. Available online: https://owasp.org/www-project-proactive-controls/ (accessed on 10 June 2021).
14. NIST I-CAT. Vulnerability Database of the National Institute of Standards and Technology (NIST). Available online: https://nvd.nist.gov/general (accessed on 10 June 2021).
15. Schneider Electric. Building a Cybersecurity Strategy for the Digital Economy, Version 3.1, Whitepaper. 2020. Available online: https://www.se.com/ww/en/download/document/Cybersecurity_eguide_09-10-19A (accessed on 10 June 2021).
16. Schneider Electric. *Cybersecurity Services and Solutions, Whitepaper*; Schneider Electric: Rueil-Malmaison, France, 2020. Available online: https://www.se.com/ww/en/download/document/Cybersecurity_eguide_09-10-19A/ (accessed on 10 June 2021).
17. Federal Office for Information Security. *Industrial Control System Security-Top 10 Threats and Countermeasures [English] v1.3-BSI-CS_005E*; Federal Office for Information Security: Bonn, Germany, 2019. Available online: https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_005E.html (accessed on 10 June 2021).
18. IT/OT Convergence–The Essential Guide. 9 March 2021. Available online: https://industrialcyber.co/analyst-corner/the-essential-guide-to-it-ot-convergence (accessed on 10 June 2021).
19. Symantec Security Response. What You Need to Know about WannaCry Ransomware. Available online: https://www.symantec.com/blogs/threat-intelligence/wannacry-ransomware-attack (accessed on 10 June 2021).
20. Jonathan, M. Hacking the Food Supply. Risk and Insurance. 27 March 2018. Available online: http://riskandinsurance.com/hackingthe-food-supply/ (accessed on 10 June 2021).
21. Barreto, L.; Amaral, A. Smart farming: Cyber security challenges. In Proceedings of the 2018 International Conference on Intelligent Systems (IS), Madeira, Portugal, 25–27 September 2018; IEEE: Manhattan, NY, USA, 2018; pp. 870–876. Available online: https://library.wur.nl/WebQuery/wurpubs/fulltext/378724 (accessed on 10 June 2021).
22. Gupta, M.; Abdelsalam, M.; Khorsandroo, S.; Mittal, S. Security and privacy in smart farming: Challenges and opportunities. *IEEE Access* **2020**, *8*, 34564–34584. [CrossRef]
23. Sontowski, S.; Gupta, M.; Chukkapalli, S.S.L.; Abdelsalam, M.; Mittal, S.; Joshi, A.; Sandhu, R. Cyber Attacks on Smart Farming Infrastructure. In Proceedings of the 2020 IEEE 6th International Conference on Collaboration and Internet Computing (CIC), Atlanta, GA, USA, 1–3 December 2020. Available online: https://ieeexplore.ieee.org/document/9319032 (accessed on 10 June 2021).
24. Kloibhofer, R.; Kristen, E.; Davoli, L. LoRaWAN with HSM as a Security Improvement for Agriculture Applications. In *International Conference on Computer Safety, Reliability, and Security*; Springer: Cham, Switzerland, 2020; Available online: https://zenodo.org/record/3999637#.YHv3mOgzbmE (accessed on 10 June 2021).
25. Kloibhofer, R.; Kristen, E.; Ameri, E.A. LoRaWAN with HSM as a Security Improvement for Agriculture Applications–Evaluation, SAFECOMP 2021-DECSoS'21 ("Dependable Smart Embedded and Cyber-Physical Systems and Systems-of-Systems"). Available online: http://www.afarcloud.eu/publications/ (accessed on 10 June 2021).
26. ISOBUS. Available online: https://www.aef-online.org/about-us/isobus.html (accessed on 10 June 2021).

27. Threats to Precision Agriculture, Homeland Security, 2018 Public-Private Analytic Exchange Program. Available online: https://www.dhs.gov/sites/default/files/publications/2018%20AEP_Threats_to_Precision_Agriculture.pdf (accessed on 10 June 2021).
28. Nai Fovino, I.; Neisse, R.; Lazari, A.; Ruzzante, G.; Polemi, N.; Figwer, M. *European Cybersecurity Centres of Expertise Map-Definitions and Taxonomy, EUR 29332 EN*; Publications Office of the European Union: Luxembourg, 2018.
29. Directorate-General for Agriculture and Rural Development (European Commission); ECORYS; Wageningen Economic Research. Study on Risk Management in EU Agriculture. 2018. Available online: https://op.europa.eu/en/publication-detail/-/publication/5a935010-af78-11e8-99ee-01aa75ed71a1 (accessed on 10 June 2021).