Threat analysis in Dairy Farming 4.0

Karl Jonatan Due Vatn[1][0009−0007−4888−043X], Georgios Kavallieratos[1][0000−0003−1278−1943], and Sokratis Katsikas[1][0000−0003−2966−9683]

Norwegian University of Science and Technology, Department of Information Security and Communications Technology, Gjøvik, Norway, Jonatan.Vatn@protonmail.com, georgios.kavallieratos@ntnu.no, sokratis.katsikas@ntnu.no

Abstract. In the era of digital transformation and automation, cybersecurity has become a critical concern in various sectors, including dairy farming. As dairy farms increasingly adopt cyber-physical systems, understanding and mitigating relevant cyber threats is paramount. This work identifies typical cyber-physical systems in a dairy farm and their interconnections to analyze potential cyber threats and risks. Regarding cyber risk, the farm management system is the most critical system of the dairy farm IT-OT infrastructure. This study provides insights into the relatively underexplored cybersecurity domain in dairy farming, establishing a foundation for future research and evidence-based policy development in this vital food production sector.

Keywords: Threat analysis · Cyber physical-systems · Dairy farms · Cyber risk.

1 Introduction

"Industry 4.0" was initially coined to describe manufacturing technologies, process automation, and data exchange trends. Nowadays, it encompasses several industry sectors beyond manufacturing, including agriculture. It describes the trend towards increasing automation and connectivity by leveraging technologies such as the Internet of Things (IoT), Artificial Intelligence (AI), and Big Data Analytics, regardless of the application domain. Accordingly, the term "Dairy Farming 4.0" describes the adoption of emerging technologies in dairy farms to facilitate functions and operations such as real-time health monitoring, real-time tracking, real-time disease detection, real-time nutrition monitoring, real-time animal welfare, real-time monitoring of milk hygiene, and vision node-based furious animal attack detection [12].

The agriculture industry is witnessing significant changes with the advent of modern technology. This transformation integrates advanced technologies such as the IoT, robotics, cyber-physical systems (CPS), and AI into farming practices. This digital transformation influences dairy farming processes and procedures. Today's dairy farms are characterized by sophisticated operations to manage and monitor livestock, optimize feeding, and automate milking processes. These operations are performed by CPSs that increase milk yield and

improve livestock health, leading to higher productivity and profitability. The employed CPSs can seamlessly share data with partners, suppliers, and governmental entities.

The integration of the CPSs constitutes a central element of the digital transformation process in any application domain. The integration is unavoidably accompanied by the enlargement and diversification of the domain's cyber risks, with existing risks being increased and new risks being introduced. The reason for this is that whereas traditional operations were designed with no need for cyber security in mind, modern IT-enabled operations are allowed to be accessed and controlled by information systems connected to the internet through interfaces that are only partially secured [9]. The vulnerabilities inherent in CPSs make dairy farms potential targets for cyber attacks. This situation poses a novel threat to the agriculture industry, which historically is accustomed to dealing with environmental threats, but not with cyber attacks.

As agriculture transitions into a more technologically advanced era, it becomes increasingly important to recognize the vulnerabilities of the infrastructure. Identifying and analyzing cyber threats becomes a crucial step to ensure the security and integrity of the CPSs that make up the infrastructure. Several attacks have already targeted the agricultural industry. One of the largest tractor companies in the world, John Deere, was shown to be vulnerable. As a result, the console of the tractors was jailbroken [16]. Researchers tested off-the-shelf dairy farm equipment, and it was found to have inadequate security, or in some cases, no security at all [2]. The FBI warned against timed attacks against the food and agricultural sector after several ransomware attacks against the sector [10, 9] that, in some cases, resulted in considerable production downtime [10]. Additionally, some parts of the dairy industry, such as retailers and suppliers, have been attacked [1] without affecting the dairy farms themselves to a great extent.

Given the significant economic role of the dairy farming industry, the number of people it employs, and its critical role in society, any disruption could have far-reaching consequences for the industry and the broader society and economy. Therefore, it is vital to consider potential cyber threats against dairy farms, towards enhancing the cybersecurity of the sector at large.

This research has been motivated by the need to improve the understanding of the cybersecurity landscape in the dairy farming industry. By first identifying the CPSs used in dairy farms and then analyzing their potential threats through a threat analysis, this study seeks to provide an overview of the system-level threats. This knowledge will help stakeholders, including farmers, equipment manufacturers, and policymakers, to take informed actions toward safeguarding the operations and the overall resilience of the dairy farming industry.

The study first identifies the CPSs deployed on a typical dairy farm to provide an understanding of the technological landscape and the attack surface. Then the research systematically explores the potential threats associated with these systems using the STRIDE threat modeling method. Finally, these threats' po-

tential impact and likelihood are assessed to estimate the accordant cyber risks. The contributions of the paper are as follows:

- A system-level model of CPSs deployed in dairy farms. The model is built based on information from high-level technical documents from the dairy farming industry.
- Based on this model, a STRIDE-based threat analysis for each CPS included in the model. This approach systematically evaluates potential cyber threats that may compromise the security attributes of the CPSs in the dairy farm.
- An assessment of the risk of CPSs in a dairy farm, based on the identified threats.

The remainder of this article is structured as follows: section 2 reviews related work. Section 3 presents the proposed CPSs model for a dairy farm. Section 4 briefly discusses STRIDE, the reasons that led us to use it, and the results of its application to the case at hand. Finally, section 5 summarizes our conclusions and proposes directions for future work.

2 Related work

The applications and architectures of the CPSs in agriculture have been explored in the literature. The potential of CPSs in a dairy farm is analyzed in [14], focusing on the new possibilities of product and process quality. Further, a framework for cyber-physical agricultural systems (CPASs) is proposed in [5] to analyze the integration of contemporary technology in the infrastructure. However, the literature only partially discusses the CPSs in dairy farms. I. A. Katsko et al. [18] discussed monitoring CPSs in milk production. The CPSs, sensors, and data exchanged in a milking production process are described in [8]. The application of CPSs in smart farming is also discussed in [13]. The technological developments and the parts of the advanced systems of dairy farms are discussed in [12]. Although the above works provide information regarding the CPSs used, a model of CPSs that describes the main functions, data flows, interconnections, and dependencies is yet to be developed.

Agarwal et al. designed a testbed to test the security of components in a dairy farm [2]. By leveraging the testbed, several vulnerabilities and open cybersecurity issues were discussed and the lack of reference architecture models in the literature was highlighted. Nikander et al. in [24] described the network of six dairy farms in Finland, emphasizing the farms' local area networks and connected devices. The analysis focused on general security threats and recommendations such as lack of awareness and implementation of firewalls. An analysis of networks in dairy farms is provided in [24, 23].

Several threats against technology in the agriculture industry were identified in [4], and several threats against confidentiality, integrity, and availability in the agriculture industry were presented in [3]. The FBI warned that farm-level data was at risk in the US and that farmers should take action to secure their data

[9]. Nikander et al. argue that most threats to dairy farms materialize through internal rather than external attacks [24].

A systematic literature review [26] identified 28 threat analysis methods or approaches . The commonly used techniques were STRIDE, attack trees, graphs and paths, MUCs (misuse cases), problem frames, and threat patterns. Another review of threat modeling techniques [27] showed that the identified techniques had widely different characteristics. The STRIDE method is selected as the most appropriate for this study, as it is widely used within the domain because of its relevance and applicability [27] and its ability to be used in combination with other methods, due to its flexibility [19, 17].

Although several works have analyzed cybersecurity in agriculture infrastructures, the security threats in dairy farming are under-researched. The research described above is primarily on general farming, not dairy farming. The systems used on a dairy farm are highly specialized and are different from other use cases. Additionally, the risks that potential threats may pose to the dairy farm infrastructure have only partially been discussed.

3 CPSs of a Dairy Farm 4.0

A graphical depiction of a dairy farm's IT-OT infrastructure model is shown in Fig. 1. The graph nodes represent CPSs, and the solid line edges represent *main* information flows. The dotted line edge from the node labeled "SS" to the node labeled "FMS" indicates *possible* information flows. The following model description includes the CPSs, their functionality, data flows, and dependencies. The CPSs have been analyzed based on information in existing system descriptions in academic literature and technical reports from the dairy farm industry, as discussed in the related work section. For each CPS, the following elements are provided: its functionality and a brief description of the system, its purpose, and its primary function within the farm. Data flows, i.e., an outline of the flow of data, including inputs and outputs to other CPSs, are also included in the model. Finally, dependencies on other *internal* systems are also included in the model. *External* systems or entities are excluded.

Farm management system (FMS): The FMS in a dairy farm is a software solution designed to optimize and streamline the operations of a dairy farm. Its primary function is to manage and monitor various aspects of dairy farming, including herd management, milk production, animal health, nutrition, and financial and staff management. In addition, the system helps dairy farmers improve their overall efficiency, productivity, and profitability, by providing a centralized data analysis and decision-making platform. The farmer and the workers on the farm operate the system [6, 21, 2]. *Functionality:* The FMS plays a critical role in four areas of the farms' operation, namely (1) Animal health management: The system helps monitor the health of each animal by tracking vaccinations, medical treatments, and regular check-ups. (2) Milk production tracking: The FMS records each cow's daily milk production data. (3) Breeding and reproduction management: The system keeps track of breeding cycles, in-

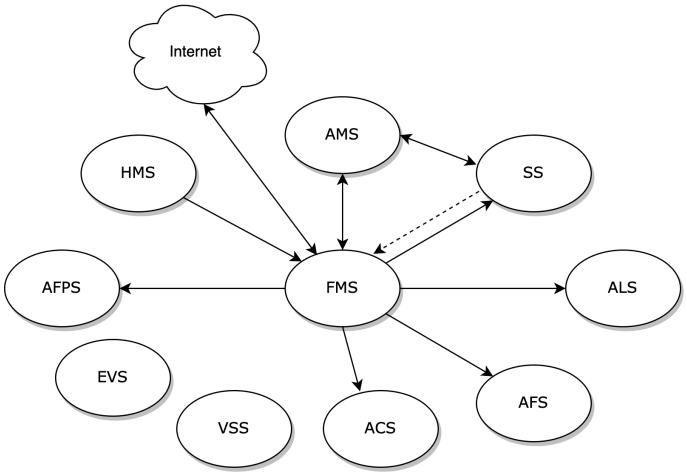

Fig. 1: Overview of systems on a dairy farm, with information flows. Legend: FMS - Farm management system, AMS - Automatic milking system, SS - Segregation system, ALS - Automatic lighting system, ALS - Automatic feeding system, ACS - Automatic cleaning system, VSS - Video surveillance system, EVS - Environment ventilation system, AFPS - Automatic feed pushing system, HMS - Herd management system.

semination dates, and calving history. (4) Food and nutrition management: The system calculates the nutritional requirements of the herd and of each individual cow, helping farmers create balanced diets and monitor food consumption. *Data flow:* The FMS receives information from all systems on the dairy farm except the Environmental Ventilation System (EVS) [2]. The FMS is the single point in the model where all data are stored, processed, and visualized. The system is connected to the internet and receives data from cloud storage. It sends quality control data of the milk to the buyer. *Dependencies:* The FMS is connected to all CPSs in the farm except the EVS.

Automatic milking system (AMS): The AMS is an advanced robot system that milks the cow. The AMS is preferred over other methods because it can optimize the milking process, reduce labor requirements, and improve overall productivity and animal welfare [15]. The system typically offers various functionalities and connects with others, relying on them for seamless and efficient operation. *Functionality:* The cow must go through the Segregation System (SS0 before the AMS. The system's primary purpose is to milk the cow. The AMS uses advanced sensors and technologies to perform its functions [7, 22, 11]. *Data flow:* The AMS sends data about milk production, quality analysis, health monitoring, feeding data, and alerts and notifications to the FMS. Health monitoring data is typically the cow's weight and body temperature. Feeding data contain the amount of concentrate the cow is fed during the visit to the AMS. *Depen-*

dencies: The AMS depends on the FMS to send and receive data and perform its functions.

Herd management system (HMS): The primary function is to collect data from sensors attached to the cow [2]. *Functionality:* According to [2], the HMS gathers information such as "eating habits, lying time, stand-up counts, step counts, and temperature." The system consists of sensors placed around the neck or leg of the cow and processes and stores data about the cows' health. These sensors also function as electronic identification tags, helping identify individual cows for interactions with other systems like segregation gates or the AMS. Such data facilitate the monitoring of health aspects such as detecting abnormal walking patterns, frequency of laying down, or changes in rumination activity. *Data flow:* The data is transmitted from the sensor to the reader via RFID and then to the controller on the Controller Area Network (CAN) bus. The controller sends the data to the FMS through Ethernet [2]. The sensors send the data to receivers in the barn at regular intervals. *Dependencies:* The HMS does not rely on other systems.

Automatic cleaning system (ACS): A self-driving robot is responsible for cleaning the space where the animals live by removing the manure from the cows [20]. *Functionality:* The robot must go between the cows to perform the necessary functions. To this end, it is equipped with advanced sensors. *Data flow:* The ACS communicates with the FMS about the planned cleaning. To enhance its operation, it can use information on the whereabouts of the cows from the HMS received through the FMS. *Dependencies:* The ACS relies on information from the FMS to identify the target area for cleaning.

Automatic feed-pushing system (AFPS): The AFPS is a robot that moves around the feed alley and pushes the food toward the cows so that they can get easier access to it. *Functionality:* The routes for the robot can be programmed manually, or the robot can autonomously navigate its path. It then uses sensory technology to identify the location of the food [20]. *Data flow:* The AFPS is connected to the FMS and gets its routes from there. *Dependencies* The AFPS relies on the FMS to get its routes from and when it should and should not operate.

Automatic feeding system (AFS): The AFS provides an efficient and precise means of delivering feed to the cows, improving productivity, and optimizing resources on the farm [20]. *Functionality:* Robots mix different feeds that suit the herd on the farm. The mixed feed is then transported to the cows via conveyor belts or by a robot. The robot distributes the feed along a path from which only the cows can eat. The cows are fed at regular intervals. When the cows eat, some of the feed gets pushed out and the cows cannot access it. *Data flow:* The AFS communicates to the FMS about the type of food and the amount needed for cows. As a result, the FMS has detailed information about how many cows will be fed and if a particular group needs more. *Dependencies:* The AFS relies on precise data from the FMS concerning the animals' dietary requirements.

Automatic lighting system (ALS): The ALS automatically adjusts the light inside the barn according to a predefined schedule or input from light sensors [20]. *Functionality:* The ALS uses sensors and control algorithms to adjust the lighting intensity and duration based on various factors, such as the time of day, cow activity, and environmental conditions. The ALS detects the light level inside and outside the barn to adjust for the proper light setting inside the barn. *Data flow:* The system sends data to the FMS about the current state of operation, including information about the lighting condition inside the barn. It receives data on when the light should be on or off. *Dependencies:* The system depends on the light setting information from the FMS to set the correct light level.

Environmental ventilation system (EVS): The EVS adjusts the temperature inside the barn via ventilation [2]. *Functionality:* The EVS is disconnected from the rest of the network and the FMS and can be accessed and adjusted via Bluetooth to a mobile phone app. *Data flow:* The EVS receives weather data such as temperature, precipitation, wind direction, and speed from sensors on the farm. Based on information from those, it adjusts the ventilation to set the right conditions inside the barn. The system is adjusted by phone and returns data about the conditions inside and the weather conditions. *Dependencies:* The system is not dependent on other systems as it is not connected to any.

Segregation system (SS): The segregation system allows the cows to pass through the farm's gates. *Functionality:* The gates are in place to ensure that only the right cows can pass through. They can move to the grazing and feeding areas, the milking robot (AMS), and the resting areas [2]. The SS ensures that the cows are only allowed to be milked a certain number of times daily [2]. *Data flow:* The system receives the cow's identity through the RFID chip on the cow. The RFID reader picks up the information at the gate [7]. Next, the system communicates with the FMS and asks if the cow is allowed through the gate or where it is supposed to go (in case of multiple gates). Finally, the FMS tells the gates to open or not [2]. *Dependencies:* When a cow enters the gate, the SS depends on the FMS to give it the correct information about whether to allow the cow through or not.

Video surveillance system (VSS): The VSS is responsible for monitoring dairy farms. *Functionality:* Video surveillance is a common feature on dairy farms [23]. The VSS is an analog or digital (IP) camera connected to a dedicated surveillance PC or IP recorder. The VSS allows the farmer to monitor the farm from one place and ensure that it operates as it should. *Data flow:* The cameras are sometimes connected to the rest of the network. Live video is transmitted from the cameras to the recorder or personal computer to facilitate the monitoring. The VSS does not need to communicate with the FMS or any other system on the farm. *Dependencies:* The VSS is not dependent on other systems in the farm.

4 Threat modeling and risk assessment

This section presents the methodology used to identify security threats and the accordant risks. The results of the analysis and of the risk assessment are discussed.

4.1 Methodology

STRIDE describes six threats: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege [25]. *Spoofing* is the capability of the adversary to pretend to be someone or something else. *Tampering* is the alteration or disruption of a disk, network, or memory of the system. *Repudiation* is a threat that refers to someone's allegation that did not do something which influenced the system's operation or was not responsible for the results derived from their actions. *Information disclosure* refers to the revelation of confidential information to unauthorized entities. *Denial of Service* refers to a violation of the availability of the system. *Elevation of Privilege* is the threat of an adversary executing unauthorized actions by abusing existing privileges. STRIDE attempts to discover potential threats and vulnerabilities as early as the design phase and analyzes each threat by answering questions corresponding to specific security properties. STRIDE facilitates the analysis of both active and passive threats. Threats that manipulate the physical environment of a sensor have not been considered in this paper.

The STRIDE threats and the CPS risk assessment are performed by using a revised form of the impact and likelihood criteria of [19, 17], as depicted in Tables 1 and 2. The risk is calculated using the risk matrix depicted in Table 3.

Level of impact	**Impact description**
High (H)	Threats that could result in the loss of human life. Threats that could result in the loss of animal life. Threats that could result in large energy loss. Threats that may cause damage to the infrastructure. Threats that will result in economic damage and client loss. Threats that will result in system malfunction.
Medium (M)	Threats that could cause process disruption in real-time. Threats that could result in miscalculations in the systems. Threats that could result in a bad reputation for the company. Threats that could result in serious harm to animals. Threats that could influence the system's integrity. Threats that could influence the system's availability. Threats that could result in legal sanctions.
Low (L)	Threats that could result in operation delay or disruption in noncritical processes. Threats that could result in leakage of non-sensitive data.

Table 1: Impact criteria

Likelihood level	Likelihood description
Very likely (V)	The adversary is highly motivated and capable, with no deployed countermeasures. Existing popular exploits which can be executed at any time. High system exposure to the internet.
Moderate (M)	The adversary is highly motivated and capable, while the system's attack prevention countermeasures are insufficient. The system's vulnerability is widely known, but the attacker has to gain physical access. Systems are not directly exposed to the internet.
Rare (R)	The attacker is not highly motivated or does not have the necessary knowledge to perform an attack, or the deployed countermeasures are sufficient. An attacker must have administrative rights to perform the attack. The system is not connected to external networks or systems.

.

Table 2: Likelihood criteria

		Impact		
		High	Medium	Low
Likelihood	Very likely	High	High	Medium
	Moderate	High	Medium	Low
	Rare	Medium	Low	Low

Table 3: Risk matrix

4.2 Threats and Risks in the Dairy Farm 4.0

The threat analysis of the CPSs of the dairy farm is presented in the following tables. The threats shown in the tables are indicative. In these tables, "T" stands for "Threat", "I" stands for "Impact," "L" stands for "Likelihood," and "R" stands for "Risk."

T	Description of threat	I	L	R
S	Since the system is exposed to the internet, an attacker could spoof the identity of a legitimate user, such as a farm employee or the farmer, to remotely gain unauthorized access to the FMS. This could lead to unauthorized modifications or theft of valuable data.	M	V	H

T	An attacker could tamper with the data stored in the FMS, such as changing milk production numbers, breeding cycles, or nutritional requirements, leading to inefficiencies in the farm operation or even financial losses and affecting the cows' health.	H	V	H
R	Without a strong system of logging and verification, an attacker could manipulate data in the FMS, such as milk production statistics or animal health records, and deny the action. This lack of accountability may raise legal issues for the company.	M	V	H
I	Information about the cows' health could be leaked, possibly leading to a disadvantage for the farmer against competitors.	M	V	H
D	An attacker could launch an attack against the system, overwhelming the FMS with traffic and causing the farm's operations to cease.	H	V	H
E	An attacker could, either on-premise or remotely, exploit vulnerabilities to elevate their privileges within the FMS, allowing them to perform actions typically reserved for privileged users. This could result in significant operational disruptions or damage to the farm's infrastructure.	H	V	H

Table 4: Threats to the farm management system (FMS)

T	**Description of threat**	**I**	**L**	**R**
S	An attacker could spoof ID tags so that the system thinks another cow is in the AMS. This could result in improper feeding, incorrect medication dosing, or inappropriate milking schedules.	M	M	M
T	Tampering with the milk quality control systems could result in the delivery of poor-quality milk, posing significant damage to the farmer's reputation. Tampering with the quality control data could lead the system to allow infected or bad milk into the milk tanks, potentially destroying all the milk in the tank.	H	M	H
R	In the absence of robust logging and audit trails, harmful changes made in the AMS, such as adjusting milk schedules or medicine doses, could be denied by the attacker. This could lead to issues in tracing accountability and in resolving adverse effects on cows' health and milk production.	M	M	M
I	Attackers could leak data related to milk production, quality analysis, or health monitoring. Since the milking process is a crucial part of the dairy farms' operation, this could impact the farm's competitiveness if competitors received the data.	H	M	H
D	An adversary may disrupt the communication between the AMS and the FMS. This may cause damage to productivity, animal welfare issues, and potential revenue loss.	H	M	H

E	An attacker may exploit vulnerabilities within the AMS to gain unauthorized access and control over system functionalities. This could lead to the manipulation of medicine dosages or interference with milking processes, ultimately affecting productivity and animal welfare.	M	M	M

Table 5: Threats to the automatic milking system (AMS)

T	**Description of threat**	**I**	**L**	**R**
S	An attacker could spoof the system by changing the cow's identity when communicating with other systems, leading to a false identification of the cow in various contexts. This can lead to incorrect health monitoring and possibly incorrect treatment decisions.	M	M	M
T	An attacker could manipulate data such as eating habits, temperature readings, and rumination activity, leading to incorrect assessments of cow health.	M	M	M
R	A threat actor denying their unauthorized alterations to sensor data, such as feeding or rumination patterns, could adversely affect the well-being of the cows and disrupt farm operations.	M	M	M
I	Data from the sensors to the receivers and from receivers to the FMS could be intercepted if improperly encrypted. This could lead to the unauthorized disclosure of sensitive information about the cows and their health.	M	M	M
D	Attackers could jam the wireless signals between the sensors and the receivers, leading to a denial of service. This could prevent the system from receiving any data from the cows, causing a disruption in monitoring and decision-making for the farmer.	L	M	L
E	If an attacker can exploit vulnerabilities in this transmission process, they could escalate their access privileges, enabling them to view and alter the transmitted data. This could lead to incorrect data being sent to the receivers and subsequently to the FMS, affecting the decisions based on this data.	M	M	M

Table 6: Threats to the herd management system (HMS)

T	Description of threat	I	L	R
S	An attacker could spoof the identity of the ACS and transmit fake location signals to the FMS, causing the FMS to not know where the robot is and consequently giving the robot incorrect cleaning routes in return, leading to incomplete or ineffective cleaning or driving into cows.	M	M	M
T	An attacker could intercept or modify the input between the ACS, FMS, and HMS, leading to erroneous cleaning schedules, wrong path planning, or loss of real-time cow location data.	L	M	L
R	In this system, any unaccounted modifications to the cleaning process of the ACS may compromise the sanitary conditions in the barn, thereby threatening the health of the animals.	L	M	L
I	An attacker could access operational data such as cow locations, cleaning schedules, or facility layout, potentially compromising the barn's operational security.	M	M	M
D	An attacker could stop the robot from working by targeting critical components (e.g., power supply, communication systems) or overloading the system with excessive or incorrect data, rendering it unable to perform its cleaning tasks.	H	M	H
E	An attacker could exploit a vulnerability in the robot's security mechanisms to gain unauthorized access, allowing them to control the robot and alter its settings.	M	M	M

Table 7: Threats to the automatic cleaning system (ACS)

T	Description of threat	I	L	R
S	An attacker could spoof a legitimate connection from the FMS and change the settings or routes of the AFPS. This could result in disrupting the feeding process and wasting energy.	L	M	L
T	An attacker could inject malicious data into the sensor network or the location module of the AFPS, altering the robot's sensing capabilities. This could result in incorrect movement and physical damage to the equipment or the animals.	M	M	M
R	An attacker could send unauthorized commands to the AFPS without leaving a trace of their actions. This would make it difficult to identify the cause of any resulting problems, such as incorrect feed-pushing patterns.	L	M	L
I	Sensory data collected by the AFPS could be intercepted by an attacker. This could reveal information about the conditions within the farm, such as the cows' health or the feed's quality.	M	M	M
D	An attacker could shut down the AFPS by overloading it with requests or exploiting a system vulnerability. This could disrupt the feed delivery process, leading to potential health issues for the cows.	M	M	M
E	An attacker could exploit a vulnerability in the AFPS to take control of its operation. This could allow them to modify the robot's behavior, potentially causing harm to the cows and disrupting the feeding process.	M	M	M

Table 8: Threats to the automatic feed pushing system (AFPS)

T	Description of threat	I	L	R
S	An attacker may spoof the identity of FMS and make the robot dispense excessive or inadequate amounts of feed, potentially disrupting the farm's operations and affecting the cows' health.	M	M	M
T	An attacker may tamper with the feeding intervals programmed into the AFS, causing the cows to be overfed or underfed, resulting in poor health or reduced milk production.	L	M	L
R	In the case of alterations in the feed's composition or quantity, every action must be traceable to the person or system who performed it since it could disrupt the nutritional balance of the cows.	M	M	M
I	An attacker may expose data such as feed types and feeding schedules, potentially causing harm to the farm's operations or reputation.	L	M	L
D	A threat actor could cause a denial of service by disrupting the AFS by overloading the system with requests, preventing the cows from receiving adequate feed.	H	M	H
E	An attacker could gain control over the AFS robot, enabling them to manipulate the feeding process, cause damage to the robot or facilities and harm the cows.	H	M	H

Table 9: Threats to the automatic feeding system (AFS)

T	Description of threat	I	L	R
S	An attacker could impersonate an authorized user and manipulate the automatic lighting system. By altering the lighting schedules, they could create undesirable conditions for the cows, leading to stress, reduced milk production, and potential health issues.	L	M	L
T	An attacker could physically or remotely tamper with the input from the light sensors, causing them to provide false readings or alter them. Improper lighting may lead to inadequate lighting conditions, negatively impacting the cows' health and productivity.	L	M	L
R	Untraceability to a specific user of actions in the ALS could lead to undetected malicious activities or repeated system faults, adversely affecting the cows' health.	L	M	L
I	An attacker could gain unauthorized access to the lighting schedules and configurations of the ALS, revealing operating patterns of the farm that could be used for potential malicious activities.	L	M	L
D	An attacker could flood requests to the controllers in the lighting system, possibly causing the lights to be faulty. This attack requires physical access to the infrastructure.	M	M	M
E	If an attacker gains administrative access to the system, they could misuse this to disrupt the lighting schedules. This could cause damage to health and productivity and, in the worst-case scenario, create unsafe working conditions for farm workers.	M	M	M

Table 10: Threats to the automatic lighting system (ALS)

T	Description of threat	I	L	R
S	An attacker could spoof the Bluetooth connection to the system and pretend to be a legitimate user. This would give the attacker access to the actuators or manipulate the EVS settings, potentially leading to harmful conditions for the animal.	M	R	L
T	By manipulating the data sent to the EVS from the app, an attacker could adjust the ventilation adjustments or give wrong temperature information from the temperature sensors.	L	R	L
R	Lack of logging events on the system could lead to the users denying having made specific EVS adjustments through the mobile app.	L	R	L
I	An interception of the communications may lead to information leakage about the farm's operating conditions; this could be used for malicious purposes.	L	R	L
D	An attacker could block the source of the weather data, causing the EVS to operate with outdated or incorrect information. This could lead to unsuitable conditions inside the barn for the animals.	H	R	M
E	An attacker with administrative rights could turn off the ventilation, making the cows overheat in warm weather.	H	R	M

Table 11: Threats to the environment ventilation system (EVS)

T	Description of threat	I	L	R
S	An attacker could clone an RFID tag, tricking the system into thinking an unauthorized cow is authorized to enter the AMS or other restricted areas. This can lead to improper segregation, causing disruptions in the milking process and potential conflicts among the cows.	M	M	M
T	An attacker could tamper with the gate's control system to disable or force it to open/close unexpectedly. This could lead to hurting the cows when they are in the segregator, letting them in or out where they do not belong, or disabling them altogether.	H	M	H
R	The repudiation of actions within this system is not permitted, as improper or unauthorized manipulation of the control system or RFID readings could jeopardize the cows' well-being and farm processes' efficiency.	M	M	M
I	An attacker may collect the usage statistics for the gates for malicious purposes. The attacker could maximize the impact of their activities by targeting the farm at the most vulnerable times.	M	M	M
D	An attacker could jam RFID signals near the gates, preventing RFID readers from accurately identifying cows and causing delays to the milking operation.	M	M	M
E	If an attacker has high privilege on the system, they can use it to override the gates and let every cow that wants to pass through to do so. This could lead to cows queuing up and ending up in the wrong place on the farm.	M	M	M

Table 12: Threats to the segregation system (SS)

T	Description of threat	I	L	R
S	An attacker could replace the genuine video feeds with recorded or manipulated footage, misleading the farmer and obscuring any activities happening in the farm.	L	R	L
T	A threat actor could tamper with the video recordings stored on the recorder or PC, altering or deleting critical evidence of incidents on the farm.	M	R	L
R	Any action carried out within the video surveillance system that impacts its function, such as manipulating video feeds or tampering with video recordings, should be attributable. Denial of responsibility for such actions could mislead the farmer and possibly lead to security breaches.	M	R	L
I	An attacker could leak feeds or recordings, potentially disclosing information about the farm's operations or personnel. The footage can be selected only to show negative incidents on the farm, damaging the farm's reputation.	H	R	M
D	An attacker could intentionally overload the system, causing the video feeds to become unavailable. This would hinder the farmer's ability to monitor the farm remotely.	L	R	L
E	An attacker could exploit vulnerabilities in the VSS to gain unauthorized control over the cameras, allowing them to manipulate the camera settings or disable them entirely.	M	R	L

Table 13: Threats to the video surveillance system (VSS)

Considering the above threat analysis results, we notice that the FMS gathered six high-risk scores. Further, three high-risk threats are identified for the AMS and two for the AFS. Therefore, these three systems are among the most critical ones. The SS and the AFPS gathered five and four, respectively, medium risk scores. This is due to their high dependence on the critical CPSs. Finally, the ALS, EVS, and VSS are characterized by low-risk levels.

The threat analysis focuses on attacks against each CPS's main properties, as described in the previous section, namely functionality, data flow, and dependencies. An essential aspect of the identified threats is the potential for harming animals; an example is the tampering threat against the segregation system. Similarly, a tampering or spoofing threat to the ACS may inflict physical damage to the infrastructure since the cows' health is highly dependent on the ACS. Furthermore, these threats may hurt the business continuity of the organization. As mentioned earlier, the FMS is crucial in the network model and acts as the central node in the model graph. However, this role makes it potentially vulnerable, as threats against the FMS could compromise the entire system due to the high dependencies on the other CPSs. A consequence is that if the FMS is compromised, wide-reaching effects across the overall system might occur. For instance, numerous spoofing threats have been identified, where an attacker could pretend to be the FMS, issuing false commands or injecting incorrect data into other systems.

Tampering and *Denial of service* threats are among the most critical for the dairy farm as they are rated as critical in four out of the ten CPSs. *Spoofing* and *Elevation of Privileges* are rated as medium lever threats while *Repudiation* and *Information Disclosure* are low level threats.

By leveraging the risk assessment performed per CPSs and per STRIDE threat, the criticality of each CPS is determined. The overall risk analysis results are depicted in Table 14 where twenty low, twenty-seven medium, and thirteen high-risk threats in the dairy farm are shown. The impact and likelihood values are estimated based on the criteria presented in Tables 1 and 2. It can be noticed that the CPSs that are exposed to the internet received the highest risk values. The AFS, ACS, HMS, and ASPS received medium-level risk scores. This is because the functions of and data flows between these CPSs are only partially exposed to the internet, hence less vulnerable to cyber attacks. Finally, the ALS, EVS, and VSS have received low-level risk scores due to limited dependencies.

System	**Low**	**Medium**	**High**	**System risk score**
FMS			6	3.0
AMS		3	3	2.5
SS		5	1	2.2
AFS	2	2	2	2.0
ACS	2	3	1	1.8
HMS	1	5		1.8
AFPS	2	4		1.7
ALS	4	2		1.3
EVS	4	2		1.3
VSS	5	1		1.2
Total	20	27	13	

Table 14: Risk assessments for all systems

Table 14 illustrates the system's low, medium, and high-risk scores. The risk score itself for each threat is calculated by the matrix shown in Table 3. The risk score per CPS and per threat is calculated by assigning numerical values to the risk scores for each threat. The threat scores were given the following values: Low=1, Medium=2, High=3. By adding these together and dividing them by the number of threats (six for each CPS), the average risk score of the system is shown. For example, the FMS gets the highest possible score of 3 (6 high-risk threats, calculated as (6*3)/6=3). Table 14 sets the CPSs in a priority list based on their criticality.

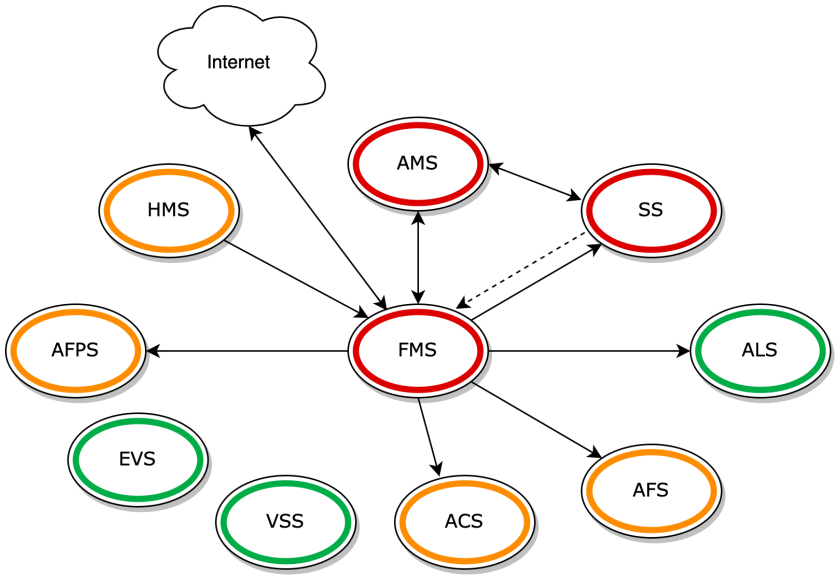

Fig. 2: Overview of systems on a dairy farm, with information flows, high-risk systems marked with red, medium-risk with orange, low-risk with green. Legend: FMS - Farm management system, AMS - Automatic milking system, SS - Segregation system, ALS - Automatic lighting system, ALS - Automatic feeding system, ACS - Automatic cleaning system, VSS - Video surveillance system, EVS - Environment ventilation system, AFPS - Automatic feed pushing system, HMS - Herd management system.

The FMS is characterized as the most critical CPSs since it is central to the model and directly connected to the internet. The AMS scored high on the risk scale due to its integral role in the farm's operations and its potential to cause significant harm to the cows if compromised. The interdependence between the AMS and the FMS also implies that a compromise in the AMS could spread to other interconnected systems. Four out of ten CPSs have received medium-level risk scores. The likelihood of attacks in such systems is low due to their low interconnectedness. Last, three systems have received low-level risk scores.

5 Conclusions

This paper discussed cybersecurity aspects of contemporary dairy farms employing IT-OT integrated technology. The CPSs of the dairy farm were presented and analyzed, considering functions, data flows, and dependencies. The cyber threats per CPSs were identified by employing the STRIDE method and analyzing attack scenarios per STRIDE threat. Tampering and Denial of service threats are

among the most critical, whilst Spoofing and Elevation of Privileges are characterized as medium-level threats. Additionally, the risks per STRIDE threat and per CPSs were assessed to identify the most critical components. In future work, further analysis of the model presented in this work will be performed, towards proposing a security reference architecture for dairy farms 4.0.

References

1. Lawrence Abrams. Pan-Asian retail giant Dairy Farm suffers REvil ransomware attack, January 2021.
2. Sharad Agarwal, Awais Rashid, and Joseph Gardiner. Old MacDonald had a smart farm: Building a testbed to study cybersecurity in smart dairy farming. In *Cyber Security Experimentation and Test Workshop*, pages 1–9, Virtual CA USA, August 2022. ACM.
3. Lawrence Baker and Richard Green. Cyber Security in UK Agriculture. 2019.
4. Aida Boghossian, Peter Mutschler, Brian Ulicny, Larry Barrett, Glenn Bethel, Michael Matson, Thomas Strang, Kellyn Wagner Ramsdell, Susan Koehler, and Scott Linsky. Threats to Precision Agriculture, 2018.
5. Stefan Chivarov, Kristian Dimitrov, and Nayden Chivarov. Algorithms for cost oriented cyber physical system (cocps) for intelligent control of animal husbandry farms. *IFAC-PapersOnLine*, 55(11):31–36, 2022.
6. DeLaval. Delpro Farm Manager, 2018.
7. DeLaval. DeLaval Landbrukskatalog 2023, 2023.
8. VT Dmytriv, IV Dmytriv, IM Horodetskyy, PP Yatsunskyi, et al. Adaptive cyber-physical system of the milk production process. *INMATEH: Agricultural Engineering*, 61(2):199–208, 2020.
9. FBI. Smart Farming May Increase Cyber Targeting Against US Food and Agriculture Sector, 2016.
10. FBI. Ransomware Attacks on Agricultural Cooperatives Potentially Timed to Critical Seasons, April 2020.
11. GEA. Gea product catalogue, 2017.
12. Anita Gehlot, Praveen Kumar Malik, Rajesh Singh, Shaik Vaseem Akram, and Turki Alsuwian. Dairy 4.0: Intelligent communication ecosystem for the cattle animal welfare with blockchain and iot enabled technologies. *Applied Sciences*, 12(14):7316, 2022.
13. Dimitris Gkoulis, Cleopatra Bardaki, Elena Politi, Ioannis Routis, Mara Nikolaidou, George Dimitrakopoulos, and Dimosthenis Anagnostopoulos. An event-based microservice platform for autonomous cyber-physical systems: the case of smart farming. In *2021 16th International Conference of System of Systems Engineering (SoSE)*, pages 31–36. IEEE, 2021.
14. Martin Höhendinger, Natascha Schlereth, Maximilian Treiber, Manfred Höld, Jörn Stumpenhausen, and Heinz Bernhardt. Potential of cyber-physical systems in german dairy farming. In *2019 ASABE Annual International Meeting*, page 1. American Society of Agricultural and Biological Engineers, 2019.
15. Renate Marie Butli Hårstad. Bonden, familien og melkeroboten – en ny hverdag. Technical Report 2/2019, RURALIS - Institutt for rural- og regionalforskning, 2019.
16. Will Jarvis. Sick Codes talks tractor hacks, September 2022.

17. B. Jelacic, D. Rosic, I. Lendak, M. Stanojevic, and S. Stoja. Stride to a secure smart grid in a hybrid cloud. In *CyberICPS/SECPRE@ESORICS*, 2017.
18. Igor A Katsko and Elena V Kremyanskaya. Cognitive monitoring of cyber-physical systems in agriculture. In *Cyber-Physical Systems and Control*, pages 422–430. Springer, 2020.
19. Georgios Kavallieratos, Sokratis Katsikas, and Vasileios Gkioulos. Cyber-Attacks Against the Autonomous Ship. In *Computer Security*, volume 11387, pages 20–36, Cham, 2019. Springer International Publishing.
20. Lely. Lely Dairy Equipment, 2014.
21. Lely. Horizon Brochure, 2020.
22. Lely. Astronaut A5 Operator Manual, 2022.
23. Onni Manninen. Cybersecurity in Agricultural Communication Networks: Case Dairy Farms. Master's thesis, JAMK University of applied sciences, 2018.
24. Jussi Nikander, Onni Manninen, and Mikko Laajalahti. Requirements for cybersecurity in agricultural communication networks. *Computers and Electronics in Agriculture*, 179, December 2020.
25. A. Shostack. *Threat Modeling: Designing for Security*. Wiley Publishing, 1st edition, 2014.
26. K. Tuma, G. Calikli, and R. Scandariato. Threat analysis of software systems: A systematic literature review. *Journal of Systems and Software*, 144:275–294, October 2018.
27. Wenjun Xiong and Robert Lagerström. Threat modeling – A systematic literature review. *Computers & Security*, 84:53–69, July 2019.