Master's thesis

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

Karl Jonatan Due Vatn

Cybersecurity in Agriculture: A Threat Analysis of Cyber-Enabled Dairy Farm Systems

Master's thesis in Experience-based Master in Information Security
Supervisor: Sokratis Katsikas
Co-supervisor: Georgios Kavallieratos
June 2023

NTNU
Norwegian University of
Science and Technology

Karl Jonatan Due Vatn

Cybersecurity in Agriculture: A Threat Analysis of Cyber-Enabled Dairy Farm Systems

Master's thesis in Experience-based Master in Information Security
Supervisor: Sokratis Katsikas
Co-supervisor: Georgios Kavallieratos
June 2023

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

NTNU
Norwegian University of
Science and Technology

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-enabled systems, understanding and mitigating potential cyber threats is crucial.

This thesis is an analysis of a cyber-enabled dairy farm. It identifies ten interconnected cyber-enabled systems, including milking, feeding, and livestock health monitoring. The farm management system (FMS) was identified as the central node in this network.

Applying a STRIDE threat analysis to each system highlighted various potential threats. These threats could negatively impact cow health, interrupt milk production, and potentially lead to significant financial and reputational damages to the dairy farming operation.

A subsequent risk assessment was conducted, with the FMS showing the highest risk score, primarily due to its central role and extensive connectivity. This finding suggests that the FMS could be a primary target for cyberattacks, and its compromise could have cascading effects on other systems. Several cyber-physical systems were also found to be at risk in this analysis.

These findings highlight the necessity for robust cybersecurity measures within the dairy farming industry to protect against potential cyber threats. Furthermore, this study contributes valuable insights into the relatively underexplored cybersecurity domain in dairy farming, providing a foundation for future research and policy development in this vital food production area.

Sammendrag

Med digital transformasjon og automatisering har cybersikkerhet blitt en kritisk faktor i ulike sektorer, inkludert melkeproduksjon. Ettersom melkegårder i økende grad tar i bruk høyteknologiske systemer, er det avgjørende å forstå og redusere potensielle trusler.

Denne masteroppgaven er en analyse av høyteknologiske melkebruk. Den identifiserer ti sammenkoblede systemer, inkludert melkesystemer, fôringssystemer og helseovervåkingssystemer for kyr. Gårdsstyringssystemet ble identifisert som det sentrale knutepunktet i dette nettverket. Ved å bruke en trusselmodeleringsverktøyet STRIDE på hvert enkelt system, ble potensielle trusler avdekket. Disse truslene kan negativt påvirke helsen til kyrne, avbryte melkeproduksjonen, og potensielt føre til betydelige økonomiske og skader på omdømme til melkeproduksjonen.

En risikovurdering ble også utført, hvor gårdsstyringssystemet fikk den høyeste risikoscoren, hovedsakelig på grunn av sin sentrale rolle og omfattende tilkoblinger til andre systemer. Dette funnet antyder at gårdsstyringssystemet kan være et primært mål for cyberangrep, og hvis dette blir kompromittert kan det føre til andre systemer blir tatt ned.

Disse funnene understreker nødvendigheten av robuste cybersikkerhetstiltak innen melkeproduksjonsindustrien for å beskytte mot potensielle cybertrusler.
Videre bidrar denne studien med verdifull innsikt i det relativt uutforskede området for cybersikkerhet i melkeproduksjonen, og gir et grunnlag for fremtidig forskning på dette området.

Preface

This thesis is the culmination of a three-year-long part-time experience-based master's degree in information security at the Norwegian University of Science and Technology (NTNU). This research, conducted from January to June 2023, represents a continuation of the work undertaken in the course IMT4205 - Research Project Planning. The project was titled *Cyber Security in Norwegian Diary Farms*.

I want to thank my supervisors from NTNU, Georgios Kavallieratos and Professor Sokratis Katsikas, for their excellent guidance during this project. Their previous research has been of great value to this thesis. Kavallieratos' optimism and support made this whole endeavor much more enjoyable.

I've devoted countless afternoons and holidays to pursuing my studies, a journey that has been both challenging and rewarding. I extend my heartfelt gratitude to my family for their unwavering support, particularly during the final intense weeks of this project. Thank you, Nina, for proofreading my thesis. Lastly, my profound appreciation goes out to my wife. I want to express my deepest gratitude to her for supporting me over the last three years. This master thesis wouldn't have been possible without her continuous support and encouragement.

Karl Jonatan Due Vatn
Evenskjer, June 2023

Contents

Figures

Tables

Chapter 1

Introduction

The agriculture industry is witnessing significant changes with the advent of modern technology. This transformation integrates advanced technologies such as the Internet of Things, robotics, cyber-physical systems (CPS), and artificial intelligence into farming practices. The dairy farming industry experiences the same transformation. Today's dairy farms are more than just cows and milking equipment; they are becoming increasingly sophisticated operations. Advanced systems are now used to manage and monitor livestock, optimize feeding, and automate milking processes. These systems help increase milk yield and improve livestock health, leading to higher profitability. Furthermore, these cyber-enabled systems can seamlessly share data with partners, suppliers, and governmental entities. Welcome to the new era of dairy farming, where modern technology plays a pivotal role.

With these tremendous technological advancements come new challenges and risks. Most notably, the rising threat of cyber attacks [1]. The previously non-connected farms are now open for outside attacks through cyber-enabled and cyber-physical systems. This situation poses a novel threat to the agriculture industry, which historically is used to deal with environmental threats, but not cyber threats. FBI has warned against timed attacks against the food and agricultural sector after several ransomware attacks against the sector [1, 2]. In some cases, the production stopped for some time [2]. Some parts of the dairy industry, such as retailers and suppliers, have been attacked [3], but the dairy farms seem to have been spared. The vulnerabilities inherent in CPS make these farms potential targets for such attacks. The term "cyber-enabled" refers to innovative systems with enhanced monitoring, communication, and connection capabilities [4]. The term "cyber-enabled dairy farm" is a label for the range of interconnected, digitally-enhanced systems in a dairy farm environment.

Dairy farming is important for Norway for a variety of reasons. First, dairy farming is a significant industry in Norway, contributing notably to the nation's economy. With over 200,000 cows distributed across approximately 6,700 dairy farms in Norway [5], it annually produces around 1.4 billion liters of milk [6]. This production scale led to Norwegian dairy farmers generating a revenue of

about 9 billion in 2012 [7].

Second, the dairy farming industry is not only economically vital but also essential from a societal perspective. The industry is part of the food supply chain, a critical societal function in Norway [8]. This emphasis on agriculture as an integral part of society parallels the situation in countries like the US, where the agriculture industry is considered a critical infrastructure. Dairy farms, typically decentralized, operate on other critical resources such as electricity, water, and sewage and depend on regular milk transport.

Third, another aspect that underscores the importance of dairy farming in Norway is its high degree of self-sufficiency in milk production [9]. Nearly all of the milk consumed in Norway and used to produce milk-based products is sourced domestically. This significant reliance on local production sharply contrasts with other food supplies in Norway, more than half of which are imported.

Given the significant economic role of the dairy farming industry in Norway and the number of people it employs, its role critical role in society, it is vital to consider potential cyber threats. Any disruptions could have far-reaching consequences, not only for the industry but for the broader Norwegian society and economy as well.

As agriculture transitions into a more technologically advanced era, it becomes increasingly important to recognize the vulnerabilities inherent in these cyber-enabled systems, especially CPS. Consequently, identifying potential cyber threats becomes a crucial step to ensure the security and integrity of these systems. In addition, the implementation of these new technologies entails vulnerabilities. Unfortunately, security is not always the priority when building new systems. The agriculture industry is not different. One example of this is when 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 [10]. Another example is when researchers tested off-the-shelf dairy farm equipment, and it was found to have inadequate security, or in some cases, no security at all [11].

This thesis addresses the growing concern about the cybersecurity of cyber-enabled dairy farms. These modern systems, while beneficial, introduce novel vulnerabilities and threats that have not yet been comprehensively explored. The potential implications are far-reaching, affecting business continuity, farm operations, equipment functionality, and animal welfare. A researcher in the field stated: "Anything that messes up the functioning of a robot can be quite catastrophic because cows need to be milked every day, fed every day. We make decisions based on the data, so anything that interferes with the data is going to affect the sustainability of that dairy farm" [12]. An overview of these systems' potential threats is needed to further research cyber-enabled farms' security.

This study aims to identify the cyber-enabled systems deployed on a dairy farm, providing an understanding of the technological landscape and potential attack points. Furthermore, the research systematically explores the potential threats associated with these systems using the STRIDE threat model. Finally, the potential impact and likelihood of these threats are measured in a risk analysis.

1.1 Justification, motivation, and benefits

The focus of this thesis is justified, given the increasing dependence of the dairy farming industry on related technologies. As these technologies continue to be integrated into dairy farming operations, concerns regarding potential risks they might introduce are growing. Furthermore, the scale at which these potentially insecure and vulnerable systems are implemented is worrisome.

The adoption of Industry 4.0 technologies in dairy farming, while advantageous in many ways, also opens the industry to a new set of cyber threats. These threats are not limited to traditional computer systems but extend to operational technologies such as automated milking systems and livestock monitoring devices.

The impact could be far-reaching and devastating if these threats are not adequately addressed. For example, an individual farm could experience significant operational disruptions, potentially leading to substantial financial losses. More broadly, a successful cyberattack could compromise the integrity of food supply chains, potentially causing shortages of dairy products at a national level.

The motivation behind this research is the need to improve the understanding of the cybersecurity landscape in the dairy farming industry. By first identifying the cyber-enabled systems used on 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 to safeguard the operations and the overall resilience of the dairy farming industry.

The STRIDE threat analysis findings will offer insights into specific threats and attack vectors, which can guide the development of targeted and adequate security measures by the suppliers of those systems. Furthermore, the outcomes of this research can contribute to developing best practices and guidelines for the dairy farming industry and promoting a culture of cybersecurity awareness and preparedness.

In conclusion, this research on identifying systems on a dairy farm and the performance of threat analysis is both timely and necessary. Timely because there is currently little research on the systems on a dairy farm and the threats against those systems [11]. Furthermore, no academic research has been published that systematically studies the threats to the cyber-enabled dairy farm. By shedding light on the potential threats in the dairy farming industry, this study will help protect the sector from cyber attacks and contribute to the resilience and sustainability of the global food supply chain.

1.2 Research questions

The first objective of this thesis is to develop a generalized topology of a cyber-enabled dairy farm that accurately represents its essential components and systems. The making of the topology includes understanding and illustrating the interconnections between different systems, their role in the dairy farm's operations,

and their integration with broader digital and physical systems.

The second objective is identifying potential cyber threats that could impact this topology. Identifying these threats is a critical step toward developing strategies to mitigate them and enhance the overall cybersecurity of dairy farms.

The third and last objective is to do a risk assessment of these threats.

These three objectives are condensed into the following research questions.

- RQ 1: Cyber-enabled systems on a dairy farm
    1. RQ 1.1: What are the cyber-enabled systems in a dairy farm?
    2. RQ 1.2: What are the properties of the cyber-enabled systems on a dairy farm?
- RQ 2: What are the threats against cyber-enabled systems on a dairy farm?
- RQ 3: What are the risks associated with the threats against cyber-enabled systems on a dairy farm?

A mixed-method approach is used to answer these research questions. For the first question, two different approaches are taken to identify the cyber-enabled systems on a dairy farm and their properties. The first identifies what is written in the academic literature about these systems. The second question studies the technical documents from suppliers of these systems. Research question two is answered by exploring different threat analysis approaches. STRIDE is chosen as the model for identifying threats. The last research question is answered by a risk assessment that estimates the likelihood and impact of the threats identified in the threat analysis.

1.3 Contributions

The major contributions of this thesis are the following:

1. The thesis develops a topology of a cyber-enabled dairy farm. The topology is built on high-level technical documents from the dairy farming industry. The topology consists of a general description of the systems found in a dairy farm.
2. Based on this topology, a high-level STRIDE threat analysis is performed on each system identified in the topology. This approach will systematically evaluate potential cyber threats compromising the systems' integrity, availability, and confidentiality within the cyber-enabled dairy farm.
3. A risk assessment is performed on these identified threats and systems. This assessment aims better to understand each threat's potential impact and likelihood. This assessment considers two factors, the potential consequences of a successful attack and the probability of such an attack occurring.

1.4 Scope

The following choices narrow the scope of the research done in this thesis. The research questions already narrowed the scope, but some additional limitations were necessary to apply. First, the geographical context for the thesis is Norway. This scope applies when making the topology and for describing the general background of the modern dairy farm. Second, dairy farming is a term that includes animals such as cows, sheep, goats, and buffalo. However, in this thesis, only cows are considered.

1.5 Thesis outline

The remainder of the thesis is structured in the following manner.

- Chapter 2 Background and related works provide the necessary background knowledge for the thesis. The chapter includes contextual information regarding the cybersecurity field of the agriculture industry and the related academic literature.
- Chapter 3 Methodology gives the reader insight into the methodology used to make the topology of a dairy farm and how STRIDE threat modeling and risk assessment are applied to that topology.
- Chapter 4 Results present the findings from the research. It describes the topology, the STRIDE-related threats to the systems, and the risk assessment.
- In Chapter 5 Discussion, the results are discussed in light of the methodology and the background. A selected number of topics are chosen for the discussion. The limits of the thesis are discussed.
- Chapter 6 Conclusion sums up the thesis, and some final remarks are given. Some suggestions are made for future research.

Chapter 2

Background and related works

This chapter provides relevant background information and related academic literature on the different topics of the thesis. The topics covered in this chapter are the following. Section 2.1 gives an introduction to the field of cybersecurity in agriculture and dairy farms. Section 2.2 covers topologies. Section 2.3 introduces threat analysis in general and STRIDE specifically. Threats against dairy farms are described in Section 2.1.

2.1 Cybersecurity in dairy farms

This chapter presents the relevant background information and related academic work in the field of cybersecurity on dairy farms.

The area of cybersecurity in dairy farming has not received much attention or been the subject of research [11]. As a result, there is a lack of research on how the systems on a dairy farm could be attacked and how they are vulnerable. This lack of research makes the cybersecurity of the dairy farming industry an open area of research.

The cybersecurity of agriculture, on the other hand, is better researched. Some of this research is relevant to dairy farming. In addition, some cybersecurity knowledge from other related fields, such as general cybersecurity considerations, IoT (Internet of Things), and CPS (cyber-physical systems) research, are also relevant. NIST defines CPS as "interacting digital, analog, physical, and human components engineered for function through integrated physics and logic" [13].

In agriculture, modern technology is being used to monitor and manage livestock's health, welfare, and performance in real time. This practice is often called precision livestock farming (PLF) or smart livestock. These terms describe the use of advanced technologies to ensure the well-being and productivity of animals continuously [14]. Such technology is used in agriculture where animals are involved, such as beef cattle, sheep, and goats. Dairy farming also uses this technology to monitor the cows. The use of the technology is described later in this chapter. The security aspects of PLF and smart livestock are relevant as the terms include dairy farming cows.

Only two papers directly address the security aspect of dairy farming [11, 15]. In a 2022 study, Agarwal et al. designed a testbed to test components' security on a dairy farm [11]. After conducting interviews with farmers and suppliers, the researchers built a testbed with components from the industry. After building the testbed, they conducted a limited number of penetration tests. The researchers concluded: "Our initial analysis indicates that the current state of cybersecurity in smart dairy farming significantly lacks maturity, and significant work is needed to improve the security of devices, networking mechanisms, and deployment architectures" [11]. Some parts of the systems had no passwords. Others sent data in clear text. In one case, the researchers could access data from users on real farms via their customer account [11].

In a 2020 paper, Nikander et al. describe the network of six dairy farms in Finland, particularly emphasizing the farms' local area networks and connected devices [16]. The paper is based on a master's thesis from 2018 by Manninen [15]. They found that while the physical cabling was in good condition and followed regulations, other aspects, such as network topology, malware protection, and system backups, were not according to standard. Furthermore, the farmers themselves were not well-informed about the details of their network and connected devices. The study concludes that there is a significant need for improvements in cybersecurity on individual farms, as many threats faced by farms come from the farmers' actions or the physical environment [16]. The study found that most farms had antivirus software installed on their computers. However, only one farm had a hardware firewall installed [15].

2.2 Topology of a dairy farm

To make a threat model of a dairy farm, the systems in question need to be described. Since no topology is available in the academic literature on dairy farming, this thesis seeks to develop one. A topology of systems is the way the systems are connected and configured. They can be connected in a variety of different ways and shapes. Some configurations are mesh, tree, bus, star, and ring topology [17]. The study of the topology of a network can help identify potential attack vectors, bottlenecks, and single points of failure in the systems.

Below is a summary of the existing academic research on the topology of dairy farms.

A 2022 paper found that there "is no proper reference architecture or network diagram available publicly that can be used to build a smart dairy farming testbed" [11]. The assumption here is that there is an overlap between the research area of threat analysis and the area of building a testbed. Since a threat model could be built more abstractly, there is not necessarily the same need for detail in system architecture as when building a testbed. In the research for the thesis, it became clear that there was not much research in the area of systems architecture of modern dairy farms.

Two papers implicitly address this area, Agarwal et al.s testbed study [11], and

the network analysis of six dairy farms in Finland Nikander et al. [15, 16]. The relevant parts of those studies are described below and will make the foundation for constructing the model needed for the further threat model.

The relevant part of the Agarwal et al. study is the acquired knowledge of the cyber-related systems on a dairy farm. Through interviews with farmers, documents, and manuals from the industry, they gained insight into the architecture of a dairy farm. Unfortunately, the paper does not appear to include all findings, only those relevant to the testbed, thus making the topology incomplete. For example, the AMS or other robotic elements that typically exist on a modern dairy farm are not documented. However, the researchers found "a few critical processes," and three processes (assumed critical) were documented in the architecture. These three are:

1. Automatic segregation gate: A segregation gate is used to direct cows to different areas on the farm based on their statistics and needs. Readers read the cow ID at the gate via the cow's neck/leg/ear responder. The cows are then directed to the grazing fields, resting areas, or the milking machine.
2. Herd monitoring: The cow's neck and leg responders continuously monitor their eating habits, lying time, stand-up counts, step counts, and temperature. These statistics are then sent to a reader at regular 15-minute intervals and forwarded to the farm management software, which provides graphs and insights to the farmer.
3. Maintaining environmental conditions: A weather ventilation system monitors and adjusts the temperature, moisture, wind speed, and direction in the barn to ensure the cows' well-being and productivity. The system uses actuators on the ventilation to provide the necessary environmental conditions for the cows [11].

The researchers translate these processes to the following systems in [11].

- Segregation system
- Herd management system
- Environmental ventilation system

The resulting analysis of the architecture and what systems were used in the testbed is shown in Figure 2.1.

The two central systems documented in this paper, and shown in Figure 2.1, are the environment ventilation system (EVS) and herd management system (HMS).

On the networking side of the dairy farm, the researcher made some discoveries, presented below and in Figures 2.2, and 2.3 [11].

The description below of dairy farm networks is taken from [11]. Dairy farms typically use a flatbed network to install devices. The network is made without any hierarchy or distributed system practices. The network lacks firewalls or DMZs (de-militarized zones), increasing its complexity due to the various devices and communication channels. The HMS operates on a local network without internet connectivity, while the herd monitoring controller connects to the internet for remote monitoring. The EVS's master controller connects to the internet via WiFi

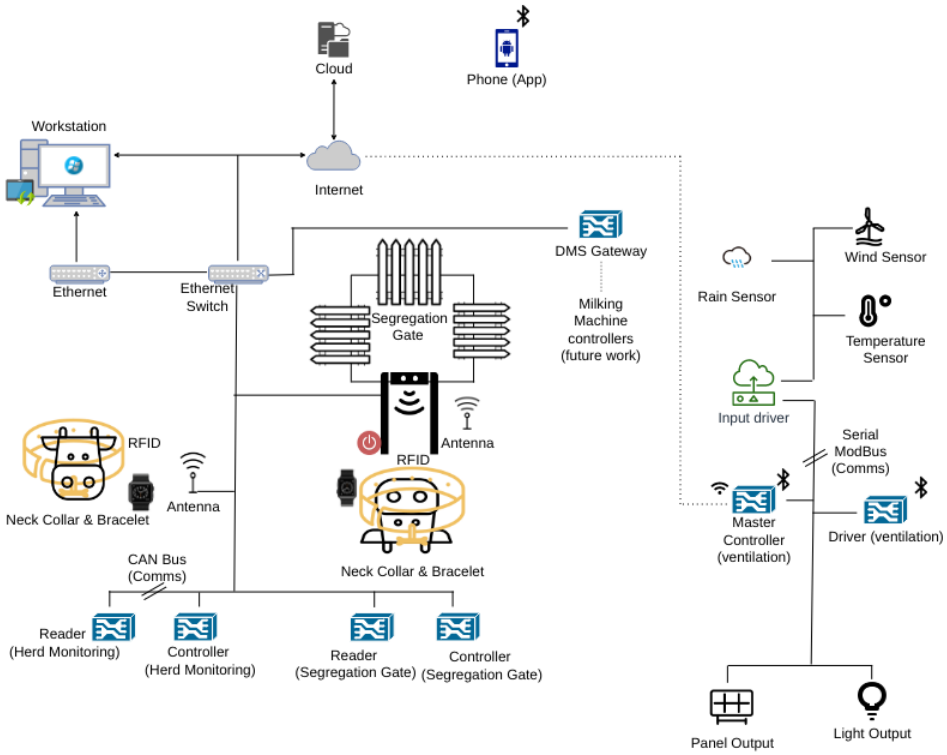


Figure 2.1: Overview of testbed architecture, from [11]

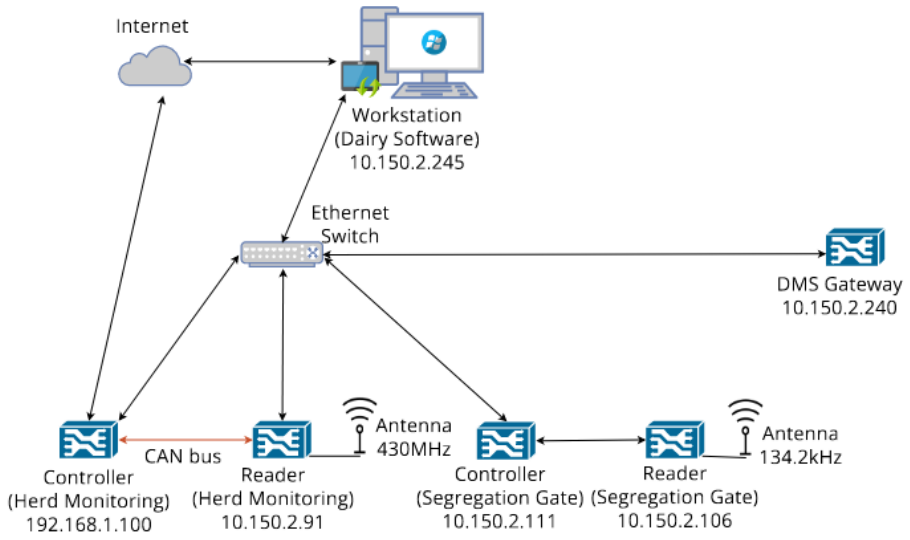


Figure 5: Network diagram of the herd management system.

Figure 2.2: Network diagram - herd management system, from [11]

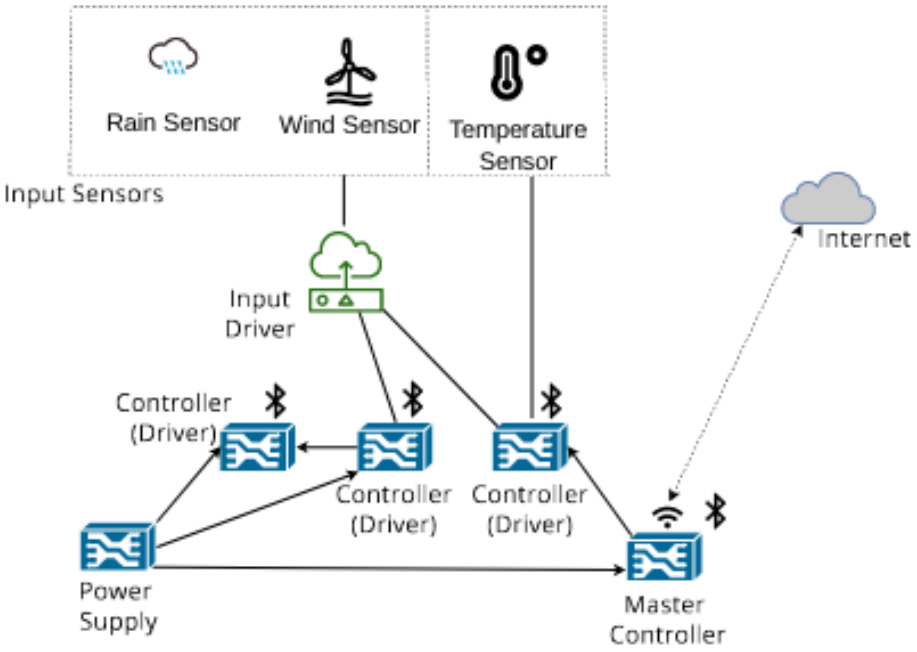


Figure 6: Network diagram of the environment ventilation system.

Figure 2.3: Network diagram - environmental ventilation system, from [11]

Table 2.1: Summary of findings - from [15]

Category	Findings
Cow activity monitoring	Four out of six farms had cow activity monitoring
Milking method	Four out of six farms had automatic milking
Feeding method	Two farms had automatic or semi-automatic feeding; the rest had manual feeding
Manure robot	Two out of six used manure robots
Video surveillance	Four out of six farms had IP cameras, with recording equipment or surveillance PC, installed

for controlling and monitoring through a smartphone app. Other controllers in the EVS connect to the master controller via serial Modbus connectivity. Bluetooth is also available to the EVS for local access through the smartphone app without internet connectivity. Other communication protocols used in the typical dairy farm network are the CAN bus for communicating between the reader and the controller on the HMS and RFID for the readers on the herd monitoring and segregation systems.

The study conducted by Manninen provides valuable insights into the network structure of a dairy farm, which can significantly aid in constructing a comprehensive topology of such systems. However, since the survey only describes six farm networks, it is impossible to generalize the findings to understand how a typical dairy farm operates. Nevertheless, some results are still relevant to this thesis, especially regarding the topology-building process; see Table 2.1.

The combined knowledge described above gives the following list of systems.

- Farm management system (FMS)
- Herd management system (HMS)
- Segregation system (SS)
- Environmental ventilation system (EVS)
- Automatic milking system (AMS)
- Automatic feeding system (AFS)
- Automatic cleaning system (ACS)
- Video surveillance system (VSS)

The details of these systems are presented in Section 4.1. The description is based on a combination of academic literature and technical documents from the suppliers.

2.3 Threat analysis

This section describes threat modeling and analysis, how it is described and used in academic literature, and different approaches to it.

In this thesis, the terms threat analysis and threat modeling are used. According to [18], there is no general agreement on what threat modeling is. According to NIST, it is "a form of risk assessment that models aspects of the attack and defense sides of a logical entity, such as a piece of data, an application, a host, a system, or an environment" [19]. Threat modeling is often performed during the development life cycle of an entity [20], but as will be shown later in the section, it can also be performed after the systems have been developed. The term "threat" is understood as "any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service" [21].

Threat modeling in this thesis will refer to using the threat model to identify threats to a system. It will be used when using STRIDE alone and not with the complementary risk assessment. Threat analysis, and sometimes risk assessment, describes assessing the threats according to their possible impact and likelihood. There seems to be some overlap between the threat modeling and analysis aspects in the academic literature, perhaps since some approaches to this process include risk analysis elements.

A systematic literature review identified 28 threat analyses or approaches [22]. The authors identified that the common techniques were STRIDE, attack trees, graphs and paths, MUCs (misuse cases), problem frames, and threat patterns [22]. Another review of threat modeling techniques showed that the techniques identified had widely different characteristics [18]. As described in Section 2.2, the level of detail in the topology available is not great. Thus, using a threat model that suits the available data makes sense.

Although the threat modeling process varies from method to method, it follows three main steps [23]:

The first step involves constructing a model of the system that's being examined. The model is constructed by creating Data Flow Diagrams (DFDs). These DFDs depict the system in design as an amalgamation of data flows, entities, processes, data stores, and trust boundaries. Subsequently, threat analysis is carried out. This process entails identifying threats within the DFD context, documenting them, and prioritizing them based on their potential impact and likelihood. Lastly, mitigation measures are implemented, such as choosing suitable countermeasures to decrease the risks identified during the threat analysis phase.

Models are approximations and simplifications of complex systems and do not represent reality perfectly. The same could be said about threat models. None of them catches all facets of threats. Threat models can be divided into what they aim to address: asset-centric, attacker-centric, or software-centric [20]. In the context of threat modeling, assets refer to valuable resources or components considered potential targets for attackers. These may include sensitive data, intellectual property, critical infrastructure, or any other element that holds value for the organization. Assets can also be "things attackers want," "things you want to protect,"

or "stepping stones to either of these" [20]. In this asset-centric approach, the threat model identifies the assets needing protection and understands the associated risks. This approach seems intuitive to use, but Shostack warns against it because it does take away the focus on what matters, namely threats [20].

The attacker-centric approach involves understanding potential adversaries' capabilities, motivations, and tactics. Organizations can gain insight into the methods and tools used to compromise their systems by analyzing the attacker's perspective. This approach shares much of its knowledge with threat intelligence. One benefit of this approach is that it makes the threats more vivid for the organization in question [20].

Lastly, the software-centric threat model focuses on the software to identify potential vulnerabilities and weaknesses within an application or system. This approach involves analyzing the software's design, implementation, and deployment to understand how attackers could exploit it. By pinpointing security flaws, organizations can take preventive measures to mitigate potential risks and enhance the overall security posture of their systems. Shostack's take on this approach focuses on making the threat model during the software development phase in question [20]. STRIDE is an example of this approach. This approach makes sense from the developer's view because they typically know the software very well but not necessarily the assets or the attackers [20].

A natural part of the software-centric approach is diagrams, often DFDs (data flow diagrams) [20]. Such diagrams demonstrate how the system or systems in question operate and communicate [20].

Below are a few of the most common threat modeling techniques.

Attack Trees This model allows you to visualize how an asset can be attacked. The attacks against the system are depicted using a tree structure, where the primary objective is the root node, and the various methods to accomplish that objective are represented as leaf nodes [24]. It is an effective way to communicate complex attack scenarios through visualization.

PASTA PASTA (Process for Attack Simulation and Threat Analysis) is a risk-centric threat modeling technique. It is an approach anchored to the business context of the systems in question [25].

OCTAVE OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) is a suite of tools, techniques, and methods for risk-based information, security, strategic assessment, and planning.

One way of looking at threat modeling is to identify where the focus of threat modeling lies. Three common approaches are the asset-, the attacker-, and the system/software-centric approaches [20]. There are upsides and downsides to the different approaches. Among the system/software-centric approaches, STRIDE is the most common one [18].

2.3.1 STRIDE

The STRIDE methodology is used for identifying a set of security threats [20]. It is an acronym of the threat categories, or threat types, Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege [26]. The method is used for enumerating the threats that can exist towards the system, parts of the system, or the connections between the systems (the data flow) [20]. STRIDE does not offer an evaluation of the threats identified. The threat modeling process results show the *possible* ways an attacker *could* attack the system, not the actual likelihood of the threat manifesting, i.e., risk evaluation.

The STRIDE methodology is chosen for this thesis due to the following reasons.

First, it enjoys widespread usage within the domain, underpinning its relevance and applicability [18]. This widespread adoption does not necessarily imply superiority over other models but speaks to its practical utility and acceptance. Second, the variety of cases that STRIDE is used for makes it easier to apply. Third, the data available in this case is scarce, so a model that is flexible and usable in many cases is preferable. Last, STRIDE, a well-documented and accessible methodology, is readily available to researchers. The details of the STRIDE method and how it is applied in this thesis are described in Section 3.2.3.

STRIDE has also been applied at different levels of systems description. Some of the published research on STRIDE shows the method used in very detailed descriptions of systems. An example is [27], where smart devices in telehealth were analyzed using STRIDE. The method has also been proven to be applied in cases where a more general description of the systems is used [4, 28].

STRIDE is combined with other methods since STRIDE does not rank the threats in any way and is not a complete method for assessing threats [20, 23]. In some papers [27, 29, 30], another method, DREAD, was combined with STRIDE. DREAD is a subjective method for assessing the threats that are discovered, e.g., by using STRIDE, and is an acronym for Damage, Reproducibility, Exploitability, Affected users, Discoverability [20]. HARA is applied in [30], a paper that applies STRIDE, and DREAD, to the automotive domain, specifically self-driving cars. HARA stands for Hazard Analysis and Risk Assessment and is commonly used when assessing safety concerns. The combination with the security-focused STRIDE resulted in the method SAHARA, an acronym for Safety-Aware Hazard Analysis and Risk Assessment. Another example of how to combine STRIDE is shown in [4, 28]. Here the authors used a risk matrix to rank the threats after the likelihood of them occurring and established criteria for the level of impact of the threats. The threats are then set to either low, medium, or high according to the matrix.

Table 2.2: Risk matrix - from [4]

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

The different ways that STRIDE is used in combination with other methods show the flexibility of the method. Furthermore, the way STRIDE has been applied to systems with a general description of the systems shows that it applies to the case in this thesis.

As with other models, STRIDE has some potential weaknesses. They are discussed in Section 5.5.

2.3.2 Risk assessment

In addition to the STRIDE analysis, a risk assessment is also conducted. Risk is here understood as the "measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence" [31]. Each threat is evaluated according to its potential impact and likelihood. The impact and likelihood criteria are defined after a model presented in [28]. STRIDE was applied with an impact and likelihood matrix in an industrial control system setting. The descriptions of the potential impact and likelihood were inspired by the NIST 2002 publication *NIST SP 800-30 - Risk management guide for information technology systems* [32] (superseded by *SP 800-30 Rev. 1* in 2012) [28].

This risk assessment was also used in [4], where STRIDE was combined with this matrix when assessing cyber-enabled ships. The content of the two lists is similar to the one presented in the original but much more readable and fluent. The criteria for the impact are listed in three categories, High (H), Medium (M), and Low (L). For likelihood, the categories are Very Likely (VL), Moderate (M), and Rare (R). The details of the categories are presented in Section 3.2.4. The risk assessment result is in the format of a combined score of the impact and the likelihood of the threat, presented in Table 2.2. These criteria lists are used for the risk assessment documented in Section 3.2.

2.4 Threats against dairy farming

This section presents the current cyber threats to the modern agriculture industry. The sources used are industry and governmental reports. This section constitutes the basis for identifying threats using STRIDE, as presented in Section 3.2.

Cyber-related threats to the farming industry are not a theoretical viewpoint. Actual attacks have already taken place, and in 2016 FBI warned that farm-level data was at risk in the US and that farmers should take action to secure their data [1].

The threats facing the technology in the precision agriculture industry are primarily the same as those facing other industries, namely "data theft, stealing resources, reputation loss, destruction of equipment, or gaining an improper financial advantage over a competitor" [33].

Nikander et al. argue that most threats to dairy farms are internal attacks, not external [16]. This could be due to the lack of care for the equipment installed in harsh environments and the poorly installed or mismanaged devices.

There have been cases where ransomware has been used against the farming industry [1]. Other threats that have been highlighted are the threat that hacktivists may destroy data related to the use of genetically-modified organisms (GMOs) or pesticides [1].

Two reports have addressed the new threats to modern agriculture. A public-private partnership in the US in 2018 identified threats to precision agriculture [33]. The other was a report from the agriculture industry from 2019 done in the UK [34]. The threats are summarized below and sorted according to the CIA-triad (Confidentiality, Integrity, Availability).

Not all of these threats are relevant for the dairy farming context since this study also addresses other types of agriculture, especially crop farming, which has other associated threats.

2.4.1 Threats to confidentiality

Threats to confidentiality include intentional and unintentional data theft from decision support systems and farm management systems and deliberate disclosure of confidential industry information [33, 34]. Other threats include foreign access to unmanned aerial system data and unscrupulous sales of confidential data [33]. Motivations for such attacks include activism, market manipulation, or identifying struggling farms for acquisition. Such leaks could harm reputations and delay technology adoption [34].

2.4.2 Threats to integrity

Integrity threats include intentional falsification of data to disrupt the agricultural sectors, the insertion of rogue data into sensor networks that could damage crops or herds, and insufficiently vetted machine learning models with potential adverse effects [33]. Such attacks could undermine consumer confidence, cause financial

harm, expose record falsification, or be part of a nation-state attack. A cyber attack on these systems could significantly impact food companies and the wider economy [34].

2.4.3 Threats to availability

Availability threats are related to equipment availability, particularly during critical farming periods. Disruption to positioning, navigation, and timing systems can also cause significant problems [33]. Potential targets include warehouse HVAC systems, SCADA systems, logistics software, and distribution vehicles [34]. Rural broadband unreliability is another primary concern, and foreign-manufactured equipment could be remotely disabled [33]. Potential motivations include activism, nation-state attacks, or market manipulation by criminal gangs [34].

Chapter 3

Methodology

In this chapter, the methodology of the thesis is presented. The first part is a description of the steps needed to make the topology of the cyber-enabled farm. The second part presents the STRIDE method and the risk assessment process.

3.1 Making the topology

In section 2.2, the systems on a dairy farm from the academic literature are documented. Very little research is done on a dairy farm network or topology. That means there is a lack of knowledge about how the networks vary, how large they are, what components exist, which brand they are, and how they are configured.

There are different ways to address this lack of knowledge. The goal of this step is to make a topology that is suited for threat analysis. It should also have some future validity.

There is an argument to be made for a topology that closely resembles systems currently in use on dairy farms. When applied to a threat model, a topology will give insight into how threats are today. First, there is the problem of variations between dairy farms. For example, some farms have few systems relevant to cybersecurity threat analysis. Secondly, a topology that resembles today's situation will be outdated.

The other option is to create a topology considering future aspects of how a dairy farm uses technology. This approach has limitations. It is hard to predict which technologies will be implemented and how they will be implemented and connected.

As described in 2.1, a lack of research into the topology of cyber-enabled dairy farms impacts the methodology in this thesis. Since no threat analysis has been conducted on cyber-enabled systems on a dairy farm, it makes sense first to make a threat model of how it looks now and then later build on that topology when considering new technologies. Regarding the problem of variation and to make the topology more relevant, the thesis seeks to identify the existing state-of-the-art systems already in place but from different suppliers. State-of-the-art technologies available in other countries will also be examined.

There is little reason to believe Norwegian dairy farmers will not implement new technologies, given that Norway has sufficient capital to invest and is an early technology adopter.

The following sources to make the topology will be used.

- Existing descriptions of the systems in academic literature, described in Section 2.2.
- Document study of technical documents from the dairy farm industry.

The research objective is to achieve a topology suitable for a high-level STRIDE threat model. The topology needs to be described in enough detail. Since it aims to be vendor-neutral, it cannot be specific on what type of soft or hardware it uses.

3.1.1 Document study

The document study will focus on reading documents from different equipment suppliers from the dairy farming industry. Three of the biggest names in Europe and the USA are Lely, DeLaval, and GEA Group. The documents that will be used are technical documents, brochures, and manuals of dairy farming equipment.

3.1.2 Identification of new systems

(rephrase and adjust so that it fits in M. can be moved to another place in M) Information from three of the largest suppliers of equipment and systems to dairy farms was consulted to identify systems not described in the academic literature. These suppliers were Lely Industries N.V. (shortened Lely), DeLaval, and GEA Group AG (shortened GEA). These suppliers' technical documents, brochures, and website content were searched through to look for new systems.

Some limits were set in the search process. The systems should be able to communicate with other systems on the farm, i.e., cyber-enabled. To limit the scope and not make the types of systems too diverse, systems not directly tied to the cows or the milking process were not considered, such as milk and manure processing systems.

3.2 Threat analysis

This section provides a general description of threat modeling and STRIDE in particular. The threat analysis represented in Section 4 is based on the methods described in both the general part and the STRIDE part of this section, as well as the risk assessment. How STRIDE is applied in academic literature is described in Section 2.3.

3.2.1 Threat modeling in general

According to the National Institute of Standards and Technology (NIST), threat modeling is a "form of risk assessment that models aspects of the attack and de-

fense sides of a logical entity, such as a piece of data, an application, a host, a system, or an environment" [19]. Adam Shostack, an often-cited source on this topic, provides a more straightforward definition. Threat modeling is "about using models to find security problems" and a method to "anticipate the threats that could affect you" [20]. In his book *Threat Modeling: Designing for Security*, which will often be cited in this section, he describes the different aspects of threat modeling in detail. Shostack states that the following four questions as essential in threat modeling:

1. What are you building?
2. What can go wrong?
3. What should you do about those things that can go wrong?
4. Did you do a decent job of analysis?

All but question three are relevant to this thesis. Question three is relevant to the cybersecurity of dairy farming, but since the STRIDE methodology does not cover countermeasures, it falls out of the scope of this thesis.

The methodology side of the first question, "What are you building?" is answered in the last part of this chapter, in Section 3.1. The methodology part of the second question, "What can go wrong?" is answered here. The last question, "Did you do a decent job of analysis," is discussed in Section 5.4.

3.2.2 STRIDE

STRIDE is a qualitative and subjective threat modeling process. It is a software-centric approach to threat modeling. Developed by Loren Kohnfelder and Praerit Garg in 1999 at Microsoft, it was initially designed for internal use to identify threats during the software development cycle's design phase [35]. STRIDE continues to be used today at Microsoft and is now an integral component of their Threat Modeling Tool (TMT) and the Security Development Lifecycle (SDL). The TMT, which is freely available, helps with the creation of Data Flow Diagrams (DFDs) and applying the STRIDE methodology. STRIDE has now become a widely used methodology for threat modeling [18].

STRIDE is an acronym for Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege, which are six categories of threats. From the attackers' point of view, these threats can be seen as ways of threatening the target [23]. The threats are linked to several fundamental principles in information security; see Table 3.1.

Below is a more detailed description of the different threat categories. The sources for the examples of attacks in each category are from the *Elevation of Privilege card game* and general threat descriptions by Adam Shostack [20]. The general description is from Howard and Leipners *Secure Development Lifecycle* [35]. These descriptions are used to identify threats against dairy farm systems, presented in Section 3.2.

Table 3.1: STRIDE threat categories - from [20]

Threat	**Property violated**	**Threat definition**
Spoofing	Authentication	Pretending to be something or someone other than yourself.
Tampering	Integrity	Modifying something on disk, on a network, or in memory.
Repudiation	Non-repudiation	Claiming that you didn't do something or were not responsible. Repudiation can be honest or false, and the key question for system designers is, what evidence do you have?
Information disclosure	Confidentiality	Providing information to someone not authorized to see it.
Denial of service	Availability	Absorbing resources needed to provide service.
Elevation of privilege	Authorization	Allowing someone to do something they're not authorized to do.

Spoofing Spoofing is when an attacker assumes the identity of something or somebody [35]. Spoofing could happen at a user, server, client, process, or code level. An example is when the server or client password is easy to guess or not present. The login credentials could also be stolen from other places, such as leaked credential databases on the internet [20].

Tampering Tampering threats refer to malicious actors' harmful alteration of data or code. Tampering could occur when the code or data is at rest or between two points. Without integrity protection for data or code on the network, a malicious actor can alter the data [35]. Another example is when the key exchange in the crypto part of the system is poorly written. The attacker can use these faults to get access to the system. When data is sent, and the receiving party does not verify the integrity of the data upon arrival, they cannot determine if the data was altered or manipulated during the transmission [20].

Repudiation A repudiation threat is when an attacker dispute having carried out a specific action and where other parties cannot verify or challenge this claim [35]. For instance, when a user conducts a prohibited action in a system that cannot track the malicious operation, they present a repudiation threat. A system without logging capability will be unable to track user activity on the system [20].

Information disclosure Information disclosure threats relate to the unintentional exposure of data or information [35]. Such threats might involve situations where a user can access a file for which they have not been granted permission or instances where an intruder successfully intercepts and reads data being transferred between computers [20].

Denial of service Denial of service attacks makes a system unavailable or unusable by denying or degrading it for the user [20]. The attacks can be aimed at either the client or server side. Furthermore, it can be from an authenticated source or anonymous. Lastly, it can be temporary or persistent [20].

Elevation of privilege Elevation of privilege threats uses a vulnerability in the system to gain higher privileges. An example is for an anonymous user to gain low-level access or a low-level access user to gain admin or root control [35]. The threat also pertains to the type of access the attacker has. For example, if the attacker can enter arbitrary code into the system, it is considered a severe Elevation of Privilege threat [20].

3.2.3 Threat modeling process

There is no conclusive manual for utilizing STRIDE [36]. This part of the threat analysis is the second step in the process, as mentioned earlier by Adam Shostack [20]. In this thesis, the threat modeling process applied is the following. On each identified system in the cyber-enabled farm, one threat is identified in each of the STRIDE threat categories. As described above, multiple threats could be identified in each system. The reason for only identifying one threat in each category is the following. The systems in question are not described at a detailed level, so the threat must be described at a system level, similar to that of [4, 28].

When pinpointing potential threats to a system, the primary focus is on external, intentionally malicious threats. However, this approach overlooks the possibility of internal and unintentional threats, which might substantially affect the system's operation, business continuity, and reputation.

When using STRIDE to identify threats, the goal is to show what might go wrong if the threats are not considered [20]. Exactly how it can go wrong, or if there are defense mechanisms in place to stop the threat, is not part of the scope of this threat modeling process.

Some threats will be a mix of each category, so labeling them with only one threat category can be difficult [20]. The goal is to identify the threats, so which category it falls into is less important [20].

3.2.4 Risk assessment

The risk assessment part of the thesis is done with the method detailed in Section 2.3.2. The likelihood criteria used in [4] are retained as they are. The following

Table 3.2: Impact criteria - based on [4]

.

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 wide energy loss. Threats that may cause damage to the infrastructure. Threats that will lead to personal information leakage. Threats that will result in economic damage and client loss. Threats that will result in system malfunction.
Medium (M)	Threats that could cause procedure disruption in real-time. Threats that could result in miscalculations in the systems, thus influencing the operations. Threats that could result in a bad reputation for the company and client dissatisfaction. Threats that may cause information disclosure. 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. Threats that could cause network information leakage.
Low (L)	Threats that could result in operation delay or disruption in non-critical procedures. Threats that could result in leakage of non-sensitive data.

changes are made to the impact criteria to suit the dairy farming field.

To include the possibility for the systems to hurt the animals on the farm, "Threats that could result in the loss of animal life" are added to the "High" in the impact category. "Threats that could result in serious harm to animals" are added to "Medium" and is in place to include the possibility of the systems seriously hurting the cows. The content of both criteria lists is otherwise revised for minor grammatical errors. The lists are presented in Tables 3.2 and 3.3.

Neither of the two identified articles [4, 28] that have used this approach have provided a detailed description of how to perform the risk assessments. The following procedure is therefore used.

The risk assessment is done on every threat identified using STRIDE. For a threat to be placed in one of the categories, it is enough that one criterion is fulfilled. For example, it is enough for a threat to have an impact that "will result in system malfunction" to be considered a "High" impact threat and check only the likelihood criteria "High system's exposure to the Internet" to have the score "Very Likely." Using the Impact/Likelihood matrix gives a risk score of "High"; see Table 3.4.

Table 3.3: Likelihood criteria - based on [4]

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 countermeasures are insufficient to prevent the attack. 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.

The risk analysis of each threat is done on a best-effort basis. In cases where there is not enough information to place a threat in the categories, the principle of "assume the worst" is used, i.e., placed in the "high" impact or "very likely" category.

The combined STRIDE analysis and risk assessment results are presented in a table; see Table 3.5, where T stands for Threat, I for Impact, L for Likelihood, and R for Risk. The possible outcomes of the Impact are H (High), M (Medium), and L (Low). For likelihood, it is V (Very Likely), Moderate (M), and R (Rare). The combined score using the risk matrix is expressed in column R as H (High), M (Medium), and L (Low).

Table 3.4: Risk matrix - from [4]

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

Table 3.5: Template for the STRIDE analysis

T	**Description of threat**	**I**	**L**	**R**
S				
T				
R				
I				
D				
E				

Chapter 4

Results

In this chapter, the results of making the topology of a dairy farm are presented, along with the threat analysis performed on that topology. First, new systems are described. Second, the ten systems identified on a dairy farm are described according to their functionality, data flow, and dependencies. Finally, the results of the threat modeling and risk assessment is presented.

4.1 The topology of a dairy farm

In this section, the results of making the topology are presented. First, new systems are presented. Then, in Section 4.2, those systems are described in detail.

Two new systems were identified using the approach and criteria outlined in Section 3.1.2.

- The automatic feed-pushing system (AFPS) - robots that move around in the feeding area in the barn and push the food toward where the cows are, enabling them to reach and eat it.
- The automatic lighting system (ALS) - the system which provides lighting in the barn. The FMS is connected to ALS to operate the lighting.

Together with those systems already described in the literature, it makes the following list of ten cyber-enabled systems.

- Farm management system (FMS)
- Herd management system (HMS)
- Segregation system (SS)
- Environmental ventilation system (EVS)
- Automatic milking system (AMS)
- Automatic feeding system (AFS)
- Automatic cleaning system (ACS)
- Video surveillance system (VSS)
- Automatic feed-pushing system (AFPS)
- Automatic lighting system (ALS)

4.2 Description of systems

In this section, the different systems are described.

The more details about the system in question, the better for the threat model. However, as demonstrated in [4], a STRIDE analysis could also be performed on systems without a very detailed description of the systems. The lack of a detailed description will also be the case in this thesis. The following categories will be used as a guide for describing the systems. Some systems are better described than others because more details were found.

- Functionality - a brief description of the system, its purpose, and primary function within the farm.
- Data flow - an outline of the flow of data. Including inputs and outputs to other systems.
- Dependencies - internal dependencies on other systems. External systems or entities are not identified. The extent to which one system depends on another is primarily determined by how much it relies on the latter. A typical scenario is whether the data received from the other system is necessary for the operation of the system in question.

Most of the details below are from gathering data from technical documents from the three significant suppliers of dairy farm systems. However, the descriptions gathered from the academic literature are acknowledged and cited.

4.2.1 Farm management system

Unless specifically mentioned, the description of the FMS below is based on technical documents from two different vendors [37, 38].

In [11], the FMS is called "dairy management software" and is only described indirectly through other systems.

Functionality The farm management system (FMS) on 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.

For the relevance of this thesis, the FMS plays a critical role in four areas of the farms' operation. 1) animal health management. The system helps monitor the health of each animal by tracking vaccinations, medical treatments, and regular check-ups. It also provides alerts and reminders for upcoming health-related events. 2) Milk production tracking: The FMS records each cow's daily milk production data. This information helps the farmers analyze trends and make better, data-driven decisions for improving productivity. 3) Breeding and reproduction

management: The system keeps track of breeding cycles, insemination dates, and calving history. It also provides notifications for upcoming breeding-related events to optimize reproduction efficiency. 4) Food and nutrition management: The system calculates the nutritional requirements of the herd and the individual cow, helping farmers create balanced diets and monitor food consumption.

The FMS also provides tools to control other systems, such as setting routes on the ACS.

Data flow In the testbed model made in [11], the FMS receives information from all systems on the dairy farm except the environmental ventilation system (EVS).

In the surveyed documents, the FMS receives data from all the other cyber-enabled systems on the farm. The FMS is the single point in the topology where all data is stored, used, and visualized for the farmer. 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 the other cyber-enabled systems on the farm. It works as the control center, and many tasks can be done remotely, either through PC or mobile phone software. However, it must obtain and deliver the correct data to other systems to serve its function. Other systems, such as the AMS, could lose vital operational functions if not fed data correctly.

4.2.2 Herd management system

The surveyed documents do not clearly define the herd management system (HMS). However, as described in [11], the primary function is to collect data from responders attached to the cow.

Functionality According to [11], the HMS gathers information such as "eating habits, lying time, stand-up counts, step counts, and temperature." The system consists of responders placed around the neck or leg of the cow. They gather data from the cows and transmit them wirelessly to receivers. The information is sent to the FMS regularly [11]. The information is stored and processed in the FMS and used to make informed decisions about the cows' health. The system is considered a sensor system.

These sensors also function as electronic identification tags, helping identify individual cows for interactions with other systems like segregation gates or Automated Milking Systems (AMS). Specific sensors can track attributes like a cow's activity level, stride, and rumination levels, with some potential for local data storage and processing [39].

Collectively, this data helps monitor diverse health aspects such as detecting abnormal walking patterns, frequency of laying down, or changes in rumination

activity. All of which offer invaluable insights to farmers, enabling early identification of potential health issues.

Data flow The data is transmitted from the responder to the reader via RFID and then to the controller on the CAN bus. The controller sends the data to the FMS through Ethernet [11]. It sends data to the FMS about the condition of the cows.

The sensors send the data to receivers in the barn at regular intervals. Finally, the data is sent to the FMS from the receivers, where the data is stored and processed for further analysis [40].

Dependencies Since the HMS is a passive sensory system, the system does not rely on other systems to function.

4.2.3 Segregation system

Functionality The segregation system allows the cows to pass through the farm's gates. 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 resting areas [11]. Where the cows are allowed to go is dependent on different factors. In the case of the AMS, the SS ensures that the cows are only allowed to be milked a certain number of times daily. In the case of the grazing and feeding, and resting areas, restrictions may be put in place to ensure that only specific cows are allowed to be with each other. The system relies on the ID tag on the cow that identifies to the system via the reader which cow is trying to use the segregation gates [11]. The gates are opened and closed pneumatically [39].

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 [41]. 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 [11].

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.

4.2.4 Environmental ventilation system

The surveyed literature does not describe the environmental ventilation system (EVS) in detail. Instead, the description of the system relies entirely on [11].

Functionality The EVS adjusts the temperature inside the barn via ventilation. The cows produce heat, and the temperature needs to be just right for them to thrive. The ventilation is installed in the barn to adjust the conditions inside. The airflow through the ventilation is adjusted by actuators that the controllers control. The system is disconnected from the rest of the network and 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, and wind direction and speed from sensors on the farm. Based on information from those, it adjusts the ventilation to give 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 other systems.

4.2.5 Automatic milking system

The automatic milking system (AMS) is an advanced robot that milks the cow. One or more robots could be installed on the farm. It comes in many different variants. The one considered here is the type that the cow walks into on its own and gets milked a few times a day. The AMS is preferred over other methods because it can optimize the milking process, reduce labor requirements, and improve overall productivity and animal welfare [42]. The system typically offers various functionalities and connects with others, relying on them for seamless and efficient operation.

The description below is solely from the surveyed documents from DeLaval, Lely, and GEA [40, 41, 43].

Functionality The cow must go through the segregation gate (SS) before it enters the AMS.

The system's main purpose is to milk the cow. It uses four robotic arms with suction cups that latch on the cow's teats. It uses laser sensors and 3D cameras to gauge the cow's position in the AMS to latch on.

Before milking, the teats of the cow are sterilized. During the milking, the cow is fed with concentrate to encourage the cow to come into AMS and keep it still during milking. The concentrate is a type of food. Medicine can be added to the concentrate if needed. After the milk is pumped from the cow, the milk is analyzed for signs of mastitis (inflammation in the udder tissue), impurities, and quality control. If the milk is not up to quality standards, it is pumped out to the sewer system so it does not affect the rest of the milk in the storage tank.

After milking, the teats are cleaned and disinfected. Everything the AMS does is done according to the individual need of the cow. The system uses the ID tag, usually RFID, on the cow to know which cow has entered the machine. If the cow

is known to deliver milk of low quality, the milk is automatically pumped into the sewer after milking. The cow is permitted to be milked a specified number of times daily. If the cow tries to exceed this number, it is not allowed through the AMS gates.

Data flow The SS asks the FMS if the cow is allowed through to the AMS. The AMS sends data about milk production, quality analysis, health monitoring, feeding data, and alerts and notifications to the FMS. Milk production data encompass the quantity of milk produced, the timing of the milking process, and the specific instances when each cow is milked. Milk quality parameters include such data as fat and protein content, somatic cell count, and lactose levels. 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. If something goes wrong in the AMS, a cow is sick, or service is needed, alarms are sent to the FMS. The FMS can be set to forward error messages to the farmer.

Dependencies For the correct, individualized treatment of the cow, the AMS needs to identify the cow correctly through the ID tag. In addition, for the proper treatment of the cow, the history of the cow is needed from the FMS.

4.2.6 Automatic feeding system

Although mentioned briefly in [15], the description of the automatic feed system (AFS) below is gathered from [39].

The AFS provides an efficient and precise means of delivering feed to the cows, improving productivity, and optimizing resources on the farm.

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 a robot that transports the feed. In this case, the robot version of the AFS. 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 the feed, some of it gets pushed out so the cows cannot access it. The same robot can then push the feed so that cows can 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 depends on accurate data from the FMS about how much food is needed to be delivered to cows.

4.2.7 Automatic cleaning system

Although mentioned briefly in [15], the description of the automatic cleaning system (ACS) below is gathered from [39].

Functionality A self-driving robot pushes the manure in front of itself to remove the manure from the cows. The floor is slatted (small in the floor), and as the robot pushes the manure in front of itself, it falls below and is further processed. The robot must go between the cows to do its job, so it has sensors to detect if the cows are in their way. It does move around the cows or stop if necessary. The robot's path can be pre-set or make the route based on the cow's location. The robot travels 6 km/h, weighs up to 340 kg, and travels 9-18 m/min.

Data flow The ACS communicates with the FMS about the planned cleaning. To enhance its operation, it can use the information about the whereabouts of the cows from the HMS received through the FMS to avoid trying to clean where there are lots of cows gathered.

Dependencies The ACS relies on information from the FMS to know when it should clean the floors.

4.2.8 Video surveillance system

The description of the system is only gathered from academic literature, as it is not described in the surveyed literature.

Functionality According to [15], video surveillance (VSS) is a common feature on dairy farms. It is either an analog or digital (IP camera) and connected to a dedicated surveillance PC or IP recorder. The VSS allows the farmer to monitor the farm from one place and ensures that it operates as it should.

Data flow In the case of [15], the cameras were, in some cases, connected to the rest of the network. Live video is transmitted from the cameras to the recorder or PC and shown on a monitor. It does not need to communicate to the FMS or any other system on the farm.

Dependencies The VSS is not dependent on other systems on the farm to operate.

4.2.9 Automatic feed-pushing system

Functionality The automatic feed-pushing system (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 the food. The routes for the robot can be programmed manually,

or the robot can autonomously navigate its path. It then uses sensory technology to identify where the food is and how close it is to the cows [39].

Data flow The AFPS is connected to the farm management system (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.

4.2.10 Automatic lighting system

The description below is solely based on the surveyed documents. The automatic lighting system (ALS) automatically adjusts the light inside the barn according to a preplanned schedule or input from light sensors [39].

Functionality The automatic lighting system, 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 AL detects the light level inside and outside the barn to adjust for the proper light setting inside. The proper light setting gives the cows better quality of life and thus could increase production.

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 give the cows the correct amount of light.

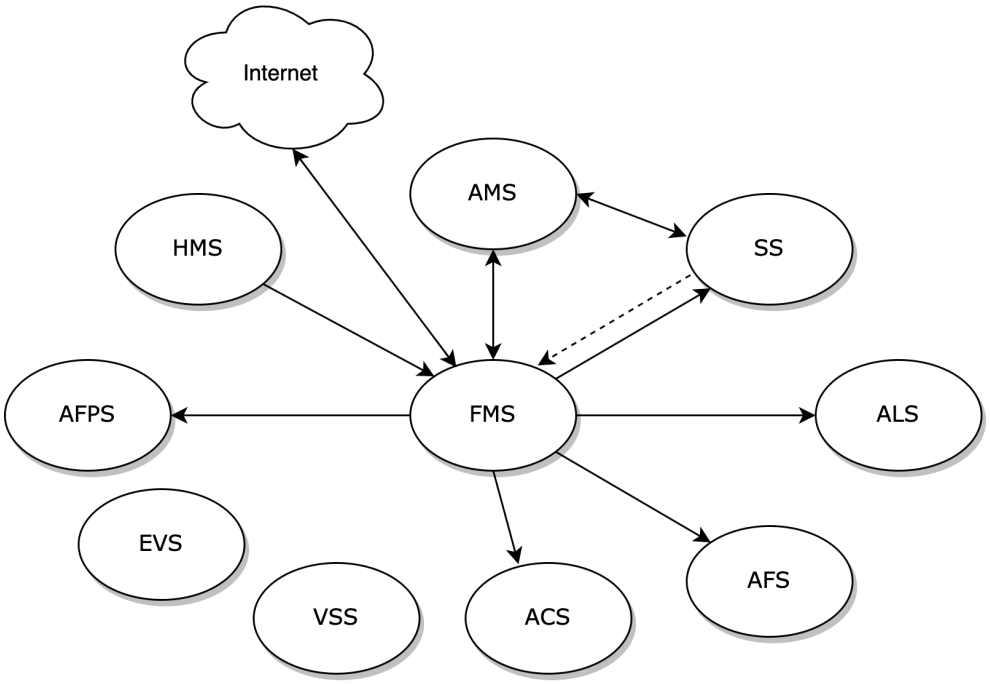
4.2.11 A topology of dairy farm

The information above, combined with the description of systems in Section 2.2, gives the following overall description of systems.

Figure 4.1 shows how the systems are connected. Some data flows both ways in all the systems connected to the FMS. The directional line represents the *main* flow of information. The dotted line from the SS to the FMS indicates that some information flows from the SS to the FMS.

The Farm Management System (FMS) is a central hub for the different cyber-enabled systems on a dairy farm. It manages and monitors different aspects of the farm, including herd management, milk production, animal health, and nutrition. For example, it interacts with the Herd Management System (HMS) to collect data from cows to monitor their health and make informed decisions on other operations. The FMS interacts with the Segregation System, which uses ID tags to control the movement of cows, allowing them to access specific areas like grazing

Figure 4.1: Overview of systems on a dairy farm, with information flows



areas, the milking robot (AMS), and resting areas. Although not directly connected to the FMS, the Environmental Ventilation System is crucial for maintaining a suitable temperature in the barn and adjusting the ventilation based on weather data.

The Automatic Milking System, a vital part of the farm, relies on the FMS and the SS to identify cows and provide their history for individualized treatment. It milks the cows, analyzes the milk, and returns data to the FMS. It also relies on the Segregation System to let the cows into the farm.

The Automatic Feeding System relies on the FMS for data on how much feed is needed for each cow, using robots to deliver the feed and robots to push the feed into the correct position. The Automatic Cleaning System, which cleans the barn floor, and the Automatic Feed-Pushing System, which pushes food toward the cows, rely on FMS data for their operation. The Video Surveillance System, although not connected to the FMS, provides essential farm monitoring. Lastly, the Automatic Lighting System uses sensors to adjust lighting based on various factors. All these systems work together, primarily through the FMS, to optimize the operations of a dairy farm.

4.3 Threat modeling and risk assessment

Below are the results of the STRIDE analysis and risk assessments performed on the systems described above. The results are presented in tables. The threat modeling is done by applying the STRIDE method explained in Section 3 with knowledge of threats described in Section 2.4. In most of the STRIDE categories, only one threat is considered. For the risk assessment part of the analysis, each threat is ranked according to the methods described in Section 3.2.4. Sections 5.3 and 5.4 discuss the discovered threats and risk assessment.

Table 4.1: Threats to the farm management system (FMS)

T	Description of threat	I	L	R
S	Since the system is internet-connected, an attacker could spoof the identity of a legitimate user, such as a farm employee or the farmer, using remote access to gain unauthorized access to the FMS. This could lead to unauthorized modifications or data theft of valuable information.	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 health of the cows.	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 makes it challenging to identify and address the source of discrepancies or malicious activity.	M	V	H
I	Information about the health of the cows could be leaked, possibly leading to a disadvantage to the farmer against competitors	M	V	H
D	An attacker could launch an attack against the system, for example, a distributed denial of service (DDoS) attack, overwhelming the FMS with traffic and causing it to become unresponsive and halting the farm's operations.	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 higher-level users. This includes actions such as altering important settings, deploying malicious software, or disabling critical system features of the system. This could result in significant operational disruptions or damage to the farm's infrastructure.	H	V	H

Table 4.2: Threats to the herd management system (HMS)

T	Description of threat	I	L	R
S	Each cow is identified by a unique electronic ID. An attacker could spoof the system by changing the cow's identity when it communicates 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	Data from the sensors are sent to receivers wirelessly, which introduces the possibility of data being intercepted and tampered with during transmission. An attacker could manipulate the data, such as eating habits or temperature readings and rumination activity, leading to incorrect assessments of cow health.	M	M	M
R	Given the importance of the monitoring and decision-making processes of the HMS, the repudiation of actions within this system is not allowed. 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 it's not properly 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	The data from the sensors is sent to the receivers wirelessly. If an attacker can exploit vulnerabilities in this transmission process, they could potentially 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 4.3: Threats to the segregation system (SS)

T	Description of threat	I	L	R
S	An attacker could intercept and modify communication between the RFID reader and FMS, masquerading as the legitimate FMS to grant or deny access. 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 pneumatic 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 don't 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 pneumatic 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 then maximize the impact of their activities by targeting the farm at the most vulnerable times.	M	M	M
D	An attacker could use a jammer to 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 be able to. This could lead to cows queuing up and ending up in the wrong place on the farm.	M	M	M

Table 4.4: Threats to the environment ventilation system (EVS)

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 adjustments to the EVS through the mobile app, potentially leading to disputes about who did what.	L	R	L
I	If the Bluetooth connection or mobile app is not secured properly, an attacker could intercept the transmitted data. This might reveal sensitive information about the farm's operating conditions, which 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. Alternatively, the attacker could overload the Bluetooth connection or mobile app, preventing legitimate users from accessing and controlling the system.	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 4.5: Threats to the automatic milking system (AMS)

T	Description of threat	I	L	R
S	The AMS rely on the ID tag on the cow to identify it. An attacker could spoof these ID tags so 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 distribution of poor-quality or contaminated milk, posing a significant threat to the dairy industry and the reputation of the farmer. Tampering with the quality control data could lead the system to pass infected or bad milk to 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 resolving the adverse effects on cows' health and milk production.	M	M	M
I	Attackers could leak sensitive data such as milk production, quality analysis, health monitoring, and feeding data. Since the milking process is a crucial part of dairy farms' operation, this could impact the farm's competitiveness if competitors received the data.	H	M	H
D	Disrupting the communication between the AMS and the FMS is a critical denial of service threat. If the AMS cannot receive the necessary cow history data, it may fail to provide proper individualized treatment, leading to reduced productivity, animal welfare issues, and potential revenue loss.	H	M	H
E	If an attacker exploits vulnerabilities within the AMS systems 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 4.6: Threats to the automatic feeding system (AFS)

T	Description of threat	I	L	R
S	An attacker may pose as the 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 gain unauthorized access to the AFS, exposing sensitive 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	A threat actors could potentially gain control over the AFS robot, enabling them to manipulate the feeding process, cause damage to the robot or facilities, or even harm the cows.	H	M	H

Table 4.7: Threats to the automatic cleaning system (ACS)

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 not to 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, suboptimal 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 are unfortunate, since such actions could compromise the sanitary conditions in the barn, thereby threatening the health of the animals.	L	M	L
I	An attacker could access sensitive data such as cow locations, cleaning schedules, or facility layout, potentially compromising the barn's operational security or allowing for targeted sabotage in the future.	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, alter its settings, or extract sensitive data.	M	M	M

Table 4.8: Threats to the video surveillance system (VSS)

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 on 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 that took place 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 clearly attributable. Denial of responsibility for such actions, which could mislead the farmer and possibly lead to security breaches, is unacceptable.	M	R	L
I	An attacker could leak feeds or recordings, potentially disclosing sensitive 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 4.9: Threats to the automatic feed pushing system (AFPS)

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 improper feeding times or taking inefficient routes, 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 or knowledge of where it is. This could result in incorrect movement and even physical damage to the equipment or the animals when the robot collides.	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 sensitive 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 or disrupting the feeding process.	M	M	M

Table 4.10: Threats to the automatic lighting system (ALS)

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. If the system that controls the light, the FMS, gets false readings, it is led to adjust the lighting improperly. This could lead to improper lighting conditions, negatively impacting the cows' health and productivity.	L	M	L
R	If actions in the ALS are untraceable to a specific user, it could lead to undetected malicious activities or repeated system faults, adversely affecting the cows' health and productivity.	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 and offering a window for further malicious activities.	L	M	L
D	An attacker could flood the controllers in the lighting system with the request, possibly causing the lights to fault. This must be done on-site since the system isn't connected to the internet or other systems.	M	M	M
E	If an attacker gains administrative access to the system, they could misuse this to disrupt the lighting schedules, or even turn off the lights entirely. This could cause undue stress to the cows, potentially affecting their health and productivity, and in the worst-case scenario, could create unsafe working conditions for farm workers.	M	M	M

Chapter 5

Discussion

The discussion part addresses the results in light of the research questions. Each research question is discussed separately, and relevant topics from the background and related works are discussed when relevant.

5.1 RQ 1.1: What are the cyber-enabled systems in a dairy farm?

Ten identified cyber-enabled systems on a dairy farm were discovered in this thesis. These are listed below.

- Farm management system (FMS)
- Herd management system (HMS)
- Segregation system (SS)
- Environmental ventilation system (EVS)
- Automatic milking system (AMS)
- Automatic feeding system (AFS)
- Automatic cleaning system (ACS)
- Video surveillance system (VSS)
- Automatic feed-pushing system (AFPS)
- Automatic lighting system (ALS)

The first eight systems in the list were found in the relevant academic literature. All of these systems were also found in the document analysis. The last two, the AFPS and ALS, were identified through document analysis; see Section 4.1 for details.

The question of what constitutes a system is worth mentioning. There were some discrepancies between the systems descriptions in the literature and those in the document analysis. In Agarwal et al., the segregation system (SS) and the herd management system (HMS) are regarded as one system, called "herd management." In this thesis, the systems are separate. The SS is the system where the cows are let in and out of areas according to farm management systems (FMS)

rules. The cows are identified by an id in the form of a chip on the cow and let in and out through gates around the farm. The HMS is the various sensing capabilities that are placed on the cow. The responders available have a varying number of functions. Some responders have the SS and the HMS functionality, while others only have SS functionality. In both cases, the two main functions are distinct in what they do. This separate functionality is the reason for splitting the systems into two systems.

Since the threat analysis mainly focuses on one threat in each category, splitting the systems to show the different threats makes sense. An alternative approach could involve considering the SS and HMS as two distinct entities, categorizing them as sub-systems rather than treating them as a single system. Another possibility would be to treat the SS and HMS not as one but as two separate systems, calling them sub-systems.

The systems that are identified in this thesis are separate physical entities. Another way of identifying a system is to consider it logically separate from another. The reason for identifying and separating the systems at their physical level is because of two reasons. First, due to the physical nature of most of the systems, e.g., the ACS, on a dairy farm, and those systems being connected, there will be many physical systems. These systems could be called cyber-physical systems since they are connected to a more extensive system with sensors and actuators, i.e., systems that interact with the physical world. Second, the data studied in this thesis, the technical documents from equipment suppliers to dairy farms, describe the physical nature of the systems, not their logical side.

5.2 RQ 1.2: What are the properties of the cyber-enabled systems on a dairy farm?

The centrality-aspect of the topology A property of the cyber-enabled topology is that there is a central node in the topology, the FMS. This feature aligns with the findings from [16]. The Agarwal et al. study does not address the centrality aspect of the topology, as it only addresses three systems [11]. The central node is connected to all the other systems except the VSS and EVS. It works as a centralized data collection, analysis, and decision-making hub. The FMS allows for remote management of the farm. It receives and delivers data to the other systems to make them function correctly. It is also responsible for quality control data sent to the milk buyer, reinforcing its central role in the farm's operations.

A centralized network like this makes the central node in that network a target for attackers. If other systems are heavily dependent on this central node for their operation, the ramifications of any malfunction become significantly more extensive. The details of how reliant the other nodes are on the central node are not in the scope of the thesis. Some comments, however, could be made on the topic. If the nodes rely entirely on the central node for information exchange and operational input to work, an attack on the central node could halt all operations.

On the other hand, if there are mechanisms in place for the peripheral nodes to communicate directly in the event of a central node failure or at the normal state, the impact of an attack may be less severe. These mechanisms could include alternative routes, peer-to-peer connections, or backup nodes. The results indicate that the FMS stores and processes many data and decisions. Still, it is unknown to what degree the other nodes, such as the SS, rely on constant communication with the FMS to operate or if the SS stores the access privileges locally. If the Segregation System (SS) does not operate properly, the cows may be unable to access the Automated Milking System (AMS). This lack of access to the AMS could prevent the cows from being milked, negatively impacting their health.

Cyber-physical systems The results show that the systems are considered cyber-physical systems (CPS). Such systems are designed to orchestrate a network of interactive elements that collaborate toward achieving complex tasks. In a cyber-enabled dairy farm, systems like the automatic milking system (AMS), automatic feeding system (AFS), and environmental ventilation system (EVS) are examples of CPS at work. Embedded systems and networks monitor and control the physical processes in these systems, with feedback loops where physical processes affect computations and vice versa. For example, the AFS uses near real-time data from the farm management system (FMS) to adjust feeding schedules and quantities, thereby optimizing the physical process of feeding in response to computational data.

Connections to the EVS and VSS Although the results did not find that the EVS and VSS systems were connected to the FMS, they could be connected in a future configuration. Technological advances continue enhancing our capacity to create more interconnected systems, making them more efficient. The FMS remotely controls many variables inside the barn, so why not the temperature? The same could be said for the VSS.

Varying degrees of complexity The different systems have varying degrees of complexity. For example, the FMS is an IT system that processes data from the connected systems but also sometimes controls those systems. The Automated Milking System (AMS) is a complex system combining various technologies to function effectively. It incorporates robotic systems, such as the arm that attaches to the cow's teats, securing the suction cups. Additionally, it features a sophisticated quality control system tasked with analyzing the milk's quality. It also includes a variety of sensors for various monitoring purposes, along with human-machine interfaces for interactive control and management. On the other end of the scale, systems such as the SS or the ACS have one function.

In the literature surrounding modern dairy farms, recent technological advancements are described many different ways. For example, terms like IoT, AIoT/IoTA, "smart," OT, and CPS describe similar technologies.

The connections between the different systems are not described in this thesis. However, in threat analysis, the connections constitute an essential part of the analysis since the connections, not only the systems, could be vulnerable. Therefore, STRIDE can be used to identify threats towards those connections, but more details than were available are needed.

5.3 RQ 2: What are the threats against cyber-enabled systems on a dairy farm?

In the description of the threats, the word attacker is used. The word is a placeholder for a willing and able person or group attacking the system. In most threats discovered, a remote-located attacker is imagined as the perpetrator, although an internal attacker can do the same.

In Section 3.2, each system on the cyber-enabled farm is analyzed using the methodology described in Section 3. The STRIDE threat analysis in this thesis is performed at a high level, with the whole system as part of the analysis. It does not go into the specifics of each system. Instead, it only considers attacks against the main properties described: functionality, data flow, and dependencies.

In addition, the threat analysis is technology neutral. The spoofing threat of the ACS is an example of a technology-neutral threat. It highlights the possibility of making the robot receive the incorrect location data, regardless of the type of location data. This technology neutrality is a benefit as it does not specify which type of location data it is, so when it comes to mitigating the threat, it could come from technologies such as GPS, WiFi, or others.

Threats to animal welfare An essential aspect of the threats discovered is the potential for harming the animals. An example is the tampering threat against the segregation system (SS). The control mechanism of the pneumatic gates can be overridden and close, trapping the cow in one area or closing when the cow is in the gate, thus hurting the cow. This threat exemplifies how an OT-related threat can have a physical impact. The same argument could be made for the tampering or spoofing threat to the automatic cleaning system (ACS). Here the cows' health is threatened by fully automatic, heavy robots that can hurt the cows by ramming into them.

Threats to business continuity Another aspect of the identified threats is the threats to business continuity. Although identifying such processes is not a part of the scope of the thesis, the threats identified still relate to them. For example, one essential process on the dairy farm is milk production. Therefore, many of the threats are related to this process. The obvious example is the AMS.

Farm management system As mentioned earlier, the farm management system (FMS) is crucial in the network topology - it acts as the central node. However, this

role makes it potentially vulnerable, as threats against the FMS could compromise the entire system, given that other sub-systems depend on the FMS for data processing and operational needs. A consequence is that if the FMS is compromised, it could have wide-reaching effects across the system. 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.

To illustrate, consider the automatic feeding system (AFS). The AFS relies on accurate data from the FMS to determine the feeding quantity and schedule for the cows. However, if an attacker successfully spoofs the identity of the FMS, they could give the wrong data to the AFS. As a result, the AFS could provide the wrong amount of feed or feed the animals at incorrect times. This example demonstrates how the central role of the FMS can make it a significant point of vulnerability within the system.

Local variations The implications of threats against the EVS can vary based on the climate of the dairy farm. In regions where temperatures fluctuate to extremes - either excessively high or low - the potential consequences of a malfunctioning EVS become more severe because the cows might overheat or freeze.

Lack of threats to the ALS In the automatic lighting system, threats in two threat categories were not found (information disclosure and elevation of privilege). This lack of threat is because of a lack of information about the system.

5.4 RQ 3: What are the risks associated with the threats against cyber-enabled systems on a dairy farm?

The risk assessment part of the threat analysis was conducted after the STRIDE analysis. The STRIDE method lacks a proper risk assessment of the threats discovered. The risk assessment part was added because it would make it easier to understand and identify possible severe threats to the dairy farm. In this section, the results from the risk assessment are discussed.

When considering what the risks are to the cyber-enabled dairy farm, one way of looking at this is to see the farm as a whole. The sum of the low to high scores on the risk scoring indicates that. Table 5.1 shows 20 low, 27 medium, and 13 high-risk threats to the dairy farm.

5.4.1 Risk scoring

When the likelihood score was set, three criteria were available: the criterion regarding the adversary's motivation and capability, one about the existence of known exploits, and finally, one regarding the system's exposure to the internet and other systems. The first two were out of scope for this thesis, but the last was not. Therefore, the likelihood criteria were set according to how it was connected.

Table 5.1: Risk assessments for all systems

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	

Since this was the only criterion being used, the likelihood score was set to the same across the different threats on each system.

Of the ten systems, only one was set to Very Likely, the FMS. It can be remotely controlled, is connected to almost all other systems, and is operated by different operators. Seven systems were set to Moderate and two to rare, the EVS and the VSS.

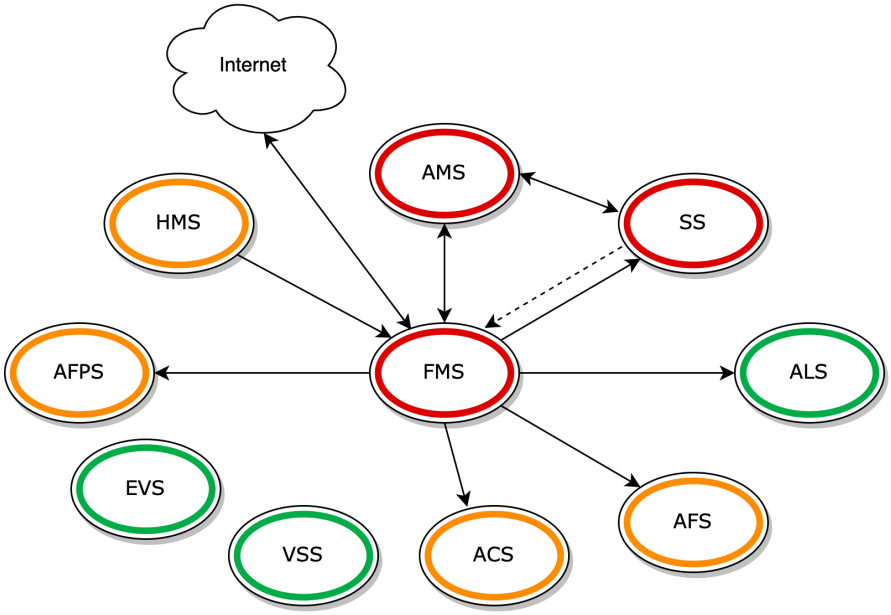
The likelihood scores for many systems may have been undervalued, as the existence of known exploits and the presence of a motivated adversary would ordinarily raise these scores.

5.4.2 High and low-risk systems

Breaking down the risk scores at a system level shows that some systems are at higher risk in a threat scenario. Table 5.1 presents the system's low, medium, and high-risk scores. In addition, a "system risk score" was calculated by assigning numerical values to the risk scores. The threat scores on each threat were given the following values: L=1, M=2, H=3. By adding these together and dividing them by the number of threats (6), 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). The lowest score was the VSS, with a system risk score of 1.13/3. The VSS has all low scores except for one, which was medium. Figure 5.1 shows the systems connected, with the highest ranked systems, according to risk, marked in red.

The FMS has every risk assessed at high because the system is directly internet-connected and thus gets the highest likelihood score. In addition, as discussed above, it acts as a single node in the network and is vital for information stor-

Figure 5.1: Overview of systems on a dairy farm, with information flows, high-risk systems marked with red, medium-risk with orange, low-risk with green



age and operational control for almost all other systems. Therefore, each threat is scored with medium or high impact. The FMS is a linchpin in the farm's operations. Any compromise of it, either through an intrusion or manipulation of data, could cascade across the farm, leading to devastating consequences for livestock welfare, production efficiency, and the farm's economic situation.

The Automatic Milking System (AMS) represents a critical juncture between a cyber-enabled dairy farm's digital and physical aspects. As a cyber-physical system, the AMS scored high on the risk scale in the threat analysis due to its integral role in the farm's operations and its potential to cause significant harm to the cows if compromised. This system employs advanced robotics and sensors to streamline the milking process, improving efficiency and productivity. However, its direct interface with the cows and its connectivity to the FMS introduces a set of serious threats. If a malicious actor exploited the AMS, it could lead to an irregular milking process, causing physical harm to the cows and affecting the farm's productivity. The interdependence between the AMS and the FMS also implies that a compromise in the AMS could spread to other interconnected systems.

The systems incorporating robotic capabilities like the AMS, ACS, and the automatic feeding and pushing system (AFPS) are of particular concern. The identified threats against these systems, if realized, could directly impact the physical welfare of the cows. For example, an attacker could tamper with these systems, causing irregularities or malfunctions and potentially harming the animals physically.

These examples emphasize the necessity of robust cybersecurity measures

within a cyber-enabled dairy farm to protect against such threats. It also highlights the importance of risk assessments in identifying potential vulnerabilities and developing strategies to mitigate them, thereby ensuring the safety and efficiency of the farm's CPS.

5.4.3 Countermeasures

Several strategies can be implemented to counter the potential threats identified in a cyber-enabled dairy farm. Although not part of the scope of the thesis, it is worth mentioning nonetheless.

The National Institute of Standards and Technology (NIST) does not offer specific agricultural industry guidelines, but other relevant frameworks can be used. For example, the *Framework for Improving Critical Infrastructure Cybersecurity* [31] offers a structured and prioritized approach to managing cybersecurity risks. It is comprehensive and flexible, and allows for tailoring to specific systems and processes, ensuring all potential vulnerabilities are addressed and resilience against cyber threats is strengthened across the infrastructure. More general guidelines can also be used, like the *Risk Management Framework* (RMF) [44]. The RMF provides a systematic, six-step process for managing security and privacy risks, allowing for proactive identification, assessment, and mitigation of threats.

In addition to NIST guidelines, other industry best practices and cybersecurity standards should be considered for a comprehensive defense strategy. These include using firewalls and intrusion detection systems, implementing robust access controls, regularly patching and updating the system software, and ongoing staff training in cybersecurity awareness.

Implementing such countermeasures should be an ongoing process, continually adapting to evolving threats and advancements in cybersecurity measures. By doing so, the farm can maintain a robust security posture, protecting the well-being of the animals, ensuring business continuity, and maintaining the integrity of its systems.

5.5 Limitations

This section discusses the study's significant limitations, each with potential implications for the validity and generalizability of the findings.

Sample size The study relies on a small sample of technical documents for its topology, which may constrict the results' generalizability. This limitation could induce biases and may not accurately reflect real-world system deployments or omit specific systems entirely. The way the systems split, e.g., the SS and the HMS, could be viewed otherwise if the sample size had been broader and the details better. Future research could offset this limitation by incorporating a broader and more diverse set of technical documents and performing field studies on more

systems, thereby representing a more comprehensive range of systems and use cases.

Level of detail in topology The level of detail in the topology of the systems studied is low, primarily due to insufficient data detail in the technical documents used for the research. This lack of detail can lead to an incomplete understanding of the systems and their potential vulnerabilities.

STRIDE The study uses STRIDE, a methodology originating from the IT sector, to address cybersecurity. While this approach has been extended to other sectors, including those with operational technology (OT) elements, its inherent limitations are noteworthy. Primarily, the STRIDE method focuses on six specific threats and may not encompass all potential threats that could arise in a context such as dairy farming. Furthermore, STRIDE's qualitative nature renders it subjective, which could lead to inconsistencies across different analysts.

Safety This thesis also emphasizes the safety aspect discovered during the research. While STRIDE does not address this directly, the thesis outlines some potential consequences. For example, a study on the automotive industry combined STRIDE with a safety-related model for a more comprehensive analysis [30]. Something similar could be done to the cyber-enabled dairy farm.

Finally, the research was constrained by the lack of previous studies into the cybersecurity of dairy farming. While this research gap motivated the topic exploration, it simultaneously limited the depth and scope of this thesis.

Chapter 6

Conclusion

The main goal of the thesis was to address the underdeveloped cybersecurity field in the dairy farming context. Three main research questions were formulated to guide the research. The questions address what the cyber-enabled systems on farms are, their properties, the threats towards them, and the risk that these threats pose. The topology was produced by studying existing academic literature and technical documents from the dairy farming industry. It showed that a large part of the modern dairy farm is cyber-enabled and connected. Ten systems were identified, most of which were connected to a central node in the network, the farm management systems (FMS).

A STRIDE threat analysis was conducted on every identified system using this topology. The analysis showed that many of the systems had the potential to do great harm to the cows, stop milk production and do financial and reputational damage to the farm.

Finally, a previously created list of impact and likelihood criteria was used to evaluate the risk of all the threats identified from the STRIDE analysis. The risk assessment showed that the farm management systems (FMS) had the highest risk score of all the ten systems. Being connected to the internet and almost all other systems could harm cows by providing wrong information to other systems. Since the FMS contains valuable health data about the cows, it introduces the possibility of giving them improper treatment. In addition, CPS systems, such as the dairy farm's automatic milking system (AMS), were shown to potentially threaten the cows' health if attacked by an adversary. This research underscores the importance of comprehensive cybersecurity strategies in safeguarding the CPS's efficient and safe operation within dairy farming.

6.1 Future work

The topology of the modern dairy farm could be further studied. A more robust and grounded model could be built by conducting fieldwork and validating the topology with the dairy industry or farmers. This thesis only scratches the surface

of the complex systems on a dairy farm. How the systems interact and are connected could further explain how threat actors could attack the systems. Other threat models and analyses could show other facets and broaden the view of how these systems could be attacked. Although outside the scope of this thesis, a closer look at the actual threats, i.e., threat actors and threat landscape surrounding the dairy farms or agriculture in general, is worth studying to estimate how likely the threats are. This research could extend to the entire food chain, of which dairy farming is important.

Bibliography

[1] FBI, *Smart Farming May Increase Cyber Targeting Against US Food and Agriculture Sector*, 2016. [Online]. Available: https://info.publicintelligence.net/FBI-SmartFarmHacking.pdf (visited on 05/03/2023).

[2] FBI, *Ransomware Attacks on Agricultural Cooperatives Potentially Timed to Critical Seasons*, Apr. 2020. [Online]. Available: https://www.ic3.gov/Media/News/2022/220420-2.pdf (visited on 05/04/2023).

[3] L. Abrams, *Pan-Asian retail giant Dairy Farm suffers REvil ransomware attack*, en-us, Jan. 2021. [Online]. Available: https://www.bleepingcomputer.com/news/security/pan-asian-retail-giant-dairy-farm-suffers-revil-ransomware-attack/ (visited on 05/04/2023).

[4] G. Kavallieratos, S. Katsikas, and V. Gkioulos, "Cyber-Attacks Against the Autonomous Ship," en, in *Computer Security*, vol. 11387, Cham: Springer International Publishing, 2019, pp. 20–36. DOI: 10.1007/978-3-030-12786-2_2. [Online]. Available: http://link.springer.com/10.1007/978-3-030-12786-2_2 (visited on 02/17/2023).

[5] SSB, *Husdyrhald*, May 2022. [Online]. Available: https://www.ssb.no/jord-skog-jakt-og-fiskeri/jordbruk/statistikk/husdyrhald (visited on 03/02/2023).

[6] Landbruksdirektoratet, *Råvarestatistikk*, nb, 2022. [Online]. Available: https://www.landbruksdirektoratet.no/nb/statistikk-og-utviklingstrekk/utvikling-i-jordbruket/ravarestatistikk (visited on 03/02/2023).

[7] SSB, *Stor variasjon i omsetning i jordbruket*, no, Jan. 2013. [Online]. Available: https://www.ssb.no/jord-skog-jakt-og-fiskeri/artikler-og-publikasjoner/landbrukstellinga (visited on 05/09/2023).

[8] DSB, "Vital functions in society," en, DSB, Tech. Rep., 2017. [Online]. Available: https://www.dsb.no/globalassets/dokumenter/rapporter/kiks-ii_english_version.pdf (visited on 05/05/2023).

[9] Landbruksdirektoratet, *Markedsrapport 2021*, 2021. [Online]. Available: https://www.landbruksdirektoratet.no/nb/filarkiv/rapporter/Markedsrapport%202021_Markeds-%20og%20prisvurderinger%20av%20sentrale%20norske%20landbruksvarer%20og%20R%C3%85K-varer.pdf/_/attachment/inline/36c6d5df-bbc8-4a21-bdc3-1253ba12f1dc:

de99a08bea2aad9e866636775deec0965e4b5cd7/Markedsrapport%202021_Markeds-%20og%20prisvurderinger%20av%20sentrale%20norske%20landbruksvarer%20og%20R%C3%85K-varer.pdf (visited on 03/02/2023).

[10] W. Jarvis, *Sick Codes talks tractor hacks*, Sep. 2022. [Online]. Available: https://therecord.media/q-a-sick-codes-talks-tractor-hacks (visited on 05/04/2023).

[11] S. Agarwal, A. Rashid, and J. Gardiner, "Old MacDonald had a smart farm: Building a testbed to study cybersecurity in smart dairy farming," en, in *Cyber Security Experimentation and Test Workshop*, Virtual CA USA: ACM, Aug. 2022, pp. 1–9, ISBN: 978-1-4503-9684-4. DOI: 10.1145/3546096.3546097. [Online]. Available: https://dl.acm.org/doi/10.1145/3546096.3546097 (visited on 02/04/2023).

[12] Virginia Tech News, *Cyber researchers protect Virginia's dairy farms, address labor shortages*, en, Mar. 2023. [Online]. Available: https://news.vt.edu/content/news_vt_edu/en/articles/2023/02/don-t-hack-our-cows--cyber-researchers-protect-virginia-s-dairy-.html (visited on 05/31/2023).

[13] NIST, *Cyber-physical system - Glossary*, EN-US. [Online]. Available: https://csrc.nist.gov/glossary/term/cyber_physical_systems (visited on 05/30/2023).

[14] K. Demestichas, N. Peppes, and T. Alexakis, "Survey on Security Threats in Agricultural IoT and Smart Farming," en, *Sensors*, vol. 20, no. 22, p. 6458, Nov. 2020, ISSN: 1424-8220. DOI: 10.3390/s20226458. [Online]. Available: https://www.mdpi.com/1424-8220/20/22/6458 (visited on 05/08/2023).

[15] O. Manninen, "Cybersecurity in Agricultural Communication Networks: Case Dairy Farms," en, M.S. thesis, JAMK University of applied sciences, 2018.

[16] J. Nikander, O. Manninen, and M. Laajalahti, "Requirements for cybersecurity in agricultural communication networks," en, *Computers and Electronics in Agriculture*, vol. 179, Dec. 2020, ISSN: 01681699. DOI: 10.1016/j.compag.2020.105776. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0168169920314812 (visited on 02/04/2023).

[17] J. M. Kizza, "Computer Network Fundamentals," en, in *Guide to Computer Network Security*, Series Title: Computer Communications and Networks, London: Springer London, 2015, pp. 3–40. DOI: 10.1007/978-1-4471-6654-2_1. [Online]. Available: https://link.springer.com/10.1007/978-1-4471-6654-2_1 (visited on 05/08/2023).

[18] W. Xiong and R. Lagerström, "Threat modeling – A systematic literature review," en, *Computers & Security*, vol. 84, pp. 53–69, Jul. 2019, ISSN: 01674048. DOI: 10.1016/j.cose.2019.03.010. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0167404818307478 (visited on 03/22/2023).

[19] NIST, "Security and Privacy Controls for Information Systems and Organizations," National Institute of Standards and Technology, Tech. Rep., Sep. 2020, Edition: Revision 5. DOI: 10.6028/NIST.SP.800-53r5. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf (visited on 03/02/2023).

[20] A. Shostack, *Threat modeling: designing for security*. Indianapolis, IN: Wiley, 2014, OCLC: ocn855043351, ISBN: 978-1-118-80999-0.

[21] NIST, *Threat - Glossary*, EN-US. [Online]. Available: https://csrc.nist.gov/glossary/term/threat (visited on 05/31/2023).

[22] K. Tuma, G. Calikli, and R. Scandariato, "Threat analysis of software systems: A systematic literature review," en, *Journal of Systems and Software*, vol. 144, pp. 275–294, Oct. 2018, ISSN: 01641212. DOI: 10.1016/j.jss.2018.06.073. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0164121218301304 (visited on 05/08/2023).

[23] D. Van Landuyt and W. Joosen, "A descriptive study of assumptions in STRIDE security threat modeling," en, *Software and Systems Modeling*, vol. 21, no. 6, pp. 2311–2328, Nov. 2021, ISSN: 1619-1366, 1619-1374. DOI: 10.1007/s10270-021-00941-7. [Online]. Available: https://link.springer.com/10.1007/s10270-021-00941-7 (visited on 03/22/2023).

[24] Bruce Schneier, *Attack Trees*, 1999. [Online]. Available: https://www.schneier.com/academic/archives/1999/12/attack_trees.html (visited on 05/10/2023).

[25] T. UcedaVélez, *PASTA Threat Modeling - Breaking Down All 7 Steps*, 2021. [Online]. Available: https://versprite.com/blog/what-is-pasta-threat-modeling/ (visited on 05/10/2023).

[26] L. Kohnfelder and P. Garg, *The threats to our products*, 1999. [Online]. Available: https://adam.shostack.org/microsoft/The-Threats-To-Our-Products.docx (visited on 03/22/2023).

[27] M. Cagnazzo, M. Hertlein, T. Holz, and N. Pohlmann, "Threat modeling for mobile health systems," in *2018 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*, Barcelona: IEEE, Apr. 2018, pp. 314–319, ISBN: 978-1-5386-1154-8. DOI: 10.1109/WCNCW.2018.8369033. [Online]. Available: https://ieeexplore.ieee.org/document/8369033/ (visited on 05/09/2023).

[28] B. Jelacic, D. Rosic, I. Lendak, M. Stanojevic, and S. Stoja, "STRIDE to a Secure Smart Grid in a Hybrid Cloud," en, in *Computer Security*, S. K. Katsikas, F. Cuppens, N. Cuppens, C. Lambrinoudakis, C. Kalloniatis, J. Mylopoulos, A. Antón, and S. Gritzalis, Eds., vol. 10683, Series Title: Lecture Notes in Computer Science, Cham: Springer International Publishing, 2018, pp. 77–90. DOI: 10.1007/978-3-319-72817-9_6. [Online]. Available: http://link.springer.com/10.1007/978-3-319-72817-9_6 (visited on 02/17/2023).

[29] A. Omotosho, B. Ayemlo Haruna, and O. Mikail Olaniyi, "Threat Modeling of Internet of Things Health Devices," en, *Journal of Applied Security Research*, vol. 14, no. 1, pp. 106–121, Jan. 2019, ISSN: 1936-1610, 1936-1629. DOI: 10.1080/19361610.2019.1545278. [Online]. Available: https://www.tandfonline.com/doi/full/10.1080/19361610.2019.1545278 (visited on 05/09/2023).

[30] G. Macher, E. Armengaud, E. Brenner, and C. Kreiner, "Threat and Risk Assessment Methodologies in the Automotive Domain," en, *Procedia Computer Science*, vol. 83, pp. 1288–1294, 2016, ISSN: 18770509. DOI: 10.1016/j.procs.2016.04.268. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S1877050916303015 (visited on 05/09/2023).

[31] NIST, "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1," en, National Institute of Standards and Technology, Gaithersburg, MD, Tech. Rep. NIST CSWP 04162018, Apr. 2018, NIST CSWP 04162018. DOI: 10.6028/NIST.CSWP.04162018. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (visited on 05/13/2023).

[32] NIST, "Risk management guide for information technology systems," en, National Institute of Standards and Technology, Gaithersburg, MD, Tech. Rep. NIST SP 800-30, 2002, Edition: 0, NIST SP 800–30. DOI: 10.6028/NIST.SP.800-30. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30.pdf (visited on 05/23/2023).

[33] A. Boghossian, P. Mutschler, B. Ulicny, L. Barrett, G. Bethel, M. Matson, T. Strang, K. W. Ramsdell, S. Koehler, and S. Linsky, *Threats to Precision Agriculture*, en, 2018. [Online]. Available: http://rgdoi.net/10.13140/RG.2.2.20693.37600 (visited on 05/03/2023).

[34] L. Baker and R. Green, "Cyber Security in UK Agriculture," en, 2019. [Online]. Available: https://research.nccgroup.com/wp-content/uploads/2020/07/agriculture-whitepaper-final-online.pdf.

[35] M. Howard and S. Lipner, *The security development lifecycle* (Secure software development series). Redmond, Wash: Microsoft Press, 2006, OCLC: ocm70211570, ISBN: 978-0-7356-2214-2.

[36] R. Khan, K. McLaughlin, D. Laverty, and S. Sezer, "STRIDE-based threat modeling for cyber-physical systems," in *2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*, Torino: IEEE, Sep. 2017, pp. 1–6, ISBN: 978-1-5386-1953-7. DOI: 10.1109/ISGTEurope.2017.8260283. [Online]. Available: http://ieeexplore.ieee.org/document/8260283/ (visited on 03/22/2023).

[37] DeLaval, *Delpro Farm Manager*, 2018. [Online]. Available: https://www.delaval.com/globalassets/inriver-resources/document/brochure/19015-delpro-farm-manager.pdf (visited on 04/11/2023).

[38] Lely, *Horizon Brochure*, 2020. [Online]. Available: https://www.lely.com/media/filer_public/ac/8b/ac8b1cc1-5753-49e6-bd7a-0c04ce1c8c2e/t4c_19002_-_t4cnext_npi_brochure_horizon-en_v05_web.pdf (visited on 04/11/2023).

[39] Lely, *Lely Dairy Equipment*, 2014. [Online]. Available: https://www.lely.com/media/lely-centers-files/brochures/published/lely_dairy_equipment_2014_-_en.pdf (visited on 02/07/2023).

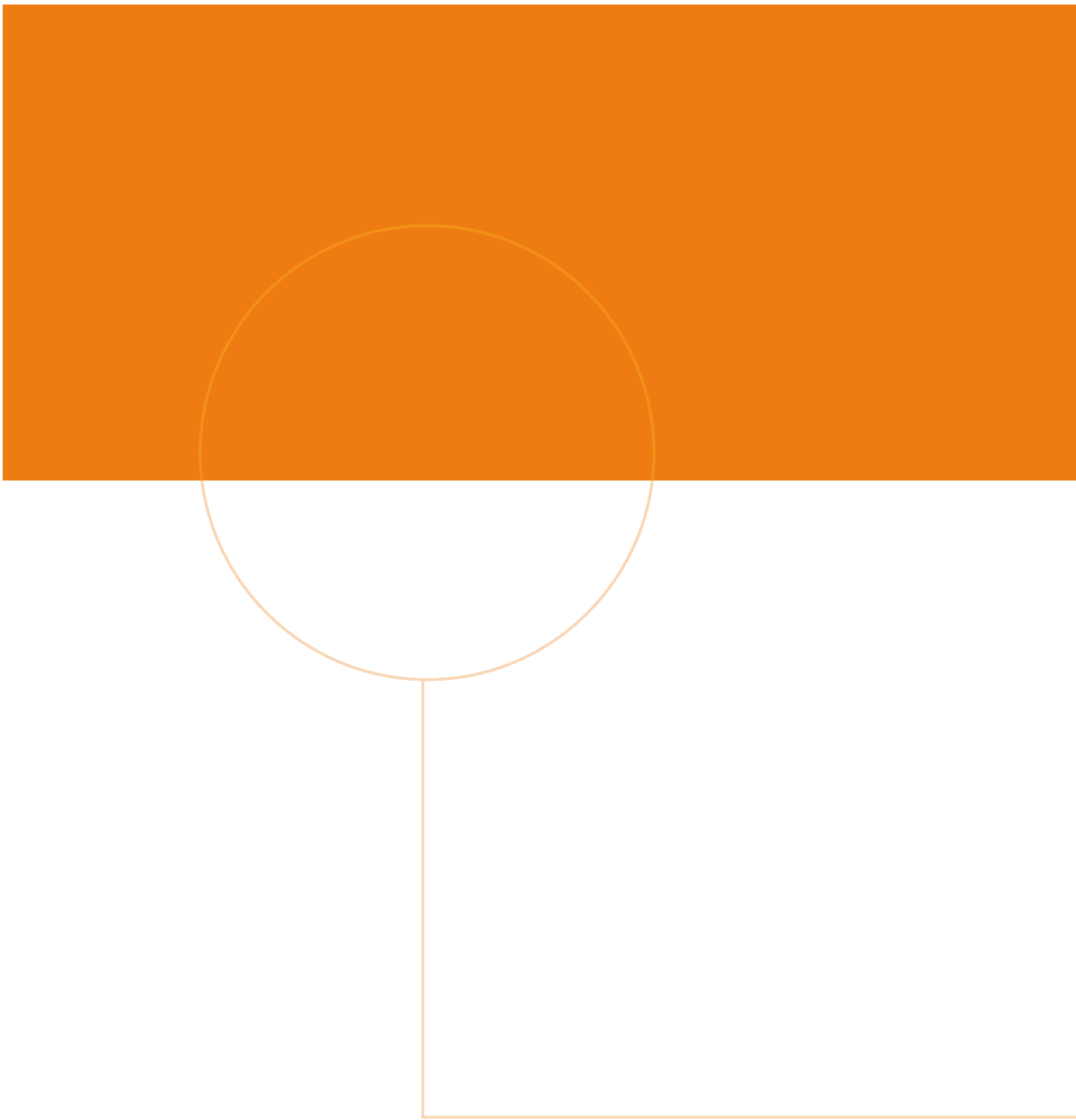
[40] GEA, *Gea product catalogue*, 2017. [Online]. Available: https://www.gea.com/en/binaries/gea-product-catalogue-barn-technology-farm-equipment-en_tcm11-39660.pdf (visited on 01/03/2023).

[41] DeLaval, *DeLaval Landbrukskatalog 2023.pdf*, 2023. [Online]. Available: https://store.delaval.com/globalassets/norway/kataloger/delaval-landbrukskatalog-2023_web.pdf (visited on 03/28/2023).

[42] R. M. B. Hårstad, "Bonden, familien og melkeroboten – en ny hverdag," RURALIS - Institutt for rural- og regionalforskning, Tech. Rep. 2/2019, 2019. [Online]. Available: https://bygdeforskning.wpenginepowered.com/wp-content/uploads/2019/01/rapport-2_19-bonden-familien-og-melkeroboten-en-ny-hverdag--r-m-b--hrstad.pdf (visited on 03/06/2023).

[43] Lely, *Astronaut A5 Operator Manual*, 2022. [Online]. Available: https://www.lelynet.com/_layouts/15/document/TechDocHandler.aspx?name=5-1005-8500-0_L_Astronaut_A5_Operator%20Manual_English%20(en).pdf&mode=view (visited on 01/03/2023).

[44] NIST, "Risk management framework for information systems and organizations," en, National Institute of Standards and Technology, Gaithersburg, MD, Tech. Rep. NIST SP 800-37r2, Dec. 2018, NIST SP 800–37r2. DOI: 10.6028/NIST.SP.800-37r2. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf (visited on 05/30/2023).



NTNU

Norwegian University of
Science and Technology