

University of Nebraska - Lincoln

DigitalCommons@University of Nebraska - Lincoln

Biological Systems Engineering--Dissertations,
Theses, and Student Research

Biological Systems Engineering

8-2022

Cybersecurity of Agricultural Machinery: Exploring Cybersecurity Risks and Solutions for Secure Agricultural Machines

Mark Freyhof

Department of Biological Systems Engineering, University of Nebraska-Lincoln,
mfreyhof2@huskers.unl.edu

Follow this and additional works at: <https://digitalcommons.unl.edu/biosysengdiss>



Part of the [Bioresource and Agricultural Engineering Commons](#)

Freyhof, Mark, "Cybersecurity of Agricultural Machinery: Exploring Cybersecurity Risks and Solutions for Secure Agricultural Machines" (2022). *Biological Systems Engineering--Dissertations, Theses, and Student Research*. 130.

<https://digitalcommons.unl.edu/biosysengdiss/130>

This Article is brought to you for free and open access by the Biological Systems Engineering at DigitalCommons@University of Nebraska - Lincoln. It has been accepted for inclusion in Biological Systems Engineering--Dissertations, Theses, and Student Research by an authorized administrator of DigitalCommons@University of Nebraska - Lincoln.

CYBERSECURITY OF AGRICULTURAL MACHINERY: EXPLORING
CYBERSECURITY RISKS AND SOLUTIONS FOR SECURE AGRICULTURAL
MACHINES

by

Mark T. Freyhof

A THESIS

Presented to the Faculty of

The Graduate College at the University of Nebraska

In Partial Fulfillment of Requirements

For the Degree of Master of Science

Major: Agricultural and Biological Systems Engineering

Under the Supervision of Professor Santosh K. Pitla

Lincoln, Nebraska

August, 2022

CYBERSECURITY OF AGRICULTURAL MACHINERY: EXPLORING
CYBERSECURITY RISKS AND SOLUTIONS FOR SECURE AGRICULTURAL
MACHINES

Mark T. Freyhof, M.S.

University of Nebraska, 2022

Advisor: Santosh K. Pitla

Modern agriculture is reliant on agricultural machinery for the production of food, fuel, and other agricultural products. The need for producing large quantities of quality agricultural products while sustainably stewarding environmental resources has led to the integration of numerous digital technologies into modern agricultural machinery, such as the CAN bus and telematic control units (Liu et al., 2021). An unintended drawback of these integrated digital technologies is the opportunity for these components to become cyberattack vectors. Cyberattack instances have increasingly targeted critical infrastructures, with numerous reports from agencies such as the Federal Bureau of Investigation (FBI) and Department of Homeland Security (DHS) warning of the significance of cyberattacks targeting the agricultural infrastructure specifically (Boghossian et al., 2018; Federal Bureau of Investigation, 2021; Federal Bureau of Investigation, 2022). Agricultural machinery, which is included in the agricultural infrastructure, has the potential to be targeted by cyberattacks, although the impacts are not well quantified or understood. This project demonstrates a hypothetical case study, where cyberattacks targeting in-season side-dress nitrogen application to corn could cause as much as \$100 or more in profit loss per acre. Literature discussing practical cybersecurity solutions for agricultural machinery from both industry and academic

institutions is absent, therefore two possible solutions were demonstrated in this project: modeling and the use of security testbeds. A four-step modeling methodology was developed and investigated as a solution in identifying the most security-critical areas of a machine. Two specific cyberattack scenarios were modeled to demonstrate the potential of the modeling methodology. A Security Testbed for Agricultural Vehicles and Environments (STAVE) was also developed as a useful solution for the identification of cybersecurity vulnerabilities to agricultural machinery (Freyhof et al., 2022). A replay attack and wireless signal recordings were performed to evaluate various components on STAVE.

AUTHOR'S ACKNOWLEDGMENTS

For guidance, I would like to thank:

Dr. Santosh Pitla

Dr. George Grispos

Dr. Cody Stolle

Dr. Rodney Rohrer

For assistance with research:

Mitchell White

Jensen Miller

Robert Ernewein

For providing testing facilities:

NCEE Labs

GRANT INFORMATION

Research funded by:

University of Nebraska Collaboration Initiative Seed Grant

“Security and Hackability Considerations of Driverless Tractors and Agricultural
Robots”.

TABLE OF CONTENTS

AUTHOR’S ACKNOWLEDGMENTS	III
GRANT INFORMATION	IV
TABLE OF CONTENTS.....	V
LIST OF TABLES	VIII
TABLE OF FIGURES	IX
CHAPTER 1: INTRODUCTION.....	1
1.1. Background and Motivation	1
1.2. Thesis Outline	4
CHAPTER 2: LITERATURE REVIEW.....	5
2.1. History of Agriculture.....	5
2.2. Introduction to Cybersecurity	9
2.3. Cybersecurity Concerns in the Agriculture Community	11
2.4. Cybersecurity Concerns to Agricultural Machinery and Vehicles	14
CHAPTER 3: IMPACTS OF CYBERATTACKS TO PRECISION AGRICULTURAL OPERATIONS	15
3.1. Background.....	16
3.2. Research Methodology	19
3.2.1. Case Study Criteria	19
3.2.2. Control Scenario	24
3.2.3. Calculating Financial Impacts.....	31
3.2.4. Attack Scenarios	34
3.3. Results.....	37
3.3.1. Attack Scenario 1	37

3.3.2.	Attack Scenario 2	42
3.3.3.	Attack Scenario 3	46
3.4.	Discussion	49
3.5.	Conclusions	52
CHAPTER 4: CYBERSECURITY MODELING FOR AGRICULTURAL MACHINERY		53
4.1.	Introduction	53
4.2.	Background	54
4.3.	Research Methodology and Materials	56
4.3.1.	Flex-Ro	56
4.3.2.	Modeling Methodology	58
4.4.	Results and Discussion	61
4.4.1.	Conceptualize	61
4.4.2.	Model Assembly	68
4.4.3.	Simulation	72
4.4.4.	Evaluate Model	74
4.5.	Conclusions	75
CHAPTER 5: UTILIZING TESTBEDS TO ANALYZE CYBERSECURITY VULNERABILITIES TO AGRICULTURAL MACHINERY		76
5.1.	Introduction	77
5.2.	Case Study	78
5.2.1.	STAVE Testbed	78
5.2.2.	Testing	83
5.3.	Discussion	87
5.4.	Conclusions	88

CHAPTER 6: OVERALL CONCLUSIONS AND FUTURE WORK	89
Conclusions	89
6.1.	89
6.2. Future Work	91
REFERENCES	93
APPENDIX A : STATEFLOW COMPONENTS USED IN THE E-STOP MODEL	107

LIST OF TABLES

Table 4.1: CASE Modeling Methodology for Agricultural Control Systems	59
Table 4.2: Normal states of the Flex-Ro E-stop subsystem as shown in Figure 4.8 ...	66
Table 4.3: Normal transition conditions as shown in Figure 4.8	66
Table 4.4: Potential states under a cyberattack as shown in Figure 4.9.....	67
Table 4.5: Transition conditions under a cyberattack as shown in Figure 4.9.....	67
Table 4.6: Useful Stateflow Components	69
Table 5.1: STAVE Components	82

TABLE OF FIGURES

Figure 2.1: Timeline of agricultural machinery and cybersecurity.....	7
Figure 3.1 Liquid Side-Dress Equipment	18
Figure 3.2: UNL Nitrogen Formula Nitrogen Credits and Timing Adjustments	22
Figure 3.3 100-acre field with 1-acre management zones	26
Figure 3.4: Estimated Corn Yield Values.....	26
Figure 3.5: Soil Nitrate Levels.....	27
Figure 3.6: Soil Organic Matter Levels	28
Figure 3.7: Total recommended nitrogen input for growing season (lbs/acre).....	29
Figure 3.8: Pre-plant recommended nitrogen application rates (lbs/acre).....	30
Figure 3.9: In-season recommended nitrogen application rates (lbs/acre)	31
Figure 3.10: Actual (calculated) corn yield values (bu/acre).....	32
Figure 3.11: Cyberattack Scenario 1.....	35
Figure 3.12: Cyberattack Scenario 2.....	36
Figure 3.13: Cyberattack Scenario 3.....	37
Figure 3.14: Prescribed vs. Actual nitrogen application rates (lbs/acre) after attack	138
Figure 3.15: Expected vs. Actual application rates of UAN32 (gal/acre) after attack	139
Figure 3.16: Expected vs. Actual (calculated) yield after attack 1	40
Figure 3.17: Potential-Profit loss or gain per acre resulting from attack 1	41
Figure 3.18: Financial impacts from attack 1	41
Figure 3.19: Prescribed vs. Actual nitrogen application rates (lbs/acre) after attack	242
Figure 3.20: Expected vs. Actual application rates of UAN32 (gal/acre) after attack	243
Figure 3.21: Expected vs. Actual (calculated) yield after attack 2	44
Figure 3.22: Potential-Profit loss or gain per acre resulting from attack 2.....	45

Figure 3.23: Financial impacts from attack 2	45
Figure 3.24: Prescribed vs. Actual nitrogen application rates (lbs/acre) after attack 346	
Figure 3.25: Expected vs. Actual application rates of UAN32 (gal/acre) after attack 347	
Figure 3.26: Expected vs. Actual (calculated) yield after attack 3	47
Figure 3.27: Potential-Profit loss or gain per acre resulting from attack 3.....	48
Figure 3.28: Financial impacts from attack 3	49
Figure 3.29: Profit and Cost Comparison Between Attacks.....	51
Figure 4.1: Flex-Ro performing a field scouting operation	57
Figure 4.2: CAN bus network of Flex-Ro	57
Figure 4.3: E-stop button on a corner of Flex-Ro.....	58
Figure 4.4: Flex-Ro remote E-stop and reset button inputs.....	62
Figure 4.5: FlexRoRun app with E-stop and reset buttons highlighted.....	63
Figure 4.6: Overview of Flex-Ro E-stop system in SAFE state.....	64
Figure 4.7: Overview of Flex-Ro E-stop system in UNSAFE state	65
Figure 4.8: Emergency Stop (E-stop) Finite State Diagram.....	66
Figure 4.9: Emergency Stop (E-stop) Finite State Diagram with Attack States.....	67
Figure 4.10: Fully assembled Stateflow model.....	70
Figure 4.11: Stateflow model within MATLAB interface.....	71
Figure 4.12: Running model and output scope	73
Figure 4.13: Stateflow model entering attack state.....	74
Figure 5.1: Flex-Ro at the Nebraska Tractor Test Lab (NTTL)	79
Figure 5.2: Flex-Ro Wireless Remote	79
Figure 5.3: STAVE (Security Testbed for Agricultural Vehicles and Environments) – Composed of components from the Flex-Ro machine	80

Figure 5.4: STAVE (Security Testbed for Agricultural Vehicles and Environments) – Composed of components from Flex-Ro wireless remote.....	80
Figure 5.5: STAVE (Security Testbed for Agricultural Vehicles and Environments) – Data acquisition and monitoring of STAVE.....	81
Figure 5.6: Noisy 2.4 GHz frequency range when recording signals from WIC devices in ‘noisy’ environment. Black line signifies current live signals while red line holds the maximum values during the current run time.	84
Figure 5.7: Copper radio frequency blocking box used to perform tests on STAVE..	85
Figure 5.8: Wireless signals between WIC devices captured on URH spectrum analyzer.	85
Figure 5.9: Sample URH recording with FSK demodulation at 2.419MHz.....	86

Chapter 1: INTRODUCTION

1.1. Background and Motivation

Modern agricultural equipment has been an essential component during the transition from small acre subsistence farming to agriculture as we know it today (Liu et al., 2021). As a result, today's modern agricultural production system is heavily dependent on agricultural machinery such as tractors and combine harvesters to efficiently produce large amounts of food, fuel, and other agricultural products. Recent increases in production and efficiency can largely be attributed to improved agronomic practices and precision agricultural techniques, enabled by the integration of digital and networking technologies into modern equipment (Freyhof et al., 2022). These technologies have allowed farmers to transition to the 'next era' of data-driven agriculture that is heavily dependent on precision agricultural practices.

According to the International Society of Precision Agriculture (ISPA), precision agriculture is a general area of agricultural management that utilizes "temporal, spatial and individual data" to make informed management decisions to improve "efficiency, productivity, quality, profitability and sustainability of agricultural production" ("Precision Ag Definition," n.d.). The continued advancements of modern technologies such as autonomy, will further the implementation of precision agricultural practices (Boubin et al., 2019). For example, John Deere recently released a tractor (Model: 8R) that will operate autonomously without an operator (Tibken, 2022). The introduction of autonomous technologies and equipment will continue to accelerate the implementation of precision agricultural practices by allowing more data to be collected and reducing

barriers to farmers such as labor shortages (Rahmadian and Widartono, 2020).

However, the increased integration of digital and autonomous technologies has created many vulnerabilities within modern agricultural equipment (Federal Bureau of Investigation, 2022; Nikander et al., 2020; Sparrow and Howard, 2021).

In the past few years, a number of cyberattacks (Federal Bureau of Investigation, 2021; McVan and Midwest, 2021) have targeted farms and other agricultural infrastructure. For example, in January 2021, a ransomware attack targeting a US farm caused around \$9 million in financial losses (Federal Bureau of Investigation, 2021), while a major meatpacking company was reported to have paid \$11 million in ransom to cybercriminals in another ransomware attack (McVan and Midwest, 2021). Multiple recent reports have warned that agricultural machinery could be the next targets for cyberattacks since agricultural production is so heavily reliant on them (Baker and Green, 2020; Boghossian et al., 2018).

This results in the question: what is being done to protect agricultural equipment, and consequentially, agricultural production systems from further cyberattacks? For the purposes of this research, the cybersecurity of agricultural machinery is defined as the process of ensuring that agricultural machinery will be available and secure to safely perform tasks as intended, without allowing critical data, for example yield or planting data collected during farming operations, to be accessed by unauthorized parties. Cybersecurity of agricultural machinery would protect against events such as ransomware, denial of service, or unsafe equipment manipulation.

In the broader agricultural community, cybersecurity research has examined solutions to areas such as IoT devices and communication networks (Demestichas et al., 2020; Ferrag et al., 2022). Other literature sources have emphasized the importance of cybersecurity to agriculture and agricultural machinery (Boghossian et al., 2018; “Risks of using AI to grow our food are substantial and must not be ignored, warn researchers,” 2022) but provide little to no practical implementation or solutions. Cybersecurity research in the automotive industry (“Automotive Cybersecurity by Design,” 2021; Burkacky et al., 2020; Yu and Luo, 2020) supports the need to include cybersecurity practices during the entire lifecycle of the vehicle or machine, including the design process. These findings are directly applicable to agricultural machinery since modern automotive and agricultural vehicles contain similar, complex digital communication structures. Since there is very limited research describing practical solutions to mitigate cyberattacks targeting agricultural machinery, there is a need for further research that could provide solutions to this emerging issue.

The problem statement for this thesis is as follows: **What potential solutions can be used to strengthen the cybersecurity and design process of agricultural machinery and vehicles?** The problem statement will be answered through three specific contributions:

- 1) Demonstrate a case study that calculates the direct financial costs associated with a specific cyberattack impacting a modern agricultural machine. The results from this approach will be discussed from the perspective of how this information can

help mitigate risk and identify potential countermeasures for the specific, modern agricultural machine.

- 2) Investigate a modeling methodology, which can be used to aid in the design of secure agricultural machinery and assist with identifying critical parts of the subsystem where cybersecurity vulnerabilities could be the most detrimental.
- 3) Develop STAVE, a Security Testbed for Agricultural Vehicles and Environments, for identifying and evaluating current machinery or prototypes for cybersecurity vulnerabilities through testbed solutions.

1.2. Thesis Outline

The following is an overview of the chapters in this thesis:

Chapter 2 presents an overview of the literature related to modern agricultural equipment, general cybersecurity terminology, and existing solutions for cybersecurity of agricultural machinery and the broader agricultural community. Further literature will be presented throughout the thesis, where appropriate for each chapter.

Chapter 3 presents an approach to analyze the costs associated with a cyberattack involving an in-season nitrogen application operation. The research contributions for this chapter will include multiple charts describing the attack, including financial analysis and a discussion of the broader impacts of cyberattacks targeting modern agricultural machinery.

Chapter 4 presents an approach to include cybersecurity as a central focus during the early design process of agricultural machinery. This approach focuses on the use of finite state machine and automata theory modeling to assist in the identification of security

threats early in the design phases of agricultural machinery. The research contribution will present a case-study, where modeling is used to aid in the design of a subsystem on an agricultural machine: Flexible Structured Robotic Platform (Flex-Ro).

Chapter 5 continues the discussion surrounding the discovery and identification of cybersecurity vulnerabilities in agricultural machinery and presents STAVE – a Security Testbed for Agricultural Vehicles and Environments, as one solution to assist in this effort. The research contribution will be the demonstration of STAVE and testbeds, as a tool to assist in the identification of cybersecurity vulnerabilities to agricultural machinery.

Chapter 6 concludes the research and presents potential areas for future research related to cybersecurity and agricultural machinery.

Chapter 2: LITERATURE REVIEW

2.1. History of Agriculture

Agriculture has seen many major advancements throughout history (Liu et al., 2021). The first agricultural revolution saw the transition from hunting and gathering to more organized agriculture as we know it today (Bowles and Choi, 2019). The second agricultural revolution saw an increase in productivity due to labor availability and the increase in production of farming grounds (“agricultural revolution,” n.d.). The third agricultural revolution of the 1950-60’s, or Green Revolution, featured the utilization of synthetic chemicals and fertilizers which greatly increased the productivity of agricultural production systems (Pingali, 2012). Modern agriculture, or the fourth agricultural

revolution, will be heavily dependent on Artificial Intelligence (AI) and autonomous solutions to solve many current challenges facing agriculture today (Chivers and Rose, 2020). Modern agriculture utilizes precision agricultural techniques which leverage highly technical equipment to improve productivity (Raj et al., 2021).

Precision agriculture plays a critical role in modern agriculture (“Precision Ag Definition,” n.d.). Modern farming equipment has made these practices possible, since this equipment has improved in the collection of high-resolution data for a variety of production systems. For example, corn production has seen the benefit of modern technologies in precision agricultural applications and practices such as variable rate applications or site-specific crop management (Daberkow and McBride, 2000). Variable rate application refers to the practice of adjusting input rates throughout a field based on a variety of input factors to maximize profit (Alley et al., 2011). Site-specific crop management is a more general term that includes variable rate application, with goals of increasing profitability and sustainability by managing resources based on the specific ‘site’ (Alley et al., 2011). Utilizing variable rate applications, for inputs such as nitrogen, is an area of research that is being practiced by numerous corn producers across the U.S. and globally (Iqbal et al., 2020; “Precision Nitrogen Application,” 2014).

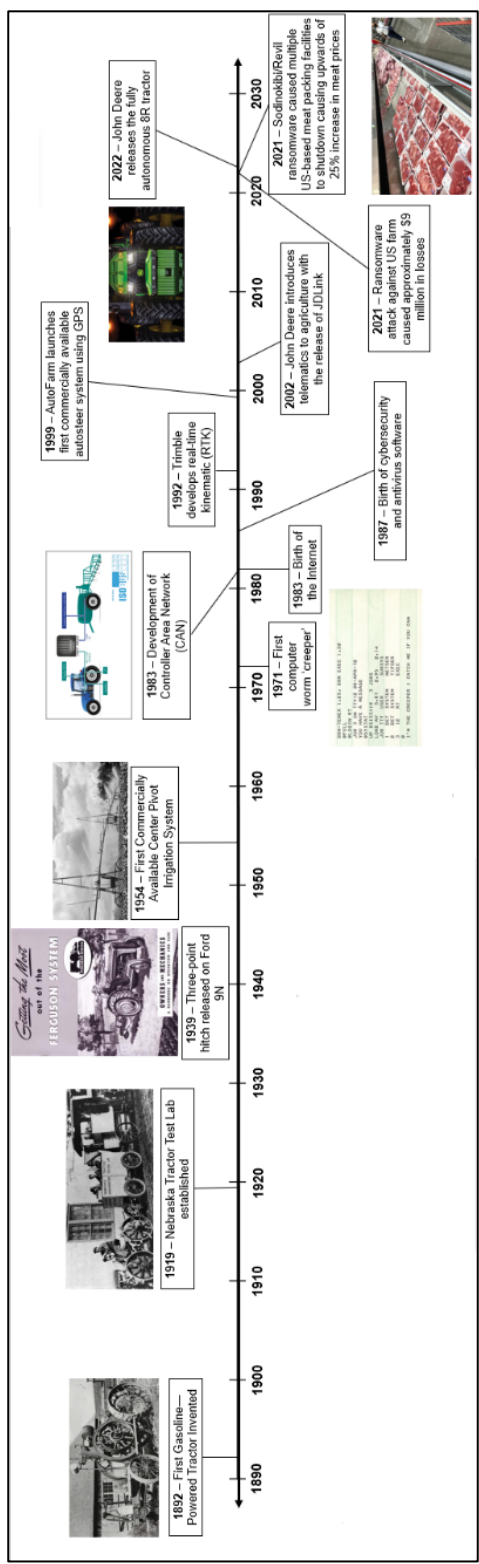


Figure 2.1: Timeline of agricultural machinery and cybersecurity

Agricultural equipment has advanced greatly since the introduction of the gasoline tractor (Figure 2.1) in 1892 (“The Tractor,” n.d.). With the increase in farming productivity and acreage per farm, agricultural equipment quickly increased in horsepower and size. The year 1920 saw the establishment of the Nebraska Tractor Test Lab (NTTL) as a means for validating tractor performance, as agricultural equipment advanced rapidly (“NTTL: Only U.S. OECD Tractor Test Lab,” n.d.). Modern agricultural equipment has been built with as much as 640 horsepower to manage the large size of many modern farms (“9 Series Tractors | 9RX 640 | John Deere US,” n.d.). Moreover, the dependence on synthetic chemicals and fertilizer during the Green Revolution, has increased the need for specialty agricultural equipment such as fertilizer applicators (“Tractors and Green Revolution in India,” n.d.). Another advancement is the introduction of Controller Area Network (CAN) in 1986, and its integration into agricultural equipment in the years that followed, which has allowed for larger equipment to offer more precision control and functionality (“CAN in Automation (CiA): History of the CAN technology,” n.d.; *John Deere CAN Bus Presentation*, 2021). Navigation innovations such as Real-Time Kinetic (RTK) and the introduction of auto-steer in 1992 and 1999 respectively, have allowed for more precise navigation of agricultural equipment (“Timeline of Ag Equipment ‘Firsts,’” 2009). Modern equipment is commonly equipped with Global Positioning System (GPS) guidance, auto-steer, CAN, telematics, and numerous other technologies that enable equipment to be used for diverse applications (Baillie et al., 2018).

Autonomous technologies have greatly advanced over the last decade, with numerous autonomous technologies being applied to the agricultural industry in efforts to improve efficiencies and reduce pressure from challenges such as labor shortages (Rose et al., 2021; Sparrow and Howard, 2021). Some examples of autonomous agricultural machinery offered by original equipment manufacturers (OEMs) include John Deere's newly released autonomous model 8R tractor (Tibken, 2022), Raven's OMNiPOWER platform ("Gains For the Farmer and the Farm," 2022), and the Monarch Electric Tractor ("Monarch Tractor Electric Tractor," n.d.). Numerous other autonomous technologies are being integrated into many other areas of agriculture, including specialty crop equipment, meatpacking, large combine harvesters and much more. The future will see a significant amount of automation be integrated into agriculture (Paukner, 2022). However, with all the introduction of autonomous technologies, cybersecurity will become a greater concern to the agricultural community.

2.2. Introduction to Cybersecurity

Cybersecurity is the protection of computer networks, data, and devices from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information (Fidler, 2017; "What is Cybersecurity?," 2019). Cybersecurity can also include securing areas where computers are used to harm the greater society such as hate crimes or cyberbullying (Veale and Brown, 2020). The recent increases in digital technologies and their integration into numerous areas of modern society, such as industrial control systems, personal home applications, automotive, agricultural, and business operations, have increased the significance of cybersecurity

(Veale and Brown, 2020). For this thesis, cybersecurity will focus mainly on the definition related to the CIA triad and the goal of securing data and computer systems from unauthorized access or attacks.

The CIA triad of cybersecurity refers to the confidentiality, integrity, and availability of cyber systems. Confidentiality in cybersecurity means that only authorized people, parties, or systems can access specific data (Pfleeger et al., 2015). This also could be known as the principle of least privilege, where only the minimum number of people necessary are given access to data (Gegick and Barnum, 2005). Within agriculture, there are many data sources where maintaining confidentiality will give a farmer a competitive advantage. For example, the leaking of confidential data pertaining to the specific operations of a farm, such as yield or agrochemical inputs, could help an adversary to ‘understand potential market drivers or to identify struggling farms with underutilized land that can be bought lower than the standard market price’ (Baker and Green, 2020). A lack of confidentiality could potentially expose a farmer or personnel’s private information, leading to identity fraud.

Integrity within the cybersecurity context means that data or systems remain consistent and unaltered, unless modified in appropriate ways by authorized parties (Pfleeger et al., 2015). In the context of agriculture, examples of data or systems that require integrity include planting population maps, fertilizer input prescriptions, heating ventilation and air conditioning (HVAC) systems to cool livestock, or livestock feeding rations (Baker and Green, 2020). Integrity in agriculture could also pertain to equipment operation commands or irrigation schedules (Chamarajnar and Ashok, 2019). The loss

of integrity of these time-critical datasets or systems could lead to significant profit losses or damages extending beyond the farming operation (Boghossian et al., 2018).

Availability within cybersecurity means that a system or dataset is useable or accessible when expected or needed (Pfleeger et al., 2015). Availability of many time-critical systems such as agricultural equipment, logistics, or operation management datasets are crucial for optimal efficiency and profitability. A loss of availability could require farmers to use legacy systems, if available, or pay a ransom to make systems available, in the case of ransomware (Baker and Green, 2020; Sontowski et al., 2020).

2.3. Cybersecurity Concerns in the Agriculture Community

Cyberattacks targeting agriculture have become more prevalent over the past few years. Two recent Federal Bureau of Investigation (FBI) reports (Federal Bureau of Investigation, 2021; Federal Bureau of Investigation, 2022) have outlined numerous cyberattacks that have targeted entities in the agricultural sector. The first report (Federal Bureau of Investigation, 2021) published in September 2021, brought awareness to the fact that ransomware attacks could cause financial loss and ultimately impact the food supply chain. An important attack highlighted in the report was the JBS meatpacking cyberattack in May 2021, that caused major disruptions to meat prices and resulted in JBS paying a \$11 million ransom (“Meat giant JBS pays \$11m in ransom to resolve cyber-attack,” 2021). Another attack targeted a US farm in January 2021, which ultimately resulted in \$9 million in losses. The second FBI report (Federal Bureau of Investigation, 2022) in April 2022 warned that ransomware cyberattacks could strategically target agricultural producers during critical seasons such as planting and

harvesting. The report noted that there were six known cyberattacks targeting grain cooperatives in the fall of 2021 and two attacks in early spring 2022.

There have also been numerous studies that have investigated cybersecurity solutions to the general agricultural community. For example, a study conducted in Finland focused on cybersecurity practices and requirements for communication networks within six dairy farms (Nikander et al., 2020). In a study conducted by (West, 2018), a prediction model framework was created to assess and quantify cybersecurity vulnerabilities in technology and the precision agricultural environment it is adapted to. Smart farming is another name for the data-driven, precision farming techniques of modern agriculture. Multiple studies discuss cybersecurity to smart farming systems such as (Barreto and Amaral, 2018) which highlights some important cybersecurity challenges to smart farming such as preventing denial of service (DoS) attacks to important IoT sensors. A thorough literature survey conducted by Demestichas et al. (2020), compiles a large amount of studies that discuss threats to smart farming and internet of things (IoT) devices in agriculture. The survey by Demestichas et al. highlights the fact that technologies, such as IoT devices, are being rapidly adopted and stakeholders need to exercise caution with how they adopt the new technologies to avoid costly cyberattacks. Gupta et al. (2020), presents more challenges to smart farming including a discussion on the multi-layer layout of the modern farming communication architecture and some examples of possible cyberattacks (Gupta et al., 2020). The Jahn Research Group discusses smart farming cybersecurity challenges related to food processing and the lack of cyber insurance coverage (Jahn et al., 2019). Yazdinejad et al.

(2021), conducted another thorough study of smart farming vulnerabilities and presented a case study on the process of a cyberattack (Yazdinejad et al., 2021). The study also presented a classification framework of attacks that target precision agriculture.

IoT devices will be common throughout smart farming and future farming practices. Ahanger and Aljumah, (2019), discuss security issues and defense mechanisms to protect IoT devices and found that there is need for improvement in the security of these devices (Ahanger and Aljumah, 2019). Ametepe et al. (2019), discusses a secure encryption method for IoT devices since the devices contain limited computational resources, as compared to larger computing devices that employ more robust data encryption methods (Ametepe et al., 2019). Angyalos et al. (2021), discusses the challenges with securing the modern agricultural system and that currently the benefits outweigh the risks of implementing modern technologies (Angyalos et al., 2021). The integrity of the data produced by IoT devices in agricultural settings is discussed in a paper by Chamarajnar and Ashok (2019) and found in their use-case analysis that threats to IoT devices could potentially be identified with 80% real-time accuracy and 90% precision. IoT-based agricultural devices and blockchain are investigated in a study by (Ferrag et al., 2020) and found that there are many areas, such as the design of practical and compatible cryptographic protocols, that need further research. Cybersecurity of IoT devices for the application of water management in agriculture, are also an important challenge to address since they could affect much more beyond the farm (Kamienski et al., 2018).

Some possible solutions to improve cybersecurity include the discussion of intrusion detection systems. A survey by (Ferrag et al., 2022) evaluates current intrusion detection

systems used to protect assets of the Agricultural 4.0 era. Prodanović et al., presents a data security model to protect agricultural wireless sensor networks (WSN) and found that it is possible to optimize hardware and software resources to protect such networks (Prodanović et al., 2020).

Cyberbiosecurity is discussed in a paper by (Duncan et al., 2019) which is the combination between cybersecurity, biosecurity, and cyber-physical security. The paper mentions the need for a coherent effort to address these issues across the United States (U.S.) agricultural landscape. Geil et al. (2018), conducted a survey of farmers in the U.S. to assess cybersecurity practices and found that there are large gaps in security knowledge in the agricultural community (Geil et al., 2018). Outside the United States, a report by researchers from Australia discussed the need for cybersecurity and if producers are properly prepared for cyberattacks (Borohl, 2021).

2.4. Cybersecurity Concerns to Agricultural Machinery and Vehicles

Agricultural machines perform many crucial tasks such as spraying, planting, and harvesting. Automation can already be found on many subsystems of current agricultural machinery, such as CNH's OptiSpread (Eckelkamp and Humphreys, 2022) on combine harvesters, with more levels of autonomy to come in the near future. Many of these automated features on agricultural machines will be controlled remotely with wireless cellular networks through platforms such as JD Operation Center application for John Deere Equipment ("Data Management | Operations Center | John Deere US," n.d.). Security of all devices and machines in the farming infrastructure will be important. Currently there are no documented cases of cyberattacks that targeted agricultural

machinery specifically, although there are some related cyber instances. A cyberattack in May 2022 targeted a major agricultural machinery manufacturer, AGCO, which resulted in the shutdown of multiple parts of their IT system (Rattigan, 2022). Although not a cyberattack, John Deere demonstrated the capability to remotely shut down tractors after they were stolen from Ukrainian farmers (Holderith, 2022).

There also has been specific research to investigate solutions to cybersecurity vulnerabilities on agricultural machinery. One study demonstrated a Denial of Service (DoS) attack to on-field sensors with applications to agricultural equipment (Sontowski et al., 2020). The limited number of practical solutions presented in literature for cybersecurity of agricultural machinery and the warning that cybersecurity of agricultural technologies and machinery is not being given enough serious consideration (Boghossian et al., 2018), highlights the need to investigate solutions for these critical agricultural machines.

Chapter 3: IMPACTS OF CYBERATTACKS TO PRECISION AGRICULTURAL OPERATIONS

This chapter presents a case study that will build a hypothetical scenario of a cyberattack targeting a critical farming operation: in-season nitrogen application to corn. An investigation of the tangible and intangible effects of the cyberattack to the farmer and broader agricultural community will be analyzed to determine how the significance of such attacks should inform cybersecurity mitigation decisions for agricultural

machinery. The quantity of financial resources that should be invested to secure agricultural machinery during the design process will also be discussed.

3.1. Background

Commodity corn production makes up about 24% of the United States (U.S.) cash crop industry with 15.1 billion bushels being produced in 2021 (Barrett, 2022). This equates to approximately \$48 billion in annual revenue (Kassel, 2022). Water, soil, light, and proper nutrients are all important for optimal corn yields, with the average US corn yield totaling 177.0 bushels/acre in 2021 (Barrett, 2022). Nitrogen is one of the key nutrients in corn production, as research has shown a high correlation between plant available nitrogen and yield (Puntel et al., 2016; Shapiro, n.d.). Nitrogen can be supplied to a corn crop from many sources such as synthetic fertilizers, manure, and crop residues. Since nitrogen is a mobile nutrient, proper management is needed to prevent nitrogen loss, resulting in negative environmental impacts and profit losses. As of March 2022, nitrogen fertilizer prices were at record highs, with costs ranging from \$0.93-\$1.10/pounds of nitrogen (Quinn and Reporter, 2022), increasing the urgency for proper nitrogen management practices.

Nitrogen management has been an important topic of research for many years in efforts to increase farmer's profits and decrease the negative environmental impacts resulting from poor management practices (Cassman et al., 2002). Most farmers rely on synthetic fertilizers as a main source of nitrogen for their corn crops, with common synthetic nitrogen fertilizers being Anhydrous Ammonia (NH₃), Urea, and UAN(28-32%) (Sellars and Nunes, 2021). Anhydrous Ammonia can be injected into the soil in the

fall or early spring before planting and is the source from which many other synthetic nitrogen fertilizers are made (Sellars and Nunes, 2021). Urea can be broadcast as a dry fertilizer and incorporated into the soil to prevent nitrogen volatilization (Shaver, 2014). Urea Ammonium Nitrate (UAN 28-32%) are liquid fertilizers that can be applied in-season and are typically safer to handle than other synthetic nitrogen fertilizers (Sellars and Nunes, 2021; Shaver, 2014). Research has shown that corn requires nitrogen at various points during the growing season, with the highest uptake occurring around V10 (Bender et al., 2013; “Nitrogen stabilizers,” 2018; Sellars and Nunes, 2021). To prevent nitrogen losses due to leaching or volatilization after an early season nitrogen application, in-season nitrogen applications have been recommended so the corn crop can utilize nitrogen soon after it is applied (Shaver, 2014). Side-dress nitrogen application of liquid fertilizer or fertigation have become common methods for in-season nitrogen application (Stansell, 2021).

Since there are multiple forms of nitrogen fertilizer, different types of fertilizer application equipment have evolved. Broadcast spreaders are used to apply granular nitrogen fertilizer. Anhydrous ammonia fertilizer injection equipment is built to handle pressurized anhydrous ammonia, where modern equipment is capable of variable rate applications. Liquid side dress equipment is built to inject liquid nitrogen sources close to the crop. Side dress equipment has evolved from ground driven units to hydraulic or electrically controlled units that are capable of variable rate applications. The rest of the background section will focus on nitrogen side-dress equipment as applied to this case study.

Nitrogen side-dress equipment is built around some fundamental technologies. Liquid nitrogen fertilizer originates in a tank and is moved through a series of pumps and valves to the output nozzles (Figure 1.1). Side-dress equipment has progressed from ground driven pumps with fixed output rates to more modern equipment with variable application rate capabilities. Modern, variable-rate nitrogen equipment can be controlled over the CAN bus, operating under the ISOBUS or ISO 11783 protocol (“NUTRI-PLACER® 920 & 2800 FERTILIZER APPLICATORS,” n.d.). Commands are sent from the tractor which control the pressure and flow rate produced from a pump on the implement. Section control valves are utilized downstream from the pump, to control the flow to various sections or nozzles across the implement. Finally, nozzles are sized to facilitate the proper flow rates needed for a given operation. Flow meters and pressure gauges are built into the implement which provide feedback on the current state of the implement over the CAN bus, which can be displayed on the virtual terminal in the tractor. This allows the operator to get real-time feedback on the state of the operation.

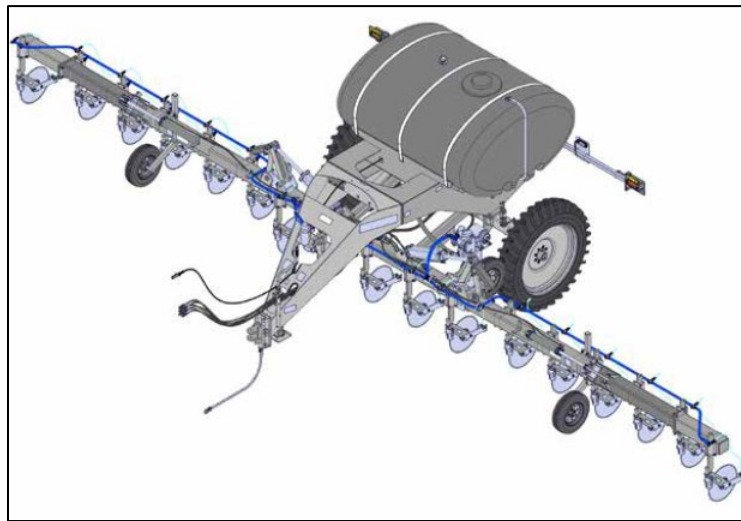


Figure 3.1 Liquid Side-Dress Equipment

This chapter will contribute to this thesis by demonstrating the potential financial significance that a cyberattack targeting a precision agricultural operation could have by providing charts, financial estimates, of discussions of the attacks. Section 3.2 outlines the research methodology used to analyze and calculate the tangible and intangible impact of a cyberattack to in-season nitrogen operations. Section 3.3 describes the results and analysis of three hypothetical cyberattack scenarios. Section 3.4 will also discuss the results and broader impacts to the agricultural community and future agricultural machinery.

3.2. Research Methodology

3.2.1. Case Study Criteria

Since there is a high degree of variability between farming operations, this case study will use a hypothetical 100-acre rainfed corn farming scenario, where a nitrogen side-dress application is altered by a cyberattack. The goal of this case study is to demonstrate the specific and broader impacts from a cyberattack to an agricultural operation and how they can inform mitigation and equipment design decisions. Some criteria and assumptions were needed to build this case study which fall under four categories: machinery, field location, nitrogen recommendation, and yield calculation.

First, for these cyberattacks to be feasible, the machinery will need to be modern, with variable rate capabilities. Since a cyberattack would ultimately result in the manipulation of the implement applying nitrogen, any implements without variable rate capabilities or that are not controlled by messages sent from a tractor operating the implement, will have no practical means of undergoing a cyberattack. Many large farms

in the US are equipped with modern, variable-rate application equipment which makes this assumption reasonable. A second criteria of the machinery is that the physical constraints of the implement allow for the specific cyberattack to take place. For example, the implement would need to have the capability to increase chemical application pressure and flow rate to reach the outlined attack application rates. The implement would also need application orifices that allow for a large variation in fertilizer application rates.

The location for this hypothetical case study will be Saunders County, Nebraska. Yield goals, soil nitrate levels, and soil organic matter levels will all be generated from values relative to Saunders County. The average yearly precipitation of Saunders County is 31 inches (“PRISM Climate Group at Oregon State University,” 2021) with a Hot Summer Continental Climate according to the Koppen Climate Classification (“Omaha, Nebraska Koppen Climate Classification (Weatherbase),” n.d.). The average yield for rainfed cornfields in Saunders County, Nebraska is around 155 bushels/acre for rainfed corn fields from 2008-2018 (“USDA - National Agricultural Statistics Service - Quick Stats Lite,” 2018), therefore yield target values will be set between 150-190 bushels per acre for the hypothetical scenario.

$$N_{rec} = [35 + (1.2 \times EY) - (8 \times NO_3 - N \text{ ppm}) - (0.14 \times EY \times OM) - other \text{ N credits}] \times Price_{adj} \times Timing_{adj} \quad (\text{Eq. 1})$$

where

N_{rec} = recommended nitrogen input for corn grain (lb/ac)

EY = expected yield (bu/ac)

$NO_3 - N \text{ ppm}$ = average nitrate-N concentration in the root zone (2–4 foot depth) in parts per million

OM = percent soil organic matter (min 0.5%, max 3%)
 $other\ N\ credits$ = include N from previous legume crop,
 manure and other organic material applied, and irrigation
 water N.
 $Price_{adj}$ = price adjustment coefficient
 $Timing_{adj}$ = adjustment factor for fall, spring, and split
 applications = 0.95 for split application

This case study will use the UNL nitrogen formula since it was developed using fields across Nebraska (Shapiro et al., 2019). The UNL Nitrogen formula (Eq. 1) considers numerous factors when calculating optimal nitrogen fertilizer rates (N_{rec}) for a corn crop. Expected yield (EY) is the first factor in the equation, where farmers can target specific yield goals for the upcoming corn crop based on factors such as historic yield data. This case study will assume that the yield target values are set to the highest average yield values that are appropriate for the specific field based on historic yield data. Soil nitrate levels ($NO_3 - N\ ppm$) and soil organic matter (OM) are the next factors in the equation, which can be determined through soil tests. Other nitrogen contributions (Figure 3.2) from previous legumes, manure, crop residues, and irrigation water are also factored into the equation. Finally, nitrogen application timing (Figure 3.2) and price adjustment (Eq. 2) are used to adjust the recommended amount of nitrogen for a given corn crop.

Table I. Estimated N credit from legumes and other crops for medium/fine textured soil and coarse soils.			Table II. Timing adjustment factors ($Timing_{adj}$) and definitions for adjusting calculated N rate for fine-medium textured soil and coarse texture soils.			
Legume Crop	Fertilizer-N reduction by soil texture (lb/acre)		Timing	Definition	Timing _{adj} Factor by soil texture	
	Fine-Medium ¹	Coarse ²			Fine-Medium ¹	Coarse ²
Soybean	45	35	Split (BMP)	At least 30 percent of N applied by sidedress and fertigation N	0.95	1.00 (when >60% in-season)
Dry bean	25	25	Mostly pre-plant	Less than 30 percent sidedress and fertigation N and preplant N>fall N	1.00	Do not apply
Alfalfa (70–100% stand, >4 plants/ft ²)	150	100	Mostly fall	Mostly fall applied N and less than 30 percent sidedress and fertigation N	1.05	Do not apply
Alfalfa (30–69% stand, 1.5–4 plants/ft ²)	120	70				
Alfalfa (0–29% stand, <1.5 plants/ft ²)	90	40				
Sweet clover and red clover	80% of credit allowed for alfalfa					
Sugar beets	50	50				

¹All textural classes except those defined under coarse textured
²Includes sand, loamy sand, and sandy loam

Figure 3.2: UNL Nitrogen Formula Nitrogen Credits and Timing Adjustments

$$Price_{adj} = 0.263 + \left(0.1256 * \frac{P_{corn}}{P_{nitrogen}}\right) - \left(0.00421 * \left(\frac{P_{corn}}{P_{nitrogen}}\right)^2\right) \quad (\text{Eq. 2})$$

where

$Price_{adj}$ = price adjustment coefficient

P_{corn} = price of corn (\$/bu)

$P_{nitrogen}$ = price of nitrogen (\$/lb)

$$EY = \max [EY_{min}, \min \left[EY_{max}, \frac{\left(\frac{N_{rate}}{Price_{adj} \times Timing_{adj}} + (8 * NO_3 - N \text{ ppm}) - 35 + \text{other N credits}\right)}{1.2 - (0.14 * OM)} \right] \right] \quad (\text{Eq. 3})$$

where:

EY = expected yield (bu/ac)

EY_{min} = minimum expected yield (bu/ac)

EY_{max} = maximum expected yield (bu/ac)

N_{rate} = recommended nitrogen input for corn grain (lb/ac)

$NO_3 - N \text{ ppm}$ = average nitrate-N concentration in the root zone (2–4 foot depth) in parts per million

OM = percent soil organic matter (min 0.5%, max 3%)

other N credits = include N from previous legume crop, manure and other organic material applied, and irrigation water N.

$Price_{adj}$ = price adjustment coefficient

$Timing_{adj}$ = adjustment factor for fall, spring, and split

applications = 0.95 for split application

$$AY = \max [EY_{min}, \min \left[EY_{max}, \frac{\left(\frac{N_{rate,act}}{Price_{adj} \times Timing_{adj}} + (8 \cdot NO_3 - N \text{ ppm}) - 35 + other \ N \ credits \right)}{1.2 - (0.14 \cdot OM)} \right]] \quad (\text{Eq. 4})$$

where:

AY = actual yield (bu/ac)

EY_{min} = minimum expected yield (bu/ac)

EY_{max} = maximum expected yield (bu/ac)

$N_{rate,act}$ = actual nitrogen input for corn grain (lb/ac)

$NO_3 - N \text{ ppm}$ = average nitrate-N concentration in the root zone (2–4 foot depth) in parts per million

OM = percent soil organic matter (min 0.5%, max 3%)

$other \ N \ credits$ = include N from previous legume crop, manure and other organic material applied, and irrigation water N.

$Price_{adj}$ = price adjustment coefficient

$Timing_{adj}$ = adjustment factor for fall, spring, and split applications = 0.95 for split application

A real case study could try these scenarios on actual corn and measure the resulting yield after the cyberattacks. Since this case study is only building hypothetical scenarios, a formula derived from the UNL nitrogen formula will be used to calculate yield. Expected (EY) and actual yield (AY) will be calculated by rearranging the UNL Nitrogen formula to solve for yield. Eq. 3 and Eq. 4 demonstrate how EY and AY are calculated respectively. The maximum and minimum attainable yield on this field (EY_{max} and EY_{min}) will be set as follows. A 30-bushel yield boost above expected yield values will be the maximum attainable yield if nitrogen is overapplied above prescribed rates. The 30-bushel yield boost is an arbitrary number and is set to limit maximum yield values that are unrealistic for the specific conditions and location of this hypothetical scenario. This

assumes that yield target values (EY) are set at the highest, reasonably attainable value across the field, therefore gaining more than a 30-bushel yield boost by overapplying nitrogen would be unrealistic. The minimum attainable yield value will be 100-bushels. This means that if no nitrogen is applied to the planted corn, the corn would still yield 100-bushels. The reality is yield values could be lower than 100-bushels if no nitrogen is applied, but this number is set to limit unrealistically low yield values. Corn prices vary depending on market prices and the quality of the corn being sold. For this study, it will be assumed that all corn will be sold at a constant price of \$7.53 based on the market price as of March 22, 2022 (“Corn PRICE Today | Corn Spot Price Chart | Live Price of Corn per Ounce | Markets Insider,” n.d.). Since this case study scenario will be based on an application of UAN32, a nitrogen price of \$1.10/lb will be used based on prices as of March 22, 2022 (Quinn and Reporter, 2022).

Since nitrogen is a key nutrient in the production of corn, the following scenarios will look to demonstrate the potential profit losses incurred from cyberattacks to in-season nitrogen applications for corn. The first section will outline what a typical in-season nitrogen application operation would look like, while the following sections will discuss three potential attack scenarios and their impacts.

3.2.2. Control Scenario

All hypothetical scenarios in this case study will use a 100-acre corn field, divided into 100, one-acre management zones (Figure 3.3). The UNL nitrogen formula (Eq. 1) will be used to calculate nitrogen needs for each one-acre section for optimal corn production. Figure 3.4 shows the hypothetical 100-acre corn field, with yield goals for

each one-acre section. Yield goals were selected randomly from a range of 150-190 bushels/acre based on historic yield values for rainfed corn fields in Saunders County, Nebraska (“USDA - National Agricultural Statistics Service - Quick Stats Lite,” 2018). Figure 3.5 shows the 100-acre field with various soil nitrate levels, selected randomly from a range of 2.0-4.0ppm which are realistic for fields with fine-textured soil in central Nebraska (Shapiro et al., 2019). Similarly, soil organic matter values were randomly selected from a range of 1.8-2.2% which are also realistic for fields with fine-textured soil in central Nebraska (“Soil Management for Increased Soil Organic Matter (G2283),” n.d.). The timing factor will be set at 0.95 since nitrogen applications will be split between at-planting and in-season applications. All case study scenarios will use a nitrogen price of \$1.10 per pound (Quinn and Reporter, 2022) and a corn price of \$7.53 per bushel (“Corn PRICE Today | Corn Spot Price Chart | Live Price of Corn per Ounce | Markets Insider,” n.d.) which are based on current average prices as of March 22, 2022. Using Eq. 2 the price adjustment factor is calculated to be 0.926. All these same input values and methods will be used across all attack scenarios in this case study.

100 Acre Field										
	A	B	C	D	E	F	G	H	I	J
1	1 acre									
2										
3										
4										
5										
6										
7										
8										
9										
10										

Figure 3.3 100-acre field with 1-acre management zones

Corn Expected Yield (EY) [150-190 bu/acre on 100-acre rainfed field, Saunders County, NE] =RANDBETWEEN(150,190)										
	A	B	C	D	E	F	G	H	I	J
1	175	157	174	168	152	189	181	175	180	158
2	161	162	188	172	167	190	151	165	180	157
3	150	190	184	185	151	182	176	153	174	157
4	150	172	178	183	174	173	155	156	185	178
5	163	152	150	161	186	170	174	184	150	153
6	162	160	152	171	184	178	165	170	172	160
7	169	189	155	155	164	189	162	168	162	186
8	180	174	169	176	189	188	184	161	169	189
9	156	163	187	153	166	162	168	159	162	162
10	174	164	190	171	170	181	190	151	176	175

Figure 3.4: Estimated Corn Yield Values

Soil nitrate levels (NO ₃ -N) [2.0-4.0ppm on 100-acre field, Saunders County, NE] =(RAND()*2)+2										
	A	B	C	D	E	F	G	H	I	J
1	3.1	2.6	3.0	3.8	2.8	2.6	3.3	3.3	3.5	3.4
2	2.8	3.7	2.7	2.2	3.9	3.1	2.2	2.2	2.2	2.4
3	3.7	2.0	2.3	2.4	3.2	4.0	3.7	3.1	2.1	2.9
4	3.3	2.7	3.0	3.0	2.2	2.7	3.0	2.5	2.0	2.1
5	2.0	3.9	2.7	3.7	2.1	3.8	2.3	2.1	3.4	2.4
6	2.6	3.9	3.6	3.5	3.4	3.8	2.3	2.5	3.5	3.4
7	2.9	3.7	3.9	2.6	3.0	2.2	2.6	2.6	3.2	2.5
8	2.3	2.3	2.6	2.7	4.0	2.1	3.6	2.7	3.4	2.1
9	2.8	2.2	3.8	2.2	2.1	3.1	2.2	2.8	3.1	3.3
10	3.9	3.4	3.9	2.0	3.5	3.3	2.4	3.9	2.4	2.5

Figure 3.5: Soil Nitrate Levels

Soil Organic Matter (OM) [1.8-2.2% on 100-acre field, Saunders County, NE] $=(\text{RAND}()*0.4)+1.8$										
	A	B	C	D	E	F	G	H	I	J
1	2.2	2.2	2.0	2.0	2.1	2.0	1.9	2.0	2.0	1.8
2	2.0	2.1	1.8	2.1	2.1	2.0	1.8	2.2	1.9	2.1
3	2.0	2.1	1.8	1.9	1.8	2.0	2.1	1.8	2.0	2.0
4	1.9	1.8	2.0	2.2	2.1	1.9	1.9	2.1	1.9	1.9
5	2.1	1.9	2.0	1.9	2.1	1.9	1.8	2.2	1.8	2.2
6	2.1	2.1	2.1	2.1	2.2	1.9	2.1	2.0	1.8	2.1
7	2.0	1.9	2.0	1.9	1.8	1.9	2.1	1.9	1.9	2.1
8	2.1	2.1	2.2	2.0	2.2	2.1	2.2	2.1	2.0	2.0
9	2.1	1.9	2.0	2.0	2.1	2.1	2.0	2.2	1.9	1.8
10	2.1	1.8	2.1	1.8	2.0	1.9	1.8	2.0	2.1	1.8

Figure 3.6: Soil Organic Matter Levels

Using Eq. 1, nitrogen needs (N_{rec}) can be calculated for acre A1. By using input values of $EY = 175 \text{ bu/ac}$, $NO_3 - N = 3.1 \text{ ppm}$, $OM = 2.2\%$, $other \text{ N credits} = 0$, $Price_{adj} = 0.926$, and $Timing_{adj} = 0.95$, N_{rec} can be calculated to be 147 lb/ac for acre A1. This same method will be used to calculate total nitrogen recommendations for each acre in the 100-acre field (Figure 3.7).

Total Recommended Nitrogen Input (Nrec) [lbs/acre]										
	A	B	C	D	E	F	G	H	I	J
1	147	136	151	140	132	165	157	149	152	138
2	142	135	168	152	136	163	141	145	162	139
3	126	167	167	166	134	149	145	136	157	137
4	131	155	154	154	154	153	137	137	169	162
5	147	128	134	137	164	143	160	161	131	135
6	141	132	126	142	152	149	146	150	149	134
7	146	159	129	140	146	170	142	151	140	162
8	158	153	146	153	151	167	150	140	143	168
9	135	149	156	138	148	138	152	136	143	142
10	142	142	154	159	143	156	171	125	155	159

Figure 3.7: Total recommended nitrogen input for growing season (lbs/acre)

For all application scenarios in this paper, the nitrogen applications will be split 25% at planting and 75% in-season. This is consistent with many field trials and recommendations for in-season nitrogen management (Shapiro et al., 2019). The in-season applications will be applied through liquid side-dress applications using the fertilizer source UAN32. Only the in-season side-dress operation, or 75% of the total nitrogen applied to the field will be affected by the cyberattack. Figure 3.7 shows the total nitrogen needs calculated using the UNL nitrogen formula for the 100-acre field in this case study. Figure 3.8 demonstrates the pre-plant and in-season nitrogen needs for the 100-acre field. These same nitrogen recommendations remain the same across all scenarios in this case-study.

First Nitrogen Application Actual Rates [lbs/acre]										
	A	B	C	D	E	F	G	H	I	J
1	37	34	38	35	33	41	39	37	38	35
2	35	34	42	38	34	41	35	36	40	35
3	31	42	42	41	33	37	36	34	39	34
4	33	39	38	38	39	38	34	34	42	41
5	37	32	34	34	41	36	40	40	33	34
6	35	33	31	36	38	37	37	38	37	33
7	37	40	32	35	36	42	36	38	35	40
8	40	38	36	38	38	42	37	35	36	42
9	34	37	39	35	37	35	38	34	36	36
10	35	36	39	40	36	39	43	31	39	40

Figure 3.8: Pre-plant recommended nitrogen application rates (lbs/acre)

Second Nitrogen Application Actual Rates [lbs/acre]										
	A	B	C	D	E	F	G	H	I	J
1	110	102	113	105	99	123	117	112	114	104
2	106	101	126	114	102	122	105	109	121	104
3	94	125	125	124	100	112	109	102	118	103
4	98	116	115	115	116	115	103	102	127	122
5	110	96	101	103	123	107	120	121	99	101
6	106	99	94	107	114	112	110	113	112	100
7	110	119	97	105	109	127	107	113	105	121
8	119	114	109	115	114	125	112	105	107	126
9	101	112	117	104	111	104	114	102	107	107
10	106	107	116	119	108	117	129	94	116	119

Figure 3.9: In-season recommended nitrogen application rates (lbs/acre)

3.2.3. Calculating Financial Impacts

Profit potential loss or gain (P_{LG}) will be used to compare cyberattack scenarios. The first step in calculating profit is to calculate the expected and actual yield for the given scenario. Expected yield (EY) and actual yield (AY) will be calculated using Eq. 3 and 4 respectively. For the control case, $AY = EY$, since no cyberattack occurs. For the attack scenarios, there will be a difference in expected and actual yield values, which will lead to a difference in revenue and profit. Figure 3.10 shows the expected or actual yield values for the control case.

Total Actual Corn Yield (AY) [bu/acre, AYmin=100bu/acre, AYmax=EY+30bu/acre]										
	A	B	C	D	E	F	G	H	I	J
1	175	157	174	168	152	189	181	175	180	158
2	161	162	188	172	167	190	151	165	180	157
3	150	190	184	185	151	182	176	153	174	157
4	150	172	178	183	174	173	155	156	185	178
5	163	152	150	161	186	170	174	184	150	153
6	162	160	152	171	184	178	165	170	172	160
7	169	189	155	155	164	189	162	168	162	186
8	180	174	169	176	189	188	184	161	169	189
9	156	163	187	153	166	162	168	159	162	162
10	174	164	190	171	170	181	190	151	176	175

Figure 3.10: Actual (calculated) corn yield values (bu/acre)

After calculating yield values, Eq. 5-11 can be used to calculate P_{LG} . Eq. 5 is used to calculate total expected revenue (R_{exp}) for the field. Based on an expected yield total (EY_{tot}) of 16,983bu and the price of corn (v_{corn}) of \$7.53/bu, the total expected revenue for the control case comes to \$127,882. Eq. 6 can be used to calculate the expected cost of nitrogen fertilizer, C_{exp} . Using a value of 14,758lbs of total recommended nitrogen ($N_{tot,exp}$) for the field and a nitrogen cost ($c_{nitrogen}$) of \$1.10/lb, the total expected cost can be calculated at \$16,232 for the control scenario. Eq. 7 can then be used to calculate total expected profit (P_{exp}) which totals \$111,648 for the control case. Since all case study scenarios will use the same nitrogen recommendation starting values, all scenarios will

have an expected profit of \$111,648. Similar to Eq. 5, actual revenue (R_{act}) can be calculated using Eq. 8. For the control case, $R_{act} = R_{exp} = \$127,882$ since expected and actual yield values are the same. C_{act} can be calculated to \$16,232 for the control case, by using Eq. 9. P_{act} is calculated at \$111,648 for the control case using Eq. 10. Finally, P_{LG} can be calculated to \$0 for the control case using Eq. 11, since no cyberattack occurs. This same method will be used to calculate profit loss or gain for all attack scenarios.

$$R_{exp} = EY_{tot} * v_{corn} \quad (\text{Eq. 5})$$

where:

R_{exp} = expected revenue (\$)

EY_{tot} = expected total yield (bu)

v_{corn} = value of corn grain (\$/bu)

$$C_{exp} = N_{tot,exp} * c_{nitrogen} \quad (\text{Eq. 6})$$

where:

C_{exp} = expected total cost (\$)

$N_{tot,exp}$ = expected total pounds of nitrogen to be applied (lb)

$c_{nitrogen}$ = cost of nitrogen per pound (\$/lb)

$$P_{exp} = R_{exp} - C_{exp} \quad (\text{Eq. 7})$$

where:

P_{exp} = total expected profit (\$)

R_{exp} = expected revenue (\$)

C_{exp} = expected total cost (\$)

$$R_{act} = AY_{tot} * v_{corn} \quad (\text{Eq. 8})$$

where:

R_{act} = actual revenue (\$)

AY_{tot} = actual total yield (bu)

v_{corn} = value of corn grain (\$/bu)

$$C_{act} = N_{tot,act} * c_{nitrogen} \quad (\text{Eq. 9})$$

where:

C_{act} = actual total cost (\$)

$N_{tot,act}$ = actual total pounds of nitrogen to be applied (lb)

$c_{nitrogen}$ = cost of nitrogen per pound (\$/lb)

$$P_{act} = R_{act} - C_{act} \quad (\text{Eq. 10})$$

where:

P_{act} = total actual profit (\$)

R_{act} = actual revenue (\$)

C_{act} = actual total cost (\$)

$$P_{LG} = P_{exp} - P_{act} \quad (\text{Eq. 11})$$

where:

P_{LG} = profit loss or gain (\$)

P_{exp} = total expected profit (\$)

P_{act} = total actual profit (\$)

3.2.4. *Attack Scenarios*

This section outlines the strategy of the attack scenarios. The cyberattack for this case study will target the tractor and implement applying side dress nitrogen. The goal of the cyberattack will be to increase or decrease prescribed application rates while applying the same cumulative total of prescribed nitrogen across the field. Many other attack scenarios could be assessed such as applying as much nitrogen as possible over the smallest area. This case study looks specifically at this strategic attack to assess if a cyberattack strategy

could be used that causes significant financial loss while making the operation appear normal. Figure 3.11 shows the attack strategy for attack scenario 1. Each one-acre subsection of the field is adjusted by a factor of 50%, 75%, 100%, 150% or 200% of prescribed rates. For example, acre B5 would apply 50% of the prescribed rate of nitrogen while acre H4 would apply 200% of prescribed rates. The placement of the rate adjustment acres is random across the field.

Attack 1 - % of Prescribed N Rates										
	A	B	C	D	E	F	G	H	I	J
1	100%	150%	50%	100%	50%	150%	100%	50%	50%	200%
2	200%	75%	75%	100%	50%	100%	75%	50%	100%	50%
3	75%	150%	150%	200%	150%	75%	150%	75%	50%	200%
4	50%	100%	50%	75%	75%	100%	100%	200%	50%	100%
5	150%	50%	150%	50%	200%	75%	50%	50%	200%	150%
6	75%	150%	75%	75%	100%	200%	200%	100%	100%	50%
7	100%	75%	100%	50%	100%	50%	150%	100%	150%	100%
8	50%	50%	150%	100%	50%	50%	150%	75%	75%	50%
9	50%	200%	100%	50%	150%	150%	50%	100%	50%	50%
10	50%	75%	100%	150%	75%	200%	50%	50%	100%	150%

Figure 3.11: Cyberattack Scenario 1

Attack scenario 2 takes a more strategic approach to the placement of the attack. The attack will result in applications of 45% and 280% of prescribed rates across the field.

Figure 3.12 demonstrates the layout of attack 2.

Attack 2 - % of Prescribed N Rates										
	A	B	C	D	E	F	G	H	I	J
1	45%				280%	45%				280%
2										
3										
4										
5										
6										
7										
8										
9										
10										

Figure 3.12: Cyberattack Scenario 2

Attack scenario 3 again takes a strategic approach to fertilizer prescription rate adjustment throughout the field. Figure 3.13 demonstrates attack 3, where fertilizer rates are applied at 75%, 100%, or 200% of prescribed rates.

Attack 3 - % of Prescribed N Rates										
	A	B	C	D	E	F	G	H	I	J
1	100%	25%	200%	25%	100%	25%	200%	25%	200%	100%
2										
3										
4										
5										
6										
7										
8										
9										
10										

Figure 3.13: Cyberattack Scenario 3

3.3. Results

This section will present how each of the cyberattack scenarios will affect the prescribed nitrogen rates across hypothetical field. The resulting yield values will be calculated along with the potential profit loss or gain for each cyberattack scenario.

3.3.1. Attack Scenario 1

All attack scenarios result in a deviation from prescribed nitrogen application rates. Figure 3.14 shows in-season nitrogen application rates after attack 1. For attack 1, $N_{tot,exp} = 14,758\text{lb}$ and $N_{tot,act} = 14,781\text{lb}$. Since there is a 23lb or 0.2% increase in

actual vs. prescribed rates, the attack satisfies the assumptions that total cumulative pounds of prescribed and applied nitrogen to the field remains constant.

Second Nitrogen Application Recommendation [lbs/acre at 75% of total Nrec in-season application]										
	A	B	C	D	E	F	G	H	I	J
1	110	102	113	105	99	123	117	112	114	104
2	106	101	126	114	102	122	105	109	121	104
3	94	125	125	124	100	112	109	102	118	103
4	98	116	115	115	116	115	103	102	127	122
5	110	96	101	103	123	107	120	121	99	101
6	106	99	94	107	114	112	110	113	112	100
7	110	119	97	105	109	127	107	113	105	121
8	119	114	109	115	114	125	112	105	107	126
9	101	112	117	104	111	104	114	102	107	107
10	106	107	116	119	108	117	129	94	116	119

Second Nitrogen Application Actual Rates [lbs/acre]										
	A	B	C	D	E	F	G	H	I	J
1	110	153	57	105	50	185	117	56	57	208
2	213	76	95	114	51	122	79	54	121	52
3	71	188	188	248	150	84	163	77	59	206
4	49	116	58	86	87	115	103	205	63	122
5	166	48	151	51	247	80	60	60	197	152
6	79	148	71	80	114	224	220	113	112	50
7	110	89	97	52	109	64	160	113	158	121
8	59	57	164	115	57	63	168	79	81	63
9	51	223	117	52	166	155	57	102	54	53
10	53	80	116	179	81	234	64	47	116	179

Figure 3.14: Prescribed vs. Actual nitrogen application rates (lbs/acre) after attack 1

UAN32 will be used as the source of nitrogen for in-season nitrogen applications. UAN32 is 32% nitrogen by weight (“Technical Data Sheet: Urea Ammonium Nitrate,” n.d.). Figure 3.15 shows the UAN32 application rates in gal/ac required to attain the nitrogen application rates shown in Figure 3.14. The cyberattack resulted in an additional 7gal above the total prescribed amount of UAN32 applied across the field.

Second UAN32 Liquid Nitrogen Application Expected Rates [gal/acre]										
	A	B	C	D	E	F	G	H	I	J
1	31	29	32	30	28	35	33	32	32	29
2	30	29	36	32	29	35	30	31	34	30
3	27	36	36	35	28	32	31	29	34	29
4	28	33	33	33	33	33	29	29	36	35
5	31	27	29	29	35	30	34	34	28	29
6	30	28	27	30	32	32	31	32	32	29
7	31	34	28	30	31	36	30	32	30	34
8	34	33	31	33	32	36	32	30	31	36
9	29	32	33	30	31	29	32	29	30	30
10	30	30	33	34	31	33	37	27	33	34

Second UAN32 Liquid Nitrogen Application Actual Rates [gal/acre]										
	A	B	C	D	E	F	G	H	I	J
1	31	43	16	30	14	53	33	16	16	59
2	60	22	27	32	15	35	22	15	34	15
3	20	53	54	71	43	24	46	22	17	58
4	14	33	16	25	25	33	29	58	18	35
5	47	14	43	15	70	23	17	17	56	43
6	23	42	20	23	32	64	62	32	32	14
7	31	25	28	15	31	18	46	32	45	34
8	17	16	47	33	16	18	48	22	23	18
9	14	63	33	15	47	44	16	29	15	15
10	15	23	33	51	23	67	18	13	33	51

Figure 3.15: Expected vs. Actual application rates of UAN32 (gal/acre) after attack 1

By using Eq. 4, the actual yield can be calculated for each acre across the 100-acre field. Figure 3.16 shows a comparison between expected and actual yield after attack 1. The total expected yield, EY_{tot} , for the field remained at 16,983bu while the actual corn yield, AY_{tot} , totaled 15,243bu for the field. This resulted in a 1,740bu loss as a result of the cyberattack. On a per-acre basis, this equates to a 17.4bu yield penalty per acre for the hypothetical 100-acre field.

Corn Expected Yield (EY) [150-190 bu/acre on 100-acre rainfed field, Saunders County, NE] =RANDBETWEEN(150,190)											Total Actual Corn Yield (AY) [bu/acre, AYmin=100bu/acre, AYmax=EY+30bu/acre]										
	A	B	C	D	E	F	G	H	I	J		A	B	C	D	E	F	G	H	I	J
1	175	157	174	168	152	189	181	175	180	158	1	175	187	104	168	100	219	181	106	110	188
2	161	162	188	172	167	190	151	165	180	157	2	191	131	150	172	103	190	119	100	180	100
3	150	190	184	185	151	182	176	153	174	157	3	121	220	214	215	181	147	206	122	102	187
4	150	172	178	183	174	173	155	156	185	178	4	100	172	107	146	138	173	155	186	108	178
5	163	152	150	161	186	170	174	184	150	153	5	193	100	180	100	216	137	102	108	180	183
6	162	160	152	171	184	178	165	170	172	160	6	129	190	122	137	184	208	195	170	172	100
7	169	189	155	155	164	189	162	168	162	186	7	169	152	155	100	164	111	192	168	192	186
8	180	174	169	176	189	188	184	161	169	189	8	106	102	199	176	117	110	214	128	136	111
9	156	163	187	153	166	162	168	159	162	162	9	100	193	187	100	196	192	100	159	100	100
10	174	164	190	171	170	181	190	151	176	175	10	107	132	190	201	137	211	112	100	176	205

Figure 3.16: Expected vs. Actual (calculated) yield after attack 1

Using Eqs. 5-11, total profit loss and profit loss per acre can be calculated. Figure 3.17 shows the profit loss or gain for each 1-acre section of the 100-acre field. The farmer would remain profitable but lose \$13,129 of potential profit (P_{LG}) across the 100-acre field because of attack 1. This averages to about \$131/ac of potential profit loss. Figure 3.18 shows a financial summary of the financial impacts from attack 1. An adjustment in the (EY_{max} and EY_{min}) values, relative to average yield, could affect the per-acre profitability.

Difference Between Actual and Expected Profit (PLG) [\$]										
	A	B	C	D	E	F	G	H	I	J
1	0	170	-463	0	-337	158	0	-460	-468	112
2	109	-209	-251	0	-427	0	-210	-430	0	-372
3	-194	157	157	89	171	-231	166	-203	-481	113
4	-322	0	-472	-244	-240	0	0	113	-510	0
5	165	-339	171	-403	90	-217	-476	-509	117	170
6	-221	171	-198	-223	0	103	105	0	0	-397
7	0	-243	0	-357	0	-516	167	0	168	0
8	-495	-480	166	0	-481	-519	164	-220	-221	-519
9	-366	103	0	-342	165	169	-449	0	-408	-408
10	-444	-213	0	160	-221	97	-513	-332	0	160

Figure 3.17: Potential-Profit loss or gain per acre resulting from attack 1

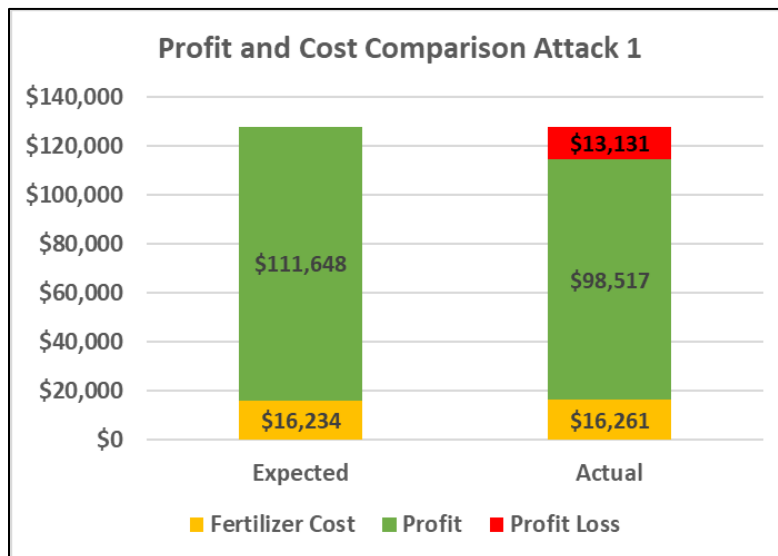


Figure 3.18: Financial impacts from attack 1

3.3.2. Attack Scenario 2

Figure 3.19 demonstrates in-season nitrogen input rates after attack 2 as compared to the prescribed rates. Nitrogen totals of $N_{tot,exp} = 14,758\text{lbs}$ and $N_{tot,act} = 14,733\text{lbs}$ are essentially equal with only a 25lb or 0.2% difference. This again satisfies the assumption that the cumulative total of recommended and applied nitrogen remains essentially equal.

Second Nitrogen Application Recommendation [lbs/acre at 75% of total Nrec in-season application]										
	A	B	C	D	E	F	G	H	I	J
1	110	102	113	105	99	123	117	112	114	104
2	106	101	126	114	102	122	105	109	121	104
3	94	125	125	124	100	112	109	102	118	103
4	98	116	115	115	116	115	103	102	127	122
5	110	96	101	103	123	107	120	121	99	101
6	106	99	94	107	114	112	110	113	112	100
7	110	119	97	105	109	127	107	113	105	121
8	119	114	109	115	114	125	112	105	107	126
9	101	112	117	104	111	104	114	102	107	107
10	106	107	116	119	108	117	129	94	116	119

Second Nitrogen Application Actual Rates [lbs/acre]										
	A	B	C	D	E	F	G	H	I	J
1	60.6	56.1	62.3	57.6	277	67.9	64.6	61.5	62.6	291
2	58.6	55.5	69.4	62.5	286	67.1	58	59.8	66.7	291
3	51.8	68.9	69	68.3	281	61.6	59.8	56.2	64.9	288
4	54	63.8	63.3	63.4	323	63.1	56.6	56.4	69.6	341
5	60.7	52.8	55.4	56.6	345	59	65.8	66.4	54.2	283
6	58.1	54.4	51.9	58.6	320	61.5	60.4	61.9	61.5	281
7	60.3	65.6	53.4	57.6	306	70	58.8	62.2	57.8	340
8	65.3	63	60.1	63.2	318	68.9	61.8	57.8	59.1	353
9	55.6	61.4	64.5	57.1	310	56.9	62.7	56.2	58.9	298
10	58.6	58.7	63.7	65.5	301	64.5	70.7	51.6	63.8	334

Figure 3.19: Prescribed vs. Actual nitrogen application rates (lbs/acre) after attack 2

Figure 3.20 demonstrates the UAN32 rates for this scenario. There is a 7gal reduction in UAN32 applied over the 100-acre field as a result of attack 2.

Second UAN32 Liquid Nitrogen Application Expected Rates [gal/acre]										
	A	B	C	D	E	F	G	H	I	J
1	31	29	32	30	28	35	33	32	32	29
2	30	29	36	32	29	35	30	31	34	30
3	27	36	36	35	28	32	31	29	34	29
4	28	33	33	33	33	33	29	29	36	35
5	31	27	29	29	35	30	34	34	28	29
6	30	28	27	30	32	32	31	32	32	29
7	31	34	28	30	31	36	30	32	30	34
8	34	33	31	33	32	36	32	30	31	36
9	29	32	33	30	31	29	32	29	30	30
10	30	30	33	34	31	33	37	27	33	34

Second UAN32 Liquid Nitrogen Application Actual Rates [gal/acre]										
	A	B	C	D	E	F	G	H	I	J
1	17.2	15.9	17.7	16.4	78.8	19.3	18.3	17.5	17.8	82.6
2	16.6	15.8	19.7	17.8	81.4	19.1	16.5	17	19	82.8
3	14.7	19.6	19.6	19.4	79.8	17.5	17	16	18.4	81.8
4	15.3	18.1	18	18	91.9	17.9	16.1	16	19.8	96.8
5	17.2	15	15.7	16.1	98.1	16.8	18.7	18.9	15.4	80.4
6	16.5	15.5	14.8	16.6	90.8	17.5	17.2	17.6	17.5	79.9
7	17.1	18.6	15.2	16.4	86.9	19.9	16.7	17.7	16.4	96.5
8	18.6	17.9	17.1	18	90.3	19.6	17.5	16.4	16.8	100
9	15.8	17.4	18.3	16.2	88.1	16.2	17.8	16	16.7	84.8
10	16.6	16.7	18.1	18.6	85.5	18.3	20.1	14.7	18.1	94.8

Figure 3.20: Expected vs. Actual application rates of UAN32 (gal/acre) after attack 2

Yield values are displayed in Figure 3.21 resulting from attack 2. The total expected yield, EY_{tot} , remained at 16,983bu while the actual yield for the field, AY_{tot} , came to 12,692bu which results in a 4,291bu yield penalty as a result of attack 2. Over the whole field, attack 2 results in a 42.9bu/acre yield penalty.

Corn Expected Yield (EY) [150-190 bu/acre on 100-acre rainfed field, Saunders County, NE] =RANDBETWEEN(150,190)										
	A	B	C	D	E	F	G	H	I	J
1	175	157	174	168	152	189	181	175	180	158
2	161	162	188	172	167	190	151	165	180	157
3	150	190	184	185	151	182	176	153	174	157
4	150	172	178	183	174	173	155	156	185	178
5	163	152	150	161	186	170	174	184	150	153
6	162	160	152	171	184	178	165	170	172	160
7	169	189	155	155	164	189	162	168	162	186
8	180	174	169	176	189	188	184	161	169	189
9	156	163	187	153	166	162	168	159	162	162
10	174	164	190	171	170	181	190	151	176	175

Total Actual Corn Yield (AY) [bu/acre, AYmin=100bu/acre, AYmax=EY+30bu/acre]										
	A	B	C	D	E	F	G	H	I	J
1	112	100	111	110	182	120	117	113	117	188
2	102	105	120	107	197	122	100	103	113	187
3	100	119	116	117	181	119	115	100	109	187
4	100	109	114	117	204	110	100	100	116	208
5	101	100	100	105	216	111	109	115	100	183
6	102	105	100	111	214	116	103	107	111	190
7	108	123	101	100	194	119	102	106	104	216
8	113	109	106	112	219	118	120	102	109	219
9	100	102	122	100	196	103	105	101	104	192
10	114	106	125	107	200	117	120	100	111	205

Figure 3.21: Expected vs. Actual (calculated) yield after attack 2

Figure 3.22 demonstrates the potential profit loss or gain per acre. Over the entire field, total potential profit loss, P_{LG} , came to \$32,281 which averages at \$323/acre. Figure 3.23 provides a summary of the financial impacts from attack 2.

Difference Between Actual and Expected Profit (PLG) [\$]										
	A	B	C	D	E	F	G	H	I	J
1	-419	-379	-417	-387	30	-459	-425	-414	-421	20
2	-391	-377	-452	-430	23	-451	-332	-414	-444	20
3	-330	-474	-451	-452	27	-416	-409	-348	-433	22
4	-328	-416	-425	-439	-3	-420	-363	-371	-459	-15
5	-412	-344	-327	-373	-18	-391	-428	-458	-328	26
6	-398	-369	-345	-402	0	-409	-410	-418	-401	27
7	-408	-437	-356	-362	10	-464	-399	-410	-385	-14
8	-445	-432	-417	-428	1	-467	-429	-396	-398	-24
9	-372	-408	-430	-348	7	-390	-418	-389	-387	15
10	-400	-384	-436	-427	13	-424	-462	-338	-434	-10

Figure 3.22: Potential-Profit loss or gain per acre resulting from attack 2

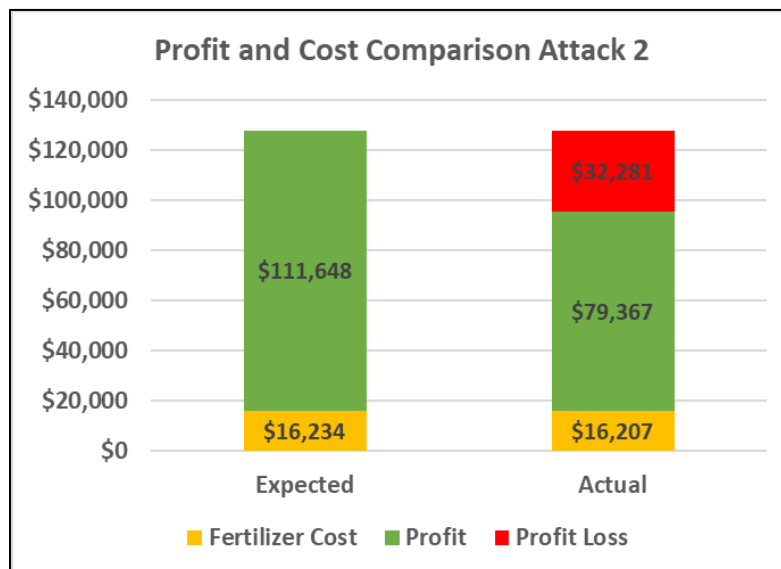


Figure 3.23: Financial impacts from attack 2

3.3.3. Attack Scenario 3

Actual nitrogen rates were affected by attack 3 as seen in Figure 3.24. Under attack 3, $N_{tot,exp}$ remained at 14,758lbs while $N_{tot,act}$, was equal to 14,795lbs applied with a resulting 37lb or 0.3% discrepancy.

Second Nitrogen Application Recommendation [lbs/acre at 75% of total Nrec in-season application]										
	A	B	C	D	E	F	G	H	I	J
1	110	102	113	105	99	123	117	112	114	104
2	106	101	126	114	102	122	105	109	121	104
3	94	125	125	124	100	112	109	102	118	103
4	98	116	115	115	116	115	103	102	127	122
5	110	96	101	103	123	107	120	121	99	101
6	106	99	94	107	114	112	110	113	112	100
7	110	119	97	105	109	127	107	113	105	121
8	119	114	109	115	114	125	112	105	107	126
9	101	112	117	104	111	104	114	102	107	107
10	106	107	116	119	108	117	129	94	116	119

Second Nitrogen Application Actual Rates [lbs/acre]										
	A	B	C	D	E	F	G	H	I	J
1	110	25.5	226	26.2	99	30.9	235	28	228	104
2	106	25.2	252	28.4	102	30.5	211	27.2	243	104
3	94.1	31.3	251	31.1	100	28	218	25.6	236	103
4	98.2	29	230	28.8	116	28.7	206	25.6	253	122
5	110	24	201	25.7	123	26.8	239	30.2	197	101
6	106	24.7	189	26.6	114	27.9	220	28.1	224	100
7	110	29.8	194	26.2	109	31.8	214	28.3	210	121
8	119	28.6	219	28.7	114	31.3	225	26.3	215	126
9	101	27.9	235	26	111	25.9	228	25.6	214	107
10	106	26.7	232	29.8	108	29.3	257	23.4	232	119

Figure 3.24: Prescribed vs. Actual nitrogen application rates (lbs/acre) after attack 3

Figure 3.25 shows the UAN32 application rates with an increase of 11 gal of total UAN32 applied of the 100acre field as a result of attack 3.

Second UAN32 Liquid Nitrogen Application Expected Rates [gal/acre]										
	A	B	C	D	E	F	G	H	I	J
1	31	29	32	30	28	35	33	32	32	29
2	30	29	36	32	29	35	30	31	34	30
3	27	36	36	35	28	32	31	29	34	29
4	28	33	33	33	33	33	29	29	36	35
5	31	27	29	29	35	30	34	34	28	29
6	30	28	27	30	32	32	31	32	32	29
7	31	34	28	30	31	36	30	32	30	34
8	34	33	31	33	32	36	32	30	31	36
9	29	32	33	30	31	29	32	29	30	30
10	30	30	33	34	31	33	37	27	33	34

Second UAN32 Liquid Nitrogen Application Actual Rates [gal/acre]										
	A	B	C	D	E	F	G	H	I	J
1	31	7	64	7	28	9	67	8	65	29
2	30	7	72	8	29	9	60	8	69	30
3	27	9	71	9	28	8	62	7	67	29
4	28	8	65	8	33	8	58	7	72	35
5	31	7	57	7	35	8	68	9	56	29
6	30	7	54	8	32	8	62	8	64	29
7	31	8	55	7	31	9	61	8	60	34
8	34	8	62	8	32	9	64	7	61	36
9	29	8	67	7	31	7	65	7	61	30
10	30	8	66	8	31	8	73	7	66	34

Figure 3.25: Expected vs. Actual application rates of UAN32 (gal/acre) after attack 3

The impact on yield from attack 3 can be seen in Figure 3.26. Attack 3 saw $EY_{tot} = 16,983\text{bu}$ and $AY_{tot} = 15,061\text{bu}$ with a 1,922bu yield penalty. This averages to a 19.2bu/acre yield penalty as a result of attack 3.

Corn Expected Yield (EY) [150-190 bu/acre on 100-acre rainfed field, Saunders County, NE] =RANDBETWEEN(150,190)										
	A	B	C	D	E	F	G	H	I	J
1	175	157	174	168	152	189	181	175	180	158
2	161	162	188	172	167	190	151	165	180	157
3	150	190	184	185	151	182	176	153	174	157
4	150	172	178	183	174	173	155	156	185	178
5	163	152	150	161	186	170	174	184	150	153
6	162	160	152	171	184	178	165	170	172	160
7	169	189	155	155	164	189	162	168	162	186
8	180	174	169	176	189	188	184	161	169	189
9	156	163	187	153	166	162	168	159	162	162
10	174	164	190	171	170	181	190	151	176	175

Total Actual Corn Yield (AY) [bu/acre, AYmin=100bu/acre, AYmax=EY+30bu/acre]										
	A	B	C	D	E	F	G	H	I	J
1	175	100	204	100	152	100	211	100	210	158
2	161	100	218	100	167	100	181	100	210	157
3	150	100	214	100	151	100	206	100	204	157
4	150	100	208	100	174	100	185	100	215	178
5	163	100	180	100	186	100	204	100	180	153
6	162	100	182	100	184	100	195	100	202	160
7	169	100	185	100	164	100	192	100	192	186
8	180	100	199	100	189	100	214	100	199	189
9	156	100	217	100	166	100	198	100	192	162
10	174	100	220	100	170	100	220	100	206	175

Figure 3.26: Expected vs. Actual (calculated) yield after attack 3

Total profit loss for this attack totaled \$14,514 with an average \$145/acre profit loss.

Figure 3.27 shows the profit loss or gain per acre, while Figure 3.28 shows the financial impacts summary from attack 3.

Difference Between Actual and Expected Profit (PLG) [\$]										
	A	B	C	D	E	F	G	H	I	J
1	0	-345	101	-426	0	-568	97	-472	101	0
2	0	-384	87	-448	0	-577	110	-400	92	0
3	0	-574	88	-538	0	-525	106	-315	96	0
4	0	-446	99	-530	0	-455	113	-337	87	0
5	0	-312	115	-374	0	-439	94	-533	117	0
6	0	-370	122	-447	0	-495	105	-434	103	0
7	0	-572	119	-328	0	-565	108	-419	110	0
8	0	-463	106	-477	0	-559	102	-373	108	0
9	0	-382	97	-313	0	-381	101	-360	108	0
10	0	-394	99	-436	0	-513	84	-307	98	0

Figure 3.27: Potential-Profit loss or gain per acre resulting from attack 3

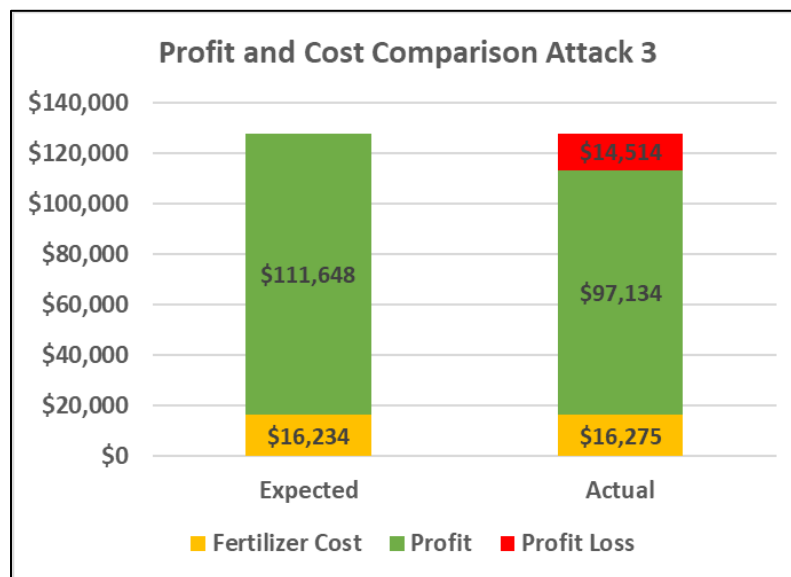


Figure 3.28: Financial impacts from attack 3

3.4. Discussion

A high yielding corn crop in modern agriculture relies on timely and precise application of nitrogen. Since determining corn yield targets, soil measurements, and recommended nitrogen input rates will continue to be more precise and site-specific as machinery and research continues to advance, any variation in optimized nitrogen input rates has the potential to cause profit loss. This case study demonstrated three scenarios where random and strategic increases and decreases of prescribed nitrogen input rates led to significant potential profit loss. A cyberattack that targets a tractor and implement applying nitrogen in-season, with the intent of varying application rates, could have major consequences. Since modern farmers are very reliant on the integrated digital technologies in agricultural machinery when applying complex nitrogen prescriptions, any change in application rates as demonstrated in these attack scenarios would be hard to detect if the digital monitoring technologies appeared normal. If the cyberattack were

also able to alter the display unit in the tractor that provides feedback on the as-applied rates, detecting these types of cyberattacks would become even harder. The future use of autonomous tractors for farming applications such as side-dress nitrogen application could add an additional level of difficulty in detecting a cyberattack such as this. On top of this, once nitrogen is already applied in a field, it is impossible to determine the exact rates that were applied, although the rates can be estimated using imaging technologies after the corn has had enough time to respond. The resulting yield penalties will be seen at harvest, although it may be hard to detect if yield variation was due to the cyberattack or other unknown issues.

The potential profit loss associated with these cyberattack situations could be significant, especially when technologies are being integrated into farming machinery to optimize fields in decreasingly smaller management zones. Before the era of precision farming, farmers would overapply many fertilizer inputs such as nitrogen, with the aim of attaining high yields. As nitrogen prices have increased, farmers have become more aware of the benefits of precision agricultural techniques for maximizing profit. Therefore, cyberattacks that target precision agricultural technologies and machinery could be very detrimental to the goals of maximizing profitability. One might argue that an overapplication of nitrogen could protect against a cyberattack such as the attacks outlined in this case study. Although that might be true if a farmer knew they would experience a cyberattack, the total amount of overapplied nitrogen needed would not only be a large financial burden but could also create other impacts to areas such as water

quality, hence the push to optimize nitrogen inputs through precision agricultural practices.

The degree of significance of a cyberattack to a precision farming operation is dependent on many factors as seen by the attack scenarios in this case study. Since a farmer could experience profit losses on the level of \$100/acre or more as demonstrated in this study (Figure 3.29), it is important that cybersecurity measures are taken to ensure the security of agricultural machinery. Although security measures could be added to an

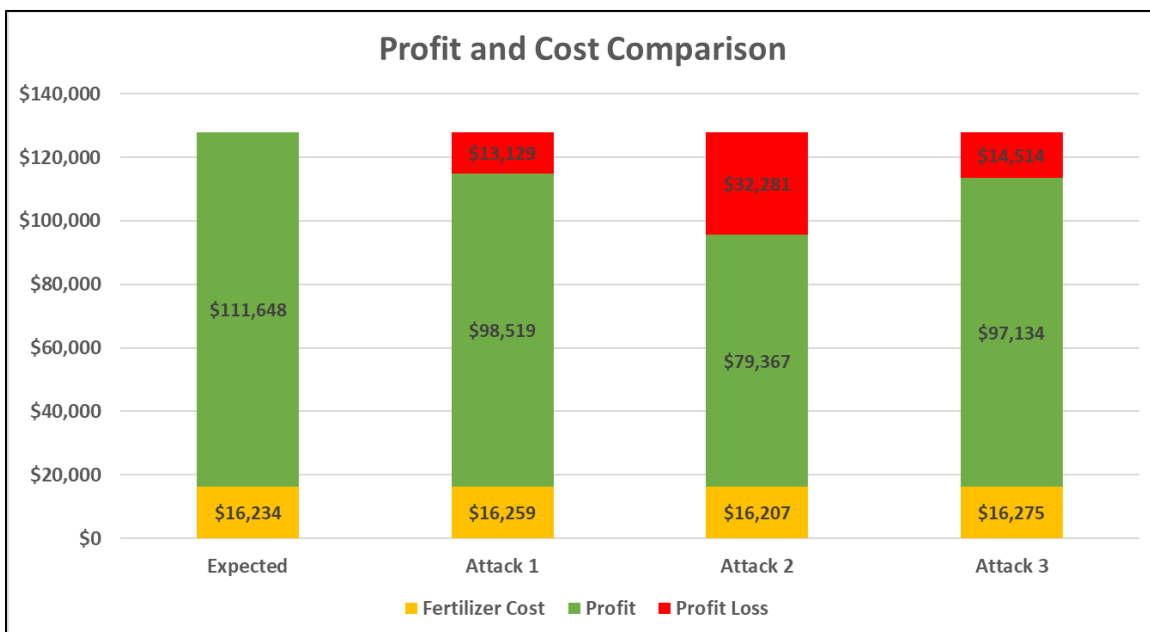


Figure 3.29: Profit and Cost Comparison Between Attacks

agricultural machine after a cyberattack occurs, including security in the design process of agricultural machinery will be a much more effective approach to preventing cyberattacks in the future. Agricultural equipment that contains the capabilities to improve security measures by methods such as software updates, while also containing hardware components that are of a high level of security will be important to include in

agricultural machinery for the future. The next chapters will address some possible design solutions for agricultural machinery.

3.5. Conclusions

This objective demonstrates multiple contributions. First, three cyberattack scenarios were outlined which targeted in-season nitrogen application. Numerous charts demonstrate what these attacks could look like and the greater financial implications of these attacks targeting in-season nitrogen application. Other precision agricultural operations, such as planting, could be targeted with cyberattacks such as the ones discussed in this chapter, resulting in major financial implications. Second, the specific financial implications of the cyberattack were discussed. Cyberattacks intending to target in-season nitrogen application could have financial implications that reach far beyond the targeted farmer. A cyberattack like this could open the door for a state-sponsored attack, intended to destabilize a country or global market. Finally, this cyberattack scenario is an example where the level of significance should drive the degree of security incorporated into agricultural machinery. The scenario might have relatively minor consequences across 100-acres, but across multiple farms or larger areas, the cyberattack could result in major impacts. There is a need for more research to provide practical solutions in improving the cybersecurity of agricultural machinery.

Chapter 4: CYBERSECURITY MODELING FOR AGRICULTURAL MACHINERY

This chapter will present a modeling methodology CASE (Conceptualize, Assemble, Simulate, Evaluate) for its usefulness as a tool for the design of secure agricultural machinery while identifying the most security-critical areas of the system under design.

4.1. Introduction

The rapid advancement of agricultural machinery in both capability and function over the past few decades, can largely be attributed to the integration of digital technologies to the machinery. These integrated digital technologies are critical to the future of agriculture but have introduced many cyberattack vectors and security concerns. For example, telematics electrical control units (TCUs) have the capability to be accessed remotely via cellular networks and allow for remote monitoring and even tuning of electrical control units (ECUs) on tractors (M. Boland et al., 2021). These telematics units have allowed for improved efficiencies on farming operations, but also provide a communication vector for cyber-attackers to target. The recent introduction of autonomous technologies and fully autonomous machinery (Tibken, 2022) has only increased the urgency for cybersecurity to agricultural machinery, since autonomous machines will rely on robust communication to operate safely (Gupta et al., 2020). Although it is possible to add security concepts after a machine is manufactured, the automotive industry has demonstrated that the inclusion of cybersecurity concepts during the design process, is the best use of time and resources in producing the most secure product (“Automotive Cybersecurity by Design,” 2021). Agricultural machinery

contains comparable complexity in machine control architecture and could benefit from the same design principles. Therefore, an important question to ask is what tools can be used to design robust and secure agricultural machinery? Current literature lacks significant solutions for secure design of agricultural machinery.

Modern agricultural machinery contains an array of complex control subsystems such as steering/navigation, engine and hydraulic control, implement operation, and emergency stop systems. Autonomous agricultural machinery will build on the subsystems of current agricultural machinery by adding more subsystems such as surrounding awareness and object detection, path planning, and improved communication systems. It is an understatement that modern agricultural machines are complex. Since there is a high degree of complexity of agricultural machinery even at the subsystem level, a tool such as modeling could be useful to design, by trialing various system configurations before proceeding further in the design process. Since both robust and secure agricultural machinery is required for the future of agriculture, this chapter will investigate if modeling could be a useful tool in the design and integration of security concepts to agricultural machinery.

4.2. Background

Modeling is a tool that is used for a wide variety of applications in agriculture such as mechanical machine design, crop yield modeling, crop harvesting logistics planning, and control system design. Some examples of modeling for agricultural mechanical machine design are discussed in a literature review paper by (Zhao et al., 2021). Modeling has also been used to predict crop yields (Oteng-Darko et al., 2012). Harvesting logistics for

agricultural crops have been modeled, to determine the most time and resource efficient path for the harvesting machinery (Evans et al., 2020). Finally, modeling has been used to develop and optimize control systems, such as HVAC systems (Afram and Janabi-Sharifi, 2015). Modeling for control system design can be based around automata theory concepts. Automata theory is a theoretical branch of computer science that studies abstract models called automata (“Basics of Automata Theory,” n.d.). Automata are models of machines that move through various states based on inputs to the model (Hopcroft et al., 2007). Finite state machines are a category of automata that work under a ‘finite’ set of operating states (Rich, 2007). Stateflow is a powerful tool that leverages the principles of automata theory and finite state machines to build complex models that can be simulated (“Stateflow - MATLAB & Simulink,” n.d.).

Cybersecurity has also benefited from modeling techniques. Cybersecurity risks are modeled in a paper by (Peng et al., 2018), that found that modeling multivariate cybersecurity risks, resulted in a more accurate prediction of the impacts of the attack. A holistic and systems approach was taken in the modeling of broader cybersecurity concepts in a paper by (Yan, 2020). A methodology for using modeling for a combination of both systems design and cybersecurity analysis will be presented in the next sections. The methodology will be assessed by means of a case study, which will leverage Stateflow as a modeling tool, since it provides a user-friendly graphical user interface to quickly build and simulate models.

4.3. Research Methodology and Materials

This section will present a methodology where Stateflow, an automata theory based modeling software, will be used to design a critical subsystem of an agricultural machine, while attempting to provide cybersecurity insight to the design process. The critical subsystem that will be modeled is the emergency stop (E-stop) system of a supervised autonomous agricultural machine, Flexible Structured Robotic Platform (Flex-Ro).

4.3.1. *Flex-Ro*

Flex-Ro, is a 57-horsepower supervised autonomous field platform (Figure 4.1) that was developed to perform low-draft agricultural operations (Murman, 2019; Werner, 2016). The machine is composed of numerous commercial off-the-shelf (COTS) components such as electronic control units (ECUs), a Kubota Engine, and electric steering motors. Flex-Ro has four independently driven and steered wheels which provide optimal flexibility and maneuverability of the platform. A centralized CAN-bus network (Figure 4.2) is a critical part of Flex-Ro as it allows for numerous ECUs to communicate and control the various subsystems on the platform. The CAN-bus network on the machine operates under the SAE J1939 protocol, along with the addition of numerous proprietary messages. The platform has been used for field scouting and crop data collection but may be used for additional tasks such as planting and spraying in the future.



Figure 4.1: Flex-Ro performing a field scouting operation

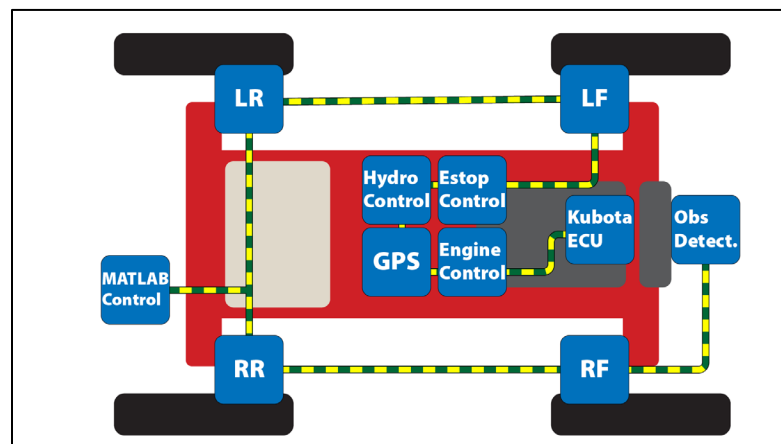


Figure 4.2: CAN bus network of Flex-Ro

Flex-Ro, an agricultural machine, contains numerous complex control subsystems. A hydraulics subsystem supplies power to each wheel motor and the wheel speed is controlled by an ECU connected to the CAN-bus network on the machine. The steering and navigation subsystem incorporates multiple steering motors and gearboxes all controlled by a network of ECUs. The steering commands originate from the Flex-Ro remote control ECU or connected computer. Steering control inputs are then integrated with Global Positioning System (GPS) location commands for autonomous navigation.

The engine on Flex-Ro contains a proprietary ECU that operates under the SAE J1939 protocol. An emergency stop (E-stop) system is another major subsystem that protects the machine and surroundings from damage. Multiple subsystems will be added to Flex-Ro in the future as it continues through research development.

The E-stop system is a critical subsystem of Flex-Ro that provides safety to the Flex-Ro machine and its surroundings. The current E-stop system was built without integrating cybersecurity, therefore this case study will aim to evaluate the current E-stop system for areas that are most vulnerable to cyberattacks.



Figure 4.3: E-stop button on a corner of Flex-Ro

4.3.2. Modeling Methodology

The modeling methodology chosen for this case study is laid out in Table 4.1. The major steps in this method include 1) conceptualization, 2) model assembly, 3) simulation, and 4) evaluating the results. Each step includes a series of questions that can be asked to aid in the development process.

Table 4.1: CASE Modeling Methodology for Agricultural Control Systems

Step 1: Conceptualize	Step 2: Assemble	Step 3: Simulate	Step 4: Evaluate
1. What is the purpose of the subsystem being designed?	1. How will the inputs/outputs be represented in the modeling software of choice?	1. Where does the model fail?	1. Which cybersecurity vulnerabilities need redundancies?
2. What is the priority of the subsystem? Low, Medium, High, Critical?	2. How will the states be represented in the modeling software of choice?	2. Does the model enter any unintended states?	2. How can the subsystem be made more efficient?
3. What are the inputs/outputs to the subsystem?	3. What are the transition conditions and how can they be represented in the modeling software of choice?	3. Do any of the modeled cybersecurity vulnerabilities cause the model to enter an unintended state?	
4. How does the subsystem specifically interact with the other subsystems of the overall machine?			
5. What are the normal operating states?			
6. What are potential attack states?			

Conceptualization is the first step in this security modeling process. Since agricultural machines are complex systems, this method breaks the larger complex system into subsystems for cybersecurity analysis, design, and modeling. The conceptualization process considers what role the subsystem plays in the larger machine, what the priority of the subsystem is, and what the inputs/outputs are to the subsystem. Determining the normal states and potential cyberattack states should be accomplished during the conceptualization step.

Assembly the model is the second step in the process. Determining how the inputs and outputs will be represented in the software of choice is the first step. Other questions that should be asked include how the states should be represented in the model and how the states are related. Since this methodology is aiming to identify cybersecurity vulnerabilities, identifying potential attack states is important. Attack states can continuously be added to the model over time to analyze what risk they pose to the overall system. This modeling methodology is an iterative process, therefore moving between the conceptualization and assembly steps is encouraged.

The value of a model is that it can be run multiple times to evaluate how the subsystem could operate in order to make improvements. Simulating the model frequently can provide insight into what features need to be present when the physical subsystem is built. The third step of simulating the model can help demonstrate where the subsystem could fail or enter any unintended states.

The final step of this methodology involves evaluating the subsystem and model to understand where improvements can be made. This includes evaluating if redundancies are needed in the subsystem or how the subsystem can be made more efficient.

4.4. Results and Discussion

This section demonstrates the Stateflow model that was developed using the proposed modeling methodology.

4.4.1. *Conceptualize*

The first step of the proposed modeling methodology is conceptualization. The six questions proposed during the conceptualization step will be addressed in this section as it pertains to the Flex-Ro E-stop system. The first question is, what is the primary function of the subsystem, or E-stop system in this case? As discussed previously, the Flex-Ro E-stop system is built to provide safety to the machine and its surroundings by preventing catastrophic damage or injury. The E-stop system will also check to make sure that all ECUs of critical systems are functioning properly. In the ideal case, the E-stop system will safely shut the machine down and bring it to a controlled stop if a malfunctioning ECU or impending damage is detected. The second question is what is the priority of the subsystem? In the case of the Flex-Ro E-stop system, the subsystem is of the highest priority. In the worst-case scenario, all computational resources on Flex-Ro should be directed to the E-stop system.

Questions three through six (Table 4.1) all share a common theme: interactions with and within the subsystem. Question three asks, what are the inputs and outputs to the subsystem? The Flex-Ro E-stop system contains some physical inputs as demonstrated

in Figure 4.3. Four physical E-stop buttons provide input signals to the E-stop system if any of the four corners of Flex-Ro physically come into contact with an obstacle. There also are digital E-stop button inputs on the Flex-Ro remote (Figure 4.4) and FlexRoRun app (Figure 4.5) that provide input messages to the E-stop system. Another input to the E-stop system is a routine heartbeat message from the ECUs that are connected to the E-stop system. If an ECU stops providing a heartbeat message, it is assumed to be functioning improperly and triggers the E-stop system to shut down Flex-Ro. The final input to the E-stop system on Flex-Ro is the digital reset button from either the Flex-Ro remote (Figure 4.4) or Flex-Ro run app (Figure 4.5). The reset button is meant to be an input from an operator to the E-stop system that it is safe to try to restart Flex-Ro. The reset button is depressed before starting the machine for normal operation or when trying to restart Flex-Ro after an E-stop trigger event occurs that shuts down the machine. The primary output from the Flex-Ro E-stop system is a message that negates current machine operation commands and instead sends a message to stop and shut down the machine.

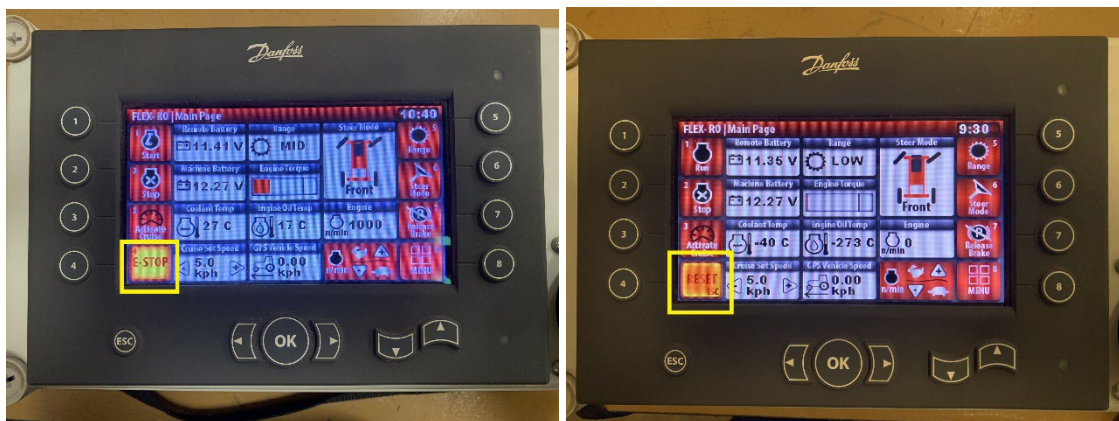


Figure 4.4: Flex-Ro remote E-stop and reset button inputs

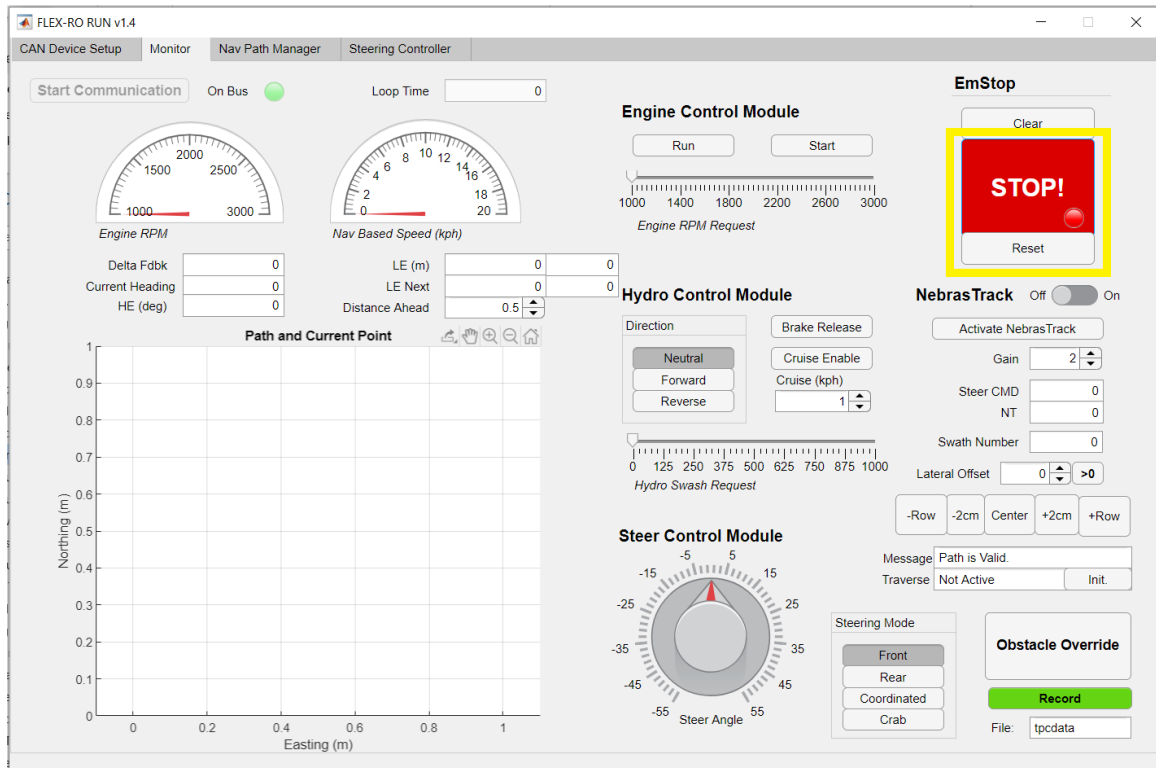


Figure 4.5: FlexRoRun app with E-stop and reset buttons highlighted

The fourth question to be asked during the conceptualization process is how the subsystem should specifically interact with other subsystems on the machine. The three main subsystems the E-stop subsystem interacts with are the hydraulics, power and engine, and steering subsystems. Each ECU on Flex-Ro has a section of code that acts as the E-stop system as demonstrated in Figure 4.6 and Figure 4.7. The hydraulics subsystem interacts with the E-stop system by sending a routine heartbeat message to indicate it is operational. If at any time the hydraulic subsystem becomes inoperable, the E-stop system will attempt to send a message to shut down the hydraulic valves and engine on Flex-Ro. The engine and power ECUs interact with the E-stop subsystem in a similar way the hydraulics subsystem does, by sending routine heartbeat messages. In

the case that the engine ECU stops sending routine heartbeat messages, an E-stop state will be triggered and messages will be sent to shut down the engine and hydraulic valves that control flow to the drive motors. The steering subsystem specifically interacts with the E-stop subsystem by transmitting the state of the E-stop buttons, positioned on the four corners of Flex-Ro.

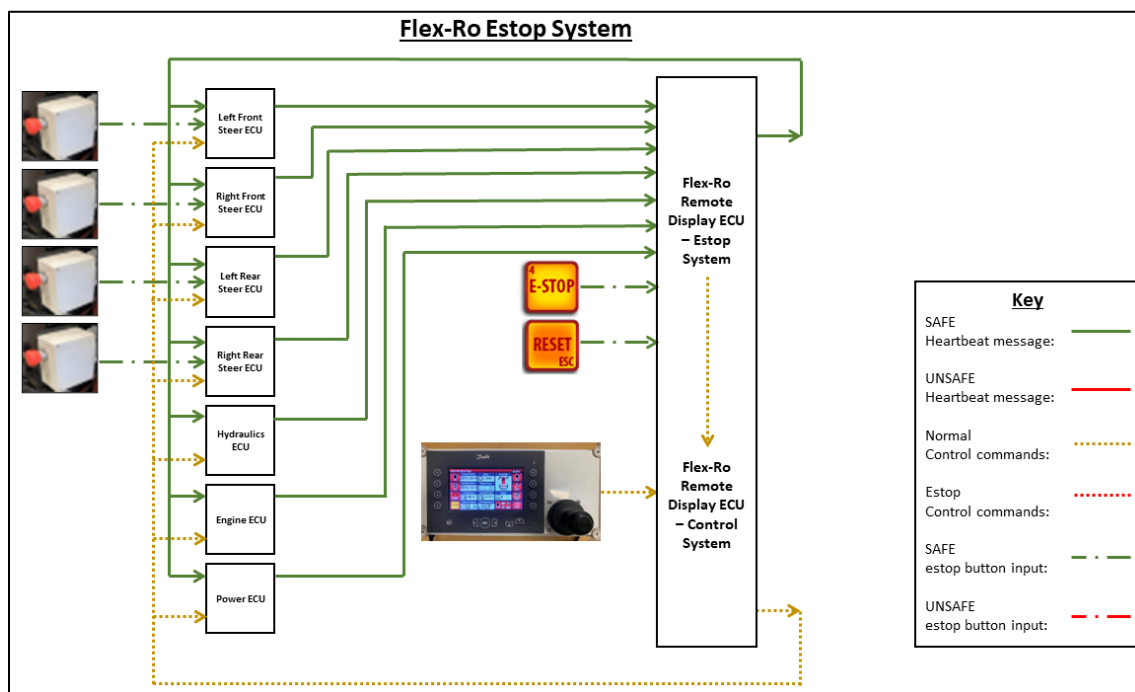


Figure 4.6: Overview of Flex-Ro E-stop system in SAFE state

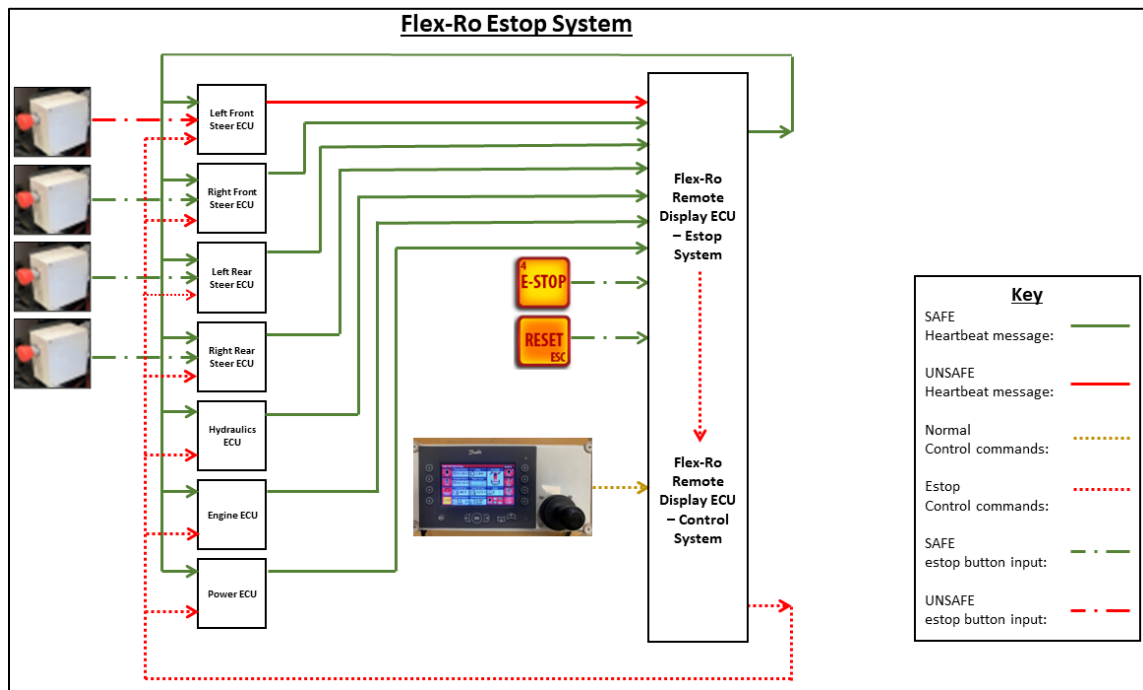


Figure 4.7: Overview of Flex-Ro E-stop system in UNSAFE state

The answers to questions five and six relating to the normal and potential attack states of the E-stop system can be answered in detail by Figure 4.8, Figure 4.9, and the tables that correspond. To summarize, there are three main states that the E-stop system could currently enter with the way the E-stop system is currently configured. Potential cyberattacks could add numerous new states that could be entered by a variety of transition conditions as demonstrated in Figure 4.9.

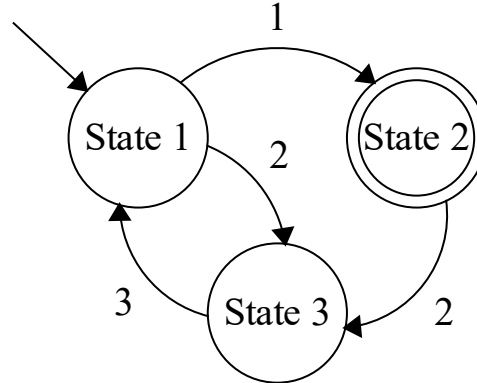


Figure 4.8: Emergency Stop (E-stop) Finite State Diagram

Table 4.2: Normal states of the Flex-Ro E-stop subsystem as shown in Figure 4.8

States	Description
State 1	Currently Checking System – UNSAFE for operation
State 2	Currently Checking System – SAFE for operation
State 3	E-stop – UNSAFE for operation

Table 4.3: Normal transition conditions as shown in Figure 4.8

Transitions	Description
1	All ECUs have been checked at least once without any E-stop conditions
2	At least one ECU has stopped responding or stop condition triggered by E-stop button input
3	E-stop reset input to system

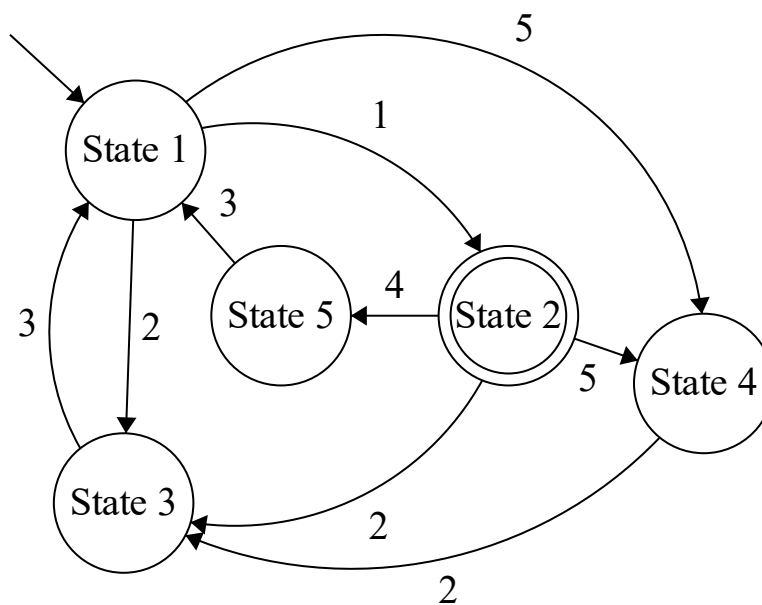


Figure 4.9: Emergency Stop (E-stop) Finite State Diagram with Attack States

Table 4.4: Potential states under a cyberattack as shown in Figure 4.9

States	Description
State 1	UNSAFE for operation
State 2	SAFE for operation
State 3	UNSAFE for operation – E-stop triggered
State 4	SAFE for operation – E-stop trigger condition targeted by cyberattack
State 5	UNSAFE for operation – E-stop trigger condition targeted by cyberattack

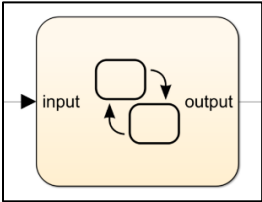
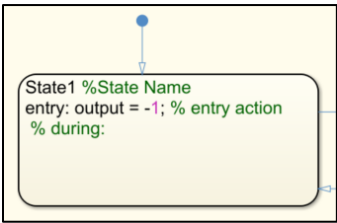
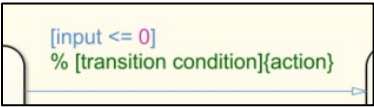
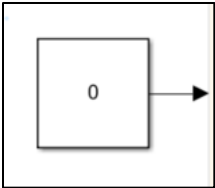

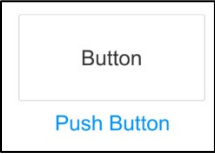
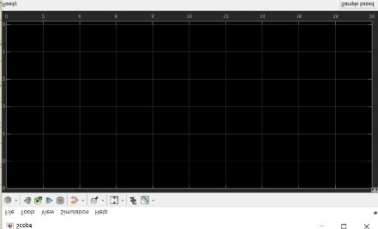
Table 4.5: Transition conditions under a cyberattack as shown in Figure 4.9

Transitions	Description
1	All ECUs have been checked at least once without any E-stop conditions
2	E-CU triggered E-stop condition
3	E-stop reset input to system
4	At least one ECU is targeted by a cyberattack and returns a false positive E-stop trigger
5	At least one ECU is targeted by a cyberattack and returns a false negative E-stop trigger

4.4.2. *Model Assembly*

It is important to determine which components in the modeling software of choice, will represent each of the inputs, outputs, states, and transition conditions of the subsystem being modeled? For this case study, Stateflow components will be used in modeling the E-stop system of Flex-Ro. The components include state blocks, transition arrows and conditions, input constants, switches, push buttons, and an output graphical scope. Table 4.6 shows a generic version of each of these components with a brief explanation of how they can be used. Figure 4.10 shows the Stateflow model while Figure 4.11 shows the full Stateflow model including the Matlab interface. Appendix A presents more details on each of the specific components of the Stateflow model.

Table 4.6: Useful Stateflow Components

Stateflow Object	Image	Use
Stateflow Chart		Provides an area where state models can be built to interact with inputs and outputs
Stateflow State		Stateflow 'states' that can model finite states
Transition Condition		Transition condition that enables a transition from one state to another
Input Constant		Input values to Stateflow chart for use in state and transition condition logic
Slider Switch		Slider switch to manually control input constants
Push Button		Push button to manually control input constants
Scope		Scope used to display outputs from the Stateflow chart

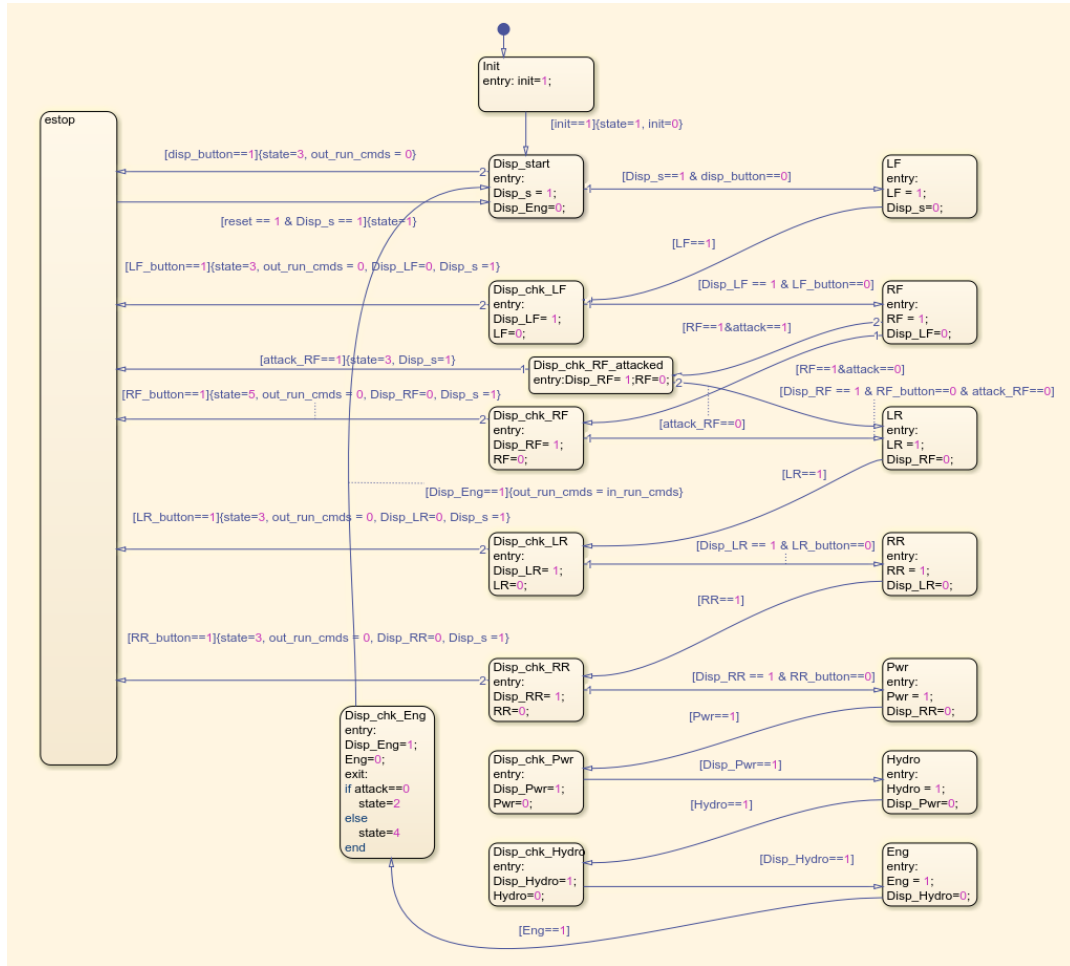


Figure 4.10: Fully assembled Stateflow model

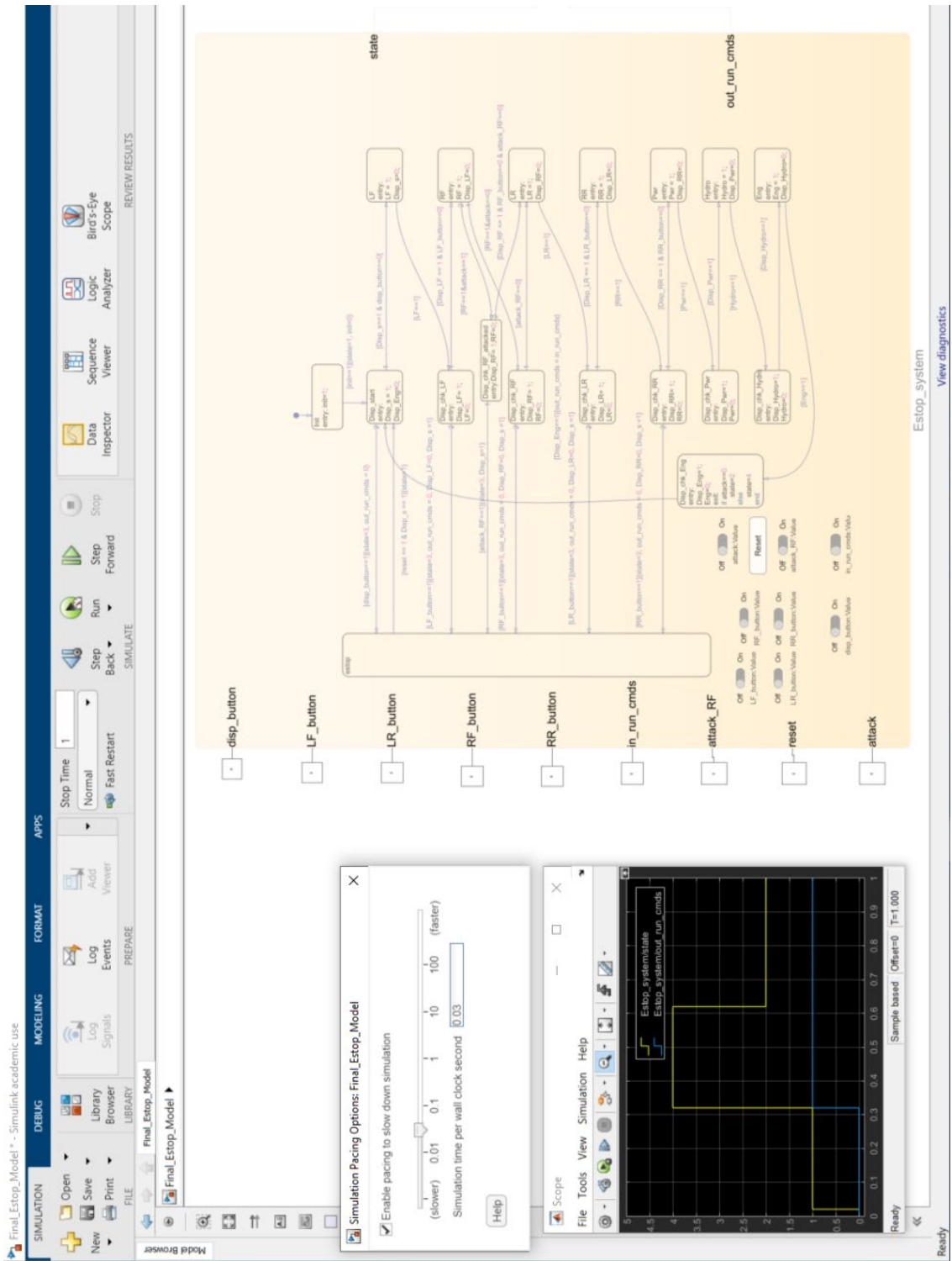


Figure 4.11: Stateflow model within MATLAB interface

4.4.3. *Simulation*

After the first build of the Stateflow model, the Matlab debuggers prevented the model from running because of undefined variables. After fully defining all the variables in the model, the model was simulated and observed to see if it accurately represents the E-stop system. Some transitions between the Display states and E-stop state were eliminated since they misrepresent how the E-stop system functions and allowed the model to enter States 2 or 4 (Figure 4.9) before all ECUs were checked. The E-stop system is currently configured to start back with the first ECU in the sequence after a reset, therefore the additional transition conditions needed to be eliminated. Stateflow provides a graphical logger that plots the output data values from the state diagram. Figure 4.12 shows some basic outputs from the graphical logger, or scope, on some of the initial runs of the model. The 'state' output value demonstrated by the yellow line, plots which of the five states from Figure 4.9 the model is operating in based on the input conditions. The out_run_cmds variable provides an output of whether the E-stop system is allowing for the communication of the input operation commands to the corresponding ECUs or if an E-stop condition has constituted the system be shut down. For example, an input command to start the engine would not be allowed to be sent until all ECUs have been verified to be operating properly and no E-stop trigger event has occurred. The blue line in Figure 4.12 demonstrates how the out_run_cmds variable is plotted over time and its relationship to the overall E-stop state.

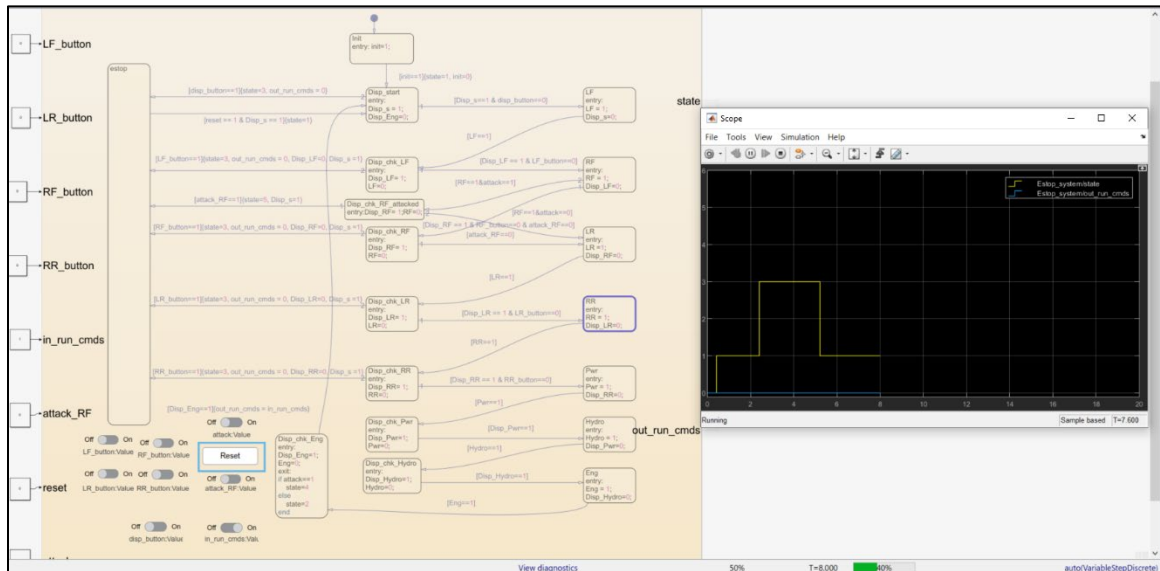


Figure 4.12: Running model and output scope

The second step after creating an initial operating model is to evaluate where the most vulnerable parts of the model exist that could possibly be targeted by a cyberattack. As conceptualized in Figure 4.9, there could be conditions where a false positive or negative E-stop trigger is sent because of a cyberattack. One way this could happen is if any of the ECUs within the E-stop system, experience a cyberattack. To model this possibility, an additional state was added to the Stateflow model to represent a compromised ECU. Figure 4.13 demonstrates the attack state that was added to the model to represent a case where an ECU stopped providing valid E-stop trigger responses.

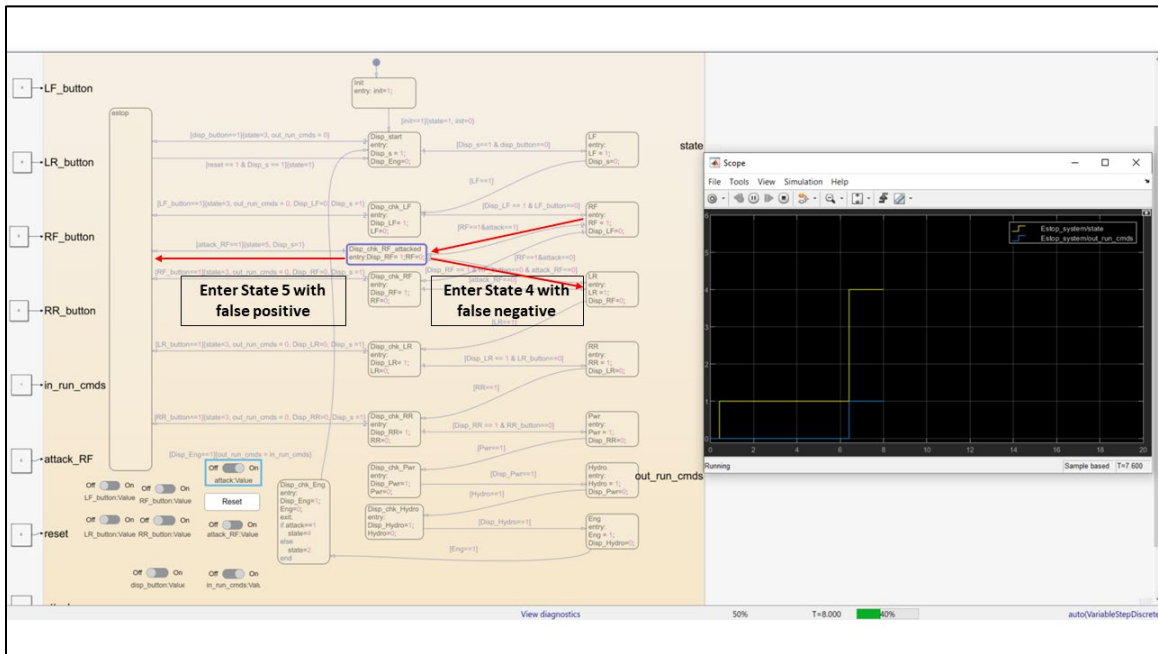


Figure 4.13: Stateflow model entering attack state

When in an attack state, the Stateflow model will bypass the normal ECU state (Disp_chk_RF) and instead read the inputs to the Disp_chk_RF_attacked state. Other attack conditions could be added to Figure 4.9 and the Stateflow model could include attacks such as Denial of Service (DoS), where the CAN bus is overloaded with messages which prevent the E-stop system from functioning.

4.4.4. Evaluate Model

Evaluating each iteration of the model is important to understanding details that need to be included while building a physical prototype of the subsystem. Details such as what specific transition conditions need to exist and what priority each ECU should interact with the E-stop system were important details that were learned while building and running the Stateflow model. For example, it is important that each ECU on the E-stop

system is checked in some order or timed sequence to confirm that all ECUs are responding properly. There would have to be some leeway given to the expected response time based on the latency of the CAN bus.

Since the CAN bus contains little to no known encryption methods, ECUs could be attacked over the CAN bus and pretend to be one of the critical system ECUs, creating problems as demonstrated in the Stateflow model. Two attack scenarios were demonstrated in this model to show what a cyberattack to the control system could look like. The model revealed that some level of security is needed that prevents the CAN bus from being accessed, otherwise an attacker could easily control the E-stop system or any operation command for that matter. The Stateflow model that was built in this case study could easily be built with more complexity, to provide more accurate simulation of the actual system. Stateflow offers CAN bus simulation blocks to further simulate an actual CAN bus. The model also demonstrated the capability of adding other features to the E-stop system, such as including object detection and avoidance. Using the methodology proposed in this chapter, these new features could be further developed through the conceptualization and modeling process.

4.5. Conclusions

The case study presented in this chapter demonstrated how modeling could be used as a tool during the design of agricultural machinery. Since agricultural machines are complex, this modeling methodology demonstrates how the complexity in designing an entire agricultural machine could be reduced by breaking it into subsystems. The modeling methodology presents how each subsystem can be designed, while being

mindful of its interaction with the overall machine. This methodology also provides the benefit of running through many design scenarios of a potential subsystem before any physical components are assembled.

The increasing need of cybersecurity for agricultural machinery will require many tools to be developed to face this rising challenge. Modeling is one method to not only design subsystems but also think about potential cyberattack scenarios and how they could be prevented from the beginning of the design process. This case study demonstrated how Stateflow was used to develop a model of the E-stop system of Flex-Ro and simulate potential attack scenarios. Although the developed model was unable to identify cybersecurity vulnerabilities without specifically building the potential vulnerabilities into the model, this methodology along with future work could be used to identify and address specific cybersecurity vulnerabilities through more wholistic analysis.

Chapter 5: UTILIZING TESTBEDS TO ANALYZE CYBERSECURITY VULNERABILITIES TO AGRICULTURAL MACHINERY

There is a need for tools and methodologies to identify secure components and software configurations for agricultural machinery. This chapter will demonstrate how the use of testbeds could aid in the identification of cybersecurity vulnerabilities and testing of critical attack vector components on agricultural machinery.

5.1. Introduction

New agricultural machinery is constantly being developed to meet the niche needs and preferences of farmers while solving the current challenges facing agriculture today. Many agricultural machines and implements are compatible with other OEM makes and models of machinery, opening the door for a variety of equipment combinations based on the farmer's preference and productivity needs. This adds challenge to the design process of agricultural machinery, as each machine needs to be compatible with a variety of machines and implements from multiple manufacturers. Standards such as ISO 11783 (ISOBUS) have made this machine compatibility possible (Lenz et al., 2007). One of the most recent innovations to agricultural machinery is autonomous technologies such as John Deere's release of their autonomous 8R tractor in January 2022 (Tibken, 2022). This tractor is embedded with numerous technologies and even the capability of being controlled via a cell phone (Tibken, 2022). With the large amounts of integrated digital technology, large selection of implement/machine combinations, and the numerous aftermarket components that are added to modern agricultural machinery, cybersecurity is becoming a concern. Two FBI reports have highlighted the potential significance of cyberattacks that target agriculture (Federal Bureau of Investigation, 2021; "Ransomware Attacks on Agricultural Cooperatives Potentially Timed to Critical Seasons - HS Today," 2022) while a report by the Department of Homeland Security has discussed threats to precision agriculture (Boghossian et al., 2018). This means that the future of agriculture depends on robust, secure, and highly functional machines.

Agricultural machines are subject to rigorous testing during the design process to confirm they will perform as designed. Mechanical, hydraulic, electrical, and software systems are all typical examples of engineered systems that are tested during the design process. A tool such as a testbed is one such way that these systems can be tested and validated for optimal performance. A testbed is simply a segment of a device or machine that is assembled so controlled tests, such as functionality and durability, can be performed. Since cybersecurity principles need to be integrated into agricultural machinery, it is important to develop tools that help with this process. Currently both industry and academic research has been focusing on this challenge, although there are no well-known solutions in literature. This chapter will present how testbeds could be a tool to identify cybersecurity vulnerabilities in the hardware and software systems of agricultural machinery, along with the identification of the most secure hardware components.

5.2. Case Study

This section will present a case study where STAVE, a Security Testbed for Agricultural Vehicles and Environments, developed during this thesis work, will be used to demonstrate how security vulnerabilities can be identified and evaluated on agricultural machinery using testbed solutions.

5.2.1. *STAVE Testbed*

The STAVE testbed consists of multiple hardware and software components from a supervised autonomous agricultural machine, Flex-Ro (Figure 5.1). Flex-Ro can be controlled by a wireless remote (Figure 5.2) or computer when operating in autonomous

mode. Since Flex-Ro is a large machine with many expensive components, it was best to build a testbed to perform cybersecurity tests on rather than Flex-Ro itself, to prevent potential damage to the machine.



Figure 5.1: Flex-Ro at the Nebraska Tractor Test Lab (NTTL)



Figure 5.2: Flex-Ro Wireless Remote

There are two main parts to STAVE. First, Figure 5.3 presents half of the testbed that replicates some of the major control components the Flex-Ro machine. Figure 5.4 presents the other major half of STAVE that replicates the Flex-Ro wireless remote (Figure 5.2). Finally, Figure 5.5 demonstrates how data was acquired from the testbed. All the major components of STAVE can be seen in Table 5.1 along with a description of their purpose.

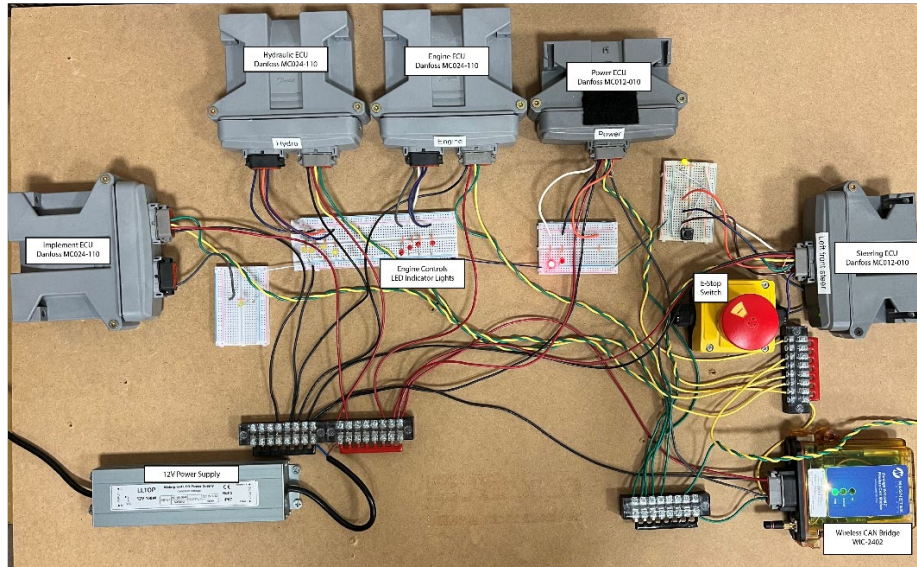


Figure 5.3: STAVE (Security Testbed for Agricultural Vehicles and Environments) – Composed of components from the Flex-Ro machine

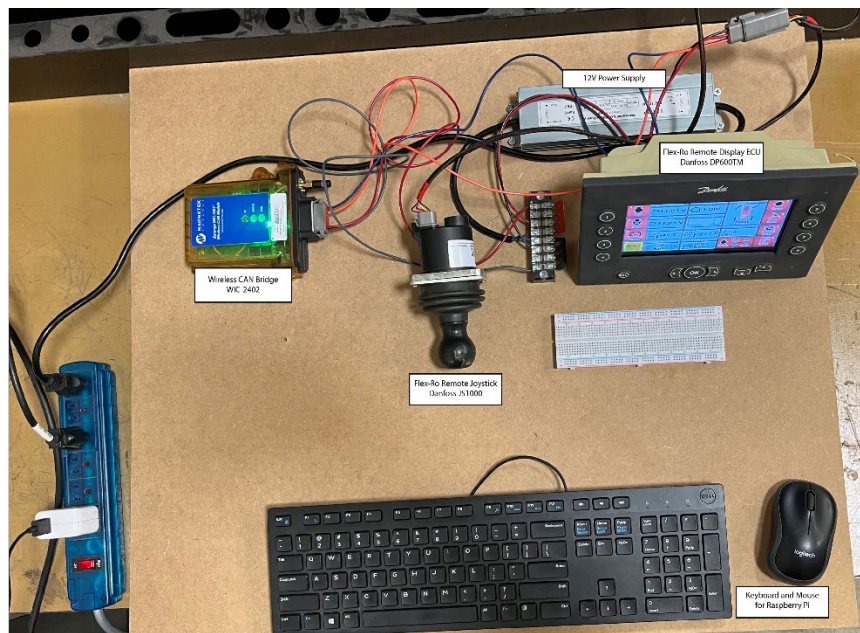


Figure 5.4: STAVE (Security Testbed for Agricultural Vehicles and Environments) – Composed of components from Flex-Ro wireless remote

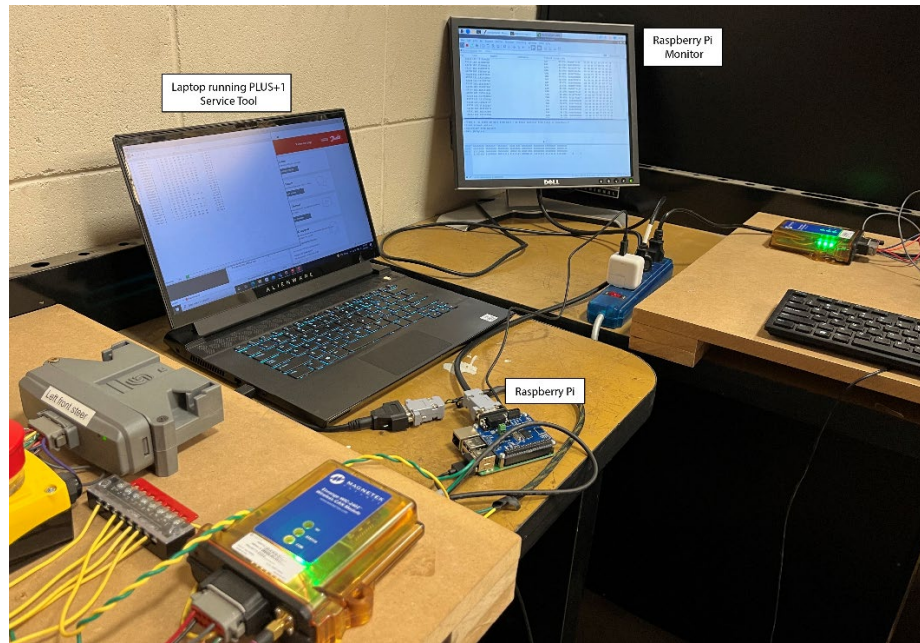


Figure 5.5: STAVE (Security Testbed for Agricultural Vehicles and Environments) – Data acquisition and monitoring of STAVE

Table 5.1: STAVE Components

Name	Part Number	Description
Implement ECU	Danfoss MC024-110	ECU that can be programmed to operate any implement attachments to Flex-Ro
Hydraulics ECU	Danfoss MC024-110	ECU that controls the hydraulic system of Flex-Ro, including the hydraulic powered wheel drive motors
Engine ECU	Danfoss MC024-110	ECU that receives engine commands from the Flex-Ro remote or computer and converts to specific CAN messages which are provided to the Kubota Engine
Power ECU	Danfoss MC012-010	ECU that controls the power system on Flex-Ro and aids in shutting down the machine under emergency stop conditions
Steering ECU	Danfoss MC012-010	One of four ECUs on Flex-Ro that control the four modes of steering and receive E-stop button inputs from the four corners of Flex-Ro
Wireless CAN Bridge	Magnetek WIC-2402	Wireless CAN bridge that allows for communication between the Flex-Ro remote and machine
Flex-Ro Remote Display ECU	Danfoss DP600	ECU that enables remote input commands to control Flex-Ro when not operating autonomously
Flex-Ro Remote Joystick	Danfoss JS1000	Joystick used to steer Flex-Ro when not operating autonomously
Raspberry Pi with CAN shield	3 Model B+ / PiCAN 2	Used to monitor CAN messages and could be programmed as an additional ECU

The majority of STAVE is a replica of the Flex-Ro control structure. Some components were not included from the Flex-Ro machine such as three of the four steering ECUs, the GPS unit (Trimble AG-372), telematics control unit (Farmobile PUC4), Kubota Engine ECU, and obstacle detection unit (ifm O3M950/O3M151). A

Raspberry Pi (Figure 5.5) was added to be able to monitor the CAN bus or act like an additional ECU on Flex-Ro. The benefit of STAVE is that it can be rearranged depending on the components that are under testing. For the specific arrangement of components on STAVE as demonstrated in the previous figures, the goal was to assess the wireless CAN bridge (WIC 2402) for cybersecurity vulnerabilities.

5.2.2. Testing

Two primary tests were carried out on STAVE with the goals of investigating the cybersecurity vulnerabilities that exist on Flex-Ro. The first test involved using the Raspberry Pi to sniff and replay messages on the CAN bus. One of the ECUs (Model: Danfoss MC024) was reprogrammed via the PLUS+1 GUIDE software, while the Raspberry pi was used to record the CAN messages on the CAN bus during the reprogramming event. After the ECU was reprogrammed, the Raspberry Pi was used to replay the programming messages on the CAN bus. The ECU that was reprogrammed using the proper PLUS+1 GUIDE software was not able to be reprogrammed by the replay messages, although the ECU was forced into a boot-loader mode. This demonstrated that if a device was able to record CAN messages and perform a simple replay attack, the ECUs on the CAN bus could potentially be forced into an inoperable mode. Further work could be done with this type of attack to see if any of the ECUs on STAVE could be reprogrammed with an additional device such as a Raspberry Pi.

The second test that was performed on STAVE was wireless sniffing of the WIC 2402 device to see if any cybersecurity vulnerabilities exist such as a lack of encryption. A HackRF device (“HackRF One - Great Scott Gadgets,” n.d.) and Universal Radio

Hacker (URH) software (Pohl and Noack, 2018) were used to ‘sniff’ the wireless traffic produced by the wireless CAN bridge devices. The wireless CAN bridge (WIC) devices were determined to operate in the 2.4 GHz frequency, which proved to be very ‘noisy’ (Figure 5.6) or cluttered with other 2.4 GHz signals.

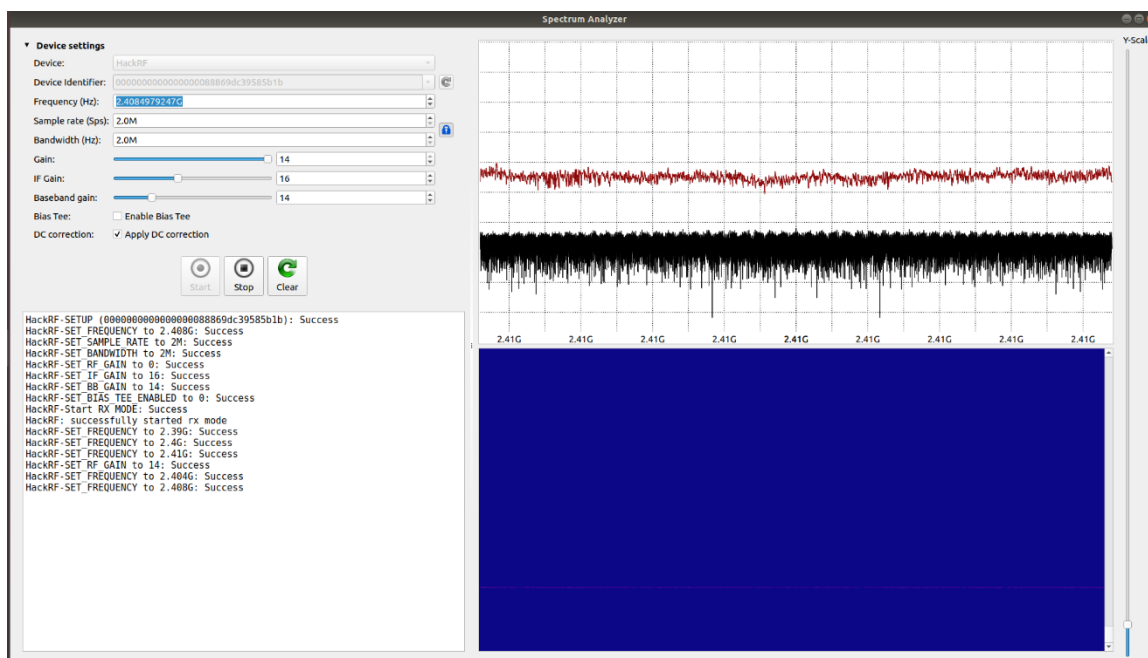


Figure 5.6: Noisy 2.4 GHz frequency range when recording signals from WIC devices in ‘noisy’ environment. Black line signifies current live signals while red line holds the maximum values during the current run time.

It was decided that to isolate the wireless frequency messages between the WIC 2402 devices, a faraday box or similar device was needed to block out outside interference. Figure 5.7 demonstrates the setup used to sniff the messages transmitted between the WIC devices.



Figure 5.7: Copper radio frequency blocking box used to perform tests on STAVE

Some important findings were discovered while sniffing the traffic. First, the WIC devices communicated with a frequency hopping pattern, which allows the transmitted messages to avoid other 2.4GHz messages. Figure 5.8 displays the spectrum analyzer from inside the copper radio frequency blocking box.

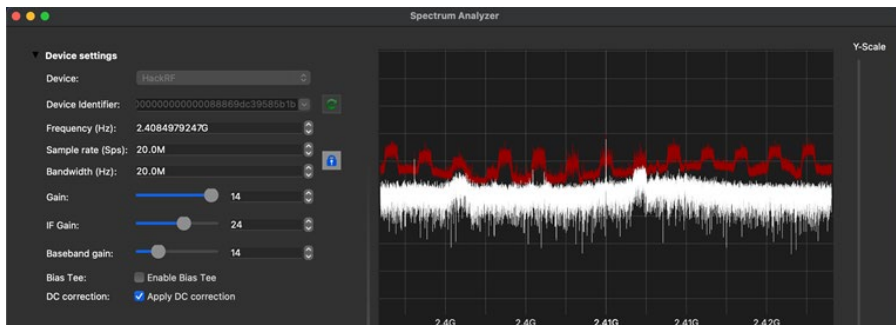


Figure 5.8: Wireless signals between WIC devices captured on URH spectrum analyzer.

It can be noted that there is a distinct frequency hopping pattern, as multiple equal-spaced peaks exist. Figure 5.9 demonstrates a sample recording from inside the box with the

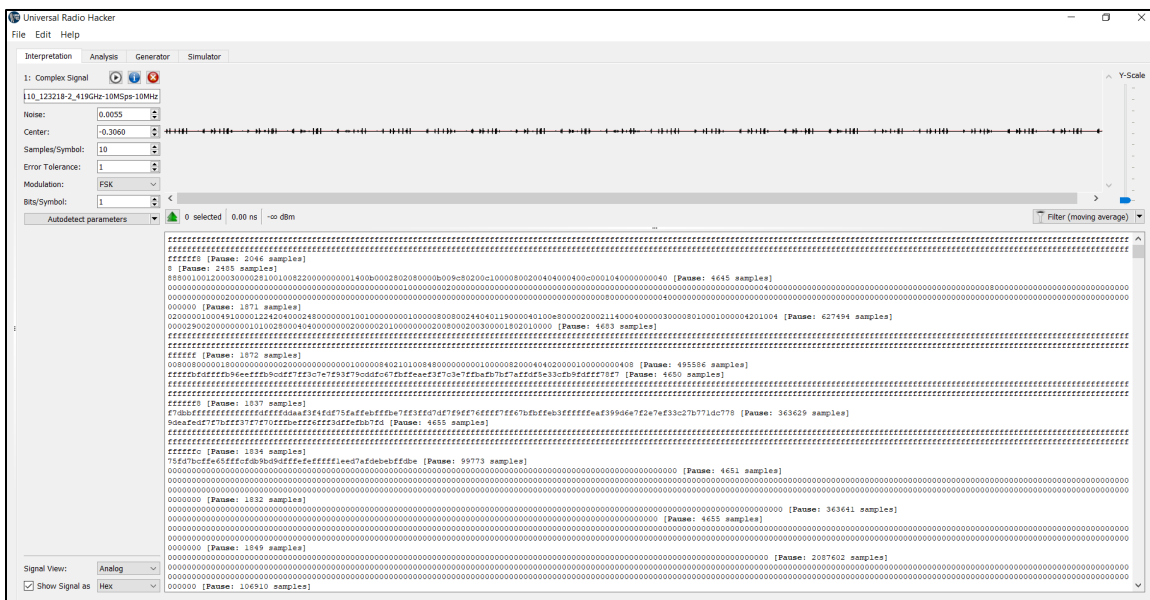


Figure 5.9: Sample URH recording with FSK demodulation at 2.419MHz

HackRF device and URH software. The URH software was unable to properly decode the recorded signals that were transmitted between the WIC devices due to an improper frequency demodulator. The WICs operate with minimum-shift keying (MSK) modulation, while the URH software is only able to decode with frequency-shift keying (FSK), phase-shift keying (FSK), and amplitude-shift keying (ASK) modulation. This presents an area of future work where a more complete analysis of the WIC device could be performed to gain a better understanding of any potential cybersecurity vulnerabilities.

The other components on Flex-Ro such as the Farmobile PUC4 could be added to STAVE in the future to assess the level of security of such devices.

5.3. Discussion

Testbeds are tools with a wide range of applications and can be used while developing agricultural machinery. For developing secure and robust agricultural machinery, testbeds can be a useful tool during the software and control systems development cycle. STAVE demonstrates the potential of testbeds for identifying cybersecurity vulnerabilities to the control systems of agricultural machinery. There are two main concepts that can be learned from STAVE.

First, testbeds are a great way to segment off sections of a complex machine for specific, targeted testing. Attempting to perform cybersecurity tests to the full Flex-Ro machine could be dangerous and challenging, at least for initial tests. STAVE also demonstrated the flexibility in testing new components that could be added to Flex-Ro. All the components on STAVE were hardware-based, meaning they had a physical ECU, rather than a computer simulated ECU and code. Some advantages to this are that the components react as they would on the actual machine, rather than an idealized ECU in a simulation. The advantage to virtual ECUs and testbed devices is more flexibility to which ‘components’ are added to the testbed, while there is no need for the purchase of additional hardware components.

The second takeaway from building STAVE was that testbeds can be great for testing multiple hardware and software configurations for cybersecurity vulnerabilities. STAVE could easily be adapted with new software and hardware components to see if the new

configurations could add more security to Flex-Ro. Professional cybersecurity penetration tests could be performed on a testbed like STAVE, by treating it like a ‘black box’ or ‘grey box’, to identify cybersecurity vulnerabilities. Once these vulnerabilities are identified, various hardware and software component configurations could be tested to see which components provide the optimal level of security. As new cybersecurity vulnerabilities arise or aftermarket components are added, the testbed will be a necessity to provide security updates to existing machines. Other testbeds could be combined with a testbed like STAVE, to experiment how agricultural implements that are connected over an implement bus could interact with the main machine. Since there are multiple machinery manufacturers with various models and styles of machine control, testing to make sure that the system under design does not become insecure with the addition of other equipment would be valuable.

5.4. Conclusions

Agricultural machinery is getting continuously more complex, with autonomous machines being the most recent major advancement. These data-driven machines will depend on more robust communication and control algorithms to reach the highest potential in the future. Cybersecurity has become a topic of discussion as these agricultural machines have become more connected, with warnings coming from agencies such as the FBI and DHS on the possible effects of cyberattacks. Therefore, there is a need for tools that will help include cybersecurity principles throughout the entire lifecycle of agricultural machinery, including the design process.

STAVE was presented as one such solution for including cybersecurity during the design process of agricultural machinery. Testbeds like STAVE can be used to identify cybersecurity vulnerabilities to the control systems of agricultural machines and improve the security of the design, including the selection of more secure components and software. Testbeds have multiple other advantages to the design process including the ability to segment off various sections of the machine for more focused testing.

The need for further tools that help improve the cybersecurity of agricultural machinery is necessary for a successful future. Therefore, this chapter can act as a starting point for future security solutions and research for agricultural machinery.

Chapter 6: OVERALL CONCLUSIONS AND FUTURE WORK

6.1. Conclusions

Agriculture has embraced many major technological advancements over the past few centuries, such as genetics, fertilization, and agricultural equipment, with the goal of responsibly producing enough food and agricultural products to support a growing population. Some of the more recent advancements include research and technologies that support precision agricultural management practices. Precision agricultural practices have demonstrated the potential to be more profitable and sustainable in the production of agricultural products. Modern agriculture has been reliant on agricultural machinery and tools to produce agricultural products, where recently these machines have become the mechanism for implementing precision agricultural practices. The future is likely to see more adoption of these new equipment technologies including the ones that implement varying levels of autonomy.

As with the adoption of any new technology, it is important to consider the potential drawbacks of adopting a new technology as compared to previous alternatives. Modern agricultural machinery is and will continue to be reliant on numerous digital technologies to implement modern agricultural practices. Similar technologies which exist on both agricultural equipment and within other critical industries have demonstrated the potential to be subjected to cyberattacks. Quantifying potential cybersecurity risks with the intent to make better design decisions is an important step for the smart adoption of these new equipment technologies. Chapter 3 presented a case study that looked at one potential scenario and outcome of a cyberattack that targeted in-season nitrogen application to corn. The case study was not attempting to argue against precision agricultural practices but rather present a method for assessing potential outcomes of cyberattacks when making cybersecurity design decisions for agricultural machinery. Overall, thorough cybersecurity risk assessment and a cybersecurity strategy is needed to protect current and upcoming agricultural machinery from cybersecurity threats.

With the awareness of need for cybersecurity of agricultural machinery, there have been no well-known publicly available solutions produced by either industry or academic research to address the challenge of cybersecurity. This thesis presented two potential solutions: modeling and security testbeds. The CASE modeling method as discussed in chapter 4, is a way to include cybersecurity principles in the initial design process of a new machine. Modeling can be a starting point for finding the most secure setup of an agricultural machine control system. A Stateflow model was built and evaluated to

demonstrate how this type of modeling could be useful in the secure design of agricultural machinery.

The second solution that was demonstrated was the use of testbeds for discovering cybersecurity vulnerabilities and making smart hardware and software selection decisions. STAVE was presented as an example of how a testbed was used to investigate the cybersecurity of Flex-Ro. Testbeds provide many benefits and ultimately are a great way to investigate cybersecurity vulnerabilities without causing damage to the larger machine.

6.2. Future Work

There is room for further research into the topic of cybersecurity of agricultural machinery. The two broad areas for future research to build on this project include general cyberattack risk assessment and specific cybersecurity solutions for agricultural machinery. First, a general cyberattack risk assessment would involve identifying potential cybersecurity vulnerabilities to all areas of agriculture and agricultural machinery. This could include the assessment of tractors, IoT devices, and digital ag-tech apps. Another part of this assessment would involve determining potential cyberattack scenarios and the financial impact they could impose. Further, the probability of such attacks along with the documented instances of attacks could be used to determine the financial investment needed to improve cybersecurity within agriculture and agricultural machinery. The results of this risk assessment process could be provided to the agricultural community along with education on cybersecurity practices that should be implemented to protect each individual or company in the agricultural industry.

The second area of future research would include the development of practical cybersecurity tools and solutions to improve the cybersecurity of agricultural machinery. The two solutions of modeling and testbeds, presented in this project, could be areas of future research. Additional modeling techniques and customized solutions for improving the design and cybersecurity of agricultural machinery could be developed. Further development of testbed solutions could provide a practical means for cybersecurity assessment of prototypes during the design process of agricultural machinery. Other solutions beyond modeling and testbeds could be developed to improve cybersecurity practices. The future of agriculture will be dependent on the choices made today to prepare for the challenges of tomorrow.

REFERENCES

- 9 Series Tractors | 9RX 640 | John Deere US. (n.d.). Retrieved May 22, 2022, from <https://www.deere.com/en/tractors/4wd-track-tractors/9rx-640/>
- Afram, A., Janabi-Sharifi, F. (2015). Gray-box modeling and validation of residential HVAC system for control system design. *Applied Energy*, 137, 134–150. <https://doi.org/10.1016/j.apenergy.2014.10.026>
- agricultural revolution. (n.d.). <https://doi.org/10.1093/oi/authority.20110803095356757>
- Ahanger, T. A., Aljumah, A. (2019). Internet of Things: A Comprehensive Study of Security Issues and Defense Mechanisms. *IEEE Access*, 7, 11020–11028. <https://doi.org/10.1109/ACCESS.2018.2876939>
- Alley, M., Thomason, W., Holshouser, D., Roberson, G. T. (2011). Precision Farming Tools: Variable-Rate Application, 17.
- Ametepe, A. F.-X., Ahouandjinou, S. A. R. M., Ezin, E. C. (2019). Secure Encryption by Combining Asymmetric and Symmetric Cryptographic Method for Data Collection WSN in smart Agriculture. In *2019 IEEE International Smart Cities Conference (ISC2)* (pp. 93–99). <https://doi.org/10.1109/ISC246665.2019.9071658>
- Angyalos, Z., Botos, S., Robert, S. (2021). The importance of cybersecurity in modern agriculture. *Journal of Agricultural Informatics*, 12. <https://doi.org/10.17700/jai.2021.12.2.604>
- Automotive Cybersecurity by Design. (2021, February 16). Retrieved May 21, 2022, from <https://www.guardknox.com/automotive-cybersecurity-by-design/>

- Baillie, C., Lobsey, C., Antille, D., McCarthy, C., Thomasson, J. (2018). *A review of the state of the art in agricultural automation. Part III: Agricultural machinery navigation systems*. <https://doi.org/10.13031/aim.201801591>
- Baker, L., Green, R. (2020). Cyber Security in UK Agriculture. *NCC Group*, 41.
- Barreto, L., Amaral, A. (2018). Smart Farming: Cyber Security Challenges. In *2018 International Conference on Intelligent Systems (IS)* (pp. 870–876). <https://doi.org/10.1109/IS.2018.8710531>
- Barrett, J. (2022, January 12). Corn and soybean production up in 2021, USDA Reports
Corn and soybean stocks up from year earlier, Winter Wheat Seedings up for 2022. Retrieved March 22, 2022, from <https://www.nass.usda.gov/Newsroom/2022/01-12-2022.php>
- Basics of Automata Theory. (n.d.). Retrieved June 21, 2022, from <https://cs.stanford.edu/people/eroberts/courses/soco/projects/2004-05/automata-theory/basics.html>
- Bender, R. R., Haegele, J. W., Ruffo, M. L., Below, F. E. (2013). Modern Corn Hybrids' Nutrient Uptake Patterns, *97*(1), 4.
- Boghossian, A., Linsky, S., Brown, A., Mutschler, P., Ulicny, B., Barrett, L. (2018). *Threats to Precision Agriculture*.
- Borohl, J. (2021). Cyber security threats – are we prepared?
- Boubin, J., Chumley, J., Stewart, C., Khanal, S. (2019). Autonomic Computing Challenges in Fully Autonomous Precision Agriculture. In *2019 IEEE*

International Conference on Autonomic Computing (ICAC) (pp. 11–17).

<https://doi.org/10.1109/ICAC.2019.00012>

Bowles, S., Choi, J.-K. (2019). The Neolithic Agricultural Revolution and the Origins of Private Property. *Journal of Political Economy*, 127(5), 2186–2228.

<https://doi.org/10.1086/701789>

Burkacky, O., Deichmann, J., Klein, B., Pototzky, K., Scherf, G. (2020). Cybersecurity in automotive: Mastering the challenge, 34.

CAN in Automation (CiA): History of the CAN technology. (n.d.). Retrieved May 22, 2022, from <https://www.can-cia.org/can-knowledge/can/can-history/>

Cassman, K. G., Dobermann, A., Walters, D. T. (2002). Agroecosystems, Nitrogen-use Efficiency, and Nitrogen Management, 31(2), 9.

Chamarajnar, R., Ashok, A. (2019). Integrity Threat Identification for Distributed IoT in Precision Agriculture. In *2019 16th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)* (pp. 1–9).

<https://doi.org/10.1109/SAHCN.2019.8824841>

Chivers, C.-A., Rose, D. (2020, September 4). The fourth agricultural revolution is coming – but who will really benefit? Retrieved May 21, 2022, from <http://theconversation.com/the-fourth-agricultural-revolution-is-coming-but-who-will-really-benefit-145810>

Corn PRICE Today | Corn Spot Price Chart | Live Price of Corn per Ounce | Markets Insider. (n.d.). Retrieved April 16, 2022, from <https://markets.businessinsider.com/commodities/corn-price>

- Daberkow, S. G., McBride, W. D. (2000). Adoption of precision agriculture technologies by U.S. farmers. *Proceedings of the 5th International Conference on Precision Agriculture, Bloomington, Minnesota, USA, 16-19 July, 2000*, 1–12.
- Data Management | Operations Center | John Deere US. (n.d.). Retrieved July 25, 2022, from <https://www.deere.com/en/technology-products/precision-ag-technology/data-management/operations-center/>
- Demestichas, K., Peppes, N., Alexakis, T. (2020). Survey on Security Threats in Agricultural IoT and Smart Farming. *Sensors*, 20(22), 6458. <https://doi.org/10.3390/s20226458>
- Duncan, S. E., Reinhard, R., Williams, R. C., Ramsey, F., Thomason, W., Lee, K., ... Murch, R. (2019). Cyberbiosecurity: A New Perspective on Protecting U.S. Food and Agricultural System. *Frontiers in Bioengineering and Biotechnology*, 7, 63. <https://doi.org/10.3389/fbioe.2019.00063>
- Eckelkamp, M., Humphreys, K. (2022, January 28). Autonomy in Action: These Machines Bring Imagination to Life. Retrieved July 25, 2022, from <https://www.thedailyscoop.com/news/new-products/autonomy-action-these-machines-bring-imagination-life>
- Evans, J. T., Pitla, S. K., Luck, J. D., Kocher, M. (2020). Row crop grain harvester path optimization in headland patterns. *Computers and Electronics in Agriculture*, 171, 105295. <https://doi.org/10.1016/j.compag.2020.105295>

- Federal Bureau of Investigation. (2021). *Cyber Criminal Actors Targeting the Food and Agriculture Sector with Ransomware Attacks* (TLP:White No. 20210901– 001) (p. 5).
- Federal Bureau of Investigation. (2022). *Ransomware Attacks on Agricultural Cooperatives Potentially Timed to Critical Seasons* (TLP:White No. 20220420– 001) (p. 4).
- Ferrag, M. A., Shu, L., Friha, O., Yang, X. (2022). Cyber Security Intrusion Detection for Agriculture 4.0: Machine Learning-Based Solutions, Datasets, and Future Directions. *IEEE/CAA Journal of Automatica Sinica*, 9(3), 407–436.
<https://doi.org/10.1109/JAS.2021.1004344>
- Ferrag, M. A., Shu, L., Yang, X., Derhab, A., Maglaras, L. (2020). Security and Privacy for Green IoT-Based Agriculture: Review, Blockchain Solutions, and Challenges. *IEEE Access*, 8, 32031–32053. <https://doi.org/10.1109/ACCESS.2020.2973178>
- Fidler, B. (2017). Cybersecurity governance: a prehistory and its implications. *Digital Policy, Regulation and Governance*, 19(6), 449–465.
<https://doi.org/10.1108/DPRG-05-2017-0026>
- Freyhof, M., Grispos, G., Pitla, S., Stolle, C. (2022). Towards a Cybersecurity Testbed for Agricultural Vehicles and Environments, 6.
- Gains For the Farmer and the Farm. (2022, March 28). [text/html]. Retrieved March 28, 2022, from <https://ravenprecision.com/driverless-ag/omnipower>

- Gegick, M., Barnum, S. (2005, September 14). Least Privilege | CISA. Retrieved May 24, 2022, from <https://www.cisa.gov/uscert/bsi/articles/knowledge/principles/least-privilege>
- Geil, A., Sagers, G., Spaulding, A. D., Wolf, J. R. (2018). Cyber security on the farm: an assessment of cyber security practices in the United States agriculture industry. *International Food and Agribusiness Management Review*, 21(3), 317–334. <https://doi.org/10.22434/IFAMR2017.0045>
- Gupta, M., Abdelsalam, M., Khorsandroo, S., Mittal, S. (2020). Security and Privacy in Smart Farming: Challenges and Opportunities. *IEEE Access*, 8, 34564–34584. <https://doi.org/10.1109/ACCESS.2020.2975142>
- HackRF One - Great Scott Gadgets. (n.d.). Retrieved June 25, 2022, from <https://greatscottgadgets.com/hackrf/one/>
- Holderith, P. (2022, May 3). John Deere Tractors Stolen by Russia in Ukraine Remotely Disabled. Retrieved June 9, 2022, from <https://www.thedrive.com/news/john-deere-tractors-stolen-by-russia-in-ukraine-remotely-disabled>
- Hopcroft, J. E., Motwani, R., Ullman, J. D. (2007). *Introduction to automata theory, languages, and computation* (3rd ed). Boston: Pearson/Addison Wesley.
- Iqbal, J., Wortmann, C., Maharjan, B., Puntel, L. (2020, April 29). Tips for In-season Nitrogen Management in Corn. Retrieved March 23, 2022, from <https://cropwatch.unl.edu/2020/tips-season-nitrogen-management-corn>

- Jahn, D. M. M., Oemichen, W. L., Treverton, D. G. F., David, S. L., Rose, A., Brosig, M. A., ... Hutchison, W. K. (2019). Cyber Risk and Security Implications in Smart Agriculture and Food Systems, 20.
- John Deere CAN Bus Presentation.* (2021). Retrieved from <https://www.youtube.com/watch?v=6-SkCw3I3dI>
- Kamienski, C., Kleinschmidt, J., Soininen, J.-P., Kolehmainen, K., Roffia, L., Visoli, M., ... Fernandes, S. (2018). SWAMP: Smart Water Management Platform Overview and Security Challenges. In *2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)* (pp. 49–50). <https://doi.org/10.1109/DSN-W.2018.00024>
- Kassel, K. (2022, February 4). Corn, soybeans accounted for over 40 percent of all U.S. crop cash receipts in 2020. Retrieved March 22, 2022, from <http://www.ers.usda.gov/data-products/chart-gallery/gallery/chart-detail/?chartId=76946>
- Lenz, J., Landman, R., Mishra, A. (2007). Customized Software in Distributed Embedded Systems: ISOBUS and the Coming Revolution in Agriculture, 18.
- Liu, Y., Ma, X., Shu, L., Hancke, G. P., Abu-Mahfouz, A. M. (2021). From Industry 4.0 to Agriculture 4.0: Current Status, Enabling Technologies, and Research Challenges. *IEEE Transactions on Industrial Informatics*, 17(6), 4322–4334. <https://doi.org/10.1109/TII.2020.3003910>
- M. Boland, H., I. Burgett, M., J. Etienne, A., M. Stwalley III, R. (2021). An Overview of CAN-BUS Development, Utilization, and Future Potential in Serial Network

Messaging for Off-Road Mobile Equipment. In F. Ahmad & M. Sultan (Eds.),

Technology in Agriculture. IntechOpen. <https://doi.org/10.5772/intechopen.98444>

McVan, M., Midwest, I. (2021, October 13). FBI says ransomware attacks on food and agriculture industry are increasing. Retrieved January 13, 2022, from <https://investigatamidwest.org/2021/10/13/fbi-says-ransomware-attacks-on-food-and-agriculture-industry-are-increasing/>

Meat giant JBS pays \$11m in ransom to resolve cyber-attack. (2021, June 10). *BBC News*. Retrieved from <https://www.bbc.com/news/business-57423008>

Monarch Tractor Electric Tractor. (n.d.). Retrieved March 28, 2022, from <https://www.monarchtractor.com/>

Murman, J. N. (2019). Flex-Ro: A Robotic High Throughput Field Phenotyping System, 153.

Nikander, J., Manninen, O., Laajalahti, M. (2020). Requirements for cybersecurity in agricultural communication networks. *Computers and Electronics in Agriculture*, 179, 105776. <https://doi.org/10.1016/j.compag.2020.105776>

Nitrogen stabilizers. (2018, April 24). Retrieved March 26, 2022, from <https://andersonscanada.com/2018/04/24/nitrogen-stabilizers/>

NTTL: Only U.S. OECD Tractor Test Lab. (n.d.). Retrieved June 30, 2022, from <https://tractortestlab.unl.edu/>

NUTRI-PLACER® 920 & 2800 FERTILIZER APPLICATORS. (n.d.).

Omaha, Nebraska Koppen Climate Classification (Weatherbase). (n.d.). Retrieved April 13, 2022, from <http://www.weatherbase.com/weather/weather->

summary.php3?s=5527&cityname=Omaha,+Nebraska,+United+States+of+America

Oteng-Darko, P., Yeboah, S., Addy, S. N. T., Amponsah, S., Danquah, E. O. (2012).

Crop modeling: A tool for agricultural research – A review, 6.

Paukner, M. (2022, March 22). CNH Plans to Bring ‘Significant Amount’ of Autonomy

to Market By 2025. Retrieved March 28, 2022, from

<https://www.precisionfarmingdealer.com/articles/5003-cn-h-plans-to-bring-significant-amount-of-autonomy-to-market-by-2025>

Peng, C., Xu, M., Xu, S., Hu, T. (2018). Modeling multivariate cybersecurity risks.

Journal of Applied Statistics, 45(15), 2718–2740.

<https://doi.org/10.1080/02664763.2018.1436701>

Pfleeger, C. P., Pfleeger, S. L., Margulies, J. (2015). *Security in computing* (Fifth edition). Upper Saddle River, NJ: Prentice Hall.

Pingali, P. L. (2012). Green Revolution: Impacts, limits, and the path ahead. *Proceedings of the National Academy of Sciences*, 109(31), 12302–12308.

<https://doi.org/10.1073/pnas.0912953109>

Pohl, J., Noack, A. (2018). Universal Radio Hacker: A Suite for Analyzing and Attacking Stateful Wireless Protocols, 14.

Precision Ag Definition. (n.d.). Retrieved March 27, 2022, from

<https://www.ispag.org/about/definition>

Precision Nitrogen Application. (2014). Retrieved March 23, 2022, from

https://www.reacchpna.org/case_studies/precision_nitrogen

- PRISM Climate Group at Oregon State University. (2021). Retrieved April 11, 2022, from <https://prism.oregonstate.edu/normal/>
- Prodanović, R., Rančić, D., Vulić, I., Zorić, N., Bogičević, D., Ostojić, G., ... Stankovski, S. (2020). Wireless Sensor Network in Agriculture: Model of Cyber Security. *Sensors*, 20(23), 6747. <https://doi.org/10.3390/s20236747>
- Puntel, L. A., Sawyer, J. E., Barker, D. W., Dietzel, R., Poffenbarger, H., Castellano, M. J., ... Archontoulis, S. V. (2016). Modeling Long-Term Corn Yield Response to Nitrogen Rate and Crop Rotation. *Frontiers in Plant Science*, 7. Retrieved from <https://www.frontiersin.org/article/10.3389/fpls.2016.01630>
- Quinn, R., Reporter, D. S. (2022, March 24). DTN Fertilizer Trends: Nitrogen Prices Keep Setting New Records. Retrieved March 26, 2022, from <https://agfax.com/2022/03/24/dtn-fertilizer-trends-nitrogen-prices-keep-setting-new-records/>
- Rahmadian, R., Widyardono, M. (2020). Autonomous Robotic in Agriculture: A Review. In *2020 Third International Conference on Vocational Education and Electrical Engineering (ICVEE)* (pp. 1–6). <https://doi.org/10.1109/ICVEE50212.2020.9243253>
- Raj, E. F. I., Appadurai, M., Athiappan, K. (2021). Precision Farming in Modern Agriculture. In A. Choudhury, A. Biswas, T. P. Singh, & S. K. Ghosh (Eds.), *Smart Agriculture Automation Using Advanced Technologies: Data Analytics and Machine Learning, Cloud Architecture, Automation and IoT* (pp. 61–87). Singapore: Springer. https://doi.org/10.1007/978-981-16-6124-2_4

Ransomware Attacks on Agricultural Cooperatives Potentially Timed to Critical Seasons

- HS Today. (2022, April 23). Retrieved May 3, 2022, from

<https://www.hstoday.us/subject-matter-areas/cybersecurity/ransomware-attacks-on-agricultural-cooperatives-potentially-timed-to-critical-seasons/>

Rattigan, K. M. (2022, May 12). U.S. Agricultural Machinery Manufacturer Hit with

Ransomware Attack. Retrieved May 22, 2022, from

<https://www.natlawreview.com/article/us-agricultural-machinery-manufacturer-hit-ransomware-attack>

Rich, E. (2007). *Automata, Computability and Complexity: Theory and Applications*.

Pearson Education, Inc.

Risks of using AI to grow our food are substantial and must not be ignored, warn

researchers. (2022, February 23). Retrieved May 20, 2022, from

<https://www.cam.ac.uk/research/news/risks-of-using-ai-to-grow-our-food-are-substantial-and-must-not-be-ignored-warn-researchers>

Rose, D. C., Lyon, J., de Boon, A., Hanheide, M., Pearson, S. (2021). Responsible

development of autonomous robotics in agriculture. *Nature Food*, 2(5), 306–309.

<https://doi.org/10.1038/s43016-021-00287-9>

Security Tip (ST04-001). (2019, November 14). Retrieved July 2, 2021, from [https://us-](https://us-cert.cisa.gov/ncas/tips/ST04-001)

[cert.cisa.gov/ncas/tips/ST04-001](https://us-cert.cisa.gov/ncas/tips/ST04-001)

Sellars, S., Nunes, V. (2021, February 17). Synthetic Nitrogen Fertilizer in the U.S. •

farmdoc daily. Retrieved March 27, 2022, from

<https://farmdocdaily.illinois.edu/2021/02/synthetic-nitrogen-fertilizer-in-the-us.html>

Shapiro, C. A. (n.d.). Nutrient Management Suggestions for Corn, 7.

Shapiro, C. A., Ferguson, R., Wortmann, C., Maharjan, B., Krienke, B. (2019). Nutrient Management Suggestions for Corn, 7.

Shaver, T. (2014, December). Nutrient Management for Agronomic Crops in Nebraska.

Soil Management for Increased Soil Organic Matter (G2283). (n.d.). Retrieved April 11, 2022, from

<https://extensionpublications.unl.edu/assets/html/g2283/build/g2283.htm>

Sontowski, S., Gupta, M., Laya Chukkapalli, S. S., Abdelsalam, M., Mittal, S., Joshi, A., Sandhu, R. (2020). Cyber Attacks on Smart Farming Infrastructure. In *2020 IEEE 6th International Conference on Collaboration and Internet Computing (CIC)* (pp. 135–143). Atlanta, GA, USA: IEEE.

<https://doi.org/10.1109/CIC50333.2020.00025>

Sparrow, R., Howard, M. (2021). Robots in agriculture: prospects, impacts, ethics, and policy. *Precision Agriculture*, 22(3), 818–833. <https://doi.org/10.1007/s11119-020-09757-9>

Stansell, J. (2021). Development and Automation of a Sensor-Based Fertigation Management Framework for Improved Nitrogen Use Efficiency and Profitability in Irrigated Row Crop Production Systems. *Embargoed Master's Theses*.

Retrieved from <https://digitalcommons.unl.edu/embargotheses/207>

Stateflow - MATLAB & Simulink. (n.d.). Retrieved June 21, 2022, from

<https://www.mathworks.com/products/stateflow.html>

Technical Data Sheet: Urea Ammonium Nitrate. (n.d.).

The Tractor. (n.d.). Retrieved May 22, 2022, from <https://www.froelichtractor.com/the-tractor.html>

Tibken, S. (2022, January 6). John Deere breaks new ground with self-driving tractors you can control from a phone. Retrieved February 25, 2022, from

<https://www.cnet.com/tech/mobile/john-deere-breaks-new-ground-with-self-driving-tractors-you-can-control-from-a-phone/>

Timeline of Ag Equipment 'Firsts.' (2009, September 23). Retrieved May 22, 2022, from

<https://www.farm-equipment.com/articles/4269-timeline-of-ag-equipment-firsts>

Tractors and Green Revolution in India. (n.d.). Retrieved May 22, 2022, from

<https://tractorguru.in/tractor-blog/tractors-and-green-revolution-in-india>

USDA - National Agricultural Statistics Service - Quick Stats Lite. (2018, May 4).

Retrieved April 18, 2022, from

https://www.nass.usda.gov/Quick_Stats/Lite/index.php#85BC54D5-B1F8-305A-9ABD-DC552A929DF0

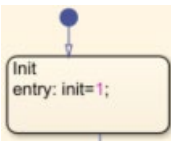

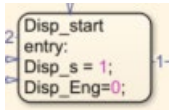
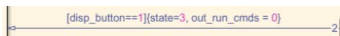

Veale, M., Brown, I. (2020). Cybersecurity. *Internet Policy Review*, 9(4).

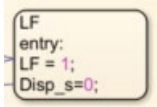
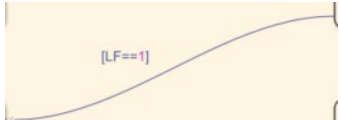
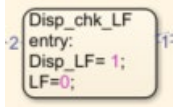
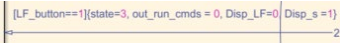

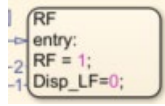
<https://doi.org/10.14763/2020.4.1533>


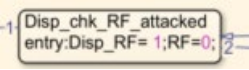


Werner, J. P. (2016). FLEX-RO: DESIGN, IMPLEMENTATION, AND CONTROL OF SUBASSEMBLIES FOR AN AGRICULTURAL ROBOTIC PLATFORM, 162.

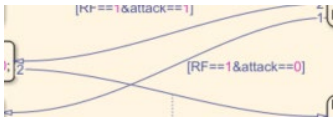
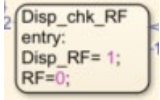



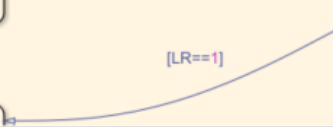
- West, J. (2018). A Prediction Model Framework for Cyber-Attacks to Precision Agriculture Technologies. *Journal of Agricultural & Food Information*, 19(4), 307–330. <https://doi.org/10.1080/10496505.2017.1417859>
- Yan, D. (2020, January 16). A Systems Thinking for Cybersecurity Modeling. arXiv. Retrieved from <http://arxiv.org/abs/2001.05734>
- Yazdinejad, A., Zolfaghari, B., Azmoodeh, A., Dehghantanha, A., Karimipour, H., Fraser, E., ... Duncan, E. (2021). A Review on Security of Smart Farming and Precision Agriculture: Security Aspects, Attacks, Threats and Countermeasures. *Applied Sciences*, 11(16), 7518. <https://doi.org/10.3390/app11167518>
- Yu, J., Luo, F. (2020). A Systematic Approach for Cybersecurity Design of In-Vehicle Network Systems with Trade-Off Considerations. *Security and Communication Networks*, 2020, 1–14. <https://doi.org/10.1155/2020/7169720>
- Zhao, H., Huang, Y., Liu, Z., Liu, W., Zheng, Z. (2021). Applications of Discrete Element Method in the Research of Agricultural Machinery: A Review. *Agriculture*, 11(5), 425. <https://doi.org/10.3390/agriculture11050425>

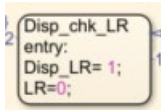

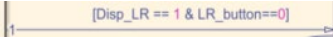
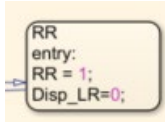
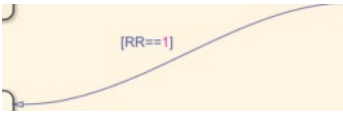
Appendix A: Stateflow Components Used in the E-stop Model

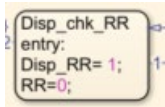
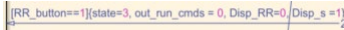

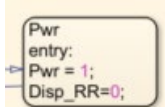
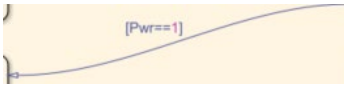
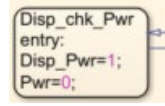
Name	Image	Function	State (1-5) based on Figure 4.9
Init		Entry into the model. Same as turning on the power supply to the Flex-Ro machine and remote.	
Initialization to Disp_start transition		Transitions from initialization state to Disp_start state when init=1 (init is just a placeholder variable to force a transition from one state to another). Enters state 1 in Figure 4.9.	
Disp_start		Initial state of the Flex-Ro display ECU. Display ECU starts by checking itself for an E-stop trigger condition.	1,2,4
Disp_start to E-stop transition		Transition to E-stop state if the E-stop button (disp_button) on the Flex-Ro display ECU gets pressed	
Disp_start to LF transition		Transition to LF state which signifies a heartbeat message being sent to the left-front steer ECU	


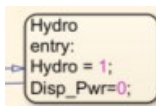
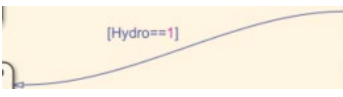
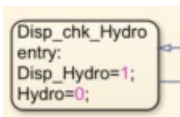

LF	 <pre> LF entry: LF = 1; Disp_s=0; </pre>	Represents the left-front steer ECU as it receives a heartbeat message from the display ECU and input signals from the attached E-stop button	1,2,4
LF to Disp_chk_LF transition	 <p>[LF==1]</p>	Transition representing response heartbeat message being sent from the left-front ECU back to the Display ECU	
Disp_chk_LF	 <pre> Disp_chk_LF entry: Disp_LF= 1; LF=0; </pre>	State where the display ECU receives heartbeat message from LF and either transitions to an E-stop state or continues checking ECUs	1,2,4
Disp_chk_LF to E-stop transition	 <p>[LF_button==1] state=3, out_run_cmds = 0, Disp_LF=0 Disp_s = 1</p>	Transition to E-stop state if the LF E-stop button gets pressed and enter state 3 from Figure 4.9	
Disp_chk_LF to RF transition	 <p>[Disp_LF == 1 & LF_button==0]</p>	Transition to RF state which signifies a heartbeat message being sent to the right-front steer ECU	
RF	 <pre> RF entry: RF = 1; Disp_LF=0; </pre>	Represents the right-front steer ECU as it receives a heartbeat message from the display ECU and input signals from the attached E-stop button	1,2,4

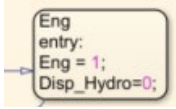
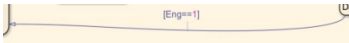
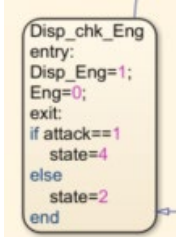
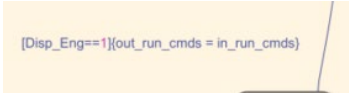
RF to Disp_chk_RF_ attacked transition		Transition representing response heartbeat message being sent from the left-front ECU back to the Display ECU under a cyberattack	
Disp_chk_RF_ attacked state		Represents the display ECU under a cyberattack state as it receives a heartbeat message from the right-front ECU. The display ECU is still able to receive and transmit messages, although the messages could be altered.	4
Disp_chk_RF_ attacked to E- stop transition		Transition to E-stop state if the Disp_chk_RF_attacked interprets that the RF E-stop button is pressed. The actual state of the E-stop button could be either pressed or unpressed. Transition to state 5 as seen in Figure 4.9	
Disp_chk_RF_ attacked to LR transition		Transition to LR state which signifies a heartbeat message being sent to the left-rear steer ECU from the attacked display ECU	



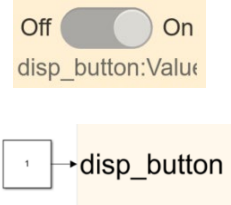
RF to Disp_chk_RF transition		Transition representing response heartbeat message being sent from the right-front ECU back to the Display ECU	
Disp_chk_RF		State where the display ECU receives heartbeat message from the right-front steer ECU and either transitions to an E-stop state or continues checking ECUs	1,2,4
Disp_chk_RF to E-stop		Transition to E-stop state if the RF E-stop button gets pressed and enter state 3 from Figure 4.9	
Disp_chk_RF to LR transition		Transition to LR state which signifies a heartbeat message being sent to the left-rear steer ECU	
LR		Represents the left-rear steer ECU as it receives a heartbeat message from the display ECU and input signals from the attached E-stop button	1,2,4
LR to Disp_chk_LR		Transition representing response heartbeat message being sent from the left-rear	

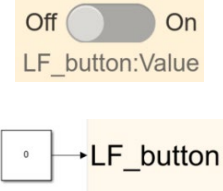
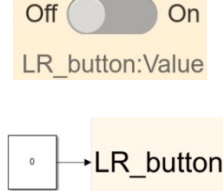
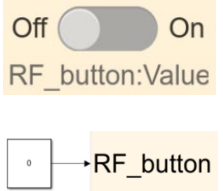
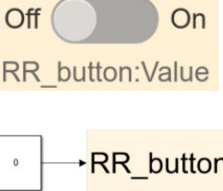
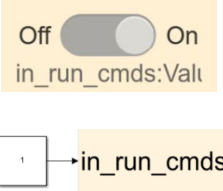
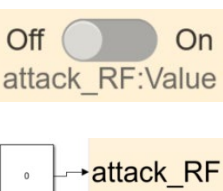
		ECU back to the Display ECU	
Disp_chk_LR		State where the display ECU receives heartbeat message from the left-rear steer ECU and either transitions to an E-stop state or continues checking ECUs	1,2,4
Disp_chk_LR to E-stop transition		Transition to E-stop state if the LR E-stop button gets pressed and enter state 3 from Figure 4.9	
Disp_chk_LR to RR transition		Transition to RR state which signifies a heartbeat message being sent to the right-rear steer ECU	
RR		Represents the right-rear steer ECU as it receives a heartbeat message from the display ECU and input signals from the attached E-stop button	1,2,4
RR to Disp_chk_RR transition		Transition representing response heartbeat message being sent from the right-rear ECU back to the Display ECU	

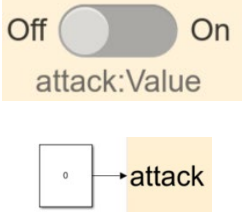
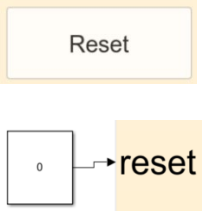

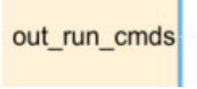
Disp_chk_RR		State where the display ECU receives heartbeat message from the right-rear steer ECU and either transitions to an E-stop state or continues checking ECUs	1,2,4
Disp_chk_RR to E-stop transition		Transition to E-stop state if the RR E-stop button gets pressed and enter state 3 from Figure 4.9	
Disp_chk_RR to Pwr transition		Transition to Pwr state which signifies a heartbeat message being sent to the power ECU	
Pwr		Represents the power control ECU as it receives a heartbeat message from the display ECU	1,2,4
Pwr to Disp_chk_Pwr transition		Transition representing response heartbeat message being sent from the Pwr ECU back to the Display ECU	
Disp_chk_Pwr		State where the display ECU receives heartbeat message from the Pwr ECU and continues checking ECUs. Diagram not currently set up to represent Pwr,	1,2,4

		Hydro, and Eng response time requirements.	
Disp_chk_Pwr to Hydro transition		Transition to Hydro state which signifies a heartbeat message being sent to the hydraulics control ECU	
Hydro		Represents the hydraulics control ECU as it receives a heartbeat message from the display ECU	1,2,4
Hydro to Disp_chk_Hydro transition		Transition representing response heartbeat message being sent from the Hydro ECU back to the Display ECU	
Disp_chk_Hydro		State where the display ECU receives heartbeat message from the hydraulics control ECU and continues checking ECUs.	1,2,4
Disp_chk_Hydro to Eng transition		Transition to Eng state which signifies a heartbeat message being sent to the engine control ECU	

<p>Eng</p>		<p>Represents the engine control ECU as it receives a heartbeat message from the display ECU</p>	<p>1,2,4</p>
<p>Eng to Disp_chk_Eng transition</p>		<p>Transition representing response heartbeat message being sent from the Eng ECU back to the Display ECU</p>	
<p>Disp_chk_Eng</p>		<p>State where the display ECU receives heartbeat message from the engine control ECU and continues checking ECUs. This is the final state of the ECU check sequence.</p>	<p>2,4</p>
<p>Disp_chk_Eng to Disp_start transition</p>		<p>Represents a transition back to the start of the ECU check sequence. Enters state 2 if all ECUs were checked without an E-stop trigger condition and no cyberattack is occurring. Enter state 4 if no E-stop trigger conditions occurred although at least one ECU is under cyberattack.</p>	

<p>E-stop</p>		<p>Represents E-stop state where at least one ECU has determined an E-stop trigger condition. Normal control commands are stopped under this state and stop/shutdown commands are sent instead.</p>	<p>3,5</p>
<p>E-stop to Disp_start transition</p>		<p>Transition from E-stop state back to state 1 where all ECUs are being checked for E-stop trigger conditions. Only happens after a reset button input is sent</p>	
<p>disp_button</p>		<p>Represents the display ECU E-stop button on the Flex-Ro remote</p>	

LF_button	 <p>Off <input type="checkbox"/> On LF_button:Value</p> <p><input type="checkbox"/> → LF_button</p>	Represents the left-front E-stop button on Flex-Ro	
LR_button	 <p>Off <input type="checkbox"/> On LR_button:Value</p> <p><input type="checkbox"/> → LR_button</p>	Represents the left-rear E-stop button on Flex-Ro	
RF_button	 <p>Off <input type="checkbox"/> On RF_button:Value</p> <p><input type="checkbox"/> → RF_button</p>	Represents the right-front E-stop button on Flex-Ro	
RR_button	 <p>Off <input type="checkbox"/> On RR_button:Value</p> <p><input type="checkbox"/> → RR_button</p>	Represents the right-rear E-stop button on Flex-Ro	
in_run_cmds	 <p>Off <input checked="" type="checkbox"/> On in_run_cmds:Value</p> <p><input type="checkbox"/> → in_run_cmds</p>	Represents any other commands sent from Flex-Ro remote to run or control Flex-Ro	
attack_RF	 <p>Off <input type="checkbox"/> On attack_RF:Value</p> <p><input type="checkbox"/> → attack_RF</p>	Represents right-front E-stop button input under a cyberattack scenario. Could be different from actual right-front button input	

attack		Input that represents whether a cyberattack is/has occurred or not	
reset		Represents reset button input from Flex-Ro remote or FlexRoRun app	
state		Output from Stateflow model that can be used to plot which 'state' from Figure 4.9 the model is in over time.	
out_run_cmds		Output that represents whether the E-stop system is allowing normal operation commands or is sending E-stop commands to stop/shutdown machine.	