THESIS

FACTORS INFLUENCING DRIVER RESPONSE TOWARD AN INSTRUMENT CLUSTER CYBERATTACK: EXPERIENCE, AWARENESS, AND TRAINING

Submitted by

Trevor F. Lanigan

Department of Systems Engineering

In partial fulfillment of the requirements

For the Degree of Master of Science

Colorado State University

Fort Collins, Colorado

Spring 2025

Master's Committee:

Advisor: Erika Gallegos

Jeremy Daily
Niccole Nelson

ABSTRACT

FACTORS INFLUENCING DRIVER RESPONSE TOWARD AN INSTRUMENT CLUSTER CYBERATTACK: EXPERIENCE, AWARENESS, AND TRAINING

Commercial Motor Vehicles (CMVs) and the trucking industry are often referred to as the backbone to the supply chain in the United States. With this has come efforts to modernize heavy vehicles just like their passenger vehicle counterparts in order to improve the safety, performance, and efficiency of the transportation of goods and materials. However, the introduction of advanced cyber-physical systems in heavy vehicles makes available a new vulnerability not previously encountered: cyberattacks. The objective of this thesis is to (1) evaluate drivers' responses to an unexpected cyberattack, (2) evaluate how awareness of the cybersecurity threat on their vehicle influences driver behavior, and (3) evaluate how the provision of a cyberattack response protocol influences driver performance. An on-road driving study with 50 participants was conducted to measure drivers' response to an unexpected cyberattack while operating a medium heavy-duty vehicle (GVWR 26,000lbs; Class 6). Each participant was randomly assigned to one of three experimental groups which received varying levels of information prior to the start of the drive. The Control group received no information regarding a possible cyberattack threat on their vehicle. The Aware group received a warning regarding a possible cyberattack threat on their vehicle. The Aware + Protocol group received the same warning as the Aware group along with a basic cyberattack response protocol. Within each group, six to seven of the participants were professional drivers (e.g., commercial truck driver, firefighter, bus driver), while the remaining 10 to 11 participants in each group were standard licensed drivers. Each of the participants experienced the same driving route and cyberattack scenario with regard to type, location, timing, and execution. Participant driving responses were measured using data collected from the vehicle CAN bus, and Racelogic VBOX3i GNSS and IMU sensors. Participant physiological responses (heart rate and electroder-

mal activity) were measured using an Empatica E4 wearable. Aditionally, participants completed a survey at the end of the experimental session to assess their driving experience, risk taking tendencies, and interpretation of the cyberattack. The findings highlight the essential role of awareness and response protocols in enhancing a driver's response to an unexpected vehicle cyberattack. The Aware + Protocol group achieved a 100% stop rate among both Standard and Professional drivers, showcasing the transformative impact of awareness and clear response guidelines compared to the Control group stop rate of 9% for Standard and 83% for Professional drivers. The Aware + Protocol group also traveled the shortest distance during the cyberattack, with Standard drivers covering 224 meters (0.139 miles) and Professional drivers 254 meters (0.158 miles), compared to the Control group's 828 meters (0.514 miles) for Standard drivers and 520 meters (0.323 miles) for Professional drivers. Furthermore, the Aware + Protocol group demonstrated the shortest reaction times, averaging 7.53 seconds, versus 16.12 seconds in the Aware group and 30.29 seconds in the Control group. These results emphasize that awareness alone is insufficient; explicit instructions significantly enhance drivers' ability to respond promptly and effectively to cybersecurity threats. By informing drivers and providing response protocols, their ability to respond appropriately to cyberattacks can be significantly improved. This information can be applied in several practical ways, such as developing cyberattack response training programs for all drivers, especially those operating heavy vehicles. Additionally, public service announcements and in-vehicle alerts could be effective in increasing awareness of cyberattack vulnerabilities. Public service announcements broadcasted through various media channels can inform a wide audience about the risks of vehicle cyberattacks and inform drivers on how to recognize and respond to such threats. In-vehicle alerts can offer real-time information and instructions, guiding drivers on immediate actions to take when a cybersecurity threat is detected.

ACKNOWLEDGEMENTS

I would like to extend my deepest gratitude to Dr. Jeremy Daily and Dr. Erika Gallegos. From the moment I learned about my opportunity to attend graduate school, they were the first to invite me into the program. Their unwavering support and guidance from the beginning of my journey at Colorado State University have been invaluable, and none of this would have been possible without them.

I also want to express my profound gratitude to my instructors from the U.S. Air Force Academy. Among them are Dr. Jade Driggs, Dr. Trae Span, Dr. Stu Turner, Dr. Chad Tossell, Dr. Nate Deming, Dr. James Walliser, and Dr. Jeff Newcamp, though this list is by no means exhaustive. Your passion and dedication galvanized my interest in Systems and Human Factors Engineering and inspired me to pursue a graduate degree. Dr. Trae Span's continued mentorship as both a graduate student and a military officer has been truly essential to my success during my time here.

Finally, I would like to express my heartfelt appreciation to the faculty, staff, and fellow students of Colorado State University, especially those in the Department of Systems Engineering. I owe a special thanks to Dr. Deb Dandaneau for her exceptional administrative support, which has ensured my smooth and successful navigation through the program. Additionally, none of this would have been possible without my research partner, Tyler Biggs.

"The views expressed are those of the authors and do not reflect the official guidance or position of the United States Government, the Department of Defense the United States Air Force or the United States Space Force."

DEDICATION

This thesis is dedicated to my family.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Chapter 1

Introduction

1.1 Motivation

The motivation for this study stems from the increasing importance of cybersecurity in the context of commercial motor vehicles (CMVs) and the critical role of understanding the human factor in ensuring effective cyberattack response procedures. With the advent of connected and computerized vehicles, cybersecurity has become a critical concern. As stated by Eiza and Ni (2017), “Damages of automotive cyberattacks can be severe and irreversible as it concerns human lives." The potential for cyberattacks throughout vehicle subsystems and the hazardous outcomes to which they can lead should not be underestimated (Wolf et al., 2004).

In the domain of cybersecurity research, humans are often referred to as “the weakest link in the chain" (Schneier, 2000). However, existing research on vehicle cybersecurity often focuses on the cyber-physical system with little consideration of the human (Linkov et al., 2019). To address this gap, it is essential to incorporate human behavior and responses into cybersecurity research, as drivers play a key role in managing and mitigating cyberattack threats (Cranor, 2008).

Previous driving simulator studies have begun to explore driver response to cyberattacks, measuring variables such as response time, driving styles, and situational awareness (Aliebrahimi & Miller, 2023; F. Zhang et al., 2019, 2023). While these studies have provided valuable insights and informed the present research, they have mainly focused on passenger vehicles, leaving a gap in understanding driver responses to cyberattacks in the context of commercial and heavy vehicle operation. Furthermore, these studies were conducted within the artificial environment of driving simulators, which, despite offering valuable insights, limit the applicability of the results to real-world driving conditions.

Given the critical role that commercial vehicles play in the transportation system and the potential catastrophic consequences of cyberattacks on these vehicles, this thesis seeks to fill the research

gap by focusing on the human factors that influence the response of a commercial vehicle driver to an unexpected instrument cluster cyberattack. In doing so, it aims to contribute valuable insights to the rapidly growing field of vehicle cybersecurity, particularly concerning driver behavior during a cyberattack.

1.2 Research Objectives

The primary objective of this research is to investigate the human factors influencing driver behavior and response to cyberattacks during commercial vehicle operation. This research is grounded in the discipline of human factors engineering, which seeks to apply the understanding of human cognitive, physical, and organizational capabilities to improve human interaction with systems and processes (Lee et al., 2017). Such insights are crucial for developing effective countermeasures that enhance driver safety and performance, ultimately contributing to the overall security of the transportation industry.

The results of the experiment seek to address the following research questions:

1. How does awareness of cybersecurity threat influence driver response to vehicle cyberattack?
    - *Hypothesis:* Increased awareness of cybersecurity threat will lead to more cautious and defensive driving behavior.
2. How does the implementation of a basic cyberattack response protocol impact driver performance?
    - *Hypothesis:* Implementing a basic cyberattack response protocol will improve driver performance and their ability to respond effectively during the cyberattack.
3. How do professional trained drivers' responses to vehicle cyberattack differ from those of standard licensed drivers?
    - *Hypothesis:* Professionally trained drivers will exhibit more effective and quicker responses to the cyberattack compared to regularly licensed drivers.

Chapter 2

Literature Review

The purpose of this literature review is to provide a comprehensive examination of the current state of research on driver responses to cyberattacks in the context of commercial motor vehicles (CMVs). This chapter explores foundational theories and models in human factors engineering, examining how these principles apply to vehicle cybersecurity. The review also analyzes cybersecurity challenges and solutions in both passenger and commercial vehicles, highlighting key differences and commonalities. In addition, it investigates the influence of cybersecurity threat awareness and priming on driver decision-making, the effectiveness of training and response protocols, and the differences in driving behavior between individuals with professional and standard experience. Finally, it includes previous studies on driver responses to unexpected vehicle cyberattacks. By narrowing the focus to these key areas, the review aims to provide a thorough understanding of the interplay between human factors and cybersecurity in CMVs, identifying gaps and opportunities for novel research.

2.1 Theoretical Framework

Human Factors Engineering (HFE) is a multidisciplinary field focused on understanding the interactions between humans and other system elements to optimize human well-being and overall system performance. According to Lee et al. (2017) in “Designing for People: An Introduction to Human Factors Engineering," HFE aims to design systems that account for human capabilities and limitations, improving safety, efficiency, and satisfaction. Human factors play a critical role in cybersecurity, as human behavior and decision-making can significantly impact security outcomes. Schneier (2000) in “Secrets and Lies: Digital Security in a Networked World," highlights the importance of understanding human vulnerabilities and integrating human factors into cybersecurity strategies. Similarly, Kumaraguru et al. (2010) emphasize the need for educating users to recognize and respond to phishing attacks, demonstrating the impact of human factors on cy-

bersecurity. More broadly, research has shown the critical role that human factors considerations on commercial drivers can have in reducing dangerous driving behaviors (J. Ahmed, Ward, et al., 2024; J. Ahmed et al., 2023; Bumgarner et al., 2024).

The Human in the Loop (HITL) Model, proposed by Cranor (2008), emphasizes the active involvement of humans in the control and decision-making processes within a system. As seen in Figure 2.1, this model integrates human knowledge and experience into system operations, ensuring that human judgment and expertise are utilized effectively. By incorporating human interaction, the HITL model enhances system performance and reliability, as humans can provide critical insights and interventions that cyber-physical systems alone may not achieve. Grobler et al. (2021) discuss the importance of designing cybersecurity systems that are tailored to human needs and capabilities, emphasizing the role of human-in-the-loop approaches in enhancing security measures. For instance, in cybersecurity, human-in-the-loop approaches can improve response times and accuracy by involving human operators in the monitoring and decision-making processes, thereby enhancing the overall security measures.

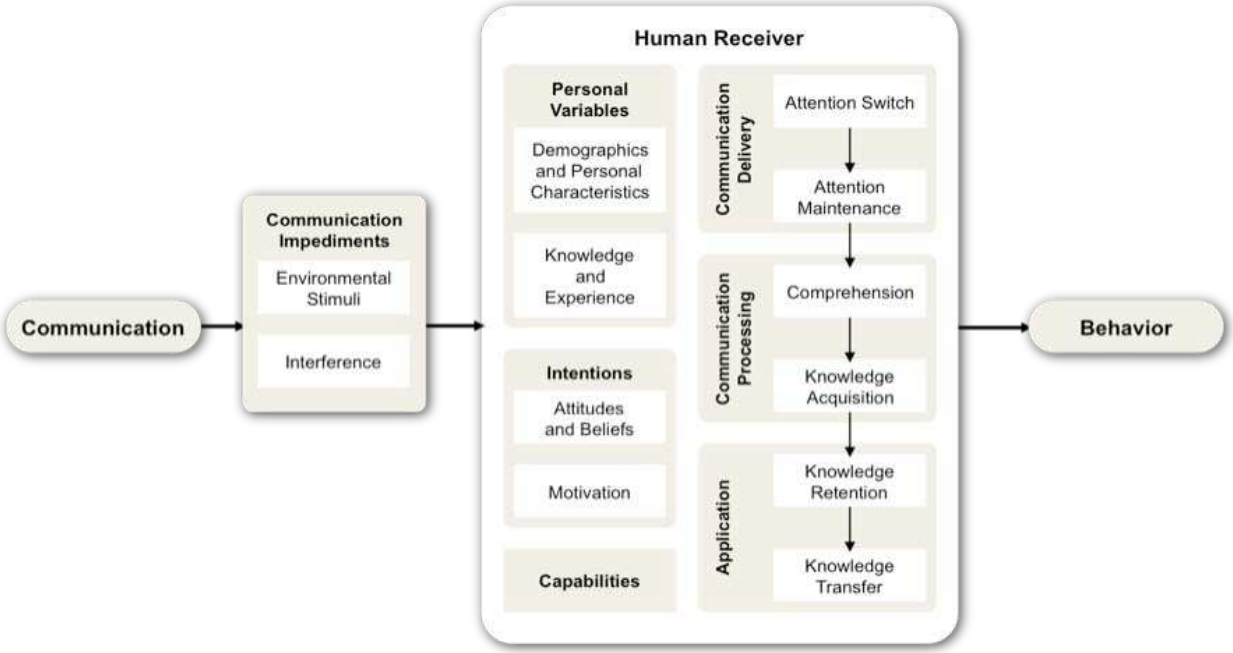


Figure 2.1: The human-in-the-loop security framework (Cranor, 2008)

Furthermore, the Information Processing Model of Cognition is a cognitive psychology theory that describes how humans perceive, process, and respond to information (Lee et al., 2017). This model, as shown in Figure 2.2, expands the understanding of the mechanisms by which people process information, make, and subsequently execute decisions. In the context of cybersecurity, the Information Processing Model of Cognition helps us understand how operators detect and respond to threats. By analyzing how information is perceived (e.g., recognizing a system malfunction), processed (e.g., determining it is a cyberattack), retrieved (e.g., recalling how to respond to a cyberattack), and responded to (e.g., executing response protocol), cybersecurity professionals can design better training programs and security measures compatible with the human cognition. Andrade et al. (2022) propose a Cognitive Cybersecurity Model, emphasizing the importance of understanding cognitive processes to improve cybersecurity measures. Additionally, Kävrestad and Naqvi (2024) highlight the cognitive challenges impacting users' cybersecurity behaviors, and stress the need for designing systems that minimize cognitive effort to enhance security.

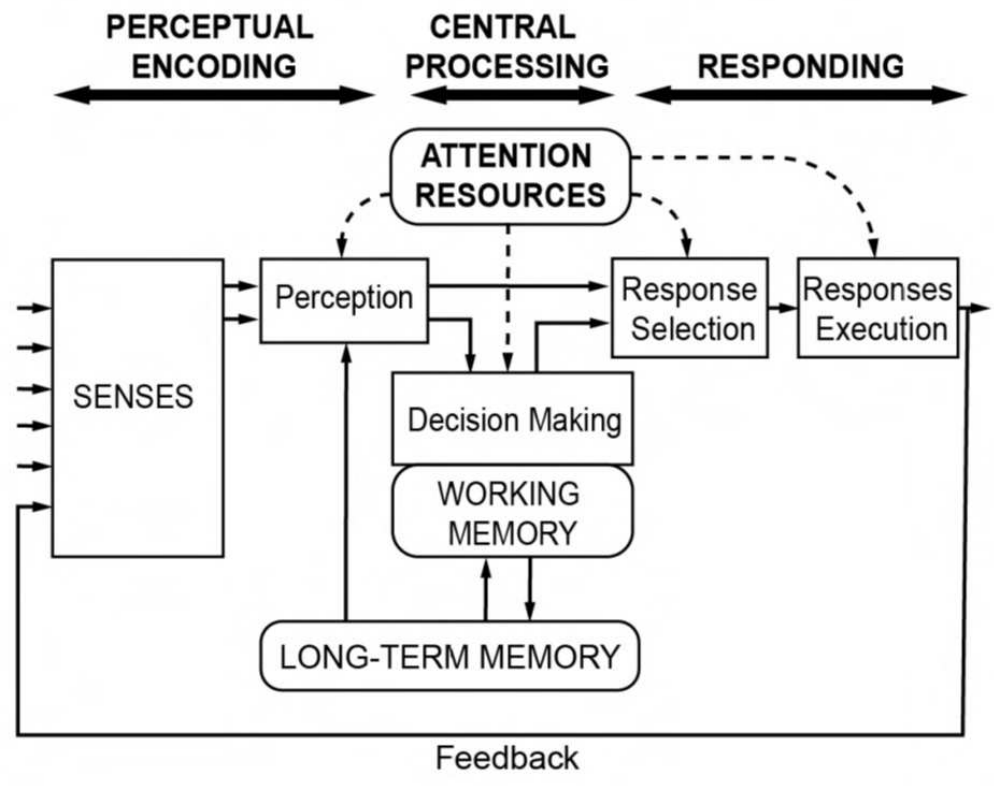


Figure 2.2: Information Processing Model of Cognition (Lee et al., 2017)

The first stage stage in the Information Processing Model of Cognition is perceptual encoding. To gain a deeper understanding of perceptual encoding, it is essential to explore Signal Detection Theory (SDT). SDT, as introduced by Tanner and Swets (1954), is a mathematical framework used to measure the ability to differentiate between signal (true threats) and noise (false alarms) under conditions of uncertainty. In cybersecurity, SDT can be applied to assess how well users can identify real cyberattack events among normal operations. This theory can help in designing systems and training programs that enhance users' sensitivity to threats while minimizing false positives, ultimately improving the overall security posture. Research by Fischhoff et al. (2016) supports the application of SDT in understanding phishing susceptibility, while Martin (2017) highlights its relevance in differentiating between genuine security threats and benign activities. As seen in Figure 2.3, response bias (criterion) indicates the variation between drivers' ability to determine whether an event is a cyberattack or a random system malfunction. For example, if a driver is primed with a possibility of a cyberattack on their vehicle, they may be more inclined to label the event (e.g., check engine light turning on) as a malicious attack by an actor that has infiltrated the vehicle systems rather than the vehicle being overdue on simple maintenance. Sharma et al. (2021) further emphasizes this element of SDT in cybersecurity by demonstrating how digital nudging techniques, such as framing and priming, can reduce user susceptibility to phishing attacks.

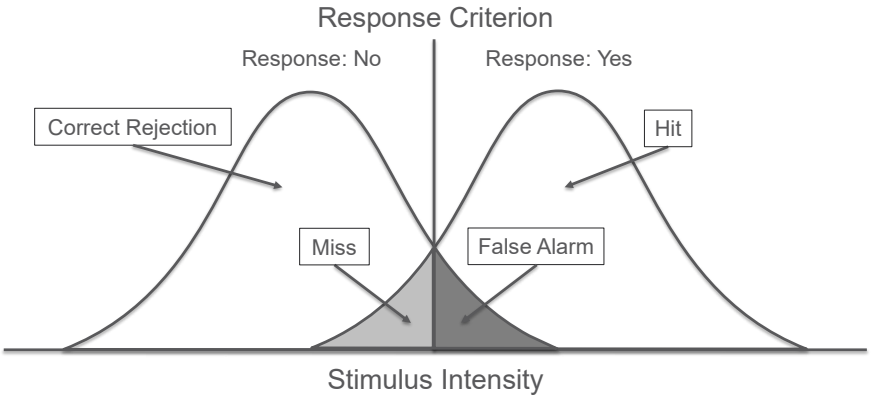


Figure 2.3: Schematic representation of signal and signal plus noise distribution. Adapted from Lee et al. (2017)

Another critical cognitive influence on visual perception is the interplay between Top-Down and Bottom-Up Processing. Top-Down Processing involves using pre-existing knowledge and expectations to interpret sensory information (Lee et al., 2017). This type of processing is guided by higher-level cognitive functions, such as memory and experience. For example, a professional driver who has previously encountered certain types of system malfunctions may quickly recognize similar issues based on familiar patterns and cues. This allows for faster identification and response to known problems. Research by Torten et al. (2018) found that cybersecurity threat awareness explained 61.2% of the variability in desktop security behavior.

On the other hand, Bottom-Up Processing relies on the actual sensory input to build final perception (Lee et al., 2017). It involves analyzing the raw data without preconceived notions or expectations. In a driving context, Bottom-Up Processing is crucial for detecting novel or unexpected system malfunctions that do not fit established patterns. This is especially the case with vehicles as many drivers lack expertise in the associated technology, increasing the likelihood of inadvertently compromising vehicle security through their actions (Parkinson et al., 2017). For instance, if standard drivers face a new type of vehicle error that has never been encountered before, they must rely on detailed analysis of sensory data to identify and understand the issue which can greatly reduce response efficacy and time.

Integrating both Top-Down and Bottom-Up Processing interventions can improve overall threat detection and response times. Innovative cybersecurity education programs, as highlighted by Aldawood and Skinner (2018), play a critical role in raising awareness and effectively reducing cybersecurity incidents. Al-Daeef et al. (2017) emphasize that effective cybersecurity training methods should engage users to enhance their awareness and ensure they retain the acquired knowledge over time by embedding training into familiar, ongoing activities. By improving awareness of cybersecurity threats, it expands drivers' expectations of vehicle malfunctions and increases sensitivity to error signals. However, when aiming to improve cybersecurity behavior, a balance must be achieved between training and cost of user responses, as this may yield counterproductive outcomes (Blythe & Coventry, 2018). For instance, if the actions a driver must take in order to mitigate

the cybersecurity threat is greater than the consequences of that threat, then the likely outcome is that of no behavior change.

2.2 Vehicle Cybersecurity

The rapid advancement of technology has significantly transformed the automotive industry, integrating sophisticated digital components and connectivity features into modern vehicles. This evolution, while enhancing convenience and functionality, has also introduced new vulnerabilities, particularly in the realm of cybersecurity. Modern vehicles, both passenger and commercial motor vehicles alike, are increasingly susceptible to cyberattacks due to their reliance on electronic control units (ECUs) and communication networks such as the Controller Area Network (CAN) bus (Checkoway et al., 2011; Koscher et al., 2010).

Research by Payne (2019) explored the vulnerabilities of the CAN bus protocol by creating a car-hacking research workstation, revealing critical insights into how replay attacks and reverse-engineering CAN bus messages can compromise vehicle security. Similarly, research by Mukherjee et al. (2016) underscores the possibility of malicious adversaries injecting foreign messages into the CAN bus with the intent of disrupting normal vehicle behavior. A security risk analysis identified several cyberattack scenarios, including joyriding, kidnapping, and large transport accidents, which could have catastrophic consequences (Meyer et al., 2021). At the Black Hat USA 2018 security conference, Tencent's Keen Security Lab demonstrated a cyberattack chain on a Tesla Model S/X that could ultimately control the steering system through the Autopilot without Autopilot being activated by the driver (Nie et al., 2018). Research by Jepson et al. (2024), highlights the variety of cybersecurity threat vectors in heavy vehicles such as Electronic Logging Devices (ELDs) that could worm between vehicles before commanding it to disable the braking system. Additionally, Malik and Sun (2020) performed a comprehensive analysis of cyberattacks against connected and autonomous vehicles, using threat modeling to identify significant threats and simulating their real-life impact to highlight the necessity of developing effective defensive strategies. They identified scenarios such as over-the-air update attacks that result in a cycle of

reboots and deactivation of emergency assistance services, including turn-by-turn navigation and automatic crash response. The effect was manifested by obscuring the field of vision and disabling critical safety features leading to unexpected accidents.

Furthermore, just like their passenger vehicle counterparts, efforts are being made to modernize commercial vehicles in order to improve the safety, performance, and efficiency of the transportation of goods and materials. This is highly impactful since the trucking industry is often referred to as the backbone to the supply chain in the United States. Within the United States in 2023, the trucking industry was responsible for transporting more than 79.6% of all intrastate shipments and contributed $389.3 billion to U.S. gross domestic product (GDP) (Bureau of Transportation Statistics, 2019, 2022, 2023). The industry employs millions of people and ensures the delivery of essential goods, from raw materials to consumer products (Bureau of Labor Statistics, 2024). Modernization of commercial vehicles has led to the integration of advanced telematics, fleet management systems, and engine management applications, making these vehicles more connected than ever before (Singh et al., 2024). However, this increased connectivity also expands the attack surface, making commercial motor vehicles vulnerable to cybersecurity threats.

With that, the cybersecurity of commercial vehicles is a growing concern, as these vehicles are not only critical to the economy, but also pose significant safety risks if compromised. A review of commercial vehicle cybersecurity was published by the National Motor Freight Traffic Association, Inc. (NMFTA) in 2015 (updated in 2016) highlighting potential threats and exploits (National Motor Freight Traffic Association, 2016). Research by Stachowski et al. (2018) indicates that heavy vehicles share many cybersecurity vulnerabilities with passenger vehicles, but their larger size and the homogeneity of commercial truck fleets can make them more attractive targets for cyberattacks. The potential consequences of a cyberattack on a heavy vehicle can range from operational disruptions to catastrophic accidents, highlighting the need for robust cybersecurity measures (Mairaj ud din & Ahmed, 2024). In the case of a cyberattack induced accident, the consequences would be devastating due to the elevated risk of severe crash damage, injury, and fatalities present in heavy commercial vehicles (M. M. Ahmed et al., 2018; Oikawa et al.,

2021; Waskito et al., 2024; Xu et al., 2019). The importance of the trucking industry in transportation cannot be overstated. Trucks are indispensable for the delivery of goods across the country, connecting businesses with customers and suppliers. The trucking industry not only supports the economy but also ensures the availability of essential goods, making it a critical component of daily life. As the industry continues to modernize, addressing the cybersecurity challenges associated with commercial vehicles becomes increasingly important to safeguard both economic stability and public safety.

2.2.1 Driver Responses to Cyberattacks

Understanding how drivers respond to unexpected cyberattacks while operating a vehicle is essential to develop effective countermeasures and improve traffic safety. Previous research has primarily focused on the technological aspects of vehicle cybersecurity, often overlooking the human factors involved (Linkov et al., 2019). This thesis aims to bridge this gap by examining drivers' responses to a cyberattack in a real driving environment on the road. Lee et al. (2017) describes human factors engineering as "a discipline that considers the cognitive, physical, and organizational influences on human behavior to improve human interaction with products and processes" (Lee et al., 2017, p. 3). By investigating the impact of experience and information on driver behavior, this research seeks to provide insights into improving both driver safety and performance during an unexpected cyberattack.

Previous research in the field of vehicle cybersecurity has predominantly utilized surveys and driving simulators to study driver responses to cyberattacks. In an interview study, Lim and Rajivan (2023) concluded that drivers are more likely to respond to a vehicle cyberattack based on instincts if it appears to be an immediate threat. A simulator study by F. Zhang et al. (2019) suggests that most drivers do not know what to do if they were to experience an unexpected cyberattack while driving. Continuing their research, F. Zhang et al. (2023) investigated the effect of driving style on responses to unexpected vehicle cyberattacks in a driving simulator, finding that drivers with higher sensation-seeking tendencies may respond in a less risky manner. Another simulator study

by Wang et al. (2024) explored the impact of cybersecurity training on driver behavior, indicating that trained drivers exhibit more controlled responses during cyberattack scenarios. Additionally, research by Parker et al. (2022) examined the influence of driver awareness on response behavior in a driving simulator, showing that forewarned drivers tend to react more appropriately to cybersecurity threats. Research by Aliebrahimi and Miller (2023) highlight the importance of cybersecurity knowledge in determining whether a driver would take over an autonomous vehicle, validating their findings using a simulator as well. Each of these previous studies demonstrate the significant role of driver characteristics and training in shaping responses to cyberattacks. While these studies provide valuable insights and have informed the design of the present study, they are limited by the artificial conditions of driving simulators.

2.3 Gaps in Literature

Despite the substantial body of research on vehicle cybersecurity, several key gaps remain, particularly in the context of driver response to cyberattacks and commercial motor vehicles (CMVs).

One major gap in current vehicle cybersecurity research is the limited focus on the human. Much of the existing literature on vehicle cybersecurity has concentrated on the technical aspects of cyber-physical systems, often overlooking the critical role of human behavior and responses. Although studies have acknowledged humans as the “weakest link" in the cybersecurity chain, there is a lack of comprehensive research that integrates human behavior into the vehicle cybersecurity framework. This thesis addresses this gap by evaluating drivers’ responses to cyberattacks.

Another significant gap is the scarcity of real-world studies. Most of the existing research has been conducted in controlled, simulated environments, which may not accurately reflect real-world driving conditions. While simulator studies provide valuable insights, they often fail to capture the complexities, unpredictability, and uncertainty of the on-road driving environment; yielding a different perceived utility of safety as would be seen in the real world. This thesis fills this gap by conducting an on-road driving study with 50 participants, offering more realistic insights into driver behavior.

Additionally, there is a lack of focus on commercial vehicles in the current literature. While there is a growing body of research on cybersecurity threats to connected and autonomous vehicles, studies specific to CMVs are limited. Given the crucial role that the trucking industry plays in the transportation system and the economy, the potential consequences of cyberattacks on these vehicles are severe. By focusing on CMVs, this thesis contributes valuable knowledge to a critical, yet under-researched, area of vehicle cybersecurity.

Therefore, this thesis intends to reduce these gaps by providing a comprehensive examination of driver behavior and response to cyberattacks on CMVs, integrating human factors into the cybersecurity framework through a real-world driving study.

Chapter 3

Materials and Methods

An on-road driving experiment was conducted to evaluate drivers' response to an unexpected instrument cluster cyberattack. The study received IRB approval from the Colorado State University Institutional Review Board. Informed consent was obtained from each participant prior to study procedures.

3.1 Participants

The study included a total of 50 participants recruited from the local area of Fort Collins, Colorado. The inclusion criteria required participants to be over 18 years old and possess a valid U.S. driver's license. Participants were recruited through flyers, posters, direct advertising, and referrals. Recruitment efforts aimed at including approximately a third of the participants as experienced heavy vehicle operators, which was conducted by reaching out to local fire stations, bus operators, and commercial driver's license (CDL) training schools. Within the sample there were 18 (36%) participants who reported currently having a CDL or professional equivalent certificate, 4 (8%) report previously but not currently having one, and 28 (56%) never having one. Those who responded affirmatively to having a CDL were asked to specify the number of years they maintained the CDL or professional certification, with responses ranging from 1 to 48 years (Mean = 12.8, SD = 14.4). All participants were also asked if they had experience driving heavy trucks and/or large vehicles, for which 35 (70%) indicated yes, 14 (28%) indicated no, and 1 (2%) chose not to respond. Those who indicated they had experience with heavy vehicles were asked to describe their experience. The responses to this question were recorded as open-ended unstructured qualitative textual data. These responses guided the determination of the participant experience level.

As seen in Table 3.1, of the 50 drivers, 39 were male, 10 were female, and 1 identified as non-binary/third gender. Participants ranged in age from 19 to 69 years old (Mean = 34.8, SD =

15.6) with 3 choosing not to respond. Over the past five years, the average annual mileage among the drivers varied from less than 5,000 miles to more than 25,000 miles. Specifically, 6 (12%) participants reported driving less than 5,000 miles, 12 (24%) reported driving between 5,000 and 10,000 miles, 10 (20%) reported driving between 10,000 and 15,000 miles, 3 (6%) reported driving between 15,000 and 20,000 miles, 6 (12%) reported driving between 20,000 and 25,000 miles, and 13 (26%) reported driving more than 25,000 miles annually.

Table 3.1: Participant Summary Statistics

Category	**Count**
Total Participants	50
Gender	
Male	39 (78%)
Female	10 (20%)
Non-binary / Third Gender	1 (2%)
Age Category	
18 to 24	19 (38%)
25 to 34	9 (18%)
35 to 44	7 (14%)
45 to 54	3 (6%)
55 to 64	6 (12%)
65 to 74	3 (6%)
Prefer not to respond	3 (6%)
Mileage Category	
Less than 5,000 miles	6 (12%)
5,000 to 10,000 miles	12 (24%)
10,000 to 15,000 miles	10 (20%)
15,000 to 20,000 miles	3 (6%)
20,000 to 25,000 miles	6 (12%)
More than 25,000 miles	13 (26%)

3.1.1 Experimental Groups

This study employs a 3×2 multifactorial design to examine the effects of cyberattack threat information (three levels: Control, Aware, and Aware + Protocol; between-subject) and driving experience (two levels: Standard and Professional; between-subject) on driver response, as shown in Figure 3.1. Participants were allocated to the Control group first until its required number was

reached. Subsequently, participants were randomly assigned to the Aware group or the Aware + Protocol group. This method of group allocation ensured a balanced distribution of standard and professional drivers within each group. It also minimized the risk of participants in the Control group becoming aware of the cyberattack threat on the vehicle. This design allowed for the examination of the effects of awareness and experience level on driver response to a cyberattack, and the exploration of any potential interactions between the factors.

		Cyberattack Threat Information		
		Control	**Aware**	**Aware + Protocol**
Driving Experience	**Standard**	Control, Standard	Aware, Standard	Aware + Protocol, Standard
	Professional	Control, Professional	Aware, Professional	Aware + Protocol, Professional

Figure 3.1: Multifactorial Design Matrix

Cyberattack Threat Awareness Factor

Participants were divided into three groups based on their awareness of a potential cyberattack threat and provision of cyberattack response protocol, as shown in Table 3.2. The Control group (Group 1) received no information or guidance regarding the possibility of a cyberattack threat, leaving them unaware of the potential threat to the vehicle. They were instructed to drive and respond to situations normally as if the researcher was not in the vehicle with them. The Aware group (Group 2) was informed of a possible cyberattack threat with a message stating:

> For your group, there is a possible cyberattack threat on your vehicle. Whether or not the cyberattack occurs is unknown. If it does, where or when it occurs is unknown. If

it does occur, we ask that you respond to the situation as you normally would if the researcher was not in the vehicle with you.

Participants in this group were reassured, if they asked about the cyberattack, that it would not occur in a manner that would pose a risk to themselves or others on the road. The Aware + Protocol group (Group 3) was informed of a possible cyberattack threat and provided with a basic response protocol. Their message stated:

> For your group, there is a possible cyberattack threat on your vehicle. Whether or not the cyberattack occurs is unknown. If it does, where or when it occurs is unknown. In the case that it does occur, here is how you should respond.

The response protocol was provided to these participants as both a paper printout and computer slideshow, as seen in Figure 3.2. If they asked about the cyberattack, they were reassured that it would not occur in a manner that would pose a risk to themselves or others on the road.

Table 3.2: Cyberattack Threat Awareness Information by Group

Group	**Information Provided**
Control	During this drive, please drive and respond to situations normally as if the researcher was not in the vehicle with you.
Aware	For your group, there is a possible cyberattack threat on the vehicle. Whether or not the cyberattack occurs is unknown. If it does, where or when it occurs is unknown. If it does occur, we ask that you respond to the situation as you normally would if the researcher was not in the vehicle with you.
Aware + Protocol	For your group, there is a possible cyberattack threat on the vehicle. Whether or not the cyberattack occurs is unknown. If it does, where or when it occurs is unknown. In the case that it does occur, here is how you should respond (see Figure 3.2).

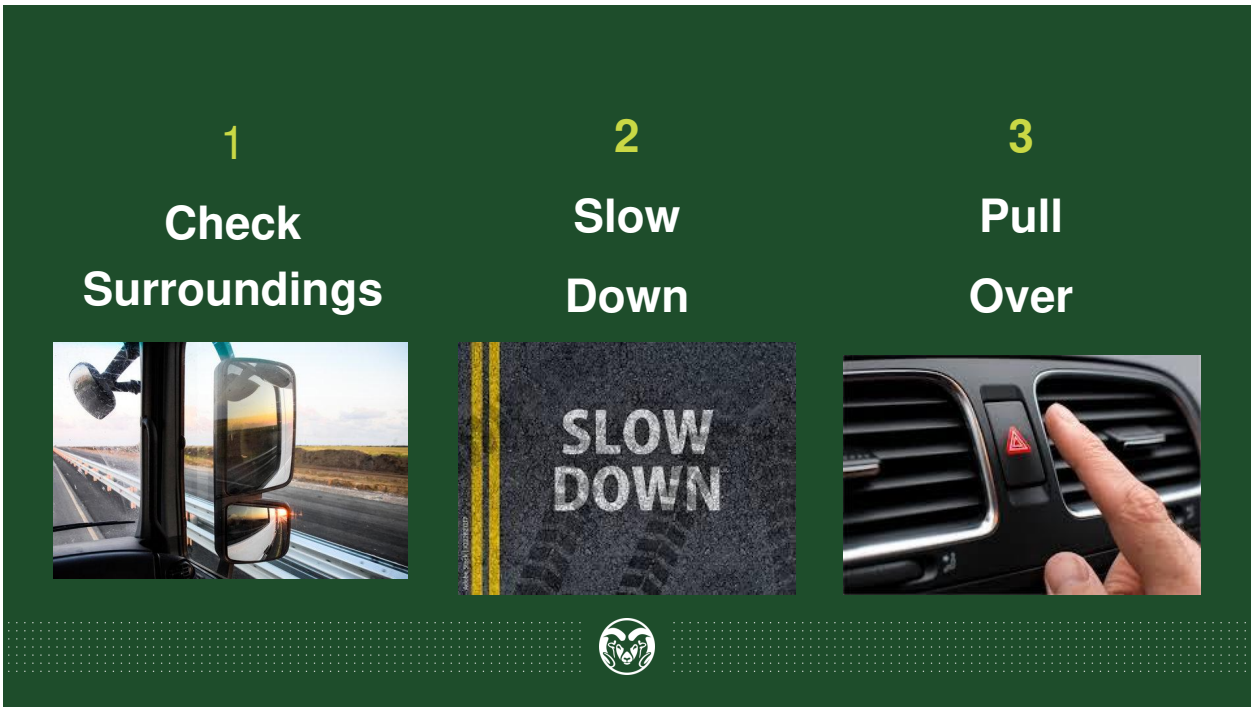


Figure 3.2: Cyberattack Response Protocol

Driving Experience Factor

Participants were classified into two categories based on their survey responses related to driving experience and background training: Standard and Professional. Those who fell into the Standard category included any participant who possessed a basic driver's license, specifically a Class C license in the United States. This group did not include any additional requirements beyond holding the Class C license.

Conversely, the Professional category was comprised of participants who held a current commercial driving license (CDL) and had substantial experience or training driving commercial motor vehicles. They reported an average annual mileage exceeding 5,000 miles. The Professional category also included individuals involved in career fields that do not require a CDL, therefore they were also categorized based on specific role descriptions and survey responses. The rationale behind this categorization was to ensure that those classified as professionals had both the necessary qualifications and practical experience, given that they routinely practiced or exercised their training. For instance, firefighters (N = 8) are exempt from requiring a CDL to operate any

fire apparatus, although they extensively train on the operation of heavy vehicles. This approach ensured that the distinction between professional and standard drivers was based on both their qualifications and practical driving experience.

Consequently, among the 50 participants, 19 were identified as professionally trained in heavy vehicle operation, while 31 had no professional training. The distribution of Driving Experience between each Cyberattack Threat Awareness group can be seen in Figure 3.3.

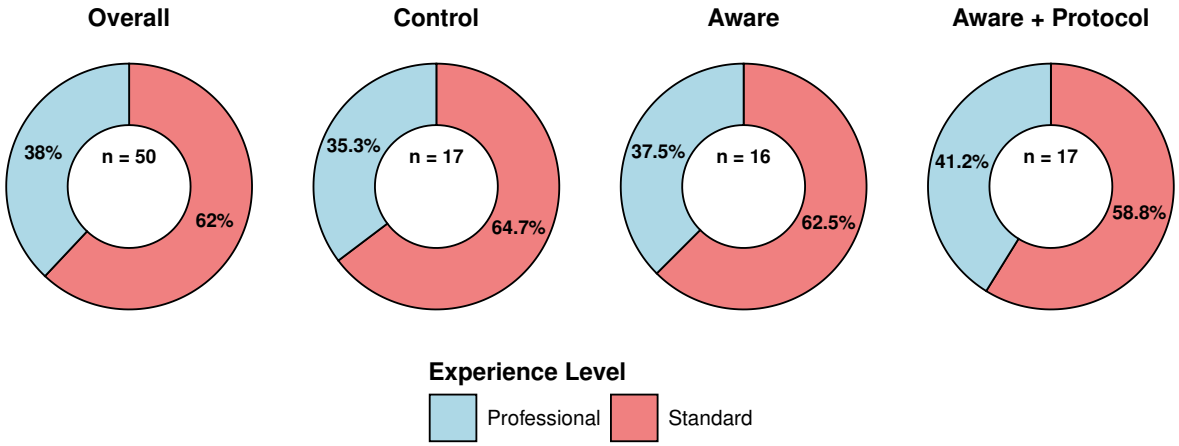


Figure 3.3: Distribution of Participants by Experience

Control Variables

To account for other potential influences on driver response, several control variables were included based on participants' self-reported responses to the survey. One of these was the Modified Manchester Driver Behavior Questionnaire (MMDBQ), which evaluated self-reported aberrant driving behaviors. This validated tool consists of ten statements about driving behaviors, with response options on a 6-point Likert scale ranging from "Never" to "Nearly all the time." Participants' responses were used to calculate a total score, with higher scores indicating more frequent aberrant driving behaviors. The average score was also calculated by dividing the total score by the total number of questions answered to account for any missed statements by the participants,

allowing for standardized comparisons. The MMDBQ has been widely used in research to predict accident involvement and offenses confirming its reliability and relevance (Sucha et al., 2014).

Additionally, the General Risk Propensity Score (GRiPS) was included to measure participants' general propensity for risk-taking behaviors. This scale consists of eight statements with response options on a 5-point Likert scale from "Strongly disagree" to "Strongly agree." Participants' responses were summed to calculate a total score, with higher scores indicating a greater propensity for risk-taking behaviors. Similar to MMDBQ, an average score was also calculated for each participant by dividing the total score by the total questions answered to account for any empty answers. This tool has been validated by D. Zhang et al. (2018) for its construct validity and predictive power and has been used in the transportation context (Pourfalatoun et al., 2023).

Finally, gender was controlled for to examine any gender-based differences in driver response, ensuring that any observed effects were not confounded by gender, and participants' age was also included as a control variable to account for potential age-related differences in driver response, providing a more accurate analysis of the main factors. Gender has been identified in previous studies as correlated with more aggressive driving behaviors (Nickkar et al., 2023) and risk-taking (J. Ahmed, Robinson, & Miller, 2024).

3.2 Experimental Equipment

The research vehicle used in this study is a 2014 Kenworth T270, classified as a medium heavy-duty vehicle (GVWR 26,000 lbs; Class 6), see Figure 3.4. This is the largest vehicle that can be driven without requiring a Commercial Driver's License (CDL). For reference, the truck is similar to what a typical person could rent from a moving company (e.g., U-Haul, Penske) with a standard Class C driver's license (i.e., no additional endorsement necessary). The vehicle is equipped with an automatic transmission, which means participants were not required to manually shift gears. The vehicle's systems communicate using the 250kbps SAE J1939 standard.

Vehicle data was acquired through the SAE J1939 CAN bus that is exposed on Pins C and D of the 9-pin diagnostics connector of the truck (J. Daily et al., 2021; J. S. Daily & Kulkarni,

2020). An additional Instrument CAN channel was recorded by splicing the instrument CAN wires and exposing it to a different channel for the recorders. Logs files were gathered using the Truck Cape with BeagleBone Black (J. Daily, 2020) and a CANLogger 3 (J. Daily, 2019). The BeagleBone Black, as shown in Figure 3.5, equipped with a heavy truck cape captures data through built-in vehicle sensors (e.g., wheel-based vehicle speed, engine speed, accelerator pedal position, etc.), and allows real-time monitoring on a laptop to ensure accurate data collection and storage. The CANLogger 3, as shown in Figure 3.6, collects the same data as the BeagleBone Black for redundancy. Additionally, a SparkFun NEO-M9N GNSS (Global Navigation Satellite System) module is employed to gather precise GNSS data, which is then transmitted through the CAN bus to the data loggers (J. Daily, 2023). This module provides reliable location tracking and heading data adding a form of redundancy to speed and acceleration data.

Figure 3.4: The CyberTruck Research Vehicle

Figure 3.5: Heavy Truck Cape with BeagleBone Black

Figure 3.6: CAN Logger 3

The RaceLogic VBOX 3i, a high-fidelity GPS-based vehicle data acquisition system, is also utilized to collect GNSS data. The VBOX 3i, as seen in Figure 3.7, is equipped with a dual antenna setup on the truck, differential GPS, and Kalman Filtering, which enhances the accuracy of location, speed, and heading measurements. Furthermore, the VBOX 3i features an inertial measurement unit (IMU) that records the vehicle's acceleration, pitch, yaw, and roll, providing comprehensive data on the vehicle's dynamics during the experiment.

Figure 3.7: Racelogic Vbox 3i

An Empatica E4 wristband, as shown in Figure 3.8, is used to collect physiological data from the driver, including heart rate, heart rate variability, and electrodermal activity (EDA) also known as galvanic skin response (GSR). Throughout various research domains, these measures have been demonstrated to be reliable indicators of stress realization via the autonomic nervous system, particularly in measuring driver stress (Miller & Boyle, 2015; Miller, 2013; Miller & Boyle, 2013). In a validation study, Schuurmans et al. (2020) supported the utilization of the Empatica E4 as a practical and valid tool for research on heart rate and heart rate variability. Moreover, in a real-world driving study, it was concluded that GSR signals could individually be a reliable source of data for stress measurement classification (Memar & Mokaribolhassan, 2021). These physiological measures allow us to identify the presence of stress states in the participants throughout the duration of the drive.

Figure 3.8: Empatica E4 Wristband

Each of the vehicle data collection tools was designed to function seamlessly via the CAN bus throughout the duration of the drive without interfering with the participants' ability to operate the vehicle. Similarly, the Empatica E4 wristband was worn by the participant, and wirelessly connected to the researchers phone through the Empatica E4 Realtime application. The setup ensured the collection of reliable and accurate data while maintaining the safety and comfort of the participants. All of the data streams contained an epoch timestamp, which facilitated merging the output from the disparate devices. A full overview and diagram of these data collection systems is provided in Biggs et al. (2024). The variables used in this study and corresponding data collection devices are shown in Table 3.3.

Table 3.3: Data Collection Devices

Data Collected	**Device**
CAN0 Engine Speed	Truck Cape with Beaglebone Black & CANLogger 3
Engine Speed	Truck Cape with Beaglebone Black & CANLogger 3
Accelerator Pedal Position	Truck Cape with Beaglebone Black & CANLogger 3
Wheel-Based Vehicle Speed	Truck Cape with Beaglebone Black & CANLogger 3
Time (CAN)	Truck Cape with Beaglebone Black & CANLogger 3
GNSS-Based Vehicle Speed	SparkFun NEO-M9N & RaceLogic VBOX 3i
Latitude	SparkFun NEO-M9N & RaceLogic VBOX 3i
Longitude	SparkFun NEO-M9N & RaceLogic VBOX 3i
Heading	SparkFun NEO-M9N & RaceLogic VBOX 3i
Time (GNSS)	SparkFun NEO-M9N & RaceLogic VBOX 3i
Heart Rate (HR)	Empatica E4
Heart Rate Variability (HRV)	Empatica E4
Electrodermal Activity (EDA)	Empatica E4
Time (Empatica)	Empatica E4

3.3 The Cyberattack

Cyberattacks can range from targeting the software that processes visual data and road infrastructure to physically tampering with the vehicle's hardware (Lima et al., 2016). In a previous study by Burakova et al. (2016), commercial vehicle network cyberattacks were carried out where they affected the SAE J1939 network to affect vehicle displays and performance. In a similar manner, the cyberattack for this research affected the network to achieve the desired effects. The cyberattack was designed to maximize its saliency to the driver by incorporating both visual and auditory cues. The cyberattack exclusively impacted the instrument cluster display and audio system of the vehicle, and did not affect any control systems in the vehicle (e.g., brakes, speed, etc). This is possible because the instrument cluster is on a controller area network (CAN) that is different from the main CAN used for SAE J1939 standard communications on the research vehicle. Two different alerting modalities were used to ensure that the driver would become immediately alerted that a cyberattack, or at least something adverse, was occurring. Hence, this approach was designed such that the analysis would capture how drivers chose to respond, rather than confounding that their response may have been influenced by not noticing the attack was occurring.

Visually, the speedometer and tachometer needles were manipulated to drop to zero from their correct positions. Additionally, all the dashboard warning lights, including the stop engine light, service engine light, brake light, ABS light, seatbelt light, turn signal lights, parking brake light, and others, were activated simultaneously. This deliberate activation of multiple warning indicators was intended to create a sense of urgency and confusion, simulating a severe vehicle malfunction scenario. Figure 3.9 shows the vehicle's instrument cluster during the cyberattack.

Figure 3.9: Instrument Cluster Cyberattack

The auditory cue consisted of a medium-pitched tone that beeped at a frequency of twice per second. This beep was similar to the sound typically heard when the driver's door is open while the keys are still in the ignition. This persistent and distinctive audio signal was designed to capture the driver's attention even within the noisy environment presented by the vehicle, ensuring the alert was unmistakable.

The cyberattack was executed using a man-in-the-middle attack technique, where a preprogrammed Arduino Teensy board was installed behind the instrument cluster and connected to the research laptop with a USB cable. This setup allowed for the injection of alternate messages through the CAN bus via a separate channel, ensuring that only the instrument cluster was affected, independent of standard vehicle systems. The execution of the cyberattack was discretely controlled by the researcher in the passenger seat. The cyberattack was activated at the same time and location for each participant while driving westbound on Laporte Avenue west of the Overland Trail intersection as seen in Figure 3.10. This moment is about halfway through the 20-mile drive on a low traffic one-mile stretch of road that had shoulder allowing space to pull off at any moment. The roadway conditions can be seen in Figure 3.11. The posted speed limit along this road was 40-mph.

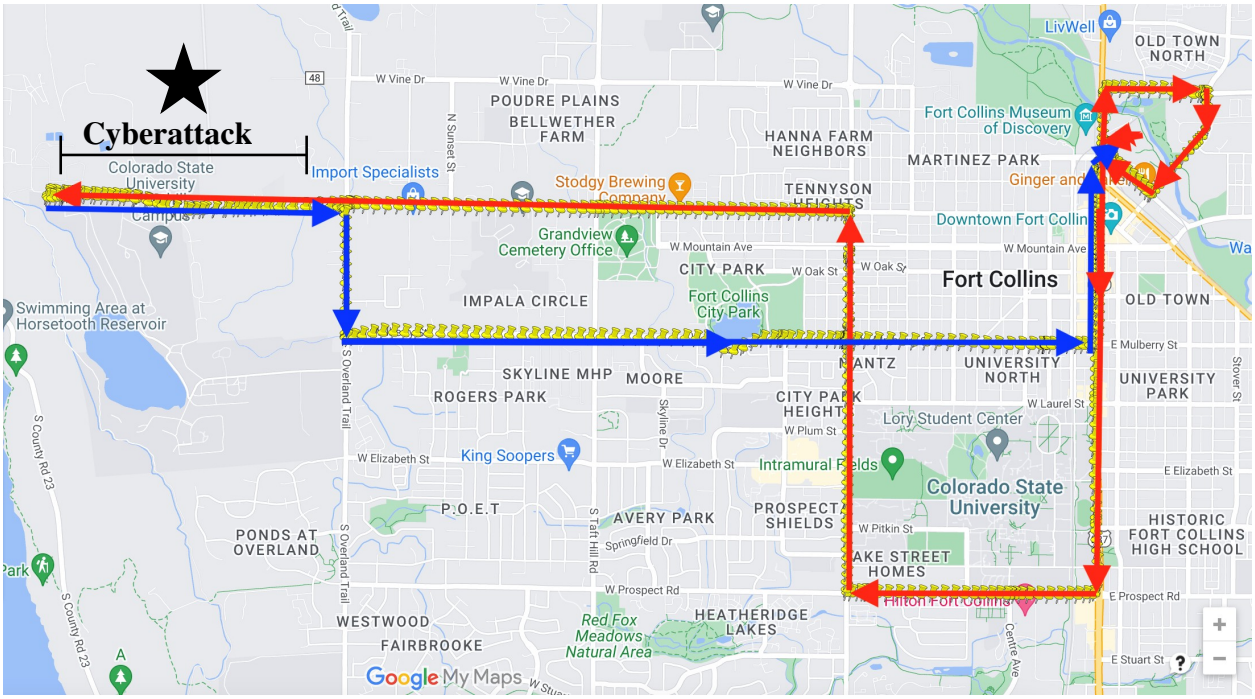


Figure 3.10: Research Route

If the driver decided to continue driving through the cyberattack, it remained active for 60 seconds before automatically deactivating. If the driver decided to pull over to the side of the road

and bring the vehicle to a complete stop, the cyberattack remained activated for at least five seconds before being shut off by the researcher in the passenger seat. The cyberattack was not executed in the presence of other vehicles, cyclists, pedestrians, or obstacles within or near the path of another vehicle.

Figure 3.11: Sample of Road Conditions with CyberTruck

3.4 Experimental Procedure

Participants were recruited through flyers, posters, direct advertising, and referrals. For reference, the interest flyer that was distributed is located in Appendix A. Interested individuals completed a Microsoft form, providing essential information such as their first name, contact details, and availability, as well as their familiarity with any ongoing research at the Colorado State University, Department of Systems Engineering, and their experience with driving heavy vehicles or box trucks. All study sessions were completed during the summer with the first participant in May 2024 and the final participant in September 2024.

The initial meeting took place at the Colorado State University Powerhouse Energy Campus building. Participants were briefed on the vehicle, study route, and told that the purpose of the study was to develop models that could uniquely identify drivers based on their driving styles, as outlined in the informed consent document shown in Appendix B. Due to the nature of single-blinded experiment, details regarding the cyberattack were concealed as required by the group the participant was assigned to. Participants were given the opportunity to ask any remaining questions before signing the informed consent document, indicating their voluntary willingness to participate in the study. Following this, the researcher and participant transitioned to the research vehicle parked in the campus parking lot.

To ensure the comfort and safety of all participants, those with no prior experience driving heavy vehicles were given ample time to practice. The practice session began with an explanation and demonstration of the vehicle's functions. Participants practiced accelerating, braking, and turning in a controlled parking lot for as long as they desired. Once they indicated readiness, they practiced driving on open roads near the campus. Practice sessions typically took between 15 to 60 minutes. No data was collected during the practice session. Upon feeling comfortable and prepared, participants drove to the starting position, where data collection commenced. Prior to beginning the drive, baseline physiological data was collected. Participants' baseline physiological data was recorded using the Empatica E4 wristband for a minimum of five minutes, with longer periods accepted if necessary. Once, the baseline reading was complete, and the researcher confirmed that all CAN bus data from the vehicle was accurately recorded via the research laptop, the participant begin driving the research route as seen in Figure 3.10.

Emphasis was placed on maintaining realistic driving behavior to ensure the research study's validity. Participants were instructed to drive as if the researcher was not present to avoid any potential distraction or influence. The researcher, seated in the passenger seat, provided navigation instructions with sufficient lead time before each turn. Participants were reminded to respond to driving situations as they normally would if the researcher were not in the vehicle and were advised not to turn off the truck at any point, as this would halt data collection. If participants

felt uncomfortable or unsafe at any moment during the drive, they were informed that they could end the drive, and the researcher would take over driving the vehicle back to the study origin. The researchers were prepared to switch positions with the participants if needed but could not take immediate control to prevent an accident. All participants completed their drives without needing the researcher to intervene.

At the conclusion of the drive, participants completed a post-drive survey on their mobile devices through the online Qualtrics survey platform. Following the survey, the researcher debriefed the participants, explaining the nature of the study and the technical details regarding the administration of the cyberattack within the vehicle. This debriefing session was not recorded as data for participant response. During the debriefing session, participants had the opportunity to voice any questions or concerns regarding the research study. Once the debrief was complete, participants received a payment of $20 in the form of an Amazon gift card. If they withdrew from the study after the practice drive or at any point thereafter, they still received full compensation.

3.5 Post-Drive Survey

Following the completion of the on-road driving session, participants were administered a post-drive survey to gather comprehensive data regarding their driving experience and reactions to the cyberattack. The survey, as shown in Appendix C, was conducted using Qualtrics XM, a web-based survey software, and was completed on a mobile smartphone immediately after the drive. Participants were given as much time as needed to complete the survey to ensure thorough and reflective responses. The survey was structured to be self-administered to minimize any potential researcher bias, although participants could ask clarifying questions if necessary. The researcher was present in the vicinity but did not monitor the participants directly to avoid any undue influence on their responses.

At the beginning of the survey, each participant was assigned a unique participant research ID number by the researcher. This number served as an identifier to track responses while maintain-

ing anonymity and confidentiality. The researcher also recorded the participant's group number, indicating the experimental group to which they were assigned (Group 1, Group 2, or Group 3).

The survey began by collecting demographic information, including the participant's gender and age. This information was essential to categorize the participants and analyze the data based on different demographic factors. Additionally, participants were asked about their driving experience, specifically if they held a Commercial Driver's License (CDL) or any professional equivalent certification. If they answered affirmatively, they were further prompted to specify the duration of their certification. Participants were also asked whether they had experience driving heavy trucks or large vehicles, with a follow-up prompt for those who answered "Yes" to briefly describe their experience. This question helped categorize participants into Standard and Professional experience categories, enhancing the analysis of their driving behavior and reactions. Furthermore, participants were prompted for information about their annual mileage, traffic violations, and crashes over the past year to assess their driving history and risk exposure.

To evaluate self-reported aberrant driving behaviors, the survey included the Modified Manchester Driver Behavior Questionnaire (MMDBQ). This assessment tool consisted of ten statements about driving behaviors, with response options on a 6-point Likert scale ranging from "Never" to "Nearly all the time." Additionally, the General Risk Propensity Score (GRiPS) was included to measure participants' general propensity for risk-taking behaviors. This assessment consisted of eight statements with response options on a 5-point Likert scale from "Strongly disagree" to "Strongly agree."

In the context of the cyberattack, the survey asked participants to reflect on their driving experience during the specific segment of the drive where the attack occurred. Four statements assessed their perceptions of the vehicle's reliability, expected behavior, safety, and the detection of any anomalies. Participants rated these statements on a 5-point Likert scale ranging from "Strongly disagree" to "Strongly agree". Finally, participants were prompted to briefly describe what they noticed about the vehicle during the drive, providing qualitative insights into their experience.

The duration of survey responses ranged between 5 to 15 minutes to complete. To ensure confidentiality and anonymity, no personally identifiable information was stored within the survey responses. Instead, each participant's responses were linked to their unique participant research ID number and group assignment. This design ensured the integrity of the data while respecting the privacy of the participants.

3.6 Data Cleaning

This section presents the detailed process for the data cleaning to ensure the accuracy and reliability of the analysis. All data cleaning and analysis were conducted using R in RStudio.

3.6.1 Survey Data Cleaning

Data Source: The data source for the survey included raw responses collected through Qualtrics XM, which were exported to a Comma-Separated Value (CSV) file format for further processing.

Data Cleaning Procedures: The initial step in data cleaning involved structuring the textual free-form responses for specific variables such as age, CDL years, and driving years. For example, participants who entered responses like "7 1/2 years" for CDL years had their responses converted to a consistent numeric format such as "7.5" years. Similarly, responses indicating the year participants received their driver's license (e.g., 2014) were converted to the number of years they had been driving (e.g., "10" years). This standardization ensured consistency and enabled comparison across all participant responses.

Next, participants were categorized based on their driving experience. Those with a current CDL who also reported experience driving heavy vehicles and an average annual mileage of more than 5,000 miles were classified as "professional." Additionally, participants who reported experience driving heavy vehicles and indicated involvement in firefighting (e.g., responses containing the word "fire") were also classified as "professional." Participants who did not meet the criteria for professional experience were classified as "standard." The reason for this categorization was to assign professional experience to individuals who have the professional training and routinely prac-

tice or exercise their training. For example, if someone currently has a CDL but only drives heavy or commercial motor vehicles once a year, they would not necessarily be considered a professional in the context of this research study. Similarly, someone who had a CDL many years ago, but not currently, has likely not received formal training or practice recently, thus would be categorized as standard. This approach demonstrates a specific methodology for categorizing professional drivers based on both qualification and practical experience.

The survey responses were then scored using predefined mappings for various questionnaires included in the survey. For the Modified Manchester Driver Behavior Questionnaire (MMDBQ), responses ranging from “Never" to “Nearly all the time" were mapped to scores from 1 to 6. Similarly, the General Risk Propensity Score (GRiPS) responses were mapped from “Strongly disagree" to “Strongly agree" with scores ranging from 1 to 5. If a participant chose not to select an option for any of the statements, a score of NA was recorded for that response. Each participant’s responses were converted to numeric scores based on these mappings. The total score for MMDBQ and GRiPS was calculated by summing each participant’s numeric scores for all statements. An average score was then calculated for each participant by dividing their total score by the number of statements they chose to respond to. If a participant did not select a response for a statement and received a score of NA, that statement was excluded when calculating the average score.

In the context of the cyberattack segment, participants’ perceptions were assessed through specific statements about the vehicle’s reliability, expected behavior, safety, and detection of anomalies. Responses to these statements were mapped to scores from 1 to 5, corresponding to “Strongly disagree" to “Strongly agree." Similar to MMDBQ and GRiPS a total and average score was calculated for this section.

3.6.2 Vehicle and GNSS Data Cleaning

Data Source: The vehicle level data was collected from multiple sources including: Truck Cape with BeagleBone Black, CANLogger 3, SparkFun NEO-M9N GNSS module, and Racelogic VBOX 3i.

Data Cleaning Procedures: The raw data from Truck Cape with BeagleBone Black and CANLogger 3 was collected in the J1939 Standard. This data was then converted to plain text format using the corresponding Parameter Group Numbers (PGN) and Suspect Parameter Numbers (SPN). A total of 108 variables were collected through the CAN bus, including critical metrics such as Accelerator Pedal Position, Wheel-Based Vehicle Speed, and Engine Speed CAN0. Each of these variables was recorded at a unique sampling rate and contained its own timestamp in epoch Unix time, representing the precise moment the variable was sampled. In instances where the Truck Cape failed to collect raw data, CANLogger 3 data was utilized instead, following the same collection method.

The raw data from the Racelogic VBOX 3i devices encompassed 76 variables, such as latitude, longitude, and velocity. This data included a single timestamp column that represented the 24-hour time in UTC for all data sampled.

To unify the vehicle data for each participant, the data from both sources was exported into a singular CSV file. The first step in preprocessing involved converting the timestamp columns for each variable to a readable POSIXct time structure in UTC time zone. Subsequently, each variable was downsampled to 1-second intervals, creating a unified timing column for all variables. During downsampling, the mean, standard deviation, maximum, and minimum were calculated over each 1-second interval to monitor potential data loss. Based on the new timing column for the CAN bus data, a time series column was established, starting at 0 and continuing at 1-second intervals throughout the data length. For any data sampled at a rate slower than 1 second, NA values were assigned for the 1-second intervals when no data was collected.

Similarly, the VBOX data timestamp column was converted to POSIXct time structure in UTC, and the data was downsampled to 1-second intervals. The mean, standard deviation, maximum, and minimum were computed for each variable over these intervals to identify any potential data loss.

After downsampling, the data from all sources needed to be aligned, as the devices did not start recording simultaneously. To ensure proper alignment, the cross-correlation between CAN bus

Wheel-Based Vehicle Speed, SparkFun Neo GNSS speed, and VBOX GNSS speed was calculated. The data sets were then synchronized based on a specified shift amount that achieved a cross-correlation of 0.99 or greater. This alignment process was documented, and the shift amount was recorded in the data file as device shifted and shift amount for each subject.

Subsequently, the period when the cyberattack was active was determined and stored within each subject's data file. For participants 1 to 12, the active period was identified based on the longitude and latitude of the set cyberattack start point, knowing the attack would remain active for up to 60 seconds or until the vehicle speed reduced to 0 km/hr for five seconds. For participants 13 to 50, the Engine Speed CAN0 data was used to identify discrepancies between the tachometer reading displayed on the instrument cluster and the actual engine speed recorded internally by the vehicle. The cyberattack was marked as active when the values differed and inactive when they matched. For instance, if Engine Speed as measured internally by the vehicle sensors was recording a value of 750, but Engine Speed CAN0 as displayed on instrument cluster reports a value of 0 that indicates the cyberattack is active. It is important to note that these discrepancies between the instrument cluster and the actual engine speed were an outcome of the cyberattack, not because of an error in data coding. Since the CAN0 engine speed represents the visual display provided to the participant, and the cyberattack resulted in the speedometer showing 0 mph, this was indicative of the cyberattack, as previously seen in Figure 3.9.

Finally, the cumulative distance traveled during the drive was calculated using the latitude and longitude data, employing the Haversine formula, and this information was stored in the data file. The Haversine formula is a common approach to calculate the distance between two points on a sphere, using latitude and longitude, which is relevant to account for the curvature of the Earth. Each subject's cleaned and processed data was saved in individual CSV files, with ID, Subject number, and Group number added for identification. Finally, all participants down sampled and aligned data were combined into a single comprehensive CSV file.

3.6.3 Empatica E4 Wristband Data Cleaning

Data Source: The Empatica E4 wristband data was collected to monitor physiological responses, including Electrodermal Activity (EDA), Blood Volume Pulse (BVP), Inter-Beat Interval (IBI), Skin Temperature (TEMP), and Acceleration (ACC).

Each subject's Empatica E4 data was stored in unique CSV files. The format for these CSV files is as follows:

- The first row is the initial time of the session expressed as a Unix timestamp in UTC.
- The second row is the sample rate expressed in Hz.

The CSV files included:

- **TEMP.csv**: Data from the temperature sensor, expressed in degrees Celsius (°C).
- **EDA.csv**: Data from the electrodermal activity sensor, expressed in microsiemens (μS).
- **BVP.csv**: Data from the photoplethysmograph.
- **ACC.csv**: Data from the 3-axis accelerometer sensor, measured in the range [-2g, 2g], recorded in units of 1/64g. Data from the x, y, and z axes are in the first, second, and third columns, respectively.
- **IBI.csv**: Time between individual heartbeats extracted from the BVP signal. The first column represents the time (relative to the initial time) of the detected inter-beat interval, expressed in seconds (s). The second column is the duration in seconds (s) of the detected inter-beat interval.
- **HR.csv**: Average heart rate extracted from the BVP signal. The first row is the initial time of the session, expressed as a Unix timestamp in UTC, and the second row is the sample rate expressed in Hz.

Data Cleaning Procedures: The raw data from the Empatica E4 wristband was initially exported as CSV files for each participant. An initial review of these files was conducted to ensure completeness and to identify any corrupted files or missing data segments. To maintain consistency across all data sources, the timestamp columns in the raw data were converted to POSIXct time structure in the UTC time zone. This conversion facilitated the uniformity needed for data integration.

The physiological data variables, recorded at different sampling rates, were downsampled to 1-second intervals to align with other data sources. During this downsampling process, the mean, standard deviation, maximum, and minimum values were calculated for each variable over the 1-second interval to monitor any potential data loss or inconsistencies. This restructuring allowed for the data from each variable to be combined seamlessly into a single CSV file based on these common time columns.

3.7 Data Analysis

The cleaned survey, vehicle, GNSS, and physiological data was combined into a single CSV file that could be uniformly analyzed.

3.7.1 Stop Event Dependent Variable

Definition: Data analysis evaluated the dependent variable defined as stop event. This binary variable indicates whether participants stopped their vehicle during the cyberattack. A stop event is specifically defined as an instance where the vehicle's speed reduced to 0 km/h for a duration of at least five consecutive seconds. Data for this analysis was collected from the vehicle's CAN Bus Wheel-Based Vehicle Speed, SparkFun Neo GNSS speed, and VBOX GNSS speed, ensuring accurate measurement of vehicle speed and the precise timing of any stop events.

Analytical Methods: To analyze the stop event data, Firth's Logistic Regression was employed. This method was chosen due to the preliminary assessment revealing perfect separation in the dataset, where 100% of standard and professional participants in Group 3 (Aware + Protocol)

stopped. Perfect separation leads to issues with traditional logistic regression models, such as infinite estimates of the coefficients. Firth's Logistic Regression is a penalized likelihood approach that effectively handles small sample sizes or cases of perfect separation by applying a penalty to the likelihood, reducing bias in parameter estimates and providing more reliable results under these conditions (Puhr et al., 2017).

Hypothesis: The hypothesis for this analysis was that there would be no significant differences in the predicted probability of stop events between the different experimental groups. This expectation was based on the saliency of the simulated cyberattack conditions: a simultaneous failure of both the speedometer and tachometer, the activation of all dashboard warning lights including a prominent red "Stop" light, and a constant beeping alert. These conditions were designed to create a highly alarming scenario, making it unlikely that drivers would continue without stopping to assess the situation. Essentially, most participants, regardless of their group assignment or experience level, would stop their vehicle within the first 60 seconds due to the combined effects of instrument failure, warning lights, and auditory alerts.

3.7.2 Distance Traveled Dependent Variable

Definition: The dependent variable in this analysis is distance traveled during the cyberattack. This variable measures the total distance (in meters) that each participant traveled from the onset of the cyberattack until the end of it being active. Distance traveled is calculated as the difference between the cumulative distances recorded at the start and end of the cyberattack. Importantly, this includes scenarios where participants stop their vehicles during the cyberattack. If a participant stops, the cyberattack ceases, as does the determination of the distance traveled during the cyberattack. For instance, if a participant does not stop, the cyberattack continues for the full 60 seconds, resulting in the total distance traveled over that period. Conversely, if a participant stops the vehicle after 15 seconds, the cyberattack ends at that moment, and the distance reflects only the travel from the start until the stop.

Analytical Methods: To analyze the distance traveled data, an Analysis of Covariance (ANCOVA) was employed. This method was chosen because it allows the inclusion of both categorical predictors and continuous covariates. The categorical variables include group assignment, experience level, and gender. The continuous covariates include age, average GRiPS score, and average MMDBQ score. ANCOVA helps to control for significant covariates, providing a more precise estimation of the effects of group assignment and driver experience on the distance traveled. Through backward elimination, the model can be refined by removing non-significant variables to focus on more impactful ones. Once these were identified, a post-hoc analysis was performed by comparing estimated marginal mean distances traveled between different variables, confirming the findings of the analysis.

Hypothesis: The hypothesis for this analysis was that there would be a significant difference in the distance traveled during the cyberattack between the different experimental factors and level. Under regular conditions given the speed limit (40-mph) and the maximum duration of the cyberattack (60 seconds), the maximum distance traveled would be around ~1,072 meters. Therefore, it was expected that participants in Group 3 (Aware + Protocol) would travel a shorter distance compared to participants in Group 1 (Control) and Group 2 (Aware). This expectation is based on the notion that being aware of the cyberattack threat and having a response protocol will prompt drivers to reduce vehicle speed and stop more quickly, thereby reducing the total distance traveled. Additionally, it was expected that professional drivers would traveled a shorter distance than standard drivers. In essence, it was hypothesized that group assignment and driver experience would significantly reduce the distance traveled during the cyberattack.

3.7.3 Reaction Time Dependent Variable

Definition: The dependent variable for this analysis is the time to react to the cyberattack. This variable measures the time (in seconds) it takes participants to initiate a response after the onset of the cyberattack. Research by Gold et al. (2013) evaluated reaction time based on the driver's braking and steering inputs. In the present study, reaction time is determined by measuring the

time between the start of the cyberattack and the participant fully releasing their foot from the accelerator pedal. The reaction time data is recorded by the SAE J1939 SPN 91 - Accelerator Pedal 1 position. In scenarios where the participant does not release the accelerator pedal, the reaction time is 60 seconds, which is the maximum duration of the cyberattack.

Analytical Methods: To analyze the reaction time data during the cyberattack, an Analysis of Covariance (ANCOVA) was employed. Similar to distance traveled analysis, this method was chosen because it allows the inclusion of both categorical predictors (group, experience, and gender) and continuous covariates (age, average GRiPS score, and average MMDBQ score). The analysis was performed with all variables before being refined through the process of backward elimination. The first step in this reduction process involved eliminating non-significant factors, starting with those with the highest p-values. By removing non-significant covariates, the model becomes more parsimonious, making it easier to interpret the effects of the key factors on reaction time. Once significant factors were identified, a post-hoc analysis was conducted to explore pairwise comparisons between the remaining variables. Tukey's HSD (Honestly Significant Difference) post-hoc test was used to adjust for multiple comparisons, confirming the directionality of the relationships.

Hypothesis: The hypothesis for this analysis was that there would be a significant difference in reaction times between the different experimental groups. Specifically, it is anticipated that participants in Group 3 (Aware + Protocol) will exhibit shorter reaction times compared to participants in Group 1 (Control) and Group 2 (Aware). This hypothesis is grounded in the expectation that being aware of the cyberattack threat and having a defined response protocol will prompt drivers to respond more swiftly to the onset of the cyberattack. In essence, it is hypothesized that the combination of awareness and a structured protocol would enhance the speed of participants' reactions. Additionally, it was expected that driver's experience would also play a significant role in influencing reaction times, with professional drivers likely to react faster than standard drivers.

3.7.4 Cautionary Behavior Dependent Variable

Definition: The dependent variable in this analysis is Cautionary Behavior. This variable encompasses actions taken by drivers in response to perceived threats or dangers, aimed at enhancing their visual, auditory, and vehicular control capabilities, or reducing speed swiftly (Kotseruba & Tsotsos, 2021). Examples of such behaviors include checking mirrors, turning down the radio, ceasing conversations with passengers, adjusting their seat position for better visibility, positioning their hands on the steering wheel for improved control, and reducing speed.

For the purpose of this research, cautionary behavior is specifically measured via the Accelerator Pedal Position data from the vehicle. This parameter represents the ratio of the actual position of the operator's speed request input device (the accelerator pedal) to its maximum position, with the unit of measurement being percentage. Cautionary Behavior is defined using two methods: (1) instances where the accelerator pedal position is zero for at least one second, and (2) instances where the Accelerator Pedal Position is decreasing, which is determined by negative values in the derivative of Accelerator Pedal Position. The inclusion of this second measure allows for capturing moments when the driver is easing off the accelerator to reduce speed. These instances are summed to yield a total cautionary behavior score for each participant. To account for the varying lengths of cyberattacks, the total cautionary behavior score is divided by the total duration of the cyberattack for each participant. This provides the proportion of time the driver exhibited cautionary behaviors during the cyberattack, signaling the driver's intent to decelerate or stop in response to a perceived threat.

Analytical Methods: The analysis of Cautionary Behavior was conducted using Analysis of Covariance (ANCOVA). This statistical method was chosen because it allows the inclusion of both categorical predictors (group, experience, and gender) and continuous covariates (age, average GRiPS score, and average MMDBQ score). The ANCOVA model included group assignment, driver experience, gender, age, average MMDBQ score, and average GRiPS score as factors. Tukey's HSD (Honestly Significant Difference) post-hoc test was used utilized to adjust for multiple comparisons, ensuring that observed differences between levels were statistically significant.

Hypothesis: The hypothesis for this analysis was that there would be statistically significant differences in cautionary behaviors within the different experimental groups and levels of driving experience. Specifically, it is anticipated that the proportion of cautionary behaviors will increase from the Control group to the Aware group, and from the Aware group to the Aware + Protocol group. Additionally, professional drivers are expected to demonstrate a higher proportion of cautionary behavior compared to standard drivers. This hypothesis is grounded in the rationale that awareness of the cyberattack threat, coupled with a predefined response protocol, will prompt drivers to engage in more cautionary actions. Furthermore, professional drivers, due to their extensive experience, are presumed to be more adept at responding to unexpected events with cautionary behavior.

3.7.5 Electrodermal Activity Dependent Variable

Definition: Electrodermal Activity (EDA) refers to electrical changes measured at the skin's surface (Posada-Quintero & Chon, 2020). These changes are often associated with emotional arousal, cognitive load, or physical exertion. EDA is divided into two main components: tonic and phasic. Tonic EDA, or Skin Conductance Level (SCL), represents the baseline level of skin conductance in the absence of specific stimuli and varies slowly over time. Phasic EDA, on the other hand, includes Skin Conductance Responses (SCRs), which are abrupt increases in skin conductance in response to specific stimuli like sight, sound, or anticipation. For the analysis, two baseline periods were established: the initial baseline (the first 60 seconds of data) and the pre-attack baseline (the 60 seconds immediately before the start of the cyberattack). The mean, standard deviation, minimum, and maximum EDA values were calculated for both baseline periods. Comparing these baselines helped understand any changes in participants' physiological states before the cyberattack.

Analytical Methods: Next, a baseline correction was made by calculating the relative change in the EDA values recorded during the cyberattack. This was done by subtracting the mean pre-attack baseline EDA from each raw EDA data point during the cyberattack. For example, if a

subject's average pre-attack baseline EDA is two, and during the cyberattack segment a value of five was recorded, the difference between the baseline and cyberattack value is three. This means that there was an increase in EDA during the cyberattack that could indicate an increase in emotional arousal or cognitive load. Using this data, the analysis of EDA was performed using Analysis of Covariance (ANCOVA) because it allows for the inclusion of categorical predictors (group, experience, and gender) and continuous covariates (age, average GRiPS score, and average MMDBQ score). Following the outcome of the initial model, backwards elimination was performed resulting in only continuous variables to remain. Therefore, a linear regression was used to analyze the final continuous variable.

Hypothesis: The hypothesis for this analysis was that there would be statistically significant differences in EDA during the cyberattack between the experimental groups and levels of experience. It was anticipated that the the Control group will have the greatest increase in EDA from pre-attack baseline and the Aware + Protocol group will have the lowest increase in EDA from pre-attack baseline. This is because it was expected that as cyberattack threat awareness increases and a cyberattack response protocol is provided, drivers would be less surprised by the cyberattack therefore experiencing less of an emotional arousal. Similarly, professional drivers were predicted to have a reduced EDA response compared to standard drivers due to their increased exposure to vehicle malfunctions and training.

Chapter 4

Results

4.1 Participant Risk Distribution

To examine the risk distribution across different groups and experience levels, the Modified Manchester Drivers Behavior Questionnaire (MMDBQ) and the General Risk Propensity Scale (GRiPS) average scores were analyzed. The aggregated summary statistics for the whole participant pool are presented in Table 4.1.

Table 4.1: Summary of MMDBQ and GRiPS Scores

Survey	Mean	Std Dev	Median	Min	Max	Sample Size	Possible Range
MMDBQ	1.86	0.382	1.80	1.1	3.0	50	1-6
GRiPS	2.64	0.880	2.62	1.12	4.12	50	1-5

The Modified Manchester Driver Behavior Questionnaire (MMDBQ) scores have an average of 1.86 with a standard deviation of 0.382, and the General Risk Propensity scores (GRiPS) have an average of 2.64 with a standard deviation of 0.880. The median MMDBQ score is 1.80, ranging from 1.1 to 3.0, while the median GRiPS score is 2.62, ranging from 1.12 to 4.12. The sample size for both surveys is 50. These results suggest that participants, on average, demonstrate moderate to low driver behavior and risk propensity.

The distributions of MMDBQ and GRiPS scores by group and experience are depicted in Figure 4.1. As highlighted by the figure, these results indicate a minimal spread in risk scores between groups and experience levels. The relatively narrow range and clustering around the mean suggests that participants' risk behaviors are fairly consistent across the sample. This uniformity in risk scores ensures that any differences observed in other variables are less likely to be confounded by varying risk propensities among participants.

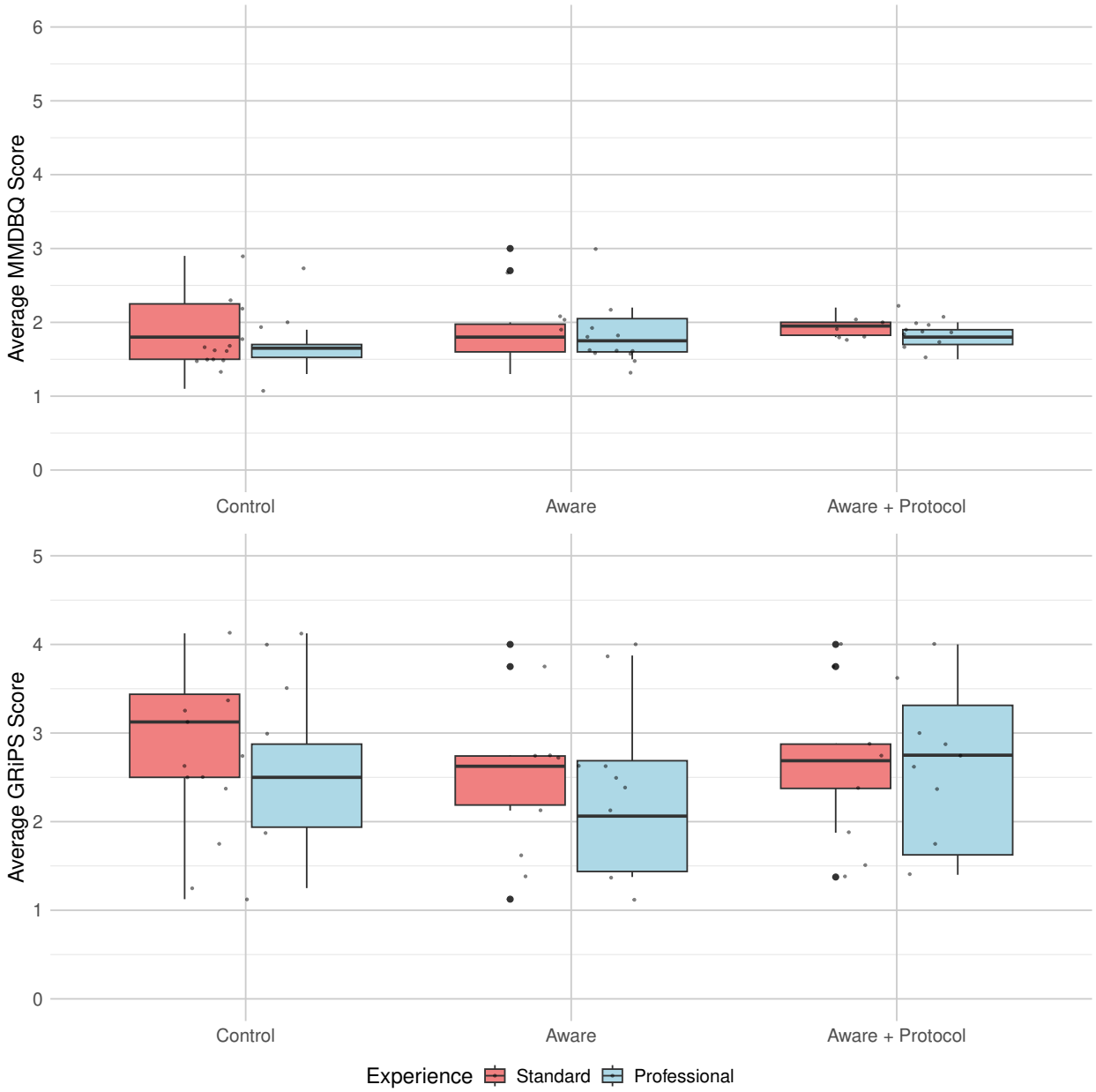


Figure 4.1: Distribution of average MMDBQ and GRiP scores by Group and Experience.

The ANOVA for the average MMDBQ scores, as shown in Table 4.2, indicate no significant main effects or interaction, with p-values of 0.812 for Group, 0.094 for Experience, and 0.785 for the Group $\times$ Experience interaction. The residuals accounted for the majority of the variance, indicating unexplained variability.

Similarly, ANOVA for the average GRiPS scores, as seen in Table 4.3, reveals no significant effects, with p values of 0.643 for Group, 0.278 for Experience, and 0.885 for the Group $\times$ Experience interaction. The residuals again represented a substantial portion of the variance. Results for both ANOVAs revealed that the differences in risk scores between the groups and experience levels were not statistically significant, indicating a relatively homogeneous distribution of risk across the sample.

Table 4.2: MMDBQ ANOVA Results for Group and Experience

Variable	**Degrees of Freedom**	**Sum of Squares**	**Mean Square**	**F-value**	**p-value**
Group	2	0.060	0.0301	0.201	0.812
Experience	1	0.439	0.4393	2.934	0.094
Group $\times$ Experience	2	0.073	0.0365	0.243	0.785
Residuals	44	6.588	0.1497	–	–

Table 4.3: GRiPS ANOVA Results for Group and Experience

Variable	**Degrees of Freedom**	**Sum of Squares**	**Mean Square**	**F-value**	**p-value**
Group	2	0.73	0.3644	0.445	0.643
Experience	1	0.99	0.9882	1.208	0.278
Group $\times$ Experience	2	0.20	0.1006	0.123	0.885
Residuals	44	35.99	0.8179	–	–

4.2 Driver Response

4.2.1 Stop Event Results

In the Control group, the proportion of stop events varied considerably between Standard and Professional drivers. As seen in Table 4.4, only 1 out of 11 Standard drivers stopped during the cyberattack, resulting in a proportion of 0.0909, or 9.09%. In contrast, 5 out of 6 Professional drivers stopped, yielding a proportion of 0.833, or 83.3%.

The Aware group also showed variability in the proportions of stop events between the two types of drivers. Among Standard drivers, 3 out of 10 stopped, corresponding to a proportion of 0.3, or 30%. All 6 Professional drivers in this group stopped, resulting in a proportion of 1, or 100%.

In the Aware + Protocol group, both Standard and Professional drivers exhibited the highest proportions of stop events. All 10 Standard drivers and all 7 Professional drivers in this group stopped their vehicles during the cyberattack, each group achieving a proportion of 1, or 100%. These results indicate a clear pattern: the group assignment and driver experience significantly influence the likelihood of stopping during a cyberattack. The Aware + Protocol group, regardless of the driver's experience level, demonstrated a perfect stop rate of 100%. Professional drivers generally showed higher proportions of stopping compared to Standard drivers across all groups. These trends are depicted in Figure 4.2.

Table 4.4: Proportion of Stop Event by Group and Experience

Group	**Experience**	**Total Stop Events**	**Total Drivers**	**Proportion Stop Events**
Control	Standard	1	11	0.09
Control	Professional	5	6	0.83
Aware	Standard	3	10	0.30
Aware	Professional	6	6	1.00
Aware + Protocol	Standard	10	10	1.00
Aware + Protocol	Professional	7	7	1.00

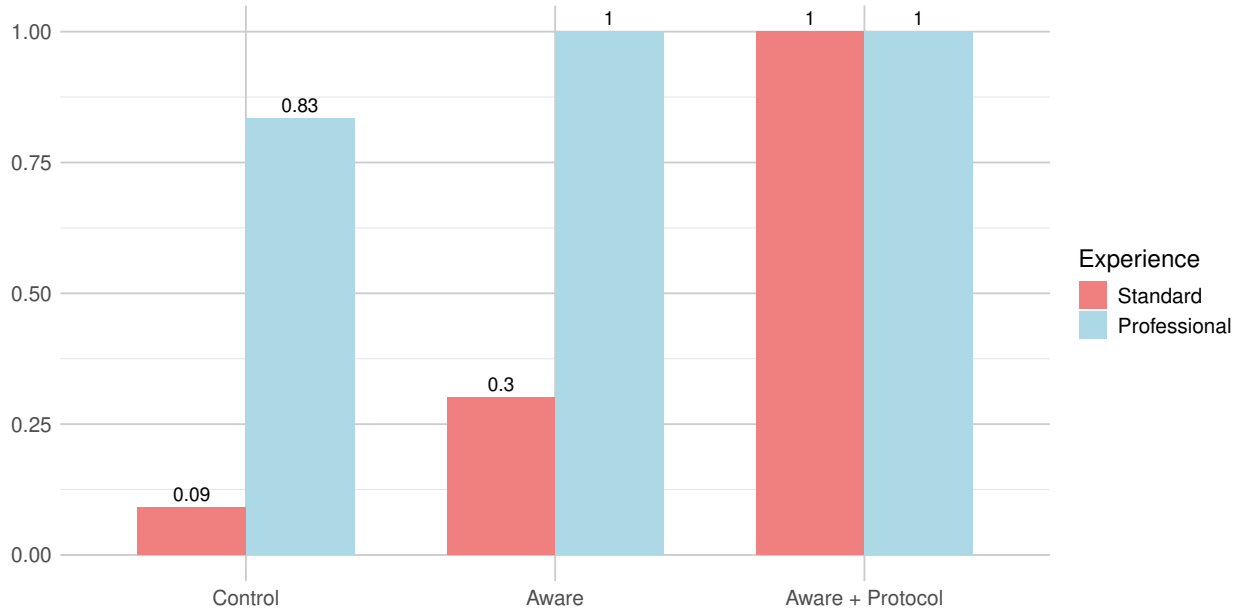


Figure 4.2: Proportion of Stop Events by Group and Experience

To understand the influence of various factors on the likelihood of drivers stopping during a cyberattack, Firth's penalized logistic regression model was employed, including several potential predictors: age, gender, average MMDBQ score, average GRiPS score, group, and driver experience. The initial model aimed to evaluate the impact of all these predictors simultaneously. Upon fitting this model, several variables, such as age, gender, average MMDBQ score, and average GRiPS score, did not significantly predict stopping behavior. The coefficients for age (-0.059, p = 0.198), gender (Male: -0.369, p = 0.737; Non-binary: -2.051, p = 0.411), MMDBQ score (-0.701, p = 0.539), and GRiPS score (-0.370, p = 0.604) all had high p-values, indicating that these factors did not substantially influence the likelihood of a driver stopping.

Given these results, the backward elimination method was used to refine the model. In this process, the non-significant variables were systematically removed from the model to focus on the predictors that had the most substantial impact. As shown in Table 4.5, the refined model ultimately included Group and Experience. Using the refined model, the likelihood of a driver stopping their vehicle based on their assigned group (Control, Aware, or Aware + Protocol) and their experience level (Standard or Professional) was evaluated.

The intercept showed a baseline likelihood of stopping for a Standard driver in the Control group (i.e., the model intercept), with a log odds of -2.10 (p = 0.0024). The log odds of stopping increased by 1.39 for drivers in the Aware group compared to the Control group, although this increase was not statistically significant (p = 0.144). However, for drivers in the Aware + Protocol group, the log odds of stopping increased significantly by 5.15 compared to the Control group ($p < 0.0001$), indicating a much higher likelihood of stopping when drivers are both aware and have a defined cyberattack response protocol. Furthermore, the experience level of the drivers played a significant role. Professional drivers had log odds of stopping that were 3.57 units higher than Standard drivers ($p < 0.0001$), indicating a significantly higher likelihood of stopping. These findings were statistically significant, underscoring the importance of driver experience in stopping behavior.

Table 4.5: Firth's Penalized Logistic Regression Model Results for Stop Events

Variable	**Coeff.**	**Std Error**	**Lower CI**	**Upper CI**	**Chi-Sq**	**p-value**
Intercept	-2.102	0.851	-4.326	-0.066	9.250	0.0024
Aware	1.390	0.985	-0.452	3.791	2.136	0.1439
Aware + Protocol	5.151	1.665	2.525	10.214	21.046	$< .0001$
Professional Driver	3.569	1.088	1.618	6.292	16.840	$< .0001$
Model Fit						
Likelihood Ratio Test: $\chi^2(3) = 34.779$, $p < .0001$ *Wald Test:* $\chi^2(3) = 16.042$, $p = 0.001$						

In addition to the regression analysis, the predicted probabilities of stopping for each combination of group and experience level were calculated based on the regression output, as seen in Figure 4.3. In the Control group, Standard drivers had a low predicted probability of stopping at 10.89%, while Professional drivers had a much higher predicted probability of 81.26%. In the Aware group, Standard drivers had a moderate predicted probability of 32.92%, with Professional drivers showing a significantly higher probability of 94.57%. In the Aware + Protocol group, both Standard and Professional drivers exhibited extremely high predicted probabilities of stopping, at 95.48% and 99.87%, respectively. The overall predicted probabilities reinforced the trend that the

combination of awareness and protocol significantly enhances the likelihood of stopping, with the Aware + Protocol group having the highest overall probability at 97.67%. These results highlight the critical role of group assignment and driver experience in influencing stopping behavior during a cyberattack.

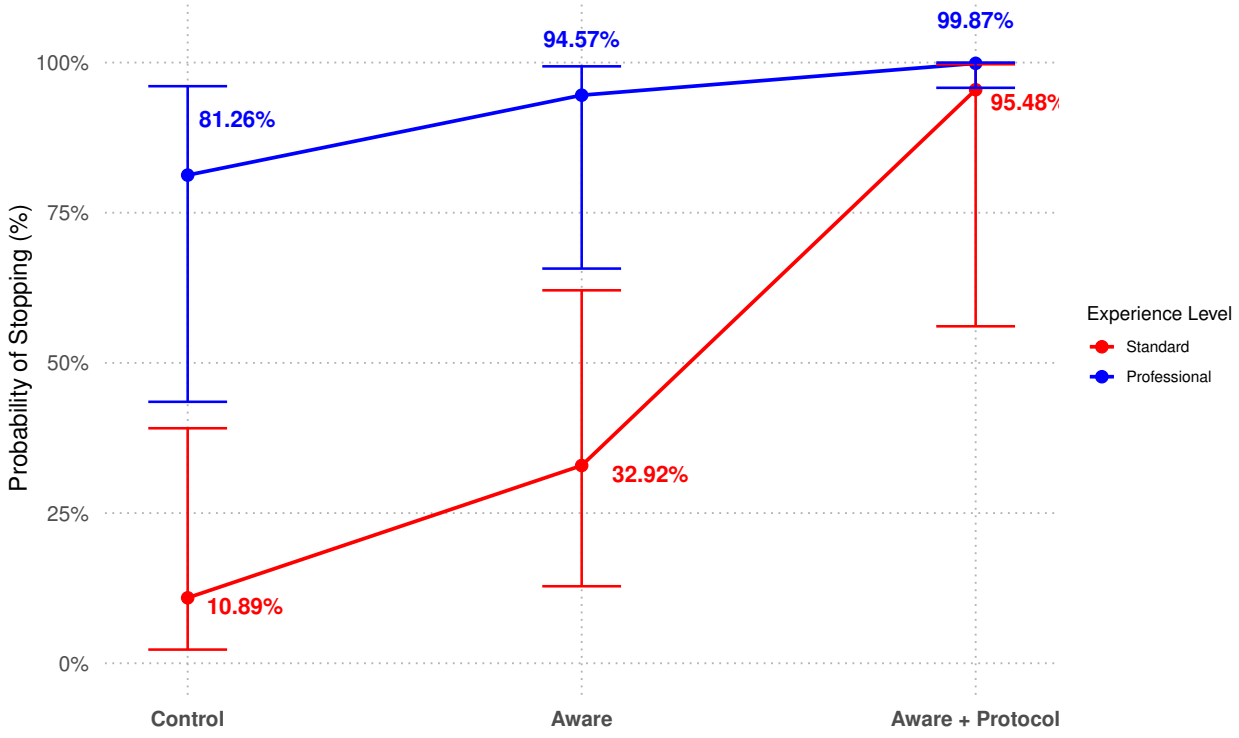


Figure 4.3: Predicted Probability of Stopping by Group and Experience

4.2.2 Distance Traveled Results

Figure 4.4 shows the mean distance traveled during cyberattack for each group and driving experience level; demonstrating the decreasing trend in distance traveled based on Cyberattack Threat Awareness group and Experience level. Similarly, Figure 4.5 shows mean distance traveled during the cyberattack based on Gender; demonstrating difference between Male and Female participants.

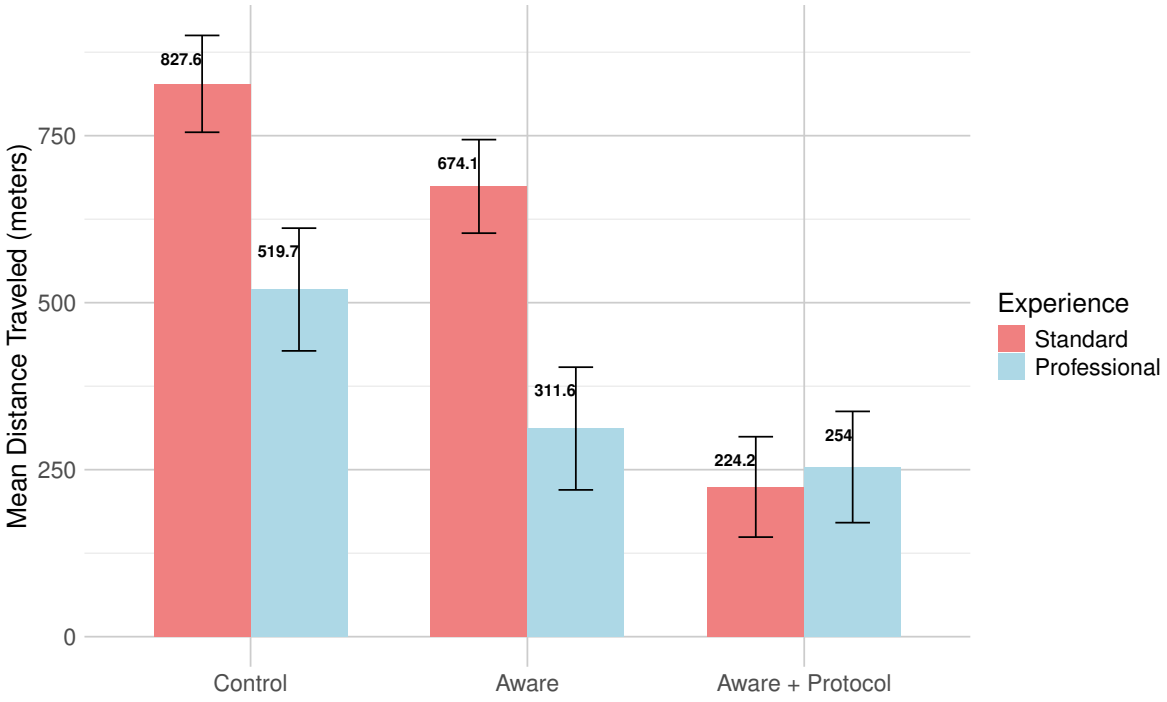


Figure 4.4: Mean Distance Traveled by Group and Experience

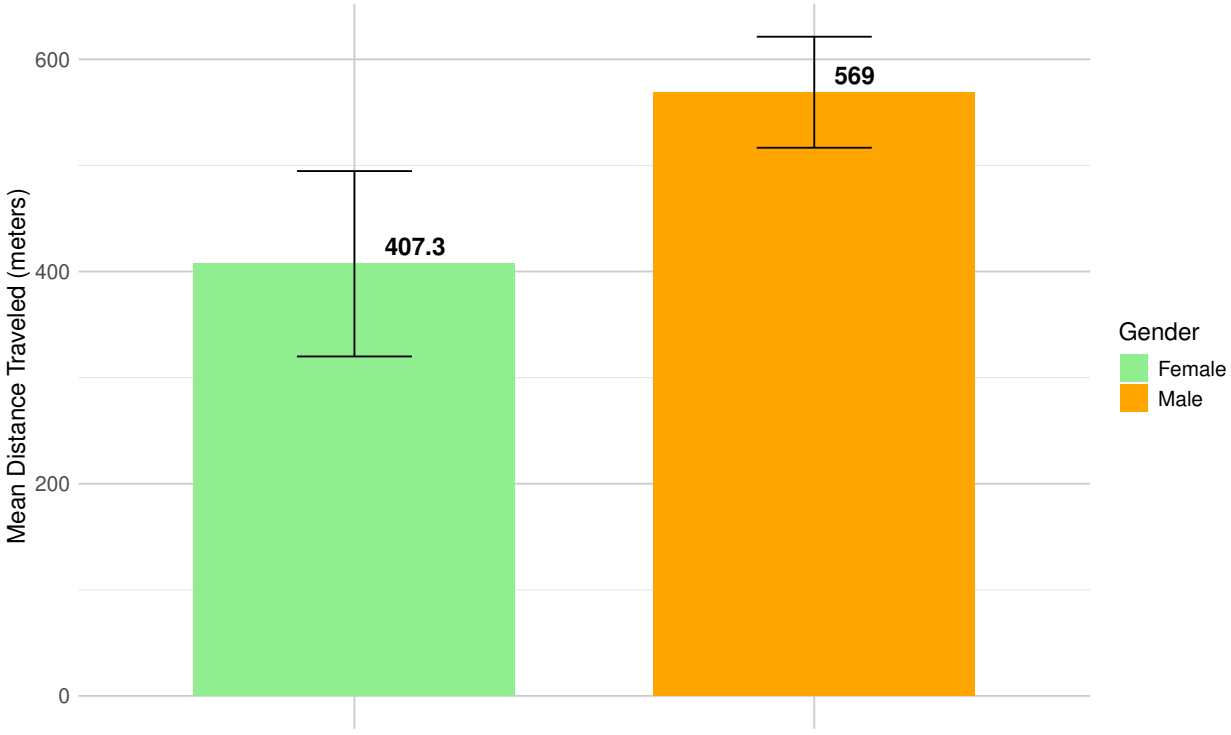


Figure 4.5: Mean Distance Traveled by Gender

Statistical analysis of distance traveled began with an analysis of covariance (ANCOVA) model that included age, gender, group, experience, average MMDBQ score, and average GRiPS score as predictors. The initial model results indicated that age (p = 0.940), average MMDBQ score (p = 0.234), and average GRiPS score (p = 0.729) were not statistically significant predictors of the total distance traveled during the cyberattack. Given the lack of significance, age, average MMDBQ, and average GRiPS were removed from the model. The revised model included the categorical variables of gender, group, and experience as predictors. This model showed that both group (F(2,42) = 20.658, $p < 0.0001$) and experience (F(1, 42) = 11.029, p = 0.003) were highly significant, while gender was marginally not significant (F(1,42) = 4.466, p = 0.053).

In the final ANOVA model, group, experience, gender, and the interaction between group and experience were included to determine their effects on the total distance traveled during a cyberattack, as seen in Table 4.6. The results indicated that male drivers traveled significantly farther than female drivers (F(1,42) = 4.666, p = 0.041). Group assignment emerged as a significant factor, with highly significant results (F(2,42) = 20.658, $p < 0.0001$), indicating a substantial impact on the distance traveled. Additionally, driver experience was found to be a significant predictor (F(1,42) = 11.029, p = 0.002), with professional drivers traveling significantly farther than standard drivers. The interaction between group and experience also proved to be significant (F(2,42) = 3.748, p = 0.032), suggesting that the effect of group on distance traveled varied depending on the driver's experience level.

Table 4.6: Distance Traveled ANOVA Results

Variable	**Degrees of Freedom (Df)**	**Sum of Squares (Sum Sq)**	**Mean Square (Mean Sq)**	**F-value**	**p-value**
Gender	1	208,053	208,053	4.466	0.041
Group	2	1,924,848	962,424	20.658	< 0.0001
Experience	1	513,800	513,800	11.029	0.002
Group:Experience	2	349,240	174,620	3.748	0.032
Residuals	42	1,956,692	46,588		

Using the final model, Estimated Marginal Means (EMMs) were computed to understand the adjusted mean values of total distance traveled during the cyberattack. EMMs offer an adjusted comparison between different levels of predictors such as gender, group, and experience. As seen in Table 4.7, the results indicated that, on average, male drivers traveled a greater distance (EMM = 525, SE = 35.5) compared to female drivers (EMM = 412, SE = 69.6). These EMMs are adjusted over the levels of group and experience, ensuring that the comparison between genders accounts for variations due to these factors. The confidence intervals suggest that the difference in distance traveled between genders is statistically significant, with males traveling farther than females on average.

Table 4.7: Estimated Mean Distance Traveled by Gender

Gender	**Estimated Mean (EMM)**	**Standard Error (SE)**	**Degrees of Freedom (Df)**	**Lower 95% CI**	**Upper 95% CI**
Female	412	69.6	42	272	553
Male	525	35.5	42	453	597

When examining the interaction between group and experience, the results elucidate variations in distance traveled. For example, standard drivers in the Control group traveled the farthest (EMM = 828, SE = 72.5), while standard drivers in Aware + Protocol traveled the least (EMM = 224, SE = 75.1). Professional drivers in Control also traveled more (EMM = 520, SE = 91.9) compared to professional drivers in Aware + Protocol (EMM = 254, SE = 83.3). Each estimated marginal mean for these pairwise combinations of group and experience are shown in Table 4.8. This analysis highlights the significant impact of group assignment and experience on the total distance traveled during a cyberattack, with notable differences depending on the combination of these factors.

Table 4.8: Estimated Mean Distance Traveled by Group and Experience

Group	Experience	Est. Mean	Std Error	Df	Lower CI	Upper CI
Control	Standard	828	72.5	42	681.3	974
Aware	Standard	674	70.0	42	532.8	815
Aware + Protocol	Standard	224	75.1	42	72.6	376
Control	Professional	520	91.9	42	334.3	705
Aware	Professional	312	91.9	42	126.2	497
Aware + Protocol	Professional	254	83.3	42	85.9	422

4.2.3 Reaction Time Results

To understand the factors that influence reaction time during a cyberattack, an analysis of covariance (ANCOVA) model was used that included the following predictors: group, experience, age, gender, average MMDBQ score, and average GRiPS score. The results showed that several variables, including age ($p = 0.402$), gender ($p = 0.402$), and average GRiPS score ($p = 0.427$), were not significant predictors of reaction time. Given the lack of significance, these variables were removed from the model. The revised model included group, experience, and average MMDBQ score as predictors. This model showed that group ($p = 0.002$) was highly significant, while experience ($p = 0.550$), and average MMDBQ score ($p = 0.557$) were not significant. Given these results, another iteration of backward elimination was performed to further refine the model, systematically removing non-significant variables to focus on the most impactful predictors.

In the final ANOVA model, group and experience were retained to determine their effects on reaction time. As seen in Table 4.9, the results indicated that group assignment was a significant factor, with an F-value (2, 46) of 6.892 and a p-value of 0.002, indicating a substantial impact on reaction time. However, level of experience did not have a significant effect ($p = 0.421$). Despite its lack of statistical significance, experience was retained in the model due to its theoretical importance and to control for potential confounding variables, ensuring a comprehensive and robust analysis.

Table 4.9: Reaction Time ANOVA Results by Group and Experience

Variable	Degrees of Freedom (Df)	Sum of Squares (Sum Sq)	Mean Square (Mean Sq)	F-value	p-value
Group	2	4,489	2,244.7	6.892	0.002
Experience	1	215	214.6	0.659	0.421
Residuals	46	14,983	325.7		

Using the final ANOVA model a Tukey HSD Post-Hoc Test was performed, as shown in Table 4.10. These results indicate that group assignment significantly influences reaction time, with notable differences observed between specific groups. Specifically, participants in the “Aware + Protocol" group demonstrated significantly faster reaction times compared to those in the “Control" group (-22.765, p = 0.002). The comparison between the “Aware" and “Control" groups were marginally not significant (-14.169, p = 0.073), while the difference between the "Aware + Protocol" and "Aware" groups was not significant (-8.596, p = 0.366). The level of experience did not show a significant impact on reaction times in this analysis (-4.263, p = 0.422).

Table 4.10: Tukey HSD Post-Hoc Test Results for Reaction Time

Comparison	Difference	Lower Bound	Upper Bound	Adjusted p-value
(Control) → (Aware)	-14.169	-29.393	1.055	0.073
(Control) → (Aware + Protocol)	-22.765	-37.756	-7.773	0.002
(Aware) → (Aware + Protocol)	-8.596	-23.820	6.629	0.366
(Standard) → (Professional)	-4.263	-14.848	6.321	0.422

In addition to the Tukey HSD Post-Hoc Test, the predicted reaction times for each Cyberattack Threat Awareness group were calculated based on the ANOVA model output. The Control group had a predicted reaction time of 30.29 seconds, the Aware group had a predicted reaction time of 16.12 seconds, and the Aware + Protocol group had a significantly reduced predicted reaction time of 7.53 seconds, as shown in Figure 4.6. These results suggest that awareness of the cyber-

attack threat and the presence of a response protocol have a positive effect on participant reaction times, regardless of experience level. The findings highlight the importance of both awareness and protocol measures in improving reaction times during an unexpected vehicle cyberattack.

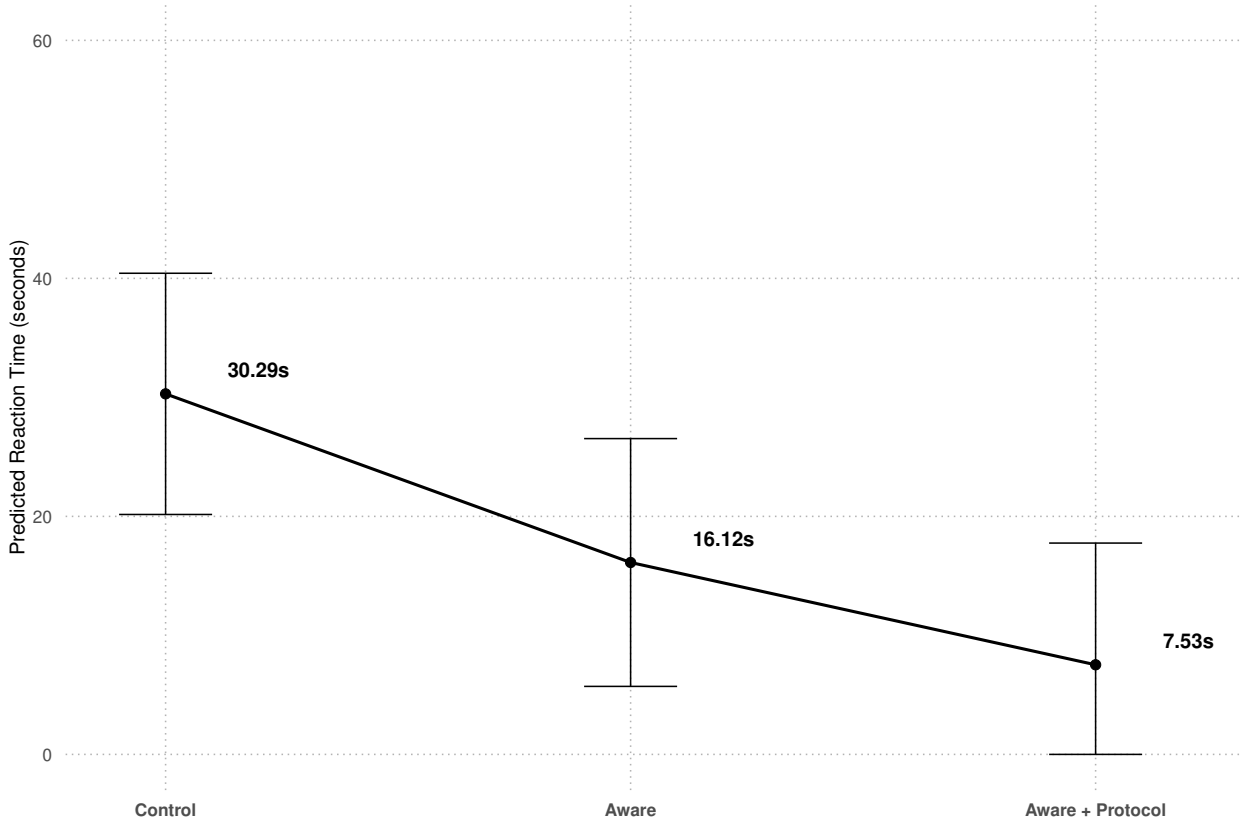


Figure 4.6: Predicted Reaction Time by Group

4.2.4 Cautionary Behavior Results

In the Control group, Standard drivers exhibited cautionary behaviors during 53% of the cyberattack duration, while Professional drivers did so for 68.6%. In the Aware group, Standard drivers had a mean cautionary behavior rate of 62.8%, and Professional drivers had a rate of 80.3%. The Aware + Protocol group showed the highest rates, with Standard drivers at 89.6% and Professional drivers at 86.6%. This trend is depicted in Figure 4.7. As cyberattack threat awareness increased

and the cyberattack response protocol was introduced, there was an increase in the proportion of cautionary behaviors exhibited during the cyberattack.

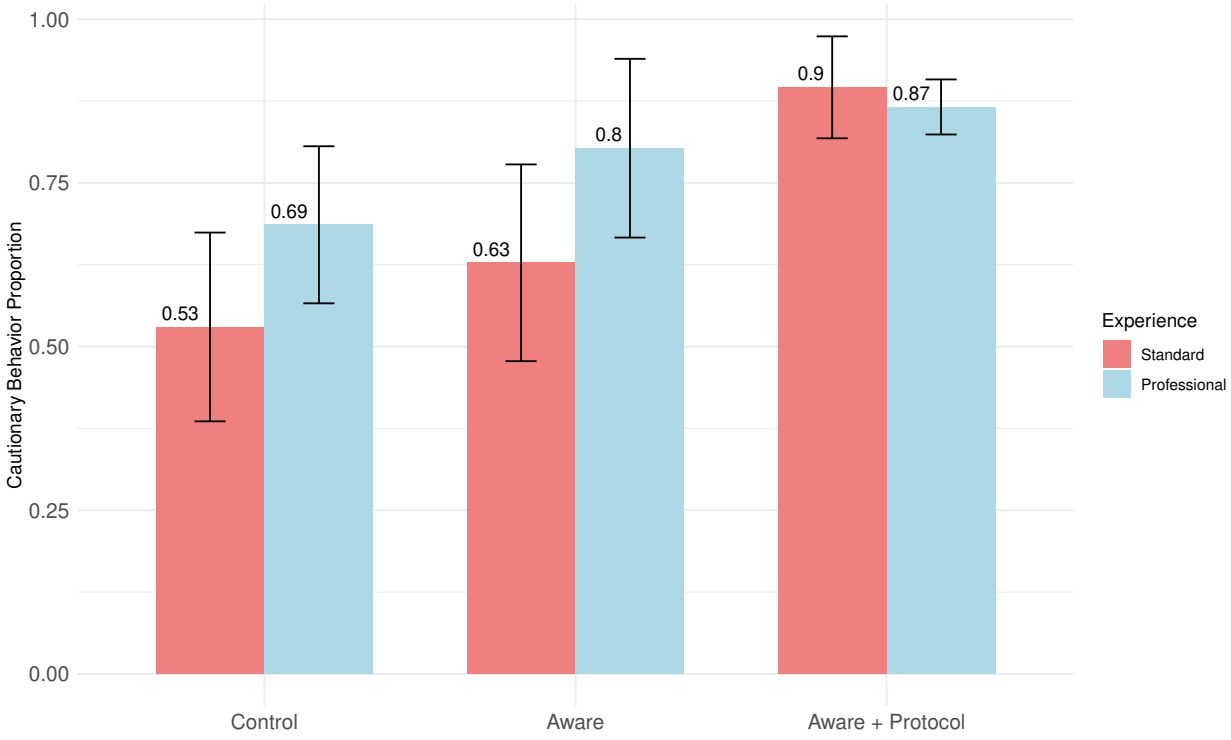


Figure 4.7: Mean Proportion of Cautionary Behavior by Group and Experience

The statistical analysis of Cautionary Behavior began with an Analysis of Covariance (ANCOVA) model that included group, experience, gender, age, average MMDBQ score, and average GRiPS score as predictors. The initial model results indicated that gender ($p = 0.806$), age ($p = 0.269$), average MMDBQ score ($p = 0.105$), and average GRiPS score ($p = 0.513$) were not statistically significant. However, group ($F(2, 38) = 21.248$, $p < 0.0001$) and experience ($F(1, 38) = 7.837$, $p = 0.008$) emerged as significant. Given these results, a backward elimination approach was performed, starting with the removal of non-significant variables to focus the model while retaining the significant predictors. The revised model included the variables group and experience. As seen in Table 4.11, the final model showed that both group ($F(2, 46) = 19.03$, $p < 0.0001$) and experience ($F(1, 46) = 7.08$, $p = 0.011$) remained significant.

Table 4.11: Cautionary Behavior ANOVA Results

Variable	Degrees of Freedom (Df)	Sum of Squares (Sum Sq)	Mean Square (Mean Sq)	F-value	p-value
Group	2	0.7039	0.3520	19.03	< 0.0001
Experience	1	0.1310	0.1310	7.08	0.0107
Residuals	46	0.8509	0.0185	–	–

These results indicate that group assignment significantly influences the proportion of cautionary behaviors, with notable differences observed between specific groups, as shown in Table 4.12. Specifically, participants in Aware + Protocol group exhibited a significantly higher proportion of cautionary behaviors compared to those in the Control group (0.2877, $p < 0.0001$). The comparison between Aware and Control group was also significant (0.1398, p = 0.0135), while the difference between Aware + Protocol and Aware was significant as well (0.1479, p = 0.0085). Additionally, Professional drivers demonstrated a significantly higher proportion of cautionary behavior compared to Standard drivers (0.1053, p = 0.0107).

Table 4.12: Cautionary Behavior Tukey HSD Results

Comparison	Difference	Lower Bound	Upper Bound	Adjusted p-value
(Control) $\rightarrow$ (Aware)	0.1398	0.0251	0.2546	0.0135
(Control) $\rightarrow$ (Aware + Protocol)	0.2877	0.1748	0.4007	< 0.0001
(Aware) $\rightarrow$ (Aware + Protocol)	0.1479	0.0332	0.2626	0.0085
(Standard) $\rightarrow$ (Professional)	0.1053	0.0255	0.1851	0.0107

4.2.5 Electrodermal Activity Results

As shown in Figure 4.8, the results suggest that that Professional participants in the Aware group displayed the highest average change in EDA, indicating a more substantial physiological response during the cyberattack compared to other groups and experiences. In contrast, Standard

drivers in group Aware + Protocol had the lowest average change EDA, implying that the implemented protocol might have mitigated the stress response effectively for these individuals. However, the large standard deviations observed, particularly in the Professional group under the Aware condition, suggest significant variability in the EDA responses. This variability may indicate that factors other than Cyberattack Threat Awareness and Experience influence EDA responses, thus potentially reducing the predictive validity of these variables in isolation.

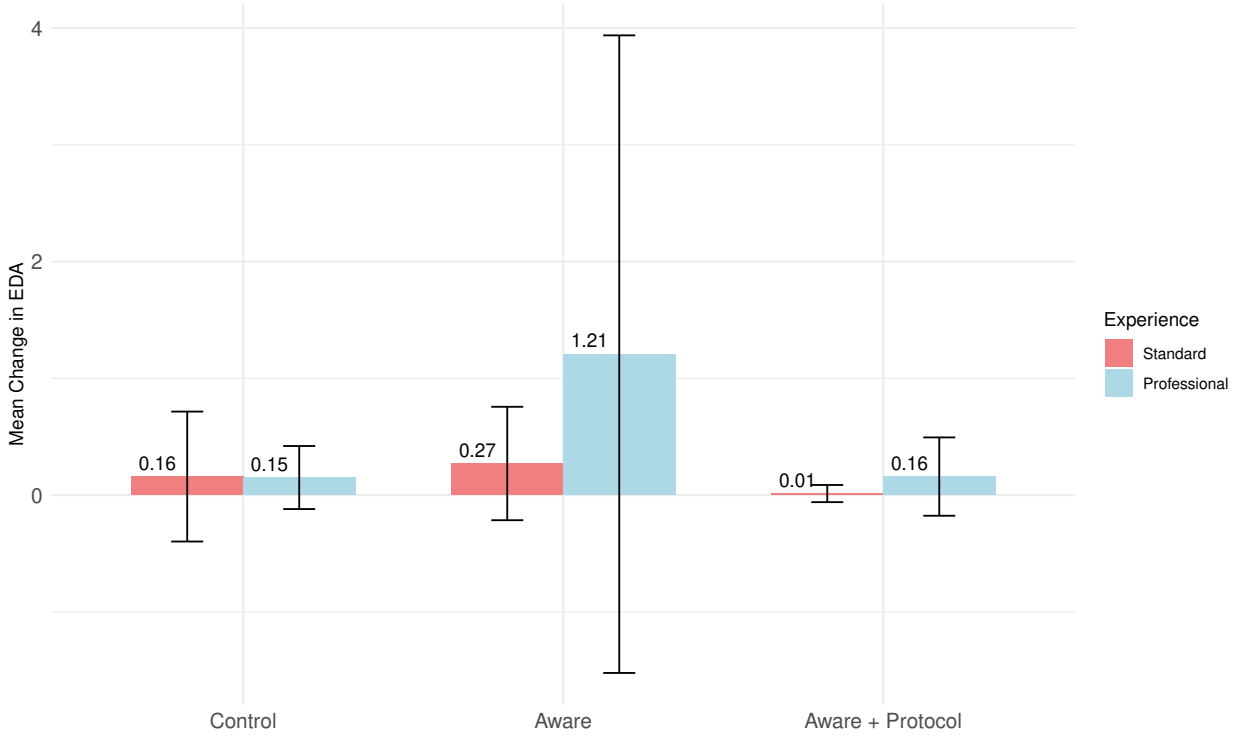


Figure 4.8: Mean Change in EDA by Group and Experience

The evaluation of Electrodermal Activity (EDA) response during the cyberattack began with an Analysis of Covariance (ANCOVA) model that included group, experience, gender, age, average MMDBQ score, and average GRiPS score as predictors, as shown in Table 4.13. The initial model results indicated that Group ($p = 0.3156$), Experience ($p = 0.2067$), Gender ($p = 0.8882$), Age ($p = 0.3936$), and average MMDBQ score ($p = 0.5229$) were not statistically significant predictors of the average EDA during the cyberattack. Although, average GRiPS score was found to be a significant predictor ($F(1, 38) = 7.121$, $p = 0.0111$).

Table 4.13: EDA Initial ANCOVA Results

Variable	Degrees of Freedom (Df)	Sum of Squares (Sum Sq)	Mean Square (Mean Sq)	F-value	p-value
Group	2	2.26	1.131	1.189	0.3156
Experience	1	1.57	1.570	1.650	0.2067
Gender	2	0.23	0.113	0.119	0.8882
Age	1	0.71	0.708	0.745	0.3936
avg MMDBQ score	1	0.40	0.395	0.416	0.5229
avg GRiPS score	1	6.77	6.774	7.121	0.0111
Residuals	38	36.15	0.951	–	–

Given the lack of significance for other factors, a revised model using backward elimination retained only the average GRiPS score as a predictor. Since the average GRiPS score is a continuous variable, the analysis transitioned from an ANCOVA to a simple linear regression model. The simplified model, as seen in Table 4.14, indicate that the average GRiPS score remained a significant predictor of EDA during the cyberattack (p = 0.0258). Higher average GRiPS scores are associated with lower EDA values during the cyberattack, specifically each unit increase in average GRiPS score decreases EDA by 0.3614. This finding highlights the potential role of risk propensity (as measured by the GRiPS score) in moderating physiological stress responses during cyberattacks. The significant relationship between average GRiPS score and EDA response supports the idea that individuals with higher propensity for risk may be better equipped to handle stress-inducing situations, resulting in lower EDA stress responses. However, the low R-squared value of 9% (0.0994) indicates that 91% of the variation in average change in EDA is not explained by the model and could be attributed to other factors not included in the analysis.

Table 4.14: Linear Regression Results for EDA by GRiPS Score

Predictor	Estimate	Std. Error	t value	p-value
(Intercept)	1.2303	0.4361	2.8210	0.0069
avg GRiPS	-0.3614	0.1570	-2.3010	0.0258
Notes				
R-squared: 0.0994, Adjusted R-squared: 0.0806 *F-statistic: 5.296 on 1 and 48 DF, p-value: 0.0258.*				

Chapter 5

Conclusions

5.1 Discussion

This thesis investigated the impact of cyberattack threat awareness and response protocols on driver behavior, focusing on five dependent variables: Stop Event, Distance Traveled, Reaction Time, Cautionary Behavior, and Electrodermal Activity. The analysis provided significant insights into how group assignment (Control, Aware, Aware + Protocol) and driver level of experience (Standard and Professional) influenced these behaviors. Additionally, potential covariates such as age, gender, driver aberrant behavior (MMDBQ), and risk propensity (GRiPS) were considered to ensure a comprehensive understanding of the factors influencing drivers' responses.

5.1.1 Participant Risk Distribution

Firstly, the results for the MMDBQ and GRiPS indicate that there is a narrow spread in risk scores between groups and experience levels. The relatively narrow range and clustering around the mean suggests that participants' risk behaviors are fairly consistent across the sample. This uniformity in risk scores ensures that any differences observed in other variables are less likely to be confounded by varying risk propensities among participants. This does not necessarily mean that MMDBQ and GRiPS are not predictors of driver response to unexpected cyberattack. Rather, the results revealed that the differences in risk scores between the groups and experience levels were not statistically significant, indicating a relatively homogeneous distribution of risk across the sample.

5.1.2 Stop Event

Moving on, in most scenarios involving severe vehicle malfunction, whether the root cause is mechanical or cybersecurity related, the expectation is that drivers pull off to the side of the road, stop the vehicle, turn off the engine, and remove the keys from the ignition. This is especially true

for commercial motor vehicles due to the catastrophic consequences of potential accidents. Therefore, it was hypothesized that, regardless of the group or experience level, all participants would stop the vehicle within the maximum duration of the cyberattack (60 seconds). This hypothesis is substantiated by the stop rate of 83% observed among Professional drivers in the Control group. If Professional drivers are considered as an optimal model for safe driving practices, these findings effectively demonstrate how a professionally trained vehicle operator would respond to an unexpected vehicle cyberattack.

However, these results diverge from the hypothesis, as evidenced by the fact that only 9% of Standard drivers in the Control group stopped the vehicle. Extrapolating these results to the general population, this implies that if an individual with a Class C driver's license experiences a severe instrument cluster cyberattack, there is only a 10.89% probability that they would pull over and stop their vehicle within the first 60 seconds of the cyberattack as determined by the model output. To put it plainly, 9 out of every 10 drivers would continue driving during an instrument cluster cyberattack, which is an alarmingly high number. This result could be attributed to the notion that most people are generally unaware of the cybersecurity vulnerabilities of their vehicles, so they could have concluded the system malfunction as transient and anomalistic as demonstrated by previous research (Huq, 2024).

With that in mind, this begs the question: How will drivers respond if they are informed of a possible cyberattack threat on their vehicle? The expectation was that responses would transition from initial confusion, "What is happening to the vehicle," to recognition, "This must be the cyberattack." The results from the Aware group, when participants were primed on the possibility of a vehicle cyberattack and not given a response protocol, showed improved stopping behavior for both Professional and Standard drivers. For Professionals, being informed of a possible cyberattack threat on their vehicle appeared to stimulate a recall of their training on how to respond to severe vehicle malfunctions, resulting in a 100% stop rate. However, cyberattack threat awareness did not always translate into the desired action of stopping the vehicle for Standard drivers, who saw a mere 20% increase in stop rate, which is still far below the Professional response rate. De-

spite this increase, 70% of Standard drivers continued driving for the duration of the cyberattack (60 seconds). This suggests that while awareness of the threat can enhance response, it may not be sufficient for those without additional professional training and experience. This result supports existing research by F. Zhang et al. (2019) that suggests drivers do not know how to respond to an unexpected cyberattack. It highlights a critical gap in the preparedness of non-professional drivers when made aware of and subsequently faced with cybersecurity threats.

Finally, in the Aware + Protocol group, where participants were primed with the same information as the Aware group but also given a basic three-line response protocol, both Professional and Standard drivers achieved a 100% stop rate. This result implies that merely informing drivers of the cybersecurity threat is not sufficient; they must be provided with simple and clear instructions on how to respond. The most astounding finding was how such minimal information could have such a significant impact on the stopping behavior of Standard drivers. The significant improvement in the Standard drivers' responses when provided with a basic protocol highlights the transformative impact of structured guidance in ensuring appropriate reactions to cyberattacks.

5.1.3 Distance Traveled

The next dependent variable analyzed was Distance Traveled during the cyberattack. It was hypothesized that participants in the Aware + Protocol group would travel a shorter distance compared to those in the Control and Aware groups, as their awareness of the cyberattack threat and response protocol would prompt them to stop the vehicle sooner. Along with that, it was hypothesized that professional drivers would travel a shorter distance than standard drivers.

Distance traveled is influenced by both the duration and speed of travel, and it is closely intertwined with stopping behavior. In a practical scenario, the greater the distance a vehicle covers during a severe system malfunction, the higher the chance of colliding with objects in a moving environment. Initially, it was hypothesized that all drivers would stop within the 60 seconds of the cyberattack; therefore, the objective of including distance traveled was to evaluate a statistically significant difference in distance traveled when stopping between the groups. However, as the

stopping behavior analysis showed, not all participants stopped their vehicles. Nonetheless, the analysis of distance traveled remains valid, as the cyberattack terminated after 60 seconds for all participants, regardless of whether they stopped.

Continuing, the results of the distance traveled analysis demonstrate that, on average, participants in the Aware + Protocol group indeed traveled a significantly shorter distance during the cyberattack compared to those in the Control and Aware groups. This finding is particularly evident among Standard drivers, who, when provided with the response protocol, were able to immediately enact the recommended stopping procedures, thus minimizing the distance traveled during the cyberattack with an estimated mean distance traveled of 224 meters (0.139 miles). Professional drivers, already skilled in handling unexpected vehicle malfunctions, consistently traveled shorter distances across all groups, further validating their proficiency in responding to such incidents. Specifically, Professional drivers in the Aware + Protocol group had an estimated mean distance traveled of 254 meters (0.158 miles).

In contrast, participants in the Control group, who were given no information about the potential for a cyberattack, traveled the greatest distances during the incident. The estimated mean distance traveled for Standard drivers was 828 meters (0.514 miles), while for Professional drivers it was 520 meters (0.323 miles). This behavior can be attributed to their lack of awareness and preparedness, which likely led to confusion and delayed responses. The absence of any prior warning or guidance left these drivers to perceive the vehicle malfunction as a transient anomaly rather than an immediate threat, resulting in continued driving.

The Aware group, while exhibiting improved responses compared to the Control group, still traveled greater distances than the Aware + Protocol group. Awareness of the potential cyberattack prompted some drivers to begin enacting cautious measures, but without a clear response protocol, many were unable to react effectively, whether it be reducing speed or bringing the vehicle to a complete stop. The estimated mean distance traveled for Standard drivers in the Aware group was 674 meters (0.419 miles), while for Professional drivers it was 312 meters (0.194 miles). This

underscores the importance of not only raising awareness of potential threats but also providing concrete guidance on how to respond.

Additionally, the analysis revealed a statistically significant influence of gender on distance traveled during the cyberattack. Male drivers, on average, traveled further than female drivers, regardless of their group or experience level. This was evidenced by the estimated mean distance which indicated that male drivers traveled 525 meters (0.326 miles) with a standard error of 35.5 meters, compared to 412 meters (0.256 miles) with a standard error of 69.6 meters for female drivers. This finding indicates the importance of considering gender-specific differences when designing and implementing vehicle cybersecurity response protocols. Tailoring these protocols to address the distinct behavioral patterns observed in male and female drivers could enhance their overall effectiveness and ensure that all drivers are adequately prepared to respond to cyberattacks.

5.1.4 Reaction Time

The third dependent variable analyzed was Reaction Time, defined as the duration between the onset of the cyberattack and the initiation of a driver's response to mitigate the impact. It was hypothesized that participants in the Aware + Protocol group would exhibit shorter reaction times compared to those in the Control and Aware groups, given their awareness of the cyberattack threat and the provision of a response protocol. Additionally, it was hypothesized that professional drivers would exhibit a faster reaction time compared to standard drivers.

Reaction time is a critical factor in determining the effectiveness of a driver's response during a cyberattack, as quicker reactions can significantly reduce the potential for harm. The results demonstrated that group assignment significantly influenced reaction times, with notable differences observed between specific groups. Participants in the Aware + Protocol group demonstrated the fastest reaction times, with an average reaction time of 7.53 seconds, supporting the hypothesis. This indicates that the combination of awareness and structured response protocols effectively enhances the drivers' ability to respond promptly to a cyberattack. In contrast, the Control group, which received no prior information about the potential for a cyberattack, exhibited the longest

reaction times, averaging 30.29 seconds. This delay can be attributed to their lack of awareness and preparedness, leading to confusion and slower recognition of the threat. The Aware group, which was informed about the possibility of a cyberattack but not given a specific response protocol, showed improved reaction times with an average of 16.12 seconds. This suggests that while awareness alone can enhance response times, it is not as effective as having a clear and actionable protocol.

Experience level did not show a significant impact on reaction times in this study. Professional drivers, despite their training and experience in handling unexpected vehicle malfunctions, did not exhibit significantly faster reaction times compared to Standard drivers when group assignments were considered. This finding emphasizes the critical importance of having a predefined response protocol, regardless of the driver's experience level.

5.1.5 Cautionary Behavior

The analysis of Cautionary Behavior revealed that group assignment and driver experience significantly influenced the proportion of cautionary actions taken during the cyberattack. Participants in the Aware + Protocol group demonstrated a markedly higher proportion of cautionary behaviors compared to those in the Control group, indicating the effectiveness of both threat awareness and response protocols in enhancing driver safety. Similarly, the Aware group showed a significant increase in cautionary behaviors compared to the Control group, although not as pronounced as the Aware + Protocol group. This aligns with the initial hypothesis that cautionary behaviors would significantly differ across experimental groups and driving experience levels. Specifically, the results support the expectation that cautionary behaviors increase from the Control group to the Aware group, and further to the Aware + Protocol group. Additionally, the higher cautionary behavior among professional drivers, as predicted, highlights the importance of experience and training in managing unexpected events. This suggests that while awareness alone can improve driver response, structured guidance is crucial for increasing cautionary actions. These findings

underscore the critical role of both awareness and structured protocols in enhancing driver safety during cyberattack threats.

5.1.6 Electrodermal Activity

The final dependent variable analyzed was Electrodermal Activity (EDA) during the cyberattack. EDA, often linked to emotional arousal, cognitive load, or physical exertion, provides valuable insights into participants' physiological states during the cyberattack. By analyzing the EDA data, the aim was to identify significant differences in physiological responses across the different awareness and experience levels. An increase in EDA can be interpreted as an increase in stress, therefore it was hypothesized that participants in the Aware + Protocol group would exhibit the smallest increase in EDA compared to those in the Control and Aware groups, as their awareness of the cyberattack threat and the response protocol would help mitigate emotional arousal. Similarly, it was hypothesized that professional drivers would experience a lower EDA response compared to standard drivers.

The initial ANCOVA model, which included Group, Experience, Gender, Age, average MMDBQ score, and average GRiPS score as predictors, indicated that only the average GRiPS score was a significant predictor of the average corrected EDA during the cyberattack. The revised linear regression model, which retained only the average GRiPS score, confirmed its significance, showing that participants with higher GRiPS scores exhibited lower physiological arousal during the cyberattack.

These results were unexpected, as factors such as Group, Experience, Gender, and Age did not significantly impact EDA during the cyberattack. However, the significance of the average GRiPS score suggests that those with a higher risk propensity are less likely to be emotionally aroused by external stimuli. This lower arousal could be due to a greater threshold to perceived threats, leading to decreased physiological responses when faced with a cyberattack. It is also possible that these individuals may have a higher threshold for emotional arousal, making them

more reactive to stressful situations. With that being said, average GRiPS only account for 9% of the variation in EDA highlighting the possibility of other significant factors not accounted for.

5.2 Limitations and Future Work

Overall, the results of this study provide a strong foundation for future research and practical interventions aimed at enhancing driver safety in the face of emerging vehicle cybersecurity threats. The critical role of cyberthreat awareness and structured response protocols cannot be overstated, as they significantly influence driver behavior and mitigate the risks associated with cyberattacks. However, there are a few limitations in this study that present themselves as opportunities for future research.

The first being that the cyberattack occurred under the same road conditions for all participants. This homogeneity limits the broader application of the results to other types of roads or driving environments. Future research should consider varying road conditions to better understand how different environments influence driver responses to cyberattacks.

Another limitation is the potential influence of the Hawthorne effect, where participants may have altered their behavior simply because they knew they were being observed in a study setting (Adair, 1984). Having the researcher in the passenger seat of the vehicle during the drive could have inadvertently influenced the drivers' behavior. Future research should evaluate how responses may vary depending on whether there are passengers in the vehicle, potentially using more covert observation methods or long-term naturalistic driving studies to minimize this effect.

Furthermore, only one type of cyberattack was used for all participants, specifically targeting the instrument cluster display and audio system with both visual and auditory cues. The cyberattack manipulated the speedometer and tachometer needles, activated all dashboard warning lights, and emitted a medium-pitched tone at a frequency of twice per second. While this design ensured the driver was immediately alerted to the cyberattack, it does not capture the variability and unpredictability of real-world cyberattacks. Cyberattacks can take many forms and impact various vehicle systems differently. This attack did not affect steering, brakes or power, all of which could

stimulate different sensations. Future research should evaluate how different types of cyberattacks may influence driver responses, considering the diverse nature of potential cybersecurity vulnerabilities.

Additionally, this study focused primarily on the immediate responses of drivers to a cyberattack. Future research should explore the long-term behavioral adaptations and psychological impacts of repeated exposure to vehicle cyberattacks. It would be beneficial to investigate whether drivers develop better coping strategies over time or if their stress and anxiety levels increase with repeated cyberattacks ultimately negatively impacting their response capability.

Despite the novel insights gained from analyzing cautionary behavior, there are opportunities for expanding the scope of this dependent variable. The reliance on accelerator pedal position data as the sole indicator of cautionary behavior may not capture the full range of defensive driving actions, such as steering adjustments or brake use. Future research could incorporate a broader array of behavioral metrics, such as gaze tracking or brake pedal position, to provide a more comprehensive understanding of driver cautionary behavior.

While this study provides valuable insights into the factors influencing EDA during a cyberattack, it is not without limitations. One significant limitation is the potential for poor readings from the EDA device due to movement artifacts. Movements or rotations of the wrist can impact the contact between the electrodes and the skin, leading to inaccurate readings (Y. Zhang et al., 2017). Future studies should consider using more advanced EDA measurement techniques or methods to minimize movement artifacts, such as incorporating additional sensors to track and correct for motion.

Moreover, the study's sample size and demographic composition may limit the generalizability of the findings. Future studies should aim to include a larger and more diverse sample to ensure that the results are applicable to a wider population. This would help to identify any potential variations in response due to cultural, geographical, or socioeconomic factors.

Finally, while this study highlighted the importance of awareness and response protocols, it did not explore the specific content and delivery methods of these protocols. Future research should

focus on identifying the most effective ways to communicate cybersecurity threats and response strategies to drivers, including the use of technology, training programs, and public awareness campaigns.

5.2.1 Heart Rate Variability as a Possible Dependent Variable

At the onset of this research study, two physiological variables were intended to be included: electrodermal activity (EDA) and heart rate variability (HRV). As discussed in previous sections, EDA was successfully collected. However, there was an issue with the data collection for HRV. Over the 60-minute driving session, the Empatica E4 wristband collected only around 10 to 20 data points for HRV for each subject. The reason for this poor data quality was likely the result of excessive movement, as the device used in this study more accurately measures HRV under motion-free resting conditions. Since heart rate and blood volume pulse data was successfully collected from the device, an attempt was made to recover the HRV data. Although, the data output from the Empatica E4 did not allow for a manual calculation for HRV. Consequently, the analysis and results related to HRV were omitted from this report.

Despite this limitation, previous research has demonstrated HRV as a valuable tool for monitoring physiological stress. For instance, a systematic review by Thielmann et al. (2022) highlights the use of HRV as an objective indicator for mental stress in individuals with different levels of effort-reward imbalance or overcommitment. Additionally, Haque et al. (2024) discuss the state-of-the-art of stress prediction from HRV using artificial intelligence, further supporting HRV's relevance in stress monitoring (Haque et al., 2024). Therefore, HRV presents itself as an opportunity for future research, particularly in its application to measuring stress responses of drivers experiencing cyberattacks while operating a vehicle.

5.3 Research Contributions

The rapid advancement of technology has transformed the automotive industry, integrating sophisticated digital components and connectivity features into modern vehicles. While enhancing

convenience, this evolution has also introduced new vulnerabilities, particularly in the domain of cybersecurity. Understanding how drivers respond to unexpected cyberattacks is crucial for developing effective countermeasures and enhancing traffic safety.

This study examined drivers' responses to cyberattacks in a realistic driving environment, focusing on three primary questions: the influence of cybersecurity threat awareness on driver behavior, the impact of basic response protocols on driver performance, and the differences in response between professionally trained and standard drivers during an instrument cluster cyberattack.

The findings illuminate the essential role of awareness and response protocols in enhancing a driver's response to an unexpected vehicle cyberattack. The Aware + Protocol group achieved a 100% stop rate among both Standard and Professional drivers, showcasing the transformative impact of clear response guidelines. This group also traveled the shortest distances during the cyberattack, with Standard drivers covering 224 meters (0.139 miles) and Professional drivers 254 meters (0.158 miles), compared to the Control group's 828 meters (0.514 miles) for Standard drivers and 520 meters (0.323 miles) for Professional drivers. Furthermore, the Aware + Protocol group demonstrated the shortest reaction times, averaging 7.53 seconds, versus 16.12 seconds in the Aware group and 30.29 seconds in the Control group.

Overall, these results suggest the importance of both informing drivers about potential threats and providing them with clear response protocols to enhance safety during cyberattacks. By informing drivers and providing response protocols, their ability to respond appropriately to cyberattacks can be significantly improved. This information can be applied in several practical ways, such as integrating cyberattack response training into existing driver education programs, especially for those operating heavy and commercial motor vehicles. Additionally, public service announcements and in-vehicle alerts could be effective in increasing awareness of cyberattack vulnerabilities. Public service announcements broadcasted through various media channels can inform a wide audience about the risks of vehicle cyberattacks and inform drivers on how to recognize and respond to such threats. In-vehicle alerts can offer real-time information and instructions, guiding drivers on immediate actions to take when a cybersecurity threat is detected.

In conclusion, this study highlights the necessity of awareness and structured response protocols in enhancing driver safety during vehicle cyberattacks. Equipping drivers with the knowledge and tools to react swiftly and effectively can significantly minimize potential harm, improving the overall safety of the transportation industry.

5.4 Publication of Results

This work, in part, was presented and published at the 2024 19th Annual System of Systems Engineering (SoSE) Conference (23 - 26 June 2024):

- Biggs, T., Lanigan, T., Ruddell, D., Gallegos, E. E., & Daily, J. (2024). Modeling a heavy-duty vehicle data collection process for authenticating driver identity and analyzing driver behavior under duress. *Proceedings of the 2024 19th Annual System of Systems Engineering (SoSE) Conference*. Tacoma, Washington, USA: June 2024.

  doi.org/10.1109/SOSE62659.2024.10620958

Also, this work has been submitted and is currently under review at a quality, high impact journal:

- Lanigan, T. F., Biggs, T., Gallegos, E. E., Daily, Reid, E. & Powers, S. Impact of cyber threat awareness on driver response to an unexpected vehicle cyberattack. Unpublished manuscript.

Bibliography

Adair, J. (1984). The hawthorne effect: A reconsideration of the methodological artifact. *Journal of Applied Psychology*, *69*(2), 334–345. https://doi.org/10.1037/0021-9010.69.2.334

Ahmed, J., Ward, N., McMahill, A., Otto, J., & Miller, E. E. (2023). Effects of emotional intelligence on dangerous driving: A comparison between commercial and non-commercial drivers. *Transportation Planning and Technology*, *46*(6), 695–709. https://doi.org/10.1080/03081060.2023.2228760

Ahmed, J., Ward, N., Otto, J., McMahill, A., & Miller, E. E. (2024). Identifying measures of emotional intelligence and dangerous driving. *Transportation Research Record*, *2678*(3), 365–375. https://doi.org/10.1177/03611981231179698

Ahmed, J., Robinson, A., & Miller, E. E. (2024). Effectiveness of signs for pedestrian-railroad crossings: Colors, shapes, and messaging strategies. *Journal of Safety Research*, *89*, 141–151. https://doi.org/10.1016/j.jsr.2024.01.003

Ahmed, M. M., Franke, R., Ksaibati, K., & Shinstine, D. S. (2018). Effects of truck traffic on crash injury severity on rural highways in Wyoming using Bayesian binary logit models. *Accident Analysis and Prevention*, *117*, 106–113. https://doi.org/10.1016/j.aap.2018.04.011

Al-Daeef, M. M., Basir, N., & Saudi, M. M. (2017). Security awareness training: A review. *Proceedings of the World Congress on Engineering*, *1*, 5–7.

Aldawood, H., & Skinner, G. (2018). Educating and raising awareness on cyber security social engineering: A literature review. *2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE)*, 62–68. https://doi.org/10.1109/TALE.2018.8615162

Aliebrahimi, S., & Miller, E. E. (2023). Effects of cybersecurity knowledge and situation awareness during cyberattacks on autonomous vehicles. *Transportation Research Part F: Traffic Psychology and Behaviour*, *96*, 82–91. https://doi.org/10.1016/j.trf.2023.06.010

Andrade, R. O., Fuertes, W., Cazares, M., Ortiz-Garcés, I., & Navas, G. (2022). An exploratory study of cognitive sciences applied to cybersecurity. *Electronics*, *11*(12), 1934. https://www.mdpi.com/2079-9292/11/12/1934

Biggs, T., Lanigan, T., Ruddell, D., Gallegos, E. E., & Daily, J. (2024). Modeling a heavy-duty vehicle data collection process for authenticating driver identity and analyzing driver behavior under duress. *2024 19th Annual System of Systems Engineering Conference (SoSE)*, 256–263. https://doi.org/10.1109/SOSE62659.2024.10620958

Blythe, J. M., & Coventry, L. (2018). Costly but effective: Comparing the factors that influence employee anti-malware behaviours. *Computers in Human Behavior*, *87*, 87–97. https://doi.org/10.1016/j.chb.2018.05.023

Bumgarner, S., Rudder, S., Gallegos, E. E., & Daily, J. (2024). Human Factors Engineering (HFE) considerations for mounting internal interfaces in heavy vehicles. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *68*(1), 748–756. https://doi.org/10.1177/10711813241282266

Burakova, Y., Hass, B., Millar, L., & Weimerskirch, A. (2016). Truck hacking: An experimental analysis of the SAE J1939 standard. *Proceedings of the 10th USENIX Conference on Offensive Technologies*, 211–220.

Bureau of Labor Statistics. (2024). Heavy and tractor-trailer truck drivers [Accessed: 10 Oct 2024]. https://www.bls.gov/ooh/transportation-and-material-moving/heavy-and-tractor-trailer-truck-drivers.html

Bureau of Transportation Statistics. (2019). Freight facts and figures: Freight transportation & the economy [Accessed: 10 Oct 2024]. https://data.bts.gov/stories/s/Freight-Transportation-the-Economy/6ix2-c8dn

Bureau of Transportation Statistics. (2022). Freight facts and figures: Moving goods in the United States [Accessed: 10 Oct 2024]. https://data.bts.gov/stories/s/Moving-Goods-in-the-United-States/bcyt-rqmu

Bureau of Transportation Statistics. (2023). Transportation economic trends [Accessed: 10 Oct 2024]. https://data.bts.gov/stories/s/28tb-cpjy

Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., Koscher, K., Czeskis, A., Roesner, F., & Kohno, T. (2011). Comprehensive experimental analyses of automotive attack surfaces. *Proceedings of the 20th USENIX Conference on Security*, 6.

Cranor, L. F. (2008). A framework for reasoning about the human in the loop. *Proceedings of the 1st Conference on Usability, Psychology, and Security*.

Daily, J. (2019). Systems Cyber - CAN-Logger-3 [Accessed: 2025-01-15]. https://github.com/SystemsCyber/CAN-Logger-3

Daily, J. (2020). Systems Cyber - Truck Cape Projects [Accessed: 2025-01-15]. https://github.com/SystemsCyber/TruckCapeProjects

Daily, J. (2023). Systems Cyber - Truck GPS [Accessed: 2025-01-15]. https://github.com/SystemsCyber/TruckGPS

Daily, J., Nnaji, D., & Ettlinger, B. (2021). Securing CAN traffic on J1939 networks. *Workshop on Automotive and Autonomous Vehicle Security (AutoSec)*. https://doi.org/10.14722/autosec.2021.23031

Daily, J. S., & Kulkarni, P. (2020). Secure heavy vehicle diagnostics. *Proceedings of the Ground Vehicle Systems Engineering and Technology Symposium (GVSETS)*. https://doi.org/10.4271/2024-01-3868

Eiza, M., & Ni, Q. (2017). Driving with sharks: Rethinking connected vehicles with vehicle cyber security. *IEEE Vehicular Technology Magazine*, *12*, 45–51. https://doi.org/10.1109/MVT.2017.2669348

Fischhoff, B., Canfield, C. I., & Davis, A. (2016). Quantifying phishing susceptibility for detection and behavior decisions. *Human Factors*, *58*(8), 1158–1172. https://doi.org/10.1177/0018720816665025

Gold, C., Damböck, D., Lorenz, L., & Bengler, K. (2013). "Take over!" How long does it take to get the driver back into the loop? *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *57*(1), 1938–1942. https://doi.org/10.1177/1541931213571433

Grobler, M., Gaire, R., & Nepal, S. (2021). User, usage and usability: Redefining human centric cyber security. *Frontiers in Big Data*, *4*. https://doi.org/10.3389/fdata.2021.583723

Haque, Y., Zawad, R., Rony, C., & et al. (2024). State-of-the-art of stress prediction from heart rate variability using artificial intelligence. *Cognitive Computation*, *16*, 455–481. https://doi.org/10.1007/s12559-023-10200-0

Huq, N. (2024). Automotive cyber security - Emerging risks and new case study insights [Published 19 July 2024, Issue Date July 2024]. *ATZ Electron Worldw*, *19*, 14–19. https://doi.org/10.1007/s38314-024-1890-0

Jepson, J., Chatterjee, R., & Daily, J. (2024). Commercial vehicle electronic logging device security: Unmasking the risk of truck-to-truck cyber worms. *Symposium on Vehicles Security and Privacy*. https://doi.org/10.14722/vehiclesec.2024.23047

Kävrestad, J., & Naqvi, B. (2024). Cognitively available cybersecurity: A systematic literature review. *Human-Centered Software Engineering Conference (HCSE)*, 345–1715. https://dl.acm.org/doi/10.1145/3451327.3451715

Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., & Savage, S. (2010). Experimental security analysis of a modern automobile. *2010 IEEE Symposium on Security and Privacy*, 447–462. https://doi.org/10.1109/SP.2010.34

Kotseruba, I., & Tsotsos, J. K. (2021). Behavioral research and practical models of drivers' attention. *CoRR*, *abs/2104.05677*. https://doi.org/10.48550/arXiv.2104.05677

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. (2010). Teaching Johnny not to fall for phish. *ACM Trans. Internet Technol.*, *10*(2). https://doi.org/10.1145/1754393.1754396

Lee, J., Wickens, C., Liu, Y., & Boyle, L. (2017). *Designing for people: An introduction to human factors engineering* (3rd). CreateSpace.

Lim, C., & Rajivan, P. (2023). Who hacked my car? Designing autonomous vehicles to support driver response to security threats. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *67*(1), 247–252. https://doi.org/10.1177/21695067231192217

Lima, A., Rocha, F., Völp, M., & Esteves-Verissimo, P. (2016). Towards safe and secure autonomous and cooperative vehicle ecosystems. *Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy*, 59–70.

Linkov, V., Zámečník, P., Havlíčková, D., & Pai, C.-W. (2019). Human factors in the cybersecurity of autonomous vehicles: Trends in current research. *Frontiers in Psychology*, *10*, 995. https://doi.org/10.3389/fpsyg.2019.00995

Mairaj ud din, Q., & Ahmed, Q. (2024). *Automated TARA framework for cybersecurity compliance of heavy duty vehicles* (Technical Paper No. 2024-01-2809). SAE. https://doi.org/10.4271/2024-01-2809

Malik, S., & Sun, W. (2020). Analysis and simulation of cyber attacks against connected and autonomous vehicles. *2020 International Conference on Connected and Autonomous Driving (MetroCAD)*, 62–70. https://doi.org/10.1109/MetroCAD48866.2020.00018

Martin, J. (2017). *Something looks phishy here: Applications of signal detection theory to cybersecurity behaviors in the workplace* [Master's thesis, University of South Florida] [USF Tampa Graduate Theses and Dissertations]. https://digitalcommons.usf.edu/etd/6728

Memar, M., & Mokaribolhassan, A. (2021). Stress level classification using statistical analysis of skin conductance signal while driving. *SN Applied Sciences*, *3*(64). https://doi.org/10.1007/s42452-020-04134-7

Meyer, S., Elvik, R., & Johnsson, E. (2021). Risk analysis for forecasting cyberattacks against connected and autonomous vehicles. *Journal of Transportation Security*, *14*, 227–247. https://doi.org/10.1007/s12198-021-00236-4

Miller, E. E., & Boyle, L. N. (2015). Driver's behavior in road tunnels: Association with driver stress and performance. *Transportation Research Record*, *2518*, 60–67. https://doi.org/10.3141/2518-08

Miller, E. E. (2013). *Effects of roadway on driver stress: An on-road study using physiological measures* [Master's thesis]. University of Washington [Available at http://hdl.handle.net/1773/23592].

Miller, E. E., & Boyle, L. N. (2013). Variations in road conditions on driver stress: Insights from an on-road study. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *57*(1), 1864–1868. https://doi.org/10.1177/1541931213571416

Mukherjee, S., Shirazi, H., Ray, I., Daily, J., & Gamble, R. (2016). Practical DoS attacks on embedded networks in commercial vehicles. *International Conference on Information Systems Security*, *10063*, 23–42. https://doi.org/10.1007/978-3-319-49806-5_2

National Motor Freight Traffic Association, I. (2016, January). *A Survey of Heavy Vehicle Cyber Security* (tech. rep.). National Motor Freight Traffic Association, Inc. Retrieved November 25, 2023, from https://nmfta.org/wp-content/media/2022/11/nmfta-heavy-duty-vehicle-cyber-security-whitepaper-v1.0.3.6.pdf

Nickkar, A., Pourfalatoun, S., Miller, E. E., & Lee, Y. J. (2023). Applying the heteroskedastic ordered probit model on injury severity for improved age and gender estimation. *Traffic Injury Prevention*, *25*(2), 202–209. https://doi.org/10.1080/15389588.2023.2286429

Nie, S., Liu, L., Zhang, W., & Du, Y. (2018). Over-the-air: How we remotely compromised the gateway, BCM, and autopilot ECUs of Tesla cars. *Proceedings of the 2018 Black Hat USA Conference*.

Oikawa, S., Matsui, Y., Kubota, N., Aomura, S., Sorimachi, K., Imanishi, A., & Fujimura, T. (2021). Features of fatal truck accidents compared with sedans. *International Journal of Automotive Technology*, *22*, 931–939. https://doi.org/10.1007/s12239-021-0084-5

Parker, J., Zhang, F., Wang, M., & Roberts, S. C. (2022). How do drivers respond to vehicle cyberattacks? A driving simulator study. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *66*(1), 737–741. https://doi.org/10.1177/1071181322661506

Parkinson, S., Ward, P., Wilson, K., & Miller, J. (2017). Cyber threats facing autonomous and connected vehicles: Future challenges. *IEEE Transactions on Intelligent Transportation Systems*, *18*(11), 2898–2915. https://doi.org/10.1109/TITS.2017.2665968

Payne, B. (2019). Car hacking: Accessing and exploiting the CAN bus protocol. *Journal of Cybersecurity Education, Research and Practice*, *2019*(1).

Posada-Quintero, H. F., & Chon, K. H. (2020). Innovations in electrodermal activity data collection and signal processing: A systematic review. *Sensors*, *20*(2). https://doi.org/10.3390/s20020479

Pourfalatoun, S., Ahmed, J., & Miller, E. E. (2023). Shared electric scooter users and non-users: Perceptions on safety, adoption and risk. *Sustainability*, *15*(11). https://doi.org/10.3390/su15119045

Puhr, R., Heinze, G., Nold, M., Lusa, L., & Geroldinger, A. (2017). Firth's logistic regression with rare events: Accurate effect estimates and predictions? *Statistics in Medicine*, *36*(14), 2302–2317. https://doi.org/10.1002/sim.7273

Schneier, B. (2000). *Secrets and lies: Digital security in a networked world*. John Wiley; Sons.

Schuurmans, A. A. T., de Looff, P., Nijhof, K. S., Rosada, C., Scholte, R. H. J., Popma, A., & Otten, R. (2020). Validity of the Empatica E4 wristband to measure heart rate variability (HRV) parameters: A comparison to electrocardiography (ECG). *Journal of Medical Systems*, *44*(11), 190. https://doi.org/10.1007/s10916-020-01648-w

Sharma, K., Zhan, X., Nah, F.-H., Siau, K., & Cheng, M. (2021). Impact of digital nudging on information security behavior: An experimental study on framing and priming in cybersecurity. *Organizational Cybersecurity Journal: Practice, Process and People*, *1*(1), 69–91. https://doi.org/10.1108/OCJ-03-2021-0009

Singh, R., Agrawal, A., & Ankur. (2024). Unveiling worldwide prospects and challenges in implementing telematics technologies in electric vehicles. In O. P. Verma, L. Wang, R. Kumar, & A. Yadav (Eds.), *Machine intelligence for research and innovations* (pp. 169–182). Springer Nature Singapore.

Stachowski, S., Bielawski, R., & Weimerskirch, A. (2018). *Cybersecurity research considerations for heavy vehicles* (Report No. DOT HS 812 636). National Highway Traffic Safety Administration. Washington, DC.

Sucha, M., Sramkova, L., & Risser, R. (2014). The manchester driver behaviour questionnaire: Self-reports of aberrant behaviour among Czech drivers. *European Transport Research Review*, *6*, 493–502. https://doi.org/10.1007/s12544-014-0147-z

Tanner, J., W. P., & Swets, J. A. (1954). A decision-making theory of visual detection. *Psychological Review*, *61*(6), 401–409. https://doi.org/10.1037/h0058700

Thielmann, B., Hartung, J., & Böckelmann, I. (2022). Objective assessment of mental stress in individuals with different levels of effort reward imbalance or overcommitment using heart rate variability: A systematic review. *Systematic Reviews*, *11*, 48. https://doi.org/10.1186/s13643-022-01925-4

Torten, R., Reaiche, C., & Boyle, S. (2018). The impact of security awareness on information technology professionals' behavior. *Computers & Security*, *79*, 68–79. https://doi.org/10.1016/j.cose.2018.08.007

Wang, M., Parker, J., Zhang, F., & Roberts, S. C. (2024). A simulator study assessing the effectiveness of training and warning systems on drivers' response performance to vehicle cyberattacks. *Accident Analysis and Prevention*, *203*, 107644. https://doi.org/10.1016/j.aap.2024.107644

Waskito, D., Bowo, L., Kurnia, S., Kurniawan, I., Nugroho, S., Irawati, N., Mutharuddin, Mardiana, T., & Subaryata. (2024). Analysing the impact of human error on the severity of truck accidents through HFACS and Bayesian network models. *Safety*, *10*(1). https://doi.org/10.3390/safety10010008

Wolf, M., Weimerskirch, A., & Paar, C. (2004). Security in automotive bus systems. *Proceedings of escar 2004 – Embedded Security in Cars Workshop*. https://api.semanticscholar.org/CorpusID:16502503

Xu, J., Wali, B., Li, X., & Yang, J. (2019). Injury severity and contributing driver actions in passenger vehicle–truck collisions. *International Journal of Environmental Research and Public Health*, *16*(19). https://doi.org/https://doi.org/10.3390/ijerph16193542

Zhang, D., Highhouse, S., & Nye, C. (2018). Development and validation of the general risk propensity scale (GRiPS). *Journal of Behavioral Decision Making*, 1–16. https://doi.org/10.1002/bdm.2102

Zhang, F., Petit, J., & Roberts, S. C. (2019). A simulator study on drivers' response and perception towards vehicle cyberattacks. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *63*(1), 1498–1502. https://doi.org/10.1177/1071181319631310

Zhang, F., Wang, M., Parker, J., & Roberts, S. C. (2023). The effect of driving style on responses to unexpected vehicle cyberattacks. *Safety*, *9*(1), 5. https://doi.org/10.3390/safety9010005

Zhang, Y., Haghdan, M., & Xu, K. S. (2017). Unsupervised motion artifact detection in wrist-measured electrodermal activity data. *Proceedings of the 2017 ACM International Symposium on Wearable Computers*, 54–57. https://doi.org/10.1145/3123021.3123054

Appendix A

Driver Research Interest Form

Colorado State University

COLORADO STATE UNIVERSITY
DEPARTMENT OF SYSTEMS ENGINEERING

DRIVER RESEARCH INTEREST FORM

Are you comfortable driving a box truck?

If so, please consider participating in our 2 hour driver research study. Scan the QR code for more information!

FINANCIAL COMPENSATION?

Immediately after the study, you will be given a **$20 Amazon gift card!**

FLEXIBLE SCHEDULING FROM APRIL TO OCTOBER

IF YOU HAVE QUESTIONS FEEL FREE TO EMAIL
TREVOR.LANIGAN@COLOSTATE.EDU

Appendix B

Informed Consent Document

SYSTEMS ENGINEERING
COLORADO STATE UNIVERSITY

ADULT PARTICIPANT INFORMED CONSENT

Department of Systems Engineering

Participant Study Title: Driver Identification Using Models Developed from Onboard Data Acquisition Devices

PRINCIPAL INVESTIGATOR: Erika Miller, PhD, Assistant Professor

CO-INVESTIGATOR(S): Jeremy Daily, PhD, Associate Professor

STUDENT INVESTIGATOR(S): Tyler Biggs, Trevor Lanigan

SPONSOR: Oak Ridge National Laboratory

WHAT IF I HAVE QUESTIONS?

For questions or concerns about the study, you may contact **Erika Miller** at **(970) 491-3346.** For questions regarding the rights of research subjects, any complaints or comments regarding the manner in which the study is being conducted, contact the CSU Institutional Review Board at: CSU_IRB@colostate.edu; 970-491-1553.

WHAT IS THE PURPOSE OF THIS STUDY?

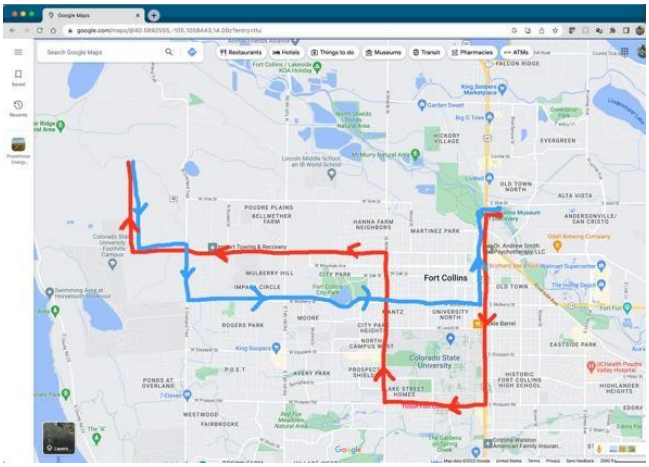
The purpose of this research study is to identify unique drivers based on driving performance data obtained from a vehicle. We will also collect heart rate data and survey responses to try to correlate to your driving data.

WHY AM I BEING INVITED TO TAKE PART IN THIS RESEARCH?

You are being asked to participate in the study because you fit these criteria: Licensed driver over 18 years old. Additionally, exclusion criteria for this study includes: Expressed discomfort driving a box truck; Impaired / uncorrected vision limiting your ability to drive a vehicle; and Medical conditions and medications that impair driving, such as ones that cause dizziness, fatigue, impaired vision.

WHERE IS THE STUDY GOING TO TAKE PLACE AND HOW LONG WILL IT LAST?

The study will start at the Powerhouse, then the parking lot behind the Powerhouse, then around city streets in Fort Collins, CO. A map of the driving route is provided in the following figure. The total study duration will be approximately 2 hours. The practice drive will take approximately 30 minutes, the study drive about 40 minutes, and a 10-minute survey.



WHAT WILL I BE ASKED TO DO?

You will be asked to first practice driving the truck around the parking lot. A member of the research team will assist you in learning how to operate the vehicle. Then, you will drive the route shown above in the figure. A member of the research team will sit in the passenger seat of the truck and help you navigate when to turn and where to go. During the drive, you will wear a heart rate monitor, which looks and feels like a typical wrist watch. After you complete this drive, you will fill out an online survey.

ARE THERE ANY BENEFITS FROM TAKING PART IN THIS STUDY?

There may be no direct benefit to you as a participant in this study. However, we hope to learn more about transport security and reliability.

WHAT ARE THE POSSIBLE RISKS AND DISCOMFORTS?

You will be driving the truck on city streets, and exposed to typical driving risks. The truck is insured through Colorado State University. Typical driving risks include minor accidents, rollover crashes, and blind spot collisions.

There is also a risk of breach of confidentiality in completing the survey. We have tried to safeguard against this by not linking your name to your survey. You can also skip any survey question you do not feel comfortable answering.

WHAT SHOULD I DO IF I BECOME INJURED?

If you are injured because of participation in this study, please contact the Principal Investigator (Erika Miller) at (970)-491-3346 or erika.miller@colostate.edu. The Colorado Governmental Immunity Act determines and may limit Colorado State University's legal responsibility if an injury happens because of this study. Should you need medical aid, you or your health insurance will be responsible for the costs

WILL I RECEIVE ANY COMPENSATION FOR TAKING PART IN THIS STUDY?

You will be compensated for participating in this research. You will receive $20 at the end of the study drive today.

WHO WILL SEE THE INFORMATION THAT I GIVE?

All information gathered in this study will be kept as confidential as possible. Your privacy is very important to us and the researchers will take every measure to protect it. Your information may be given out if required by law; however, the researchers will do their best to make sure that any information that is released will not identify you. No reference will be made in written or oral materials that could link you to this study. For this study, we will assign a code to your data so that the only place your name will appear in our records is on the consent. Only the research team will have access your data. All records will be stored in a restricted access folder and cloud-based storage system at CSU for three years after completion of the study. After the storage time, the information gathered will be destroyed. We may be asked to share the research files with the sponsor (Department of Energy and Oak Ridge Laboratories) or the CSU Institutional Review Board ethics committee for auditing purposes. Your identity/record of receiving compensation (NOT your data) may be made available to CSU officials for financial audits.

There are organizations that may inspect research records that may include yours. These organizations are required to make sure your information is kept private, unless required by law to provide information. Some of these organizations are:

- The study sponsor (Department of Energy and Oak Ridge Laboratories).
- The CSU financial management team may request an audit of research expenditure, in which only your participation in the research may be shared, but not your research data.
- The Colorado State Institutional Review Board, IRB, is a group of people who review the research with the goal of protecting the people who take part in the study.
- Office of Human Research Protections

DO I HAVE TO TAKE PART IN THE STUDY?

Your participation in this study is voluntary. You may refuse to participate in this study or in any part of this study. You may withdraw at any time without prejudice to your relations with CSU. You are encouraged to ask questions about this study at the beginning or any time during the research study.

CAN MY PARTICPATION IN THE STUDY END EARLY?

There are a number of reasons your participation could end early: You do not feel comfortable driving the truck, or the researcher does not feel comfortable in your ability to operate the vehicle. Additionally, if you are unable to complete study procedures, or if you repeatedly miss scheduled appointments.

If your participation ends early for any of the above reasons, we will contact you and let you know the reason why you will not be allowed to continue. You will receive monetary compensation only for those portions of the study that you complete.

Your information collected as part of the research, even if identifiers are removed, will not be used or distributed for future research studies.

Participant Consent:

Your signature acknowledges that you have read the information stated and voluntarily wish to participate in this research. Your signature also acknowledges that you have received, on the date signed, a copy of this document containing 4 pages.

_____ _____

Signature of participant Date

_____

Name of participant

_____ _____

Signature of research personnel obtaining informed consent Date

_____ Name

of research personnel obtaining informed consent

Appendix C

Post-Drive Survey

ID

Participant Number (to be filled out by researcher):

Group (to be filled out by researcher):

- ○ Group 1
- ○ Group 2
- ○ Group 3

Demographics/Driving History

What is your gender?

- ○ Male
- ○ Female
- ○ Non-binary / third gender
- ○ Prefer not to say

What is your age (in years)?

What is the highest level of education you have completed?

- ○ Some high school
- ○ High school diploma or equivalent
- ○ Some education beyond high school but no degree
- ○ College degree
- ○ Advanced degree (e.g., JDS, MS, or PhD)

Have you ever had a Commercial Drivers License (CDL) or Professional Equivalent Certification (i.e. special vehicle training)?

- ○ Yes, and I still do.

- ○ Yes, but not currently.
- ○ No, never.

How long did you have a CDL or Professional Equivalent Certification (in years)?

Do you have experience driving heavy trucks and/or large vehicles?

- ○ Yes
- ○ No

Briefly describe your experience driving heavy trucks and/or large vehicles.

Over the past five years, what is your average annual mileage (estimate all vehicles combined)?

- ○ less than 5,000 miles
- ○ 5,000 to 10,000 miles
- ○ 10,000 to 15,000 miles
- ○ 15,000 to 20,000 miles
- ○ 20,000 to 25,000 miles
- ○ more than 25,000 miles

In the past year, how many moving or traffic violations have you had?

- ○ 0
- ○ 1
- ○ 2
- ○ 3
- ○ 4
- ○ 5
- ○ more than 5

In the past year, how many crashes have you been in?

- ○ 0
- ○ 1
- ○ 2
- ○ 3
- ○ 4
- ○ 5
- ○ more than 5

How many years have you been driving?

Modified Manchester DBQ

How often do you do the following while driving...

	Never	Hardly Ever	Occasionally	Quite Often	Frequently	Nearly All the Time
Attempt to drive away from traffic lights in the wrong gear	○	○	○	○	○	○
Become impatient with a slow driver in the fast lane and pass on the right	○	○	○	○	○	○
Drive especially close to a car in front as a signal to the driver to go faster or get out of the way	○	○	○	○	○	○
Attempt to pass someone that you hadn't noticed to be making a left turn	○	○	○	○	○	○
Forget where you left your car in a parking lot	○	○	○	○	○	○

	Never	Hardly Ever	Occasionally	Quite Often	Frequently	Nearly All the Time
Turn on one thing, such as your headlights, when you mean to switch on something else, such as the windshield wipers	○	○	○	○	○	○
Realize that you have no clear recollection of the road along which you have just been traveling	○	○	○	○	○	○
Cross an intersection knowing that the traffic lights have already changed from yellow to red	○	○	○	○	○	○
Fail to notice that pedestrians are crossing when turning onto a side street from a main road	○	○	○	○	○	○
Angered by another driver's behavior, you catch up to them with the intention of giving him/her "a piece of your mind"	○	○	○	○	○	○

GRiPS

How strongly do you agree/disagree with the following statements...

	Strongly disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Strongly agree
Taking risks makes life more fun	○	○	○	○	○
My friends would say that I'm a risk taker	○	○	○	○	○
I enjoy taking risks in most aspects of my life	○	○	○	○	○
I would take a risk even if it meant I might get hurt	○	○	○	○	○

	Strongly disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Strongly agree
Taking risks is an important part of my life	○	○	○	○	○
I commonly make risky decisions	○	○	○	○	○
I am a believer of taking chances	○	○	○	○	○
I am attracted, rather than scared, by risk	○	○	○	○	○

Block 4

How strongly do you agree/disagree with the following statements about your study drive by the Foothills campus on Laporte Ave (at the turn around point)...

	Strongly disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Strongly agree
The vehicle seemed reliable.	○	○	○	○	○
The vehicle behaved as expected.	○	○	○	○	○
I felt safe.	○	○	○	○	○
I noticed something wrong with the vehicle.	○	○	○	○	○

Briefly describe what you noticed with the vehicle during the drive.