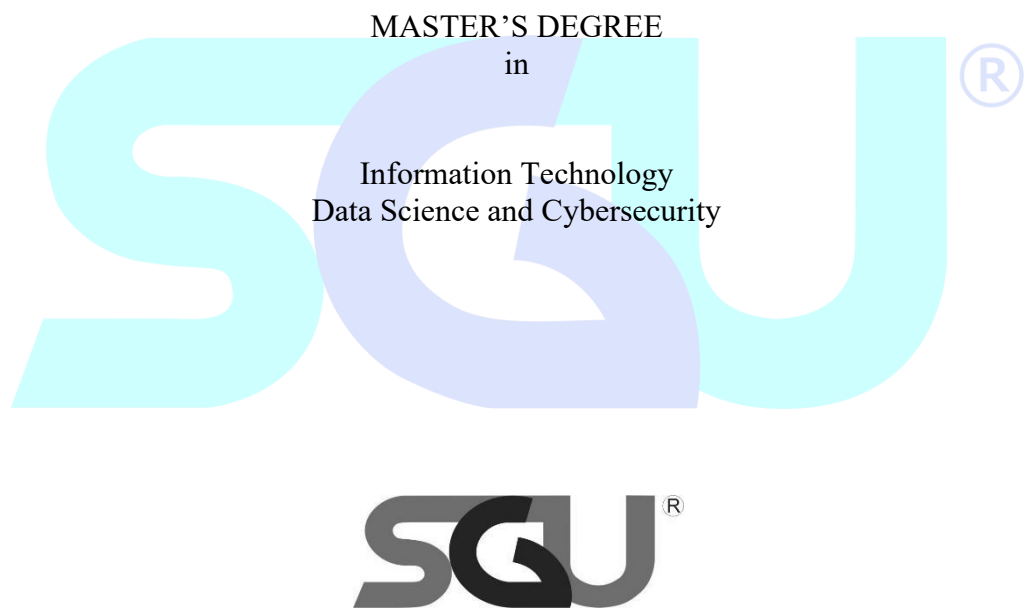


**Improving Cybersecurity Resiliency in Connected Vehicles
by Using COBIT in Car Rental Company**

By

Sit Wen Hu
22451007



SWISS GERMAN UNIVERSITY
The Prominence Tower
Jalan Jalur Sutera Barat No. 15, Alam Sutera
Tangerang, Banten 15143 - Indonesia

February 2025

STATEMENT BY THE AUTHOR

I hereby declare that this submission is my own work and to the best of my knowledge, it contains no material previously published or written by another person, nor material which to a substantial extent has been accepted for the award of any other degree or diploma at any educational institution, except where due acknowledgement is made in the thesis.

Sit Wen Hu

Student

Date

Approved by:

Dr. Ir. Mohammad Achmad Amin Soetomo, M.Sc

Thesis Advisor

Date

Dr. Ir. Heru Purnomo Ipung, M.Eng

Thesis Co-Advisor

Date

Dr. Ir. Maulahikmah Galinium, S.Kom, M.Sc.

Dean of Faculty of Engineering and
Information Technology

Date

Sit Wen Hu

ABSTRACT

IMPROVING CYBERSECURITY RESILIENCY IN CONNECTED VEHICLES BY USING COBIT IN CAR RENTAL COMPANY

By

Sit Wen Hu

Dr. Ir. Mohammad Achmad Amin Soetomo, M.Sc.

Dr. Ir. Heru Purnomo Ipung, M.Eng.

SWISS GERMAN UNIVERSITY

Connected vehicles have come with both convenience and risks. Despite positive attributes of connected vehicles that improve safety and driving experience, connected vehicles also come with its own risks toward safety and security. Various safety standards to regulate car manufacturers and their OEM in producing modern vehicles have been issued. Unfortunately, the same can not be said about security of modern vehicles. These companies tend to operate in archaic cybersecurity protocols – thus exposing customers and owners of fleet of vehicles to cybersecurity risks that are not only causing financial damage, but also could harm anyone in that vehicle. This condition is also exacerbated by different interests between car manufacturers, OEMs, fleet owners, customers, and other stakeholders, especially when related to data and privacy management. In response, regulators have issued many standards to address this but still ended in various regulations and standards that were not to address specifically to automotive cybersecurity. This in turn, would cause customers and fleet owners at complicated automotive cybersecurity regulations that are not in favor to their interests. COBIT helps to not only making sure that Enterprise Goals are aligned with IT goals, but also transforming cybersecurity mindset at every level of the company. This would require robust IT governance model and strong tone from the top to ensure risk optimization are implemented within structured and accountable process.

Keywords: Automotive Cybersecurity, COBIT, Connected Vehicles, IT Governance, ISO 21434, Car Rental.



DEDICATION

I dedicate this works for better Automotive Cybersecurity awareness in Indonesia



ACKNOWLEDGEMENTS

I wish to thank the members of my family and friends for their support, patience and good humor.



TABLE OF CONTENTS

	Page
STATEMENT BY THE AUTHOR.....	2
ABSTRACT.....	3
DEDICATION.....	5
ACKNOWLEDGEMENTS.....	6
TABLE OF CONTENTS.....	7
LIST OF FIGURES	9
LIST OF TABLES.....	11
CHAPTER 1 – INTRODUCTION	12
1.1. Background.....	12
1.2. Research Problem	17
1.3. Research Objective	17
1.4. Research Question	18
1.5. Hypothesis.....	18
1.6. Research Scope and Limitation.....	19
1.7. Significance of Study.....	19
1.8. Thesis Structure	19
CHAPTER 2 – AUTOMOTIVE CYBERSECURITY AND IT GOVERNANCE.....	20
2.1. Understanding Car Rental Business.....	24
2.2. Modern Automotive System Architecture	27
2.3 Attack Surface for Modern Vehicle	31
2.3.1 Threats posed by User Operation and Attackers’ Interference	31
2.3.2 Direct and Indirect Threats	31
2.3.3 Automotive Industry Response.....	33
2.4 Designing Governance Model That Accommodate Cybersecurity Framework....	36
2.4.1 COBIT 2019.....	36
2.4.2 NIST Cybersecurity Framework (CSF)	38
2.4.3 COBIT and NIST Addressing Cyber Resiliency	41
2.4.4. ISO 27000, ISO 21434, and UNECE R155	43
2.5 Other Standards and Best Practices	49

2.5 Selected Related Works	50
CHAPTER 3 – RESEARCH METHODS	66
3.1. Research Framework	66
3.2. Data Collection and Analytical Method	68
3.3. Evaluation Method.....	68
3.4. Validation Method	70
CHAPTER 4 – RESULTS AND DISCUSSIONS.....	72
4.1. Overview.....	72
4.2. Data Obtained	72
4.3. Data Analysis	72
4.4. Overall Survey Response	73
4.4.1 On Strategy and Policy	74
4.4.2 On Risk Assessment and Risk Management	75
4.4.3 Security Controls and Implementation	75
4.4.5 Compliance and Legal	76
4.4.6 Incidents Response and Recovery	77
4.4.7 Aftermarket Products	78
4.4.8 Investment in Automotive Cybersecurity	79
4.5 Risk assessment results	79
4.6. Recalibrating Survey Results to meet COBIT NPLF	80
CHAPTER 5 – CONCLUSIONS AND RECCOMENDATIONS.....	82
5.1. Conclusions.....	82
5.2. Future Works	82
5.3. Recommendations.....	82
GLOSSARY	83
REFERENCES	88
CURRICULUM VITAE	90

LIST OF FIGURES

Figures	Page
Figure 1. 1 Software-Based Recall vs Non-Software Based Recall	13
Figure 1. 2 Cause and Effect Diagram for Connected Vehicle Hacking	14
Figure 2. 1 Shared-Mobility business in Indonesia based on numbers of users	24
Figure 2. 2 Simplified Fleet Management System Architecture.....	26
Figure 2. 3 Automotive System Lifecycle	27
Figure 2. 4 Levels of Driving Automation.....	28
Figure 2. 5 Automotive System	29
Figure 2. 6 IPA Car System	30
Figure 2. 7 Direct Threats against Automotive System	32
Figure 2. 8 Indirect Threats against Vehicles	33
Figure 2. 9 TMC Information Quality Management Meeting Structure	34
Figure 2. 10 COBIT Core Component.....	37
Figure 2. 11 NIST Cybersecurity Function.....	38
Figure 2. 12 ISO 27000 Family (Source: (ISO IEC, 2018)	44
Figure 2. 13 ISO 21434 (Source: ISO SAE, 2021).....	47
Figure 2. 14 Aligned Lifecycle combining cybersecurity, functional safety and SOTIF (Source: (Ward & Wooderson, 2021)	48
Figure 2. 15 ISO SAE 21434 and UNECE R 155 Relationship	49
Figure 2. 16 Relationship between COBIT, ISO 27001, ISO 21434, R155, and Industry Best Practices and Guidelines.....	50
Figure 2. 17 Systematic Literature Review Process	51
Figure 2. 18 Co-Occurrence Keyword Network.....	53
Figure 2. 19 AE Cyberattack Received from Articles	56
Figure 2. 20 AE Mitigation Retrieved from Article.....	56
Figure 2. 21 OSI Stack Protocols vs AE Schema	57
Figure 2. 22 Generic Modern Vehicle Architecture	58
Figure 2. 23 The Largest Threat Surface in the World	59
Figure 2. 24 Identifying Stakeholders Need for Connected Vehicles.....	23
Figure 2. 25 FMS Simplified System Architecture	Error! Bookmark not defined.
Figure 3. 1 Number of Research form "Automotive Cybersecurity" Keyword.....	67
Figure 3. 2 Research Timeline	71
Figure 4. 1 Survey Results	73
Figure 4. 2 Overall Survey Response.....	74
Figure 4. 3 Strategy and Policy	74
Figure 4. 4 Risk Assessment and Management	75
Figure 4. 5 Security Controls and Implementation	75

Figure 4. 6 Awareness and Training	76
Figure 4. 7 Compliance and Legal	77
Figure 4. 8 Incidents Response and Survey	77
Figure 4. 9 Aftermarket Products.....	78
Figure 4. 10 Investment in Automotive Cybersecurity.....	79
Figure 4. 11 Impact and Likelihood Table.....	80
Figure 4. 12 Risk from Use Case - Before and After Control	80



LIST OF TABLES

Table	Page
Table 2. 1 Capability of IPA Car Based on Functions.....	30
Table 2. 2 Mapping Table for Functions and Threats.....	33
Table 2. 3 CSF Core Functions.....	39
Table 2. 4 CSF 2.0 Core Function and Category Names and Identifiers.....	39
Table 2. 5 NIST and COBIT Relations on to Boost Resiliency	41
Table 2. 6 Clusters of Research Scientific Field.....	53
Table 2. 7 List of Typical Attack on Vehicle and its Components.....	55
Table 2. 8 Consequences of Safety and the Applications of AE mitigation.....	57
Table 2. 9 List of Regulations, Standards and Best Practices.....	60
Table 2. 10 Identified principles of cybersecurity in vehicles and the contributions of each of selected legislative instruments	62
Table 2. 11 Review of Related Works	63
Table 3. 1 Comparison between IOT and Connected Vehicles and CIA at Risk	22
Table 3. 2 Survey Objectives	69
Table 4. 1 Risk Register for Selected Automotive Cybersecurity Use Case	79