

**ENHANCING ENTERPRISE SECURITY POSTURE: DESIGN IT/OT RISK
MANAGEMENT ON XYZ ORGANIZATION USING MULTI-CRITERIA
DECISION ANALYSIS APPROACH**

By
Brilian Adi Saputra
21551009

MASTER'S DEGREE
in
MASTER OF INFORMATION TECHNOLOGY
FACULTY OF ENGINEERING AND INFORMATION TECHNOLOGY



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

August 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.

Brilian Adi Saputra



Student

25-8-2025

Date



Approved by:



Dr. Ir. Charles Lim, Msc., Bsc.

25/8/25

Thesis Advisor

Date

Dr. Eka Budiarto, S.T., M.Sc.



Thesis Co-Advisor

25-8-2025

Date

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

Dean of Faculty of Engineering and Information Technology

Date

ABSTRACT

ENHANCING ENTERPRISE SECURITY POSTURE: DESIGN IT/OT RISK MANAGEMENT ON XYZ ORGANIZATION USING MULTI-CRITERIA DECISION ANALYSIS APPROACH

By

Brilian Adi Saputra

Dr. Ir. Charles Lim, B.SC, M.Sc. , Advisor

Dr. Eka Budiarto, S.T., M.Sc. , Co-Advisor

SWISS GERMAN UNIVERSITY



This thesis supports the Indonesian government's "Making Indonesia 4.0" initiative by addressing cybersecurity challenges in XYZ Organization, a state-owned manufacturer facing IT/OT convergence risks. With no defined maturity model or clear risk prioritization, the study develops a strategic IT/OT risk management framework using ISO/IEC 27005 and NIST SP 800-30. Applying STRIDE to the SAP-MES integration identified 34 threats, evaluated through a 5x5 likelihood-impact matrix aligned with COSO standards, highlighting 10 critical risks—such as equipment damage and backup failure—scoring 20/25. Mapped to ISO 27001 controls, tailored mitigation strategies are proposed, resulting in a structured, repeatable framework that strengthens cybersecurity governance and aligns with digital transformation and national mandates.

Keywords: IT/OT Convergence, Risk Management, Cybersecurity, Industry 4.0, STRIDE, Risk Prioritization, Multi-Criteria Decision Analysis (MCDA), Manufacturing



DEDICATION

I would like to dedicate this research project to my God, my family, my beloved country Indonesia.



ACKNOWLEDGEMENT

I would like to express my deepest gratitude to Dr. Ir. Charles Lim, B.SC, M.Sc. and Mr. Dr. Eka Budiarto, S.T., M.Sc. as my thesis advisors, and to the expert advisor who served as a valuable discussion partner. I am sincerely thankful for the time, support, and knowledge shared throughout the course of this research project and the completion of this thesis. It is through their invaluable contributions that this thesis and the entire research endeavor have reached this stage.

I would also like to thank my family for their countless moral support during my academic journey at SGU. I cannot thank you enough for the time, patience, and sacrifices that have enabled me to complete this thesis.

Lastly, I would like to express my appreciation to my direct supervisors, my team at work, and my friends, especially Batch 34 MIT SGU, for their constant encouragement and companionship. I am also grateful to the many individuals who have supported me throughout this research project, whether directly or indirectly.

Table of Contents

	Page
STATEMENT BY THE AUTHOR	1
ABSTRACT	2
DEDICATION	4
ACKNOWLEDGEMENT	5
TABLE OF CONTENTS	9
LIST OF FIGURES	10
1. INTRODUCTION	13
1.1 Background	13
1.2 Problem Statement	16
1.3 Research Objective	17
1.4 Research Question	17
1.5 Hypothesis	17
1.6 Scope and Limitation	18
1.7 Significance of Study	18
1.8 Thesis Structure	19
LIST OF TABLES	13
2. LITERATURE REVIEW	21
2.1 The Evolution of Industrial System	21
2.1.1 The First Industrial Revolution (Industry 1.0): The Dawn of Mechanization and the Factory Economy (c. 1760–1840)	22

2.1.2	The Second Industrial Revolution (Industry 2.0): The Power of Networks and Mass Production (c. 1870–1914)	23
2.1.3	The Third Industrial Revolution (Industry 3.0): The Digital Age and the Knowledge Economy (c. 1960s–2000s)	25
2.1.4	The Fourth Industrial Revolution (Industry 4.0): The Advantage of Intelligent, Integrated Systems (c. 2011–Present)	26
2.1.5	Summary of Industrial Revolutions	28
2.2	A National Strategy for Industrial Revitalization and Digital Convergence	30
2.2.1	The Imperative for Transformation: Economic Context and Rationale	30
2.2.2	The Vision and Aspirations of a Top 10 Economy	31
2.2.3	The "Making Indonesia 4.0" Implementation Blueprint	32
2.2.4	Mandating IT and OT Convergence	34
2.2.5	A National Assessment Industry 4.0 Readiness Framework	35
2.3	XYZ Organization and the National Industrial Modernization Mandate	37
2.4	Digital Transformation in Manufacturing Industry	39
2.5	The Expanded Attack Surface in IT/OT Converged Manufacturing Industries	46
2.5.1	Anatomy of an Industrial Cyber Attack: The Ransomware Threat	49
2.6	Risk Management	51
2.6.1	ISO 31000:2018 - The Enterprise-Wide Guideline	51
2.6.1.1	Core Components of ISO 31000	52
2.6.2	ISO/IEC 27005:2022 - The Information Security Specialization	56
2.6.2.1	Core Components of ISO 27005	56
2.6.3	NIST SP 800-30 Rev. 1 - The Prescriptive Assessment Guide	59
2.6.3.1	Core Components of NIST SP 800-30	60
2.6.4	Review of Established Risk Management Frameworks	63
2.6.4.1	Overview of Standard Frameworks	63
2.6.4.2	Comparative Analysis	64
2.7	Cyber Security Risk Assessment	66
2.7.1	Threat	66
2.7.2	Vulnerability	66

2.7.3	Impact	66
2.7.4	Risk Scoring	67
2.8	Threat Modelling	70
2.8.1	Threat Modelling Methodologies	72
2.8.1.1	STRIDE	72
2.8.1.2	PASTA	73
2.8.1.3	Attack Trees	73
2.8.1.4	VAST	73
2.8.1.5	TRIKE	74
2.8.1.6	OCTAVE	74
2.9	Related Works	75
3.	RESEARCH METHODS	79
3.1	Research Framework	79
4.	RESULTS AND DISCUSSIONS	87
4.1	Context Establishment	87
4.1.1	Contextual Analysis	87
4.1.2	Data Collection	88
4.1.3	Asset Identification	88
4.1.4	Data Flow Diagram	89
4.2	Risk Identification	90
4.2.1	Threat Identification	91
4.2.2	Threat List	92
4.3	Risk Analysis	93
4.3.1	Threat Likelihood	93
4.3.2	Threat Impact	93
4.3.3	Associated Risk	93
4.4	Risk Evaluation	99
4.4.1	Risk Prioritization	99
4.5	Risk Treatment	100
4.5.1	Risk Control	101
4.6	Evaluation	105

4.7	Validation	106
4.8	Results Summary	108
5.	CONCLUSIONS AND RECOMMENDATIONS	111
5.1	Conclusions	111
5.2	Recommendations	111
5.3	Future Works	112
	REFERENCES	113
A.	List of Threat Information	122
B.	Forum Group Discussion of Prioritizing Cybersecurity Risk Control . . .	134
C.	Risk Control Prioritization Formula	138
D.	Internal Stakeholder Evaluation Questionnaire	142
E.	Expert Profile and Questionnaire Answer	145
F.	Documentation of FGD and Expert Validation Process	147

List of Figures

1.1	Most Cyber Attacks in Indonesia (EnsignInfoSecurity.Pte.Ltd., 2024) . .	14
1.2	Most Targeted Industry Group in Asia-Pacific (EnsignInfoSecurity.Pte.Ltd., 2024)	15
1.3	Fishbone Diagram	16
2.1	Industrial Revolution (Michael A. Vidalis, 2022)	29
2.2	5 Pillars and 17 Areas in INDI 4.0	36
2.3	IIoT-based ICS Network (Liu et al., 2022)	45
2.4	ISO 31000 Risk Management Process (practicalrisktraining, 2025) ® .	54
2.5	ISO 27005 Information Security Risk Management Process (ISO, 2022)	57
2.6	NIST SP 800-30 Risk Assessment Process (NIST, 2012)	61
3.1	Research Framework	79
3.2	Risk Matrix (Society of Corporate Compliance and Ethics and Health Care Compliance Association, 2020)	83
4.1	Data Flow Diagram SAP-MES System	90
F.1	Documentation of Expert Validation Interview (1)	147
F.2	Documentation of Expert Validation Interview (2)	147
F.3	Documentation of Expert Validation Interview (3)	148

List of Tables

2.1	Summary of the Industrial Revolutions and Evolving Economic Impact .	29
2.2	10 National Priority in Making Indonesia 4.0	33
2.3	The Five Pillars of the INDI 4.0 Framework	37
2.4	Comparison of IT vs. OT Priorities and Characteristics	41
2.5	The Purdue Model Layers in XYZ Organization	44
2.6	Framework Comparison	65
2.7	Likelihood of Occurrence in the Context of PT XYZ	67
2.8	Impact of Compliance Risks	70
2.9	Focused Comparison of Threat Modeling Methodologies	75
2.10	Related Works Summary	76
4.1	List of Asset on Integration SAP-MES System	89
4.2	Entry Point and Trust Level	91
4.3	STRIDE Threat Mapping by Process	92
4.4	Risk Mapping	94
4.5	Risk Prioritization	99
4.6	Control Prioritization	102
A.1	Misuse Case – Brute-force Login Attempts (HMI)	122
A.2	Misuse Case – Unauthorized Control Command Injection (HMI)	122
A.3	Misuse Case – Information Disclosure (HMI)	122
A.4	Misuse Case – Denial of Service (HMI)	123
A.5	Misuse Case – Repudiation of Operator Actions (HMI)	123
A.6	Misuse Case – Unauthorized Access/Manipulation (SCADA)	123
A.7	Misuse Case – Real-time Data Tampering (SCADA)	124
A.8	Misuse Case – Denial of Service (SCADA)	124
A.9	Misuse Case – Information Disclosure from SCADA Database	124

A.10 Misuse Case – Repudiation of SCADA Actions	125
A.11 Misuse Case – Unauthorized PLC Program Modification	125
A.12 Misuse Case – Denial of Service (PLC)	125
A.13 Misuse Case – PLC Firmware/Configuration Disclosure	126
A.14 Misuse Case – PLC Spoofing (Impersonation)	126
A.15 Misuse Case – Unauthorized Access to MES GUI/Apps	126
A.16 Misuse Case – Data Tampering (MES Apps/Database)	127
A.17 Misuse Case – Denial of Service (MES Server)	127
A.18 Misuse Case – Information Disclosure from MES Database	127
A.19 Misuse Case – Repudiation of Supervisor/IT Admin Actions (MES) . .	128
A.20 Misuse Case – BAPI Call Spoofing/Tampering (MES-SAP Integration) .	128
A.21 Misuse Case – Information Disclosure (Integration Interface)	128
A.22 Misuse Case – Denial of Service (Integration Interface)	129
A.23 Misuse Case – Brute-force Login Attempts (SAP GUI)	129
A.24 Misuse Case – Session Token Hijacking (SAP GUI)	129
A.25 Misuse Case – Repudiation of User Actions (SAP GUI)	130
A.26 Misuse Case – Unauthorized Access to SAP ECC Apps/HANA	130
A.27 Misuse Case – Data Tampering within SAP ECC/HANA	130
A.28 Misuse Case – Information Disclosure from SAP HANA Database . . .	131
A.29 Misuse Case – Denial of Service (SAP ECC/HANA Server)	131
A.30 Misuse Case – Unauthorized Access to Backup Server	131
A.31 Misuse Case – Backup Data Tampering/Corruption	132
A.32 Misuse Case – Information Disclosure from Backups	132
A.33 Misuse Case – Denial of Service (Backup Server/Storage)	132
A.34 Misuse Case – Repudiation of Backup Operations	133
C.1 Risk Controls with Scores, Normalization, and Priority	139
D.1 Evaluation Questionnaire	142
E.1 Expert Profile	145
E.2 Expert Questionnaire Result - Risk Domain	145
E.3 Expert Questionnaire Result - Threat Modelling Domain	146
E.4 Expert Questionnaire Result - Compliance Domain	146