

**CYBERSECURITY RISK ASSESSMENT AND THREAT MODELING
FOR TANKER BERTHING SYSTEM IN OFFSHORE OIL AND GAS
FPSO PLATFORM**

By

Bagus Wibowo
Student ID 22451018



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

[August 2025]
Revision after the Thesis Defense on August 12th 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.

Bagus Wibowo

Student

Date



Approved by:

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

Thesis Advisor

Date

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

Thesis Co-Advisor

Date

Dr. Maulahikmah Galinium S.Kom M.Sc

Dean

Date

Bagus Wibowo

ABSTRACT

CYBERSECURITY RISK ASSESSMENT AND THREAT MODELING FOR TANKER BERTHING SYSTEM IN OFFSHORE OIL AND GAS FPSO PLATFORM

By

Bagus Wibowo

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

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

SWISS GERMAN UNIVERSITY

Digitizing FPSO systems improves operations, it also exposes them to cyberattacks that can cause financial, operational, safety, and environmental harm. Thus, ensuring continuous operation during a security incident is as vital as preventing the attack itself. The thesis emphasizes the critical importance of securing FPSO Tanker Berthing Systems (TBS). It highlights a study's recommendation for a new, more effective cybersecurity framework for TBS. This framework integrates the NIST Cybersecurity Framework's Identify and Protect functions, STRIDE threat modeling, and a Risk Matrix. This approach is lauded for its effectiveness in identifying threats (specifically the "Tanker Berthing System Application Base Station" as a key weak point) and providing a comprehensive threat modeling methodology that spans from high-level governance to detailed technical attacks.

In conclusion, the research finds that this framework improves the accuracy of identifying OT (Operational Technology) cybersecurity risks and boosts predictive cybersecurity strategies. The thesis stresses that proactive risk identification and effective threat modeling are crucial for preventing cyber incidents, cutting operational costs, and maintaining continuous, efficient, and secure offshore oil and gas operations. The core message is that securing FPSO tanker berthing systems necessitates an integrated, evolving security program, a deep grasp of cyber-physical risks, structured methodologies, constant vigilance, and robust cross-functional communication within the organization.

Keywords: Tanker Berthing Systems, FPSO, Offshore Oil and Gas, Risk Assessment, NIST CSF, STRIDE Threat Modelling, Risk Matrix.



DEDICATION

I dedicate this work for my parents, wife, children and
future of the country I loved: Indonesia



ACKNOWLEDGEMENTS

I would like to thank to Mr. Dr. Ir. Charles Lim, M.Sc., B.Sc. and Mr. Dr. Ir. Eka Budiarto, S.T., M.Sc. as my thesis guides, for giving me opportunity to work on this thesis. Under their guidance I was able to complete this thesis in a short period of time, putting me in a good position for my graduation and also gave me various ideas for making this thesis successful and unblocked at times pivoting my thought process during the course of this thesis.



TABLE OF CONTENTS

	Page
STATEMENT BY THE AUTHOR.....	2
ABSTRACT.....	3
DEDICATION.....	5
ACKNOWLEDGEMENTS.....	6
TABLE OF CONTENTS.....	7
LIST OF FIGURES	10
LIST OF TABLES.....	12
CHAPTER 1 – INTRODUCTION	13
1.1. Background.....	13
1.2. Research Problem	17
1.3. Research Objective	18
1.4. Research Question	18
1.5. Hypothesis.....	18
1.6. Research Scope and Limitation	19
1.7. Significance of Study.....	20
1.8. Thesis Structure.....	20
CHAPTER 2 - LITERATURE REVIEW	22
2.1. Onshore Oil and Gas Process.....	22
2.2. Offshore Oil and Gas Process	22
2.3. Tanker Berthing Systems.....	24
2.3.1. Challenge of Tanker Berthing Systems	25
2.4. Operational Technology Standard	25
2.4.1. IEC 62443.....	26
2.4.2. Purdue Model.....	28
2.5. Risk Management Framework.....	30
2.5.1. The National Institute of Standards and Technology (NIST) v2.0 in Maritime.....	30

2.5.2. MaCRA (Maritime Cyber Risk Assessment) Framework.....	31
2.6. Threat Modeling	31
2.6.1. Threat Modeling Framework.....	31
2.6.1.1. STPA-Sec.....	31
2.6.1.2. CORAS.....	33
2.6.1.3. MITRE ATT&CK.....	36
2.6.1.4. STRIDE.....	37
2.6.1.5. PASTA.....	40
2.6.1.6. ATTACK TREE.....	42
2.7. The relationship between a Risk Management Framework (RMF) and Threat Modeling	43
2.8. CVSS.....	45
2.9. Risk MATRIX	48
2.9.1. US Department of Defense (DoD).....	48
2.9.2. NASA's 5 × 5 Matrix Adaptation.....	48
2.10. RELATED WORKS.....	52
2.10.1. RELATED WORKS FOR RISK ASSESSMENT.....	52
2.10.1. RELATED WORKS FOR THREAT MODELLING.....	55
2.10.1. RELATED WORKS FOR RISK ASSESMENT and THREAT MODELLING	59
2.11. Finding Threats with STRIDE.....	65
2.11.1 Data Flow Diagram.....	65
CHAPTER 3 – RESEARCH METHODS	69
3.1. Research Design.....	69
3.2. Research Framework	70
3.1.1 Scope & Asset Inventory (CSF: Identify).....	73
3.1.2. Threat Modeling with STRIDE.....	73
3.2. Data Collection & Analysis.....	74
3.3. Discussion and Evaluation Method.....	74
CHAPTER 4 – RESULTS AND DISCUSSIONS.....	76
4.1. Overview.....	76

4.2. Data Obtained	77
4.3. Analytical Methode.....	78
4.3.1. System Understanding & NIST CSF: Identify.....	78
4.3.2. Threat Analysis.....	79
4.3.3. Applying STRIDE to the Tanker Berthing System.....	83
4.3.3.1. Applying STRIDE to the Tanker Berthing System Application of Data Flow Diagram.....	85
4.3.3.1. STRIDE Threat Modeling Tanker Berthing Application.....	91
4.3.3.1.1. Boundary 1: External Data Source.....	93
4.4. Discussion for Evaluation	98
4.5. Validation.....	103
CHAPTER 5 – CONCLUSIONS AND RECCOMENDATIONS	107
5.1. Conclusions.....	107
5.2. Recommendations.....	108
REFERENCES.....	111
GLOSSARY	115
APPENDIX A.....	116
APPENDIX B.....	139
APPENDIX C.....	142
CURRICULUM VITAE	145

LIST OF FIGURES

Figures	Page
Figure 1.1. Tanker Berthing Systems Tablet Computer.....	13
Figure 1.2. Oil Offloading Operation from FPSO to Tanker.....	13
Figure 1.3. Concept of Operation Tanker Berthing in OffshoreFPSO.....	15
Figure 1.4. Telemetry System with UHF Radio Communication and DGPS between FPSO and Tanker.....	16
Figure 1.5. Number of cyber incidents per impact area 2010-2023.....	16
Figure 1.6. Fish Bone Diagram.....	17
Figure 2.1 Offshore Oil and Gas Platform FPSO.....	23
Figure 2.2 Offshore Oil and Gas Process.....	23
Figure 2.3. Tanker Berthing System Human Machine Interface.....	24
Figure 2.4. IT/OT Architecture of Tanker Berthing Systems.....	25
Figure 2.5. IEC 62443 zones and conduits isolate threats.....	28
Figure 2.6. Industrial Control System Network Refer to a Purdue Enterprise Reference Architecture (PERA), or Purdue model for short.....	29
Figure 2.7. NIST Framework.....	30
Figure 2.8. Classic DFD Model.....	65
Figure 3.1. Research Design.....	70
Figure 3.2. Research Framework NIST CSF Identify, Critical Asset, STRIDE.....	71
Figure 3.3. Assets, Business Process, Governance and Supply Chain.....	72
Figure 4.1. Tanker Berthing System Infrastructure Diagram in FPSO.....	76
Figure 4.2. TBS Base Station in FPSO.....	77
Figure.4.3. Tanker Berthing Systems Decomposition.....	79
Figure.4.4. Tanker Berthing System Hierarchy.....	80
Figure 4.5. TBS Base Station Application Overview.....	82
Figure 4.6. Data Flow Diagram Level 0 of Tanker Berthing Systems.....	85
Figure 4.7. Boundary 1: DFD L1 External Data Source.....	87
Figure 4.8. Boundary 2: DFD L1 External Data Source.....	88

Figure 4.9. Boundary 3: DFD L1 External Data Source.....89

Figure 4.10. Boundary 4: DFD L1 Base Station, Alarm & Warning, Work Station...90



LIST OF TABLES

Table	Page
Table 2.1. Security Assurance Levels.....	28
Table 2.2. Addressing Spoofing.....	38
Table 2.3. Addressing Tampering.....	38
Table 2.4. Addressing Repudiation.....	39
Table 2.5. Addressing Information Disclosure	39
Table 2.6. Addressing Denial of Service	39
Table 2.7. Addressing Elevation of Privilege.....	41
Table 2.8. NIST Cybersecurity Framework Functions and Categories.....	44
Table 2.9. NIST CSF elements to STRIDE threat categories	45
Table 2.10. Risk Matrix	50
Table 2.11. Risk Level Rating Required Authority of Approval	51
Table 2.12. Summarizes of critical review of related works for Risk Assessment ...	51
Table 2.13. Summarizes of critical review of related works for Threat Modelling ...	55
Table 2.14. Summarizes of critical review of related works for Risk Assessment and Threat Modeling.....	59
Table 2.15. Summarize the comparison of related works.....	61
Table 2.16. Element of Data Flow Diagram.....	66
Table 2.17. STRIDE per Interaction: Threat Applicability.....	68
Table 3.1. Overview of the Three Components.....	71
Table 4.1. NIST CSF Asset Identification.....	81
Table 4.2. Mapping TBS Component to STRIDE.....	83
Table 4.2 Data Acquisition & Protocol Conversion (Process)	
Risk Matrix	97