ASSESSING CYBER RISKS IN CYBER-PHYSICAL SYSTEMS USING THE ATTCK FRAMEWORK

Cameron Noakes

January 2022

1 Sentence Overview

Heavy focus on Autonomous Passenger Ships (APSs) as a solution for passenger transport. The authors focus was to examine the safety and security implications of the Cyber Physical System (CPS). Results are presented from undertaking a 'Failure Modes Effects and Critical Analysis' (FMECA) on a communication architecture (determines the method and frequency by which information, attention, and intent flows between people, teams, and systems).

Population and enrichment of some ATT&CK framework components were used in the FMECA process to facilitate the tactics and methodology of attackers. Metrics are given to accompany the FMECA process through a group of graph theory-based metrics for the impact estimation of the identified risks then further integrated for extraction of the current risks and their corresponding countermeasures applied.

2 Introduction - Notes

Cyber attacks that target the maritime domain are increasing both in numbers and severity, due to the current ongoing digital transformation age we live in today. Example of prevalence is against the COSCO shipping company as a cyber attack.

APS and its security risks can directly or indirectly endanger the safety of the passengers which highlights its severity when lives are at risk on maritime

domains, such attacks are said to also cause issues with the operational environment.

3 Background

A centralized component named Autonomous Ship Controller (ASC) resides in the center of the APS network which hosts the primary and backup servers. A group of systems resides in the Risk Control Center (RCC) network for remote navigation functions, control functions, and additional ship-to-shore communication functions.

The APS communicates with the RCC through two IP-based redundant communication modules:

- Mobile Communication Module (MCM)
- APS-RCC Module

4 MITRE ATT&CK framework

For the APS systems, a popular framework of MITRE ATT&CK was used due to the comprehensive nature of ATT&CK, how well it managed to determine all main adversarial tactics and techniques and was of particular importance for APS due to its utility to identify relevant threats for its components.

The framework ATT&CK was outlined by the authors/researchers to be logically compatible with FMECA which identified the usage of this framework to be the best fitting to the current research for APS systems.

5 The Proposed Risk Assessment Approach

The mentioned FMECA process consists of three main phases:

- planning the analysis
- performing it
- finally documenting it.

The ATT&CK framework aids in the FMECA process as it describes attack techniques and tactics that can be used to induce failure scenarios to help identify risks.

An algorithm is used to determine the critical information based on given factors affecting the APS system. This paper also contributes a tool in which an algorithms is developed to identify and produce all the components an attack listed in each operation with RPN and mitigation methods for each attack.

6 What problem does this solve?

This paper outlines cyber attacks on APS systems and Cyber Physical Systems (CPS) through a process of FMECA with integrated threat modelling incorporated into the development of this process. Using this proposition enables a comprehensive risk assessment of APS and CPS infrastructure without the need of expert evaluations and judgement.

7 How do they solve it?

A quantitative risk assessment approach is proposed in this paper following a 'Failure Modes Effects and Critical Analysis' (FMECA) process model and utilizing the ATT&CK framework to develop it.

8 How do they assess it?

The approach has been evaluated through a tool using the RPN calculation and mitigation identification (RPNMI) algorithm. The tool has been used for conducting a risk assessment for the APS. The results provide current suggestions for suitable mitigation strategies to be included in the future APS security architecture to help protect the systems.

The RPNMI algorithm can calculate the overall value for each failure and from this can aid in the risk assessment process with an added benefit of measuring the proposed solutions success with it.