Thesis Portfolio

Trust and Security of Embedded Smart Devices in Advanced Logistics Systems
(Technical Report)

Human Factor on Computer Cyber Innovation
(STS Research Paper)

An Undergraduate Thesis Portfolio
Presented to the Faculty of the
School of Engineering and Applied Science
In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

By

Mai N Luu

May 8, 2021

Department of Engineering Systems and Environment

Table of Contents

Sociotechnical Synthesis

The technical topic's main goals are to find potential risks to the research and the development of embedded smart devices in advanced logistic systems. The analysis included various sections of Criteria, Initiatives, C-I Assessment, Emergent Conditions (EC), Criteria-Scenario (C-S) relevance and EC Grouping. System success criteria, research initiatives, and risks to the system are compiled. The success criteria of the system are the metrics that one uses in evaluating the success of the system. In addition to the establishment of the success criteria, initiatives are crucial for the success of the program. In the consideration of success criteria and initiatives, there are emergent conditions that can impact the ability to meet the success criteria. Potential scenarios can give rise to the emergent conditions that would impact the ability to meet the success criteria, so it is important to recognize them. To understand risks of emergent conditions, a list of Potential Scenarios is developed across innovations, environments, regulations, missions, populations and workforce behaviors, obsolescence, adversaries, etc. While the technical topic concentrates on evaluating the potential risks and scenario analysis of the advanced logistic system, the STS research focuses on researching the major threat to computer and information security that arise from humans. It is important to consider the human and social dimensions of the technology because changing in technology improves the society but society is the one that drives technological change. This paper addresses the negligence and recklessness of humans as metrics to determine potential risks to computers by human factors. The method is to collect historical data breaches by reliable sources and then categorize which cyber accident is caused by negligence or recklessness. Each scenario is weighted to indicate

how strong the effect by human factor on the scenario. The result will indicate how cybersecurity breach caused by human error affects the industry. Through the result, the paper aims to propose the possible solution to mitigate the human error in the system. The results presented in the technical and STS paper are applicable to the evaluation of security and risk for different purposes. The result of the technical paper should be of interest to developers, owners, and operators of critical infrastructure systems; while the result of the STS paper would be of broad significance in understanding major threats caused by human factors.