2015

# Submarine Pier Side Weapons Handling Risk Assessment

Vaneman, Warren; Sweeney, Joseph; Langford, Gary;
Parker, Gary; Wolfgeher, Chris; Harley, Willima

Monterey, California. Naval Postgraduate School

http://hdl.handle.net/10945/57942

# NAVAL POSTGRADUATE SCHOOL

# NAVAL RESEARCH PROGRAM

**MONTEREY, CALIFORNIA**

## SUBMARINE PIER SIDE WEAPNS HANDLING RISK ASSESSMENT

by

Dr. Warren Vaneman, Principal Investigator
Prof. Joseph Sweeney, Co-Principal Investigator
Dr. Gary Langford, Thesis Co-Advisor
Mr. Gary Parker, Research Associate
Mr. Chris Wolfgeher, Research Associate
LCDR Willima Harley, Master Degree Student

Period of Performance: 1 October 2015 – 30 June 2016

Prepared for: Navy Strategic Systems Program (SSP)
Sponsor: Mr. Brent Flaskerud, SP3015, Nuclear Weapon Security (NWS) Modeling and Simulation (M&S) and Demonstrations

# EXECUTIVE SUMMARY

## Project Summary

This research examines new methods to assess and improve Physical Protection Systems (PPS), paying specific attention to a Navy Level 3 Restricted Areas, a special type of industrial and refit zone that normally handles high value units such as aircraft carriers and ballistic missile submarines, utilizing Model Based Systems Engineering (MBSE) and System of Systems (SoS) theory to create a framework which couples architectural level PPS design with detailed discrete event security assessment and prediction techniques in order to provide decision makers and acquisition authorities a more quantitative and effective method to holistically understand a PPS and the PPS's internal and external interactions, allowing for improved capability and vulnerability analysis and the formulation of sound acquisition decisions.

This research investigates four key questions:

1. Are there gaps in the end-to-end security assessment process caused by Seemly Unrelated Security Violations (SUSV), separated by distance and time, which affect the total security of a system, which heretofore have not been identified but may be able to be identified with robust MBSE?

2. What artificial limitations imposed by traditional security analysis models can be removed by the utilization of a MBSE operational item centric approach?

3. What improvements can be realized for a SoI by treating it as a SoS and artificially splitting it into two ontologically separate systems: the SoI and the security system?

4. What insight in security system design optimization can be gained from utilizing the loss function in conjunction with MBSE for the conduct of security system analysis of alternatives?

## Background

The International Council on Systems Engineering (INCOSE) Systems Engineering Vision for 2025 states that today, "Engineers are hard pressed to keep up with the evolving nature and increasing sophistication of the threats to our cyber-physical systems. Cyber-security is often dealt with only as an afterthought or not addressed at all" (INCOSE 2014, 36). The issues identified by INCOSE are both symptoms of the problem that security, like many modern engineering problems, is very complex – complex beyond our means. Magnifying the complexity of this problem, and differentiating it from other similarly complex systems, current tools are insufficient to enable the effective design and analysis of system security.

Security Systems are subsystems of a System of Interest (SoI), designed to act as a boundary, with boundary conditions, to prevent or control access. Simple system security may consist of just a wall, and are thus just physical objects. Most modern system security consists of a multifaceted network of barriers, sensors, and humans, all interacting to fulfill the specific purpose of the security system. Making these systems even more complex, the usage of networked computers as an essential part of system security provides an additional dimension of complexity, allowing threats to utilize cyber vulnerabilities to assist in overcoming reinforced physical security and vice versa.

The objective of tools used to analyze security systems is to utilize different methods to simplify very complex, time-independent, and non-linear security systems, allowing for these systems to be evaluated in an efficient and meaningful manner. Most tools analyze the objects in the security system instead of the effectiveness of the function of security, making it nearly impossible to identify non-linear vulnerabilities, such as those resulting across security domains, or from Seemly Unrelated Security Violations (SUSV), which can occur over a wide range of distances and times.

Therefore, the Systems Engineering Community is in need of an architecture based framework that enables the assessment of the security function of a Systems of Interest that contains multi-domain security sub-systems and/or security sub-systems that are vulnerable to SUSVs.

## Findings and Conclusions (to include Process)

Research is in progress. Findings and conclusions will be available in the final report.

## Recommendations for Further Research

This research proposes a methodological approach to address research questions 1-4. The Strategic Systems Program (SSP) Nuclear Weapons Security (NWS) has been engaged in a comprehensive effort to document the security architectures in a MBSE environment. Given the existing data, an extension of this research is to assist SSP NWS use the data in their MBSE environment to address nuclear weapon security issues using, in part, the methodology being proposed by this research. This effort was not envisioned during the proposal phase, but has been found to be necessary to implement these methodological approaches. As such, the team is working with SSP NWS to help them understand their MBSE environment. This work will continue after this NRP is completed.