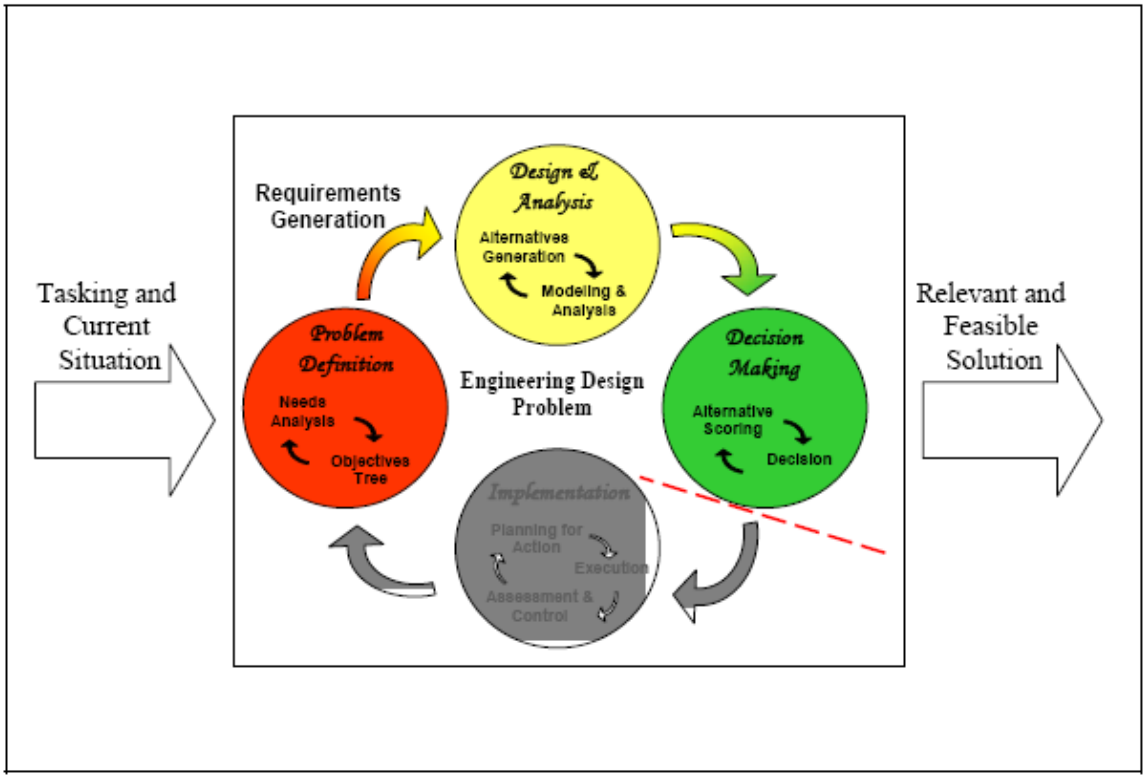
EXECUTIVE SUMMARY

The 2007 Naval Postgraduate School (NPS) Systems Engineering and Analysis (SEA) Integrated Project titled "Port Security Strategy 2012" (PSS12) was a joint product developed by eight NPS SEA students and 17 National University of Singapore (NUS) Temasek Defense Systems Institute (TDSI) students. The tasking letter from the Wayne E. Meyer Institute of Systems Engineering directed the Integrated Project to design a conceptual system of systems to improve port security measures for U.S. ports and force protection options for U.S. forces in U.S. and foreign ports. Port Security Strategy 2012 used the Systems Engineering Design Process as a tool to create a relevant and feasible solution given the tasking and on the situation postulated for the 2012 timeframe.



Systems Engineering Design Process

Following the September 11, 2001 terrorist attacks, the U.S. government shut down the air traffic system for two days and temporarily suspended the maritime

transportation system, preventing ships from entering U.S. ports. The United States realized that if a plane could be used as a feasible weapon, a ship and its cargo may also be used in a similar manner, shutting down a port and resulting in severe economic ramifications. For example in June 2002, an International Longshore and Warehouse Union strike ceased operations on all major U.S. West Coast ports. According to a Martin Associates study, a 10-day shutdown of the west coast ports cost the U.S. economy $19.4 billion. If the shutdown had extended to 20 days, the economic impact was postulated to increase to $48.6 billion dollars [1].

PSS12 involves a variety of stakeholders, each of whom holds different responsibilities. Their scopes of concerns were defined by local geography, economic, and political considerations, which led to four isolated but related areas of interest; consequently, PSS12 examined four areas concerning the range of issues raised by stakeholders. Organizations interested in port security include the Department of Homeland Security, United States Coast Guard, Marine Terminal Operators, Department of Defense, Regional & Local Police, Republic of Singapore Navy, Singapore Coast Guard, Singapore Civil Defence Force, among others. Each potential stakeholder presented different concerns, needs, and requirements, which were used to scope and bound the port security problem. Different stakeholders identified four primary areas of concern: threats originating from land (terrestrial threats), threats originating from foreign ports (source seaborne threats), threats originating from local waterways (regional seaborne threats), and threats originating from port employees (internal personnel threats). In order to address these primary areas in enough detail, it was essential to divide the team into four subgroups of five to six students each to address each issue.

Port Security 2012 formed the Terrestrial Threats Group (TTG), the Source Seaborne Threats Group (SSTG), the Regional Seaborne Threats Group (RSTG), and the Internal Personnel Threats Group (IPTG). The TTG considered threats from the land perimeter of the port to the pier-side ship. The scenario the TTG examined involved a container truck laden with explosives, which attempts to gain access to a terminal in a major U.S. port by speeding past security at the terminal’s entrance. The SSTG considered threats arriving from overseas ports. The SSTG scenario involved terrorists

coordinating a flood of containers holding weapons of mass destruction onto cargo ships bound for a domestic U.S. port. The RSTG considered waterborne surface threats from within the port boundary to the pier-side ship. The RSTG scenario involved multiple small boat attacks against moored ships and port infrastructure. The IPTG considered threats from personnel, who may or may not be employed by the port facility. The scenario the IPTG examined involved personnel collaborating to create maximum port infrastructure destruction.

Using the Systems Engineering methodology, PSS12 defined the problem and created threat scenarios. Each team constructed alternative system of systems for each scenario considered. Performance for each alternative was modeled, analyzed, and compared using predetermined measures of performance and effectiveness. Implementation deadlines and constraints contributed to alternative risks. The system implementation must be feasible within five years.

Consensus amongst the stakeholders required minimal impact on the flow of commerce in a commercial port and the flow of operations in a military port. Each alternative examined will incur research and development, procurement, and operating and support costs. Performance based on the modeling metrics, risk based on the economic or operational impact, and cost based on the total system cost are determining factors among system alternatives.

A number of modeling tools (e.g. MANA, Arena, Extend, Simkit, and/or Excel) were used by the TTG, RSTG, SSTG, and IPTG to evaluate the measures of performance effectiveness for each alternative and the status quo. Data from these models were collected and analyzed to compare these alternatives against current systems. Cost data and measures of effectiveness were coupled to determine a system that provided adequate effectiveness for reasonable cost. The model results and analysis would enable the stakeholder to make a well-informed decision regarding the employment of future systems in port security.

The key findings of the four operational scenarios are described on the following page:

Terrestrial Threats Group

- The TTG considered a possible vehicle-borne IED attack on a port facility. Perimeter security requirements significantly differ amongst all ports. Geographic, social, and legal constraints directly influence the feasibility of employing certain systems. The most important step in defending against vehicle-borne IEDs is to harden the perimeter barriers by steel-reinforced concrete blocks to the base of the existing chain link fencing.

- With the perimeter barriers in place, the gate is the only alternative point of terrestrial entry for vehicle-borne IEDs. Based on the modeling results and the cost benefit analysis, additional armed guards should not be employed due to their marginal improvement in effectiveness at high cost. Either the spike strips or pop-up barriers alternatives should be employed. While pop-up barriers are twice as effective as spike strips, they are also twice the cost.

Regional Seaborne Threats Group

- The RSTG considered multiple small boat attacks on the Port of Oakland. The small boat attack consisted of the simultaneous attack of 1, 2, 3, 4, 5, 6, 9 or 12 boats. The RSTG deployed various sensors and platforms in an attempt to successfully interrogate potential contacts of interest in order to avert an attack. A successful interrogation required the contact of interest to be in the sensor's classification/recognition/identification range for three minutes of simulation time. The percentage of terrorist successfully interrogated was the primary MOE.

- Based solely on the cost benefit analysis, the RSTG found that the addition of an Unmanned Surface Vehicle and two additional X-band radar stations (located on southern Tiburon Peninsula and at the southwest point of the former Alameda NAS) provided the most effectiveness for the least cost in one half of the scenarios. The addition of Sonar to the defense package drastically increased cost with marginal benefit. In six of the eight cases examined, the addition of a single X-band radar yielded largest improvement in terrorist detection rate over cost.

Source Seaborne Threats Group

- The SSTG considered the importation of 12 dirty containers from foreign ports. Using a transshipment hub, where thousands of containers are handled daily, terrorists can potentially introduce containers containing contraband into the shipping network. Sensors are deployed at the port of entry, crane spreaders, and holding yards to detect the presence of dirty containers. Customs inspections team would further be utilized to intrusively inspect all flagged containers suspected of container weapons of mass destruction. The primary MOEs considered include the probability

of detection, false alarm, missed detection, productivity, and average time to inspect each container.

- The best alternative is the high performance alternative which employs the Automatic Targeting System+, a gamma scanner and HAZMAT detector at the container holding and loading areas, and a fully equipped inspection station. These alternatives results in a cost of $82.67 million. A significant sensor mix is necessary for a high probability of detection. This sensor configuration should include a gamma scanner at the port of entry, radiation detectors and gamma scanners at holding areas, a scale and gamma scanner at loading areas, and a gamma scanner, HAZMAT detector, and trained animals at the intrusive inspection station.

Internal Personnel Threats Group

- The IPTG considered unauthorized employee physical access and unauthorized employee data access. Three models (Excel, Extend, and MANA) were used to determine the effectiveness of each alternative. The Extend and MANA models were integrated to produce the probability of interdiction for unauthorized physical access. Unauthorized data access was modeled using Excel.

- The current system has a 12 percent probability of interdiction for unauthorized physical access and 81 percent probability of interdiction for unauthorized data access. The presence of a mid-terminal fence with an open gate policy improved the probability of interdiction by 97 percent over the baseline. Combining communications, mid-terminal fence, and a triggered shut gate policy increased the probability of interdiction by 172 percent over the baseline.

While specific threats were examined by each of the respective groups, there remain other unexamined threats. The threats not examined in this report were not high priority threats as indicated by the PSS12 stakeholders. Some of these threats include air, mine, swimmer, underwater vehicle, and unmanned system threats.

Different agencies, whose efforts collectively provide port security, have different jurisdictions, organizational structures, and funding. A coordination problem exists amongst different agencies. The information received from the agencies must be rapidly received, displayed, interpreted and responded to in order for many of the modeled alternatives to be effective. From conducting this study, PSS12 recognized that the

fusion of data is a critical issue that needs to be addressed. Data fusion was beyond the scope of this project; however, is an area where future study is required.

Section I introduces the purpose of this study to include the background, concept of operations, operational environment, threat scenarios, scope, method, and chronology. Sections II, III, IV, and V introduce the needs analysis, alternatives generation, models, results, and analysis for the terrestrial threats group, regional seaborne threats group, source seaborne threats group, and internal personnel threats group, respectively. Section VI describes the conclusions, recommendations, and areas of future study for each of the subgroups.