MARITIME
SECURITY CENTER
A DEPARTMENT OF HOMELAND SECURITY CENTER OF EXCELLENCE

2021 Summer Research Institute
Student Research Project Abstracts

BlueROV

Abstract: The Stevens BlueROV is a remotely operated underwater vehicle (ROV) equipped with two imaging sonars and a monocular camera. This summer, the research team conducted a feasibility study to investigate the addition of robotic continuum manipulator arms to the modified BlueROV. The team was primarily interested in exploring the use of such arms for conducting high precision and energy-efficient maritime security tasks. The team met with experts in the field of Aid to Navigation (ATON) inspections and analyzed reports from local pier inspections. The team was then able to create a mission planning tool that used estimated speeds and battery usage to calculate the amount of time needed for different tasks. This tool is useful for estimating mission logistics, such as the numbers of ROVs required for a given mission. The two tasks addressed in the planning tool are pier piling inspection and ATON mooring chain inspection. Inspection of these two types of maritime infrastructure are important for public safety, along with the health of the waterways. In addition to the mission planning tool, simulations of the BlueROV with manipulator arms were created in order to demonstrate how the ROV would be able to grip onto the structures for better stability during inspection. By having the BlueROV conduct these inspections autonomously, the Coast Guard, MSC (Maritime Security Center), and other agencies could eliminate many of the risks associated with having divers inspect infrastructure. Further development of this technology could also lead to more time efficient and cost-effective missions.

Cybersecurity Risks in Offshore Windfarms

Abstract: With the emphasis on renewable energy resources, wind power is on the minds of everyone including the United States President Joe Biden, who plans to implement 30 gigawatts of offshore wind turbine energy by the year 2030. The growing development of wind farms, including onshore and offshore, might be a source of cyber-attack and could affect US critical infrastructure (CI) such as the power grid. This paper analyzes the extent to which offshore wind farms (OWF) may pose genuine cybersecurity threats to maritime operations and CI. Due to the newness of OWF, much about their potential cybersecurity threats remains unknown, thus access to information makes understanding specific attack vectors challenging. Furthermore, new cyber threats and vulnerabilities are constantly emerging. Despite mitigations, vulnerabilities remain in people, processes and technologies, and attackers are constantly trying to find new ways to break through cyber defenses. Through analyzing the elements in an OWF and their nodal connections, we have concluded that OWF are susceptible to cyber-attacks. This was determined by identifying and analyzing vulnerabilities which include: humans, offshore control centers, offshore substations, onshore substations, undersea cables, maritime vessels, and wind plants. The key scenario analyzed is the utilization of the onshore control center to gain access to the communications network and inject malware that will be transmitted to the wind turbines. Other vulnerabilities were also analyzed to demonstrate their immediate and widespread impact to secure the country's renewable energy in a cyber dominated environment. The team began its research by gaining a basic understanding of OWF and their vulnerabilities. It created an online learning tool that includes the knowledge developed; potential vulnerabilities; potential attack scenarios; frequently asked questions; and a library of resources used.

Hazardous Cargo Inspection

Abstract: An increasing number of container ship incidents such as ship fires are found to be caused by misdeclared and undeclared hazardous cargo. Container ship incidents have cost more than 100 billion dollars in lost cargo, environmental damage, and fires due to misdeclared and undeclared hazardous cargo. Overlooking these concerns could lead to damage to the cargo and vessel and more importantly, loss of life. The United States Coast Guard (USCG) inspects thousands of containers in an attempt to minimize this issue, however the United States sees over 11 million containers in imports alone, leaving the USCG unable to inspect the majority. This project aims to increase the success rate of finding non-compliant containers by targeting inspections for high-risk cargo, by developing an algorithm that can calculate the risk a container poses based on its attributes. The student team analyzed data sets of past inspections performed by the USCG and utilized this data to predict high-risk containers that should be inspected more frequently in the future. The team will also examine container numbers included in the data sets and utilize container validity calculations to find fraudulent containers. The team developed a container number calculator that automatically returns whether a container number is valid or not. In addition, the team has noted limitations in the data that the Coast Guard did not notice in the past. The resulting algorithm will be able to process input parameters such as hazard class and country of origin and identify the risk factor based on historical data.

GIS and USCG Data Visualization

Abstract: The USCG Marine Information for Safety & Law Enforcement (MISLE) database is a national repository of all maritime incidents. The database is composed of incidents related to maritime safety, security, and marine environmental protection. There is a wide range of incident types recorded in the database including search and rescue, vessel allisions, pollution reports, and security breaches to name a few. This summer's research project utilized MISLE data for the USCG Sector NY and is a continuation of work conducted in the MSC's 2020 Summer Research Institute program. This year's project uses ArcGIS and Esri software in lieu of Tableau software, to spatially display the MISLE incident data. The Dashboard is composed of a map, graphs and charts, and filters for an array data over weekly, monthly and annual time scales. The Dashboard can be used to conduct incident trend analysis and will allow for enhanced asset allocation.

Cybersecurity and Data Analysis USCG Internship Project

Abstract: Cyber-attacks on critical infrastructure including maritime information and operational technology have greatly increased over the past four years. For example, four of the world's largest global maritime shippers (i.e., CMA CGM, MSC, Maersk, and Cosco) have been impacted by varying forms of malware and ransomware, causing losses of millions of dollars and disruptions to critical supply chains including the maritime transportation system (MTS). The U.S. Coast Guard is responsible for ensuring the safety and security of the Nation's ports and waterways, including protecting the MTS against cybersecurity threats. An intern in the Stevens Maritime Security Center's 2021 Summer Research Institute engaged in a field-based internship with USCG Sector New York, to analyze the Coast Guard's process and procedures for conducting cybersecurity assessments. These assessments are a part of the Maritime Security Transportation Act (MTSA)-required facility and vessel security plans, as well as the USCG's cyber incident response efforts. The internship included accompanying Sector NY marine safety personnel on facility inspections, reviewing maritime facility cybersecurity plans, and observing the Sector's response to a suspected cyber breach on a vessel. Outcomes from the student's internship included the development of a cybersecurity assessment checklist for Coast Guard marine inspectors, a list of basic and best cybersecurity practices for maritime facility operators, and fundamental education and training recommendations for small and mid-sized maritime operators.