Reviews

Review on cybersecurity risk assessment and evaluation and their approaches on maritime transportation

Liang-Chieh Cheng[1,*], Yunpeng Zhang[2,*], Ben You[1, 2]

[1]*Department of Construction Management, College of Technology, University of Houston, Houston, TX 77004, USA*

[2]*Department of Information and Logistics Technology, College of Technology, University of Houston, Houston, TX 77004, USA*

Abstract

Maritime Transportation has become a major player in global logistics accompanied by an increasing number of cyberattacks to the vessels over the years. People begin to realize that it's critical to establish a cyber defense system on Maritime Transportation network in case the entire network would be paralyzed, which would lead to devastating consequences. Hackers, if intrude into the network successfully, can either mislead the direction of the vessels or steal or alter the information in the system, either of them would hurt the transportation business and eventually affect international trade. Cyber defense system is urgently needed to be established. As it has already been established in other sectors of the industries, an effective cyber defense system usually contains three layers: risk assessment, risk evaluation and risk mitigation. In this paper, we examine the risk assessment and evaluation methods reported in the literature and related efforts in applying them in maritime transportation network. We conclude paper with the suggestions of the directions for the future study of risk assessment and evaluation of maritime cybersecurity and our future work in the maritime cybersecurity field as well. The future work of this research is to examine the practical risk assessment and evaluation tools provided in this review to develop a comprehensive risk assessment and evaluation tool for maritime transportation infrastructure and other critical infrastructures. The expected products are cybersecurity risk framework and cybersecurity risk checklist.

Keywords:

Maritime Transportation; Cybersecurity; Risk; Assessment; Evaluation;

---

*Corresponding author. Tel.: Tel: +1 713-743-1524, Fax: +1 713-743-4032.
Email: lcheng6@central.uh.edu (Liang-Chieh Cheng, PhD, Associate Professor).
Yzhan226@central.uh.edu (Yupeng Zhang, PhD, Assistant Professor)

1 Introduction

With the rapid growth of global trade, maritime transportation has become a major player in the U.S economy. The maritime transportation, under the traditional definition, contains ports, airways, intermodal connectors and freights, it's safe to say the maritime transportation is the backbone of global trade. A secured maritime and port infrastructure brings the prosperity to U.S. economy and in larger picture, the global trade. It would be hard to image the consequences if major maritime and port infrastructure was being totally bleached and its impact on local and global security. However, at this point, although the gravity of the issue has drawn people's attentions, not much research related to maritime and port cybersecurity has been done, there's still much blank fields needs to be filled in this field. This paper will be focusing on the current state of laws and regulations about maritime and port cybersecurity in the U.S., blank that needs to be filled, review of risk assessment and evaluation approaches in other fields and the potential adaptation of methods and regulations in the review to the maritime and port cybersecurity field.

1.1 What would a possible Cyber-Attack to maritime and port infrastructure be like?

A Typical Ship Cyber-Physical System includes the following nine parts, which is showed in the Fig. 1. Ship Cyber-Physical System below.

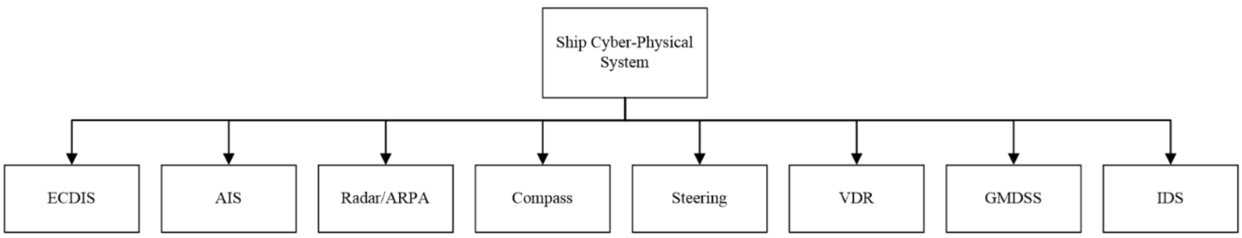

Fig. 1 Ship Cyber-Physical System

The CPS (Cyber-Physical System) entails nine different sub systems:

- ECDIS (Electronic Chart Display and Information System)
- AIS (Automatic Identification System)
- Radar/ARPA (Radio Direction and Ranging) (Automatic Radar Plotting Aid)
- Compass (Gyro, Fluxgate, GPS and others)

- Steering (Computerized Automatic Steering System)
- VDR (Voyage Data Recorder –”Black Box”)
- GMDSS (Global Maritime Distress and Safety System)
- IDS (Intrusion Detection System)

Among these nine sub-system, there are four critical but vulnerable ones: AIS, Radar, Compass and Steering. Image that if hackers took charge of all these five functions, they can literally direct the ship to where they want and they can even potential sink the ship. Set aside the lives on the ship with be in jeopardy, the goods on the ship would potentially be hijacked and never reach the destination. The reputation of the company would be ruined and if these happened to all the ships in a region that controlled by a group of hackers, the entire supply chain would be disrupted and wiped out, the consequences would be unimaginable.

1.2 Current State of Regulations and Laws related to Maritime and Port Cybersecurity

Hclmick (2008) states right after 9/11, under the force and guidance of UN International Maritime Organization (IMO), the International Ship and Port Facility Security (ISPS) Code was developed, at the same time, U.S. developed and proposed Maritime Transportation Security Act (MTSA) of 2002 which include extensive port security regulations.

Hclmick (2008) states following the Act, in 2004, the Coast Guard and Maritime Transportation Act of 2004 was proposed and it required to develop methods to improve security and sustainability of port facilities in the event of maritime transportation security incident.

Hclmick (2008) states later on, the SAFE Port Act of 2006 was proposed and it called for direct research, development, testing and evaluation efforts in furtherance of maritime and cargo security.

Papa (201) mentions the Customs Trade Partnership Against Terrorism (C-TPAT), which is a joint government-business programme to strengthen the entire supply chain and border security [60].

So is the Container Security Initiative (CSI), which is aiming to address the risk of terrorist use of a maritime container to deliver weapons, as Papa (2013) mentions.

Above are the major laws and regulations of U.S related to maritime and port security, as far as we can see, none of them specifically address the cybersecurity risks. In fact, over the past one decade, there's no major research focused on the issues of maritime cybersecurity and the ways to address the problem. As mentioned previously, there is awareness of maritime cybersecurity issues, but few bothers to study on it because there is no major accident happened that could draw people's attention. The maritime cybersecurity field is nearly blank and there's a lot needs to be done and needs to be done quickly.

2 Literature Review

As mentioned in the previous section, there is no major regulations has been establish and researches has been done in the area of maritime cybersecurity. However, in other field, extensive researches have been done and there are even implications in the industry. The section provides a review of current state of risk assessment and evaluation research in hope to give insight on adoption to maritime cybersecurity field.

2.1 Overview

Risk assessment and evaluation are critical components in cybersecurity risk management and they are part of cybersecurity Intrusion Detection System (IDS). Good risk assessment and evaluation tools and plans can help organizations and companies to prevent the attacks ahead of time and if attacks already happened, they can provide guidelines to prioritize tasks needed to be done to minimalize the consequences. Traditionally (Al-Shaer, 2014; Rana, 2015; Brancati, 2013; Zhao, 2008; Yu, 2012; Hudec, 2011; Schlicher, 2015), there are four different types of approaches for cybersecurity risk assessment and evaluation: mathematical modeling approach, analytical framework approach, statistical data approach and simulation approach. During the past years, new types of approaches have been developed and proposed. This review will discuss the work that had been done fallen into following four categories: Risk Assessment and Evaluation Policies, Attack Trees (Defense Trees, Countermeasure Trees) and System Mapping Metrics, Risk Boundary Defining and Risk Compliance Assessment, Simulation and Models.

Most of the research has been focused on two types of treats: Insider Treats (ITs) and Advanced Persistent Treats (APTs) and had targeted on two types of systems: Cyber-Physical System (CPC) and Industrial Control System (ICS). Brancati (2013) gives a clear definition of Insider Threat: a trusted entity is given the power to violate one or more rules in a given security policy. The insider threat occurs when a trusted entity abuses that power. And Rana (2015) gives a definition of Advanced Persistent Threats:

a class of cyber-attacks used to target specific information of organizations and government agencies over a longer period of time.

The reason insider threat stands out among various types of cyber-attacks is that it is very challenging to identify insiders and it's even harder to mitigate them since they often have socio-economical roots.

There are four major methods for risk assessment and evaluation: risk assessment and evaluation policies and framework, attack trees and system mapping metrics, risk boundary defining and risk compliance assessment, simulation and models.

2.2 Risk Assessment and Evaluation Policies and Framework Approach

Tundis (2015) developed an analytical procession approach to compliance assessment. The general methodology is the Support Activities (Security Concerns Identification, Standard Description Forms Identification) and Core Activities (Security Concerns Selection, Service Metadata Identification, Selection of Standards, Security Controls Identification, Matrices of Standards Definition and Matrices of Compliance Definition).

Rashid (2015) provided essentially a risk policy approach of risk assessment for Industrial Control Systems (ICS). This paper is a result of series of interviews to real-world security practitioners who are in consultancy roles with multitude of operator environments. The authors proposed steps that should be followed after the interviews: First, contextualize "How" security assessments are conducted, Second, derive security assessment challenges and principles, Third, assessing "When" assurance techniques can be used, Finally, assessing "Where" the assurance techniques can provide evidence of (non-) conformity. During the First step, five principles are derived (also known as PASIV): proximity requirements, accessibility limitations, safety requirements, impact of the assurance techniques and value generated by using an assurance technique. Then the application of PASIV is examined in three phases of Software Development Life Cycle (SDLC): development, procurement and operational. Finally, for the operational phase, the authors assess how the assurances techniques generate evidence of the 35 security control families of ISO / IEC 27001:2013.

Yu (2012) introduced an architectural approach that changes the paradigm in cybersecurity by reducing the attack surface and total cost of security. The Resilient Device Authentication System (RDAS) approach that the authors propose can provide multiple modalities of device authentication. It supports a large number of authentication events. RDAS builds physical mechanisms for establishing hardware based root-of-trust and combines traditional authentication elements in a systems that manages device identity through the life cycle of a system. That is why it’s crucial for critical infrastructures. The future work is to adapting the RDAS approach to more forms of silicon PUF (Physical Unclonable Function) circuits.

Hudec (2011) developed a risk policy/metrics approach for risk assessment and evaluation. The authors give a definition of security metrics. Then they discussed four security frameworks that contain effective security control: Control Objective for Information Technology (COBIT), ISO/IEC 17799 (ISO/IEC 27002), Information Technology Infrastructure Library (ITIL) and NIST SP 800 Series. Then the authors develop proper security metrics for different control objectives identified in those four security framework and assign weights. Finally the authors construct a model. They determine metric parameters (optimal value, worst value) and variables (value obtained and weight assigned). Then they include their model to company’s parameters such as company size and annual budget. The authors go on defining quality functions for each control objectives. The future work for the authors will be determining all the metrics, which would be used for the risk analysis, based on ISO 27000 family standards. And a model validation and comparison by risk analysis would be done after a complete design of the metric mappings.

Paoli (2013) developed a risk assessment framework approach for smart grid. The authors evaluate the security threats and health impact of the smart grid as well as the health risks of smart meters currently under implementation. A combined framework for risk management in major technological and health domains has been proposed. The framework calls for a coordinated assessment of cyber and power grid risks keeping the whole grid security and safety goals in mind and it has several steps: risk identification and threat identification; risk analysis; risk planning; risk prioritization; periodical risk tracking; risk monitoring and risk communication to management.

Sailer (2014) followed a risk analysis framework and modeling approach. The authors propose a risk analysis framework that analyzes a large amount of various security alerts and computes the reputation of diverse entities based on domain knowledge and interactions between entities. Then they develop reputation propagation algorithm to fulfill the goals that the risk analysis framework tries to achieve.

Patriciu (2014) developed a neural network approach for risk assessment. It’s a theoretically approach trying to address the high computational complexity of attack graphs by applying human immune system's concepts. The authors explain that there are common flaws in nationwide-setup Early Warning Systems and propose that there are two external tools to address this problem: Early Warning Systems based on Artificial Intelligence and Existing system implementations. The authors go on proposing an Early Warning Systems Based on Intelligent Treat Assessment. They use an intelligent method to periodically calculate the probability of certain cyber-attacks to happen. The system will trigger an early warning if certain limits are exceeded. The proposed concepts includes three estimates : probability of an event to happen will be setup based on seven levels, harm will be quantified using a six level scale, and the risk of a probable even having negative consequences will be defined using 6 levels of thresholds from zero to thirty. This approach leads the authors a Feed-Forward Backward-Propagating neural network based on two input layers, ten hidden layers and one output layer.

Choras (2013) introduced a risk assessment framework approach for ICT (Industrial Control Systems) The authors give a proposition of the consequence-oriented classification of cyber threats to critical infrastructures. The authors identifies three possible main categories of cyber-attacks on ICS: Cyber-attack with first order consequence, Cyber-attack with second order consequence and Cyber-attack with third order consequence.

Disso (2015) developed a framework approach of risk assessment and evaluation for enterprise network. It assess the security risk level of the attacks and where the malicious user's actions directing threats to the targeted system but yet not visible by the targeted system. The authors propose a scheme of detecting and mitigating the risk of occurrence of invisible attacks on any organization by deploying NIDPS (SNORT) and quantitative security risk level of the organization against invisible attacks is determined by using OWASP risk rating.

Kohli introduced a risk assessment framework approach for railway infrastructure. The framework the authors propose is Cyber Security Asset Management Tool (CAMT) Framework. They create a diamond model of cyber rail assets and they include an improved FMEA (Failure Mode Effect Analysis) in the proposed model.

Stevens (2010) developed a framework approach for risk assessment. The authors show in the paper how to use Cyber Resilience Review (CRR) to conduct assurance case method

Savola (2011) followed a framework and model approach for risk assessment and evaluation. The authors define a concept called operational assurance and they develop their methodology based on this concept. The methodology includes six steps: service modeling, metric selection, measurement, aggregation, evaluation and presentation. The authors propose an assurance profile (AP) which includes AP description, AP content and AP instantiation. The architecture of the assessment framework the authors propose has four layers: base measures layer, data collection layer, communication layer and control and data processing layer. The proposed framework has the ability to adapt various constraints.

Kazi (2015) introduced a risk policy and protocol approach for risk assessment of Industrial Control System (ICS). They use DNP security authentication to conduct security assessment.

Howard (2011) introduced a policy approach for risk assessment of smart grid. The authors introduce two types of policies: security acts (such as Guidelines on the Protection of Privacy and Transborder Flows of Personal Data) and legal considerations (such as Energy Independence and Security Act of 2007).

Hutle (2015) provided a policy approach for risk assessment for supervisory control and data acquisition systems (SCADA). The authors develop their assessment based on Smart Grid Information Security (SGIS) toolbox and the outcomes of their assessment to the system indicate the physical consequences could occur because of cyber-attacks to information assets and they may have impacts on the operational behavior of smart grid and its dependent infrastructures. The future work is to build on the lesson learnt when proposing risk assessment methodology within other projects.

Zhu (2009) provided a risk framework approach for cyber systems. The author proposes a theoretical framework called Universal Composable Framework. He first decomposes entire system into a set of security primitives and functions and then evaluates individual implementation in the environmental-based security framework and finally he formalizes a composition theorem.

2.3 Attack Trees and System Mapping Metrics

Trivedi developed an attack countermeasure tree (ACT) approach. The authors use SCADA attack as a model to present their model. They identify probability of attack and impact values of the generator nodes and sensor nodes and compute them with ROA (Return on Attack) and ROI (Return on Investment) methods. And then they carry out Single-Objective Optimization and Multi-Objective Optimization. The future work the authors propose will include complete solution of multi-objective optimization under various constraints and modeling of more dynamic scenarios such as sequential attacks, detection and mitigation in ACT (Attack Countermeasure Tree).

Brancati (2013) provided a risk assessment approach to Insider Threat (IT). The authors propose a methodology of risk assessment of insider threats including six iterative phases: system characterization, insider, insider threats, attack paths, countermeasures selection and iteration and update. In the system characterization phase, the authors identify macro-components what constitute overall architecture. The second phase consists of potential insiders profiling, their threats to the systems and their key attributes (Intent, Access, Outcome, Limits, Resource, Skill Level, Objective and Visibility). The third phase is identification and description of possible threats that can make the system vulnerable and prioritization of the attacks. Several techniques can be used in the fourth phase: attack trees, attack graphs, privilege graphs, and adversary views. The fifth phase can be supported by libraries which list the countermeasures for determined attacks. The authors propose classify countermeasures in preventive, deterrent and detection. For future works, the authors are currently working on developing a generic insider threats library both with insiders and countermeasures.

Zhao (2015) developed a system mapping approach for Cyber-Physical Systems (CPS). The authors identify typical structure of security and stability control system, then simplify model of security and stability control system. Later on, they construct failure mode of CPS, more specifically, the electric cyber-physical system (ECPS). The authors presented a probability model to calculate the reliability of ECPS as well. While building the model, scenes such as signal loss and signal transmission error were considered by the authors.

Watson provided an asset management approach. The author identify the inventory of the system and construct secure configuration (system mapping), then move on to vulnerability assessment and remediation which includes monitoring threat agent developments, monitoring vulnerability developments, monitoring logs, incidents and near misses and monitoring personnel changes and issues.

Gao (2013) developed an attack tree approach for risk assessment of cyber-physical system (CPS). They conduct a treat quantification and then they propose risk quantification of the whole path using the attack tree. They identify two attach paths and seven attack leaves (intense, time, stealth, technical personal, physical knowledge, cyber knowledge and access.

Liu (2010) developed an attack path and multiple criteria decision-making (MCDM) approach for risk assessment of power control systems. The security analysis model based on attack graph includes the following steps: basic concepts definition, construction algorithm, vulnerability function of each control step, and connection model-based vulnerability calculation. And they use analytic hierarchy process (AHP) and technique for order preference by similarity to ideal solution (TOPSIS) to conduct the risk quantification.

Kotenko (2014) developed a security metrics approach for risk assessment. The authors identify following four level of metrics: network level, attack graph and attacker level metrics, events level metrics and system level metrics. The network level includes host vulnerability (which is based on CVSS), host vulnerability to zero-day attacks, business value, host criticality and percent of systems without known severe vulnerabilities. The attack graph and attacker level includes: attack potentiality and attack impact. Event level includes dynamic attacker skill level, probabilistic attacker skill level and dynamic attack potentiality. The system level includes security level and attack surface. The future work is to fulfill further development and experimental analysis of techniques for measurement and calculation of security metrics on real examples.

2.4 Risk Boundary Defining and Risk Compliance Assessment

Al-Shaer (2014) introduced a Risk Compliance approach. The authors propose a system model, a risk assessment model and a validation plan. The proposed system model depends on compliance reports, vulnerability scoring systems and network configuration. The network configuration is just like system mapping. The authors map out network devices such as hosts and middle-boxes and their policies. And they also map out each isolation levels. They use security checklists to collect compliance state. The authors use base metrics of Common Vulnerability Scoring System (CVSS), Common Misuse Scoring System (CMSS) and Common Configuration Scoring System (CCSS). For Risk Assessment Model, the authors define a property called Infidelity which is calculated based on vulnerability scoring systems. The authors go on defining Host Infidelity and Host Exposure. And based on Host Infidelity and Host Exposure the authors develop Risk Model. The future plan for their research is to validate the hypothesis as following: enterprise risk score is correlated with the losses induced by cyberattacks

Rana (2015) introduced a risk boundary approach specifically for advanced persistent threats (APTs), which is part of Intrusion Detection Systems (IDS). Given that it’s very hard to quantify risks of APTs, estimating risk boundary is very challenging. The authors define following terms to calculate risk boundary: Threat, Threat Rate, Threat Probability, Threat Severity, Common Assignment Values (CAVs), Threat Persistence Factor, and Threat Stealthiness Factor. Then the author go on assigning values to each of these terms. Finally, the authors classified risk boundary into four domains: Low

Persistence, High Stealthiness; High Persistence, High Stealthiness; Low Persistence, Low Stealthiness; High Persistence, Low Stealthiness. The authors' future plan is to conduct a detailed investigation by considering different temporal snapshots to compare how risk boundaries change over the time.

2.5 Simulation and Models

Brancati (2013) proposed a methodology of quantitative assessment of insider threats. The methodology is more intuitive than NIST Risk Assessment procedures. It is consist of six phases: system analysis, potential insiders profiling (based on Intent, Access, Outcome, Limits. Resource, Skilled Level, Objective and Visibility), identification of possible threats, identify attack paths (how do insiders to achieve attack goals), countermeasures selection, iteration and update.

Ho (2008) introduced a model-based semi-quantitative approach. It is designed for goal-directed attacks especially for multi-stage coordinated attacks which undergoes a series of reconnaissance, penetration, attack and exploit. The authors uses partially observable Markov decision process (POMDP) to construct the model. They define five elements: s as initial state, z as initial observation, u as initial trace, g as expected goals. What makes this model stands out is that it introduces a reward signal r. To evaluate security, the authors figure out the essential elements of security rules, models and policies, and then evaluate them in a generic cost sensitive manner: they defines Dm as maintenance cost and Df as failure cost. And they assumes responses should fall into five categories: Alert for true attack, Alert for normal behavior, Silence for attack, Silence for normal operation and Misdiagnosed attack.

Ishikwa (2016) proposed a simulation based approach. It consists of two major steps: model construction and simulation. In the model construction step, the authors identified the targeted data, identify existing vulnerability, initial parameters (Model Company, the condition of information leakage, security investment, the information leakage cost. Then they use Python and R to implement the model. In the simulation step, the authors assume four scenarios and analyze relationship between total costs and the choice of investment. Need to mention that the authors have 100 million simulation trial for each scenarios and analyze the result of each of them.

Sastry (2011) proposed an approach to Industrial Control Systems (ICS). The authors analyzed the vulnerability and security problems of different types of control systems and sophisticated attacks to the systems. The authors developed attack models assuming the state of the system is measured by sensor network with measurement vector and each vector has a unique identity protected by a cryptographic key. If some sensors are under attack, the actual measurement would be different from the baseline measurement, that's how the attacks could be identified. The attacks models can be used to represent integrity attacks and DoS attacks. Subsequently, the authors develop linear model for the detection of attacks and two methods for detection (sequential detection and change detection) and they go on and develop models for steady attacks, surge attacks, bias attacks and geometric attacks. Finally the authors propose an Anomaly Detection Model (ADM) which can detect an attack and send an estimate of the state of the system to the controller of the system. After the experiments of the proposes models to Process Control System (PCS) and finds results implying that it's more important to protect against integrity attacks than DoS attacks.

Zhao (2008) introduced a simulation approach of risk assessment and evaluation. The model the authors propose can provide measurable data to help improving network security simulating various cyber-attacks and calculate security loss to estimate the impacts. First, the authors analyze the structure of the system and divided them into several types such as routers, switches, firewalls, servers, clients and personal computers. And each of them is assigned an identifier (IP Address, Mac Address or Name). And the attributes of these devices are also identified such as OS type and its vision, services and the corresponding port members, vulnerabilities, performance parameters and application patterns. In this paper, the authors use state transition graph to describe cyber-attacks, which usually contains several steps. The simulation system usually contains three parts: attack scenario module, simulation module and analysis and evaluation module. For future research, the authors will import a database which known attacks can be described by using templates to improve the simulation system and they will also figure out a method to accurately model various kinds of application patterns of network.

Schlicher (2015) provided a computational approach for Industrial Control Systems (ICS). In this paper, the authors consider the defender-practitioner stakeholder points-of-view that involve cost combined with the development and deployment consideration. They introduce a notion of cybernomics to address the issue with security economics which considers the cost/benefits to the attacker/defender to estimate risk exposure. They analyze the likelihood of the emergence of a treat and whether it would be eliminated. And if the treats cannot be eliminated, what the cost would be. The authors recommend to use game theoretic approach to address Attacker-Defender Agent Based Simulation (AD-ABS) and combine AD-ABS with an economic impact assessment. Given this is a theory paper, the future work of the authors would be collect information and examples from technology development case studies have a better insight of the problem.

Nicol (2016) introduced a summary of the approach the author proposes about risk assessment for Cyber-Physical Systems (CPS). The idea of the models that the authors are trying to make should include details that are either extracted automatically or are modeled at a fairly high level. The model includes physical and logical connections between computing entities and can include information about software running on the devices. The author creates a graph whose nodes are vulnerabilities on host with weights derived from the vulnerability scores. It focuses on whether an attacker can exploit a host and if so, what's the difficulty of doing so, measured in terms of time. On the infrastructure side the authors require: First, what a remotely connected user can cause an actuator to do should be described. Second, sets of devices to consider as targets of a coordinated attack should be identified and third, the state of the physical system should be assessed as well as all its boundary conditions. And metric should be used to identify the impact on risk of changing selected configurations and should be used to identify most cost-effective actions authors might apply on the cyber-side to reduce the risk to the infrastructure.

Koutsoukos (2016) developed a modeling approach for quantitative risk assessment. The authors start with component risk assessment, which includes component modeling, component attack trees, CVSS scoring, risk propagation, risk assessment and mitigation and attack propagation. In the first step, the authors assign attribute to every component, in the second, the component attack trees (CAT) usually represent spoofing, tampering, repudiation, information disclosure, denial of service and elevation of privilege (STRIDE). CVSS scoring provides standardized method of modeling the risk value of vulnerability attributes in attack trees. The authors go on conducing system risk assessment which includes system modeling, system attack graph and risk assessment.

Wsissbein (2010) provided a modeling approach for security risk assessments. The author propose a model with three components: First, network simulator. Second, an attack planner that shares the network attack model with the simulator. Third, a distribution of probabilities that describes for the different sorts of attackers' tools. The authors import the information specifics needed to simulator, then they take a sample of attacker tools using a pre-defined probability distribution that describes the tools that a give attacker is likely to hold. Then they define one or more objectives which are actions that the attackers may carry out successful and are supported by the simulator. The authors have plan to use their method and metric to gather information from realistic scenarios.

Hudec (2012) introduced a model-based approach. The authors proposed a formal model that map out metrics to control objectives (metric weight, optimal value, worst value), assign security clauses to security attributes (confidentiality, integrity, availability, authenticity and non-repudiation), support the model with statistics (agent, action, asset and attribute). The authors also propose formal concept analysis for the classification of security clauses from the ISO/IEC 27002:2005 standard. Later on the authors identify all the security clauses: security policy, organization of information security, asset management, human resources security, physical and environmental security, communication and operation management, access control, information system acquisition, development and maintenance, information security incident management, business continuity management and compliance. The future work is to extract the useful information from the selected metrics, evaluate it, and show the results on a discrete scale in a view of security attributes that will give a complete picture of security controls implemented in an organizations.

Liu (2013) developed a modeling approach to risk assessment. The authors develop risk assessment framework containing system configuration, vulnerability identification, attack graph building, and probability of intrusion calculation. The authors use duality element relative fuzzy evaluation method to build the framework and use dynamic model as computing algorithm and Conditional Lyapunov Exponents (CLE) as methodology. They combine dynamic model and LCE together to finish the modeling. The also build a system stability monitoring and response system.

Campbell (2008) provided a modeling approach for Cyber Infrastructure. The model is composed of two parts. A network model captures the static parts of a system and a work-flow model captures the dynamics parts of the system. Then the author conduct too chain implementation with includes CIM parsing, representing recovery workflows, mapping workflows to term-rewriting logic, analyzing workflows in term-rewriting logic and event aggregator. The future work the authors propose is to evaluate the scalability of their approach by using bigger models and see the impact on the checking time.

Patrick (2013) introduced a model approach. It’s a Monte Carlo discrete event simulation and each of the various components of the model (adversary, target, areas, paths, safeguards, actions, and response) is described in details. The authors also propose a potential attack path including the safeguard values for detection and delay. The future research will focus on testing cyber safeguards to determine accurate detection and delay values and integrate what-if analysis to show the effects of implementing different safeguards on different paths within the network to provide insight into the security benefits for specific safeguard investments or system designs and also integrate near real-time threat and vulnerability information into the model.

Zheng (2015) provided a risk assessment model approach for Industrial Control System (ICS). The authors discuss risk assessment on Industrial Automation Platform (IAP). They map the basic structure of IAP and identify relationships and communication links among IAP software and assign security metrics and consequence of the links. Later on, they use Fuzzy Analytic Hierarchy Process (AHP), Fuzzy Comprehensive Evaluation Based on Entropy Theory to develop a comprehensive assessment method and they used the method they propose to build an assessment model. The future work is to assess system by using improved algorithm to ensure more accurate results since the methods used in the paper can only quantify the threats.

Lu (2014) provided a model approach for risk assessment. The authors incorporate grey clustering method, hierarchy analysis and Delphi to build the proposed model. First, the risk assessment model is constructed with hierarchy analysis methods, which includes n indexes. Second, the author incorporate the method of Delphi. Finally they propose an improved grey clustering and incorporate it in the model.

Li (2015) developed a model approach for risk assessment. They use parameterized membership function, fuzzy rule and fuzzy reasoning method and objective function and GA-chromosome representation to realize the model. The future work is to keep working on using the model to analyze network traffic or data form other cybersecurity related domains.

Johnson (2009) introduced a model approach for cybersecurity risk assessment. The authors build attack graphs and they use extended influence diagrams for expressing defense graphs

Guo (2006) developed mathematical model approach for power system risk assessment. The authors propose two types of methods: the probabilistic assessment and the integrated risk assessment. The probabilistic assessment is to sum up the probabilities of the occurrence of all the possible cyber security risk and assess the vulnerability index of cyber systems. For integrated risk assessment, the levels of cyber security risks are categorized into five categories (very low, low, normal, high, very high) and each category is assigned a value and performance index. And the authors use the risk matrix to calculate the vulnerabilities.

Xie (2013) developed a model approach for risk assessment of Cyber-Physical Systems (CPS). The simulation and model building is based on the attack tree developed by the authors. The method includes four steps: asset identification (the methods of identification are asset management tools, active exploration tools and recording tables), treat identification (intense, stealth, time, technical personal, knowledge, treat quantization and access), vulnerability identification (management vulnerability, platform vulnerability and network vulnerability) and CPS Modeling and simulation. The authors use simulation for physical components and an emulation testbed based on Emulab to recreate the cyber components of networked industrial control systems. The future work is to take attack tree as a quantitative tool and follow the risk assessment idea in this paper to pursue the specific risk value of a whole cyber-physical system.

Berthier (2015) introduced a model approach that the authors propose a technique called CPINDEX which calculates cyber-physical security indices to measure the security level of the underlying cyber-physical setting. It takes cyber network configurations as input and calculates a cyber physical contingency ranking that indicates how serious the system's current status is.

Liu (2011) introduced a simulation approach of risk assessment for smart grid. The authors map out the architecture of the system first. Later on they build a simulation scenario based on the architecture mapped.

He (2016) provided a game theory-based model risk assessment approach for two-way communication system. The authors establish a surveillance architecture to monitor message transactions among nodes in communication networks. And the authors propose a security brief model to interpret surveillance observations. The future work includes investigating the impact of uncertainty in surveillance observations on risk levels and adapting forgetting factors in the proposed framework.

Ouksel (2014) provided a model-based approach for risk assessment and the authors adopt concepts from ontology to develop the model. In the paper, the author propose a multi-stage probabilistic threat assessment model based on sentiment analysis and semantic reconciliation. The sentiment analysis model contains several rules: semantic rules and contextual rules. The proposed model achieved 86% correct rate in assessing consumer sentiments.

Liu (2016) provided an analysis and simulation approach for risk assessment and evaluation of power system. The method the authors propose simulates the physical responses of power systems to attacks. The authors use expected load curtailment (ELC) index to quantify potential system losses due to attacks and Monte Carlo simulation to assess the attackers' capabilities.

Crowther (2009) developed a quantitative model approach for risk assessment. The authors apply Bayesian network methodology to intrusion detection system to build a cyber scoring model with is able to conduct quantitative assessment. The future work is to implement the cyber risk-scoring model in the marketplace.

Li (2015) developed a model approach for risk assessment of cyber-physical systems (CPS). The authors establish a risk assessment framework, then use three methods for risk indicator calculation: attack severity quantitative method, attack success probability quantitative method (common vulnerability scoring system, CVSS) and attack consequence quantitative method. Finally the authors proposed a risk assessment algorithm which shows detailed steps of implementation.

Li (2015) introduced a quantitative model approach for risk assessment of cyber-physical system (CPS) based on inter-dependency of vulnerabilities. The authors establish the vulnerability dependency graph and use Common Vulnerability Scoring System (CVSS) to calculate the probability of success attack. And then they use vulnerability utilization and operation mode to calculate the attack-impact. The future work is to propose an optimal strengthening scheme by determining key vulnerabilities.

Lai introduced a model approach for risk analysis for smart grids. Given that old models for smart grids cannot address many electrical properties and operational principles of power grids, the authors use power adjacency matrix (PAM).

Zhou (2015) developed a model approach for risk assessment of cyber physical power system (CPPS). The authors identify security risk element of CPPS. Then they present fast attribution reduction based on binary search algorithms. Later on, they mine risk assessment functions based on gene expression programing, which is also known as SRACPPS-RGEP (security risk assessment algorithm for cyber physical power system based on rough set and gene expression programming). Finally, they analyze the proposed model.

2.6 Other methods

Reed (2012) provided a unique approach of risk assessment using a novel technique called power fingerprinting to assess the execution integrity of critical embedded systems and detect cyber-attacks by monitoring the processor's power consumption using an external device and performing intricate signal analysis and anomaly detection.

Mo (2011) showed a structure of smart grid prevention system which includes dividing the network security domain, deploy firewall, intrusion detection system and audit system in the network boundary. The future work is to dart protection scheme of information security programs.

Rao provided a risk assessment analysis from ethical hacker's perspective. The authors propose a system of security assessment using open source tools to identify and fix security lapses.

Interrante-Grant (2013) provided risk analysis and assessment approach for cellular telecommunications systems such as public switched telephone network (PSTN) and long term evolution (LTE). The authors develop testbeds to integrate realistic telecommunication system protocols and demonstrate their weaknesses.

3 Results and discussion

The methods and strategies mentioned in the review section of this paper could potentially be fully adapted into the maritime cybersecurity system:

Risk Assessment and Evaluation Policies and Framework: it's true that every industry is different, but we can revise the policies and framework and make them work efficiently in the maritime and port infrastructure.

Attack Tree and System Mapping Metrics: we can map out the current maritime and port system and identity the vulnerable parts of it, meanwhile, based on each vulnerable part of the system, we can develop attack tree or even countermeasure trees to analyze the attacker's motivation and psychology.

Risk Boundary Defining and Risk Compliance Assessment: based on risk boundary defining, the vulnerability of maritime and port system would be exposed and we can develop risk compliance reports to develop risk mitigation plans.

Simulation and Models: as long as enough data could be collected, the algorithms used in the models of other industries would be able to be used to build maritime cybersecurity models, potentially, due to the nature differences of data from different industries, other algorithms may need to be used instead, but the concept of building models to solve the cybersecurity issues is totally valid.

4 Conclusion

This paper elaborates the gravity of maritime cyber incident, evaluates the current state of maritime and port cybersecurity research and reviews the cybersecurity risk assessment and evaluation approaches in other industries and their potential adaption to maritime and port infrastructure. The authors conclude that the approaches in other industries would be easily adapted to maritime and port cybersecurity field. The future work would be try to adapt the methods and approaches form other industries to build a maritime and port cybersecurity risk assessment and evaluation system.

Reference

Al-Shaer, E., 2014. Enterprise Risk Assessment Based on Compliance Reports and Vulnerability Scoring Systems, SafeConfig’14

Brancati, F., 2013. Insider Threat Assessment: a Model-Based Methodology, DISCCO’13

Berthier, R., 2015. CPINDEX: Cyber-Physical Vulnerability Assessment for Power-Grid Infrastructure, IEEE

Campbell, R.H., 2008. Automatic Security Assessment of Critical Cyber-Infrastructures, IEEE

Crowther, K.G., 2009. Quantitative Assessment of Cyber Security Risk using Bayesian Network-based model, IEEE

Choras, M.,2013. Current Cyber Security Threats and Challenges in Critical Infrastructure Protection, IEEE

Disso, J.P., 2015. Detection, Mitigation and Quantitative Security Risk Assessment of Invisible Attacks at Enterprise Network, IEEE

Gao, Y., 2013. Security Analysis on Cyber-Physical System Using Attack Tree, IEEE

Gordon, L.A., Loeb. M.P., et al., 2013. A Frame for Using Insurance for Cyber-Risk Management. Communications of The ACM, Vol. 46, No. 3

Guo, Z., 2006. Cyber Security Vulnerability Assessment of Power Industry, IEEE

Hudec, L., 2011. Risk Analysis supported by Information Security Metrics, CompSysTech’11

Hudec, L., 2012. Towards a Security Evaluation Model Based on Security Metrics, CompSysTech’12

Howard, J., 2011. Smart Grid Cyber Security and Substation Network Security, IEEE

Hutle, M., 2015. Smart Grid Cybersecurity Risk Assessment, IEEE

He, X., 2016. Game-Theoretic Risk Assessment in Communication Networks, IEEE

Hclmick, J.S, 2008. Port and Maritime Security: A Research Perspective, J. Tranp. Secur 1:15-28

Ishikwa, T., 2016. A Study of Security Management with Cyber Insurance, IMCOM’16, January 04-06, Danang, Viet Nam.

Johnson, P., 2009. Cyber Security Risks Assessment with Bayesian Defense Graphs and Architectural Models, IEEE

Koutsoukos, X., 2016. Software and Attack Centric Integrated Threat Modeling for Quantitative Risk Assessment, HotSos.

Kohli, S., Developing Cyber Security Asset Management Framework for UK Rail

Kazi, F., 2015. Security Assessment Framework for Cyber Physical Systems: A Case-study of DNP3 Protocol, IEEE

Kotenko, I., 2014. Security Evaluation for Cyber Situational Awareness, IEEE

Liu, C., 2013. A PMU-based Risk Assessment Framework for Power Control Systems, IEEE

Liu, C., 2011. Cyber-Power System Security in a Smart Grid Environment, IEEE

Liu, X., 2016. Power System Risk Assessment in Cyber Attacks Considering the Role of Protection Systems, IEEE

Liu, W., 2010. Security Assessment for Communication Networks of Power Control Systems Using Attack Graph and MCDM, IEEE

Lu, H., 2014. Cyber Security Risk Assessment of Communication Network of Substation Based on Improved Grey Clustering, IEEE

Li, C., 2015. Cyber Security Risk Assessment Using an Interpretable Evolutionary Fuzzy Scoring System, IEEE

Li, Z., 2015. Risk Assessment Method for Cyber Security of Cyber Physical Systems, IEEE

Li, Z., 2015. Risk Assessment Method for Cybersecurity of Cyber-Physical Systems Based on Inter-Dependency of Vulnerabilities, IEEE

Lai, L.L., Security Analysis of Smart Grid-A Complex Network Perspective, IEEE

Leeuwen, B.V., Urias, V., et al., 2013. Testbed for Cellular Telecommunication Cyber Vulnerability Analysis. IEEE Military Communication Conference

Mo, J., 2011. Information Security Requirements and Challenges in Smart Grid, IEEE

Nicol, D.M., 2016. Risk Assessment of Cyber Access to Physical Infrastructure in Cyber-Physical Systems, CPSS'16

Nostro, N., Ceccarelli, A., et al., 2013. A Methodology and supporting techniques for the quantitative assessment of insider threats. DISCCO.

Ouksel, A., 2014. Ontology-Driven Cyber-Security Threat Assessment Based on Sentiment Analysis of Network Activity Data, IEEE

Papa, P., 2013. US and EU Strategies for Maritime Transport Security: A Comparative Perspective, Vol. 28. 75-85

Paoli, G., 2013. A Risk Assessment Framework for Smart Grid, IEEE EPEC

Patriciu, V., 2014. Biologically Inspired Risk Assessment in Cyber Security using Neural Networks, IEEE

Patrick, S.W., 2013. Cyber/Physical Security Vulnerability Assessment Integration, IEEE

Rana, O., 2015. Estimating Risk Boundaries for Persistent and Stealthy Cyber-Attacks, SafeConfig'15

Rashid, A., 2015. Assurance Techniques for Industrial Control Systems (ICS), CPS-SPC'15

Rao, G.S., Security Assessment of Computer Networks-an Ethical Hacker's Perspective, IEEE

Reed, J.H., 2012. Enhancing Smart Grid Cyber Security using Power Fingerprinting, IEEE

Sastry, S., 2011. Attacks against Process Control Systems: Risk Assessment, Detection, and Response, ASIACCS'11

Savola, R., 2011. Operational Security Assurance Evaluation in Open Infrastructures, IEEE

Stevens, J.F., 2010. Goal-Based Assessment for the Cybersecurity of Critical Infrastructure, IEEE

Sailer, R., 2014. Asset Risk Scoring in Enterprise Network with Mutually Reinforced Reputation Propagation, IEEE

Schlicher, B., 2015. Risk and Vulnerability Assessment Using Cybernomic Computational Models, CIST'15

Trivedi, K.S., 2010. Cyber Security Analysis using Attack Countermeasure Trees, CSIIRW'10

Tundis, A., 2015. An Analytical Processing Approach to Supporting Cyber Security Compliance Assessment, SIN'15, September 08-10, Sochi, Russian Federation

Watson, T., Application of Asset Management in Managing Cyber Security of Complex Systems, IEEE

Wsissbein, A., 2010. The impact of predicting attacker tools in security risk assessments, CSIIRW'10

Xie, F., 2013. Cyber-Physical System Risk Assessment, IEEE

Yu, M., 2012. Resilient Device Authentication System (RDAS) through SIOMETRICS, Eighth Annual Cyber Security and Information Intelligence Workshop

Zhang, Z., Ho, P., 2008. A Model-based Semi-Quantitative Approach for Evaluating Security of Enterprise Networks, SAC'08 March 16-20, Fortaleza, Ceara, Brazil.

Zhao, J., 2008. Network Security Simulation and Evaluation, CSTST

Zhao, T., 2015. A Risk Assessment Method for Cascading Failure Caused by Electric Cyber-Physical Systems (ECPS), IEEE

Zheng, S., 2015. Cyber Security Risk Assessment for Industrial Automation Platform, IEEE

Zhou, A., 2015. Security Risk Assessment of Cyber Physical Power System Based on Rough Set and Gene Expression Programming, IEEE

Zhu, H., 2009. Towards a Theory of Cyber Security Assessment in the Universal Composable Framework, Second International Symposium on Information Science and Engineering