FRAMEWORK FOR EVALUATING THE READINESS OF CYBER FIRST RESPONDERS RESPONSIBLE FOR CRITICAL INFRASTRUCTURE PROTECTION

THESIS

Jungsang Yoon, CPT, USA

AFIT-ENG-MS-16-M-054

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT-ENG-MS-16-M-054

FRAMEWORK FOR EVALUATING THE READINESS OF CYBER FIRST RESPONDERS RESPONSIBLE FOR CRITICAL INFRASTRUCTURE PROTECTION

THESIS

Presented to the Faculty

Department of Electrical and Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

in Partial Fulfillment of the Requirements for the

Degree of Master of Science in Electrical Engineering

Jungsang Yoon, B.S.E.E.

CPT, USA

24 March 2016

AFIT-ENG-MS-16-M-054

FRAMEWORK FOR EVALUATING THE READINESS OF CYBER FIRST RESPONDERS RESPONSIBLE FOR CRITICAL INFRASTRUCTURE PROTECTION

THESIS

Jungsang Yoon, B.S.E.E.
CPT, USA

Committee Membership:

LTC Mason J. Rice, PhD
Chair

Maj Benjamin W. Ramsey, PhD
Member

Jonathan W. Butts, PhD
Member

AFIT-ENG-MS-16-M-054

Abstract

First responders go through rigorous training and evaluation to ensure they are adequately prepared for an emergency. As an example, firefighters continually evaluate the readiness of their personnel using a defined set of criteria to measure performance for fire suppression and rescue procedures. From a cyber security standpoint, however, this same set of criteria and rigor is severely lacking for the professionals that must detect, respond to and recover from a cyber-based attack against the nation's critical infrastructure.

This research provides a framework for evaluating the readiness of cyber first responders responsible for critical infrastructure protection. The framework demonstrates the development of evaluation environment, criteria and scenarios that are modeled from NFPA 1410 standards concept that is used for assessing the readiness of firefighters. The utility of framework is exhibited during a military cyber training exercise and demonstrates the ability to evaluate the readiness of cyber first responders for industrial control systems when responding to the cyber-based attacks in the scenarios. Although successful, the results and analysis provide a context to develop a physical processes simulation tool, called Y-Box. The Y-Box creates more accessible, representational, realistic and evaluation-friendly environment to enhance the framework. The Y-Box demonstrates its application through the simulation of the first two stages in a wastewater treatment plant. Its performance test demonstrates its ability to interface with different types of signals from multiple programmable logic controllers with an acceptable range of error. The utility of simulation is extended with the development of potential attacks that can be used in a cyber exercise involving industrial control systems.

AFIT-ENG-MS-16-M-054

I dedicate this thesis to my wife and daughter for their endless support and love.

Acknowledgements

I would like to sincerely thank my committee and Stephen Dunlap for the countless hours of support and encouragement throughout the research.

Jungsang Yoon

Table of Contents

Page

List of Figures

List of Tables

List of Abbreviations

FRAMEWORK FOR EVALUATING
THE READINESS OF
CYBER FIRST RESPONDERS RESPONSIBLE FOR CRITICAL
INFRASTRUCTURE PROTECTION

I. Introduction

1.1 Motivation

In a scene repeated by several motion pictures, burglars conduct a heist to steal a precious piece of art from a museum by manipulating the security camera with a recording that shows normal activities. While the guards watch the manipulated view of the museum, the thieves effortlessly steal the art without being detected.

If the guards detected the manipulated camera view, it would have prevented the precious art piece from being stolen. Just like the guards have a central role in protection of their properties as a first line of defense, the cyber first responders for Industrial Control Systems (ICS) have their own to protect against cyber-based attacks. If this type of attack is unstopped and occurs to the national critical infrastructures, the damage done can have detrimental impacts on the public's safety. Evaluation on the readiness of cyber first responders for ICS is in critical need to minimize or prevent any damage from the cyber-based attacks. Currently, the evaluation of ICS cyber professionals is not standardized and primarily conducted through exam-based certifications, lacking real-time interaction with ICS.

1.2 Research Goals and Hypotheses

This thesis presents a framework for evaluating ICS cyber professionals through the development of scenarios including evaluation criteria and environments that are enabled by a physical processes simulation tool.

The research goals are:

1. The evaluation from the framework provides valuable feedback to improve the readiness of cyber first responders for ICS.

2. The simulation tool provides an accessible, representational, realistic and evaluation-friendly ICS environment, designed to train and assess the cyber first responders for ICS.

The research hypotheses are:

1. The evaluation concept for first responders can be extended to the evaluation of the cyber first responders for ICS.

2. The evaluation of cyber first responders for ICS can be conducted in an evaluation environment that simulates physical processes.

3. Physically observable characteristics from simulated physical processes can be effectively demonstrated through visualization.

4. The simulation tool can interact with types of physical signals typically used in industrial applications and connect to multiple programmable logic controllers at once.

This research proceeds with the assumption that high cost and geographical constraint to replicate the real physical processes prevents its implementation for evaluation environment.

1.3 Thesis Layout

Chapter 1 introduces the motivation and goal of this thesis. Chapter 2 describes background information that leads to framework development for evaluating the readiness of cyber first responders for ICS and a creation of physical processes simulation tool for evaluation environments. Chapter 3 explains the methods to evaluate the framework and the simulation tool. Chapter 4 discusses the results collected in Chapter 3. Chapter 5 summarizes with the conclusions and discusses a significance of this research. This chapter offers recommendations for future work.

1.4 Special Consideration

The simulation of physical processes for the evaluation environment in Section 3.1 is developed prior to the creation of physical processes simulation tool, to partially fulfill the requirements for this research. It is used to evaluate the framework and as a pilot study to see the effectiveness of the custom application model for the physical processes simulation before the full development of the tool. Described in Section 3.2, the tool is ultimately created to complement the limitations discovered from the pilot study. The limitations are described in Section 4.1.2. Chapter 4 provides analysis of results for the framework and the tool in Section 4.1 and 4.2, respectively.

II. Background and Literature Review

Section 2.1 compares the current evaluation for first responders (e.g., firefighters) with the one for ICS cyber professionals. Section 2.2 discusses different types of industrial control systems testbeds and provide a context for the development of a physical processes simulation tool. Section 2.3 provides an overview of elements that are minimally required to replicate an evaluation environment.

2.1 Current Evaluation

Evaluation of first responders using realistic scenarios plays a vital role in determining mission readiness in the areas of public safety. It is hard to imagine a newly recruited firefighter responding to an emergency situation without the proper assessment of their ability to perform. Moreover, it is inconceivable for a fire station to respond to a burning building without evaluating their personnel on the standard tactics required to fight a fire. Indeed, it is critical that firefighters have the ability to respond appropriately for the given situations they may face, such as the ability to adequately lay the initial attack line and back-up line, and obtain the appropriate water pressure within a time limit.

To evaluate the mission readiness of firefighters, fire departments often use the NFPA 1410 national standards as a common set of criteria [6]. The NFPA 1410 provides a scenario-based standard that has been adopted by the community for evaluating the readiness of firefighter first responders. The standards use real-world scenarios and specify objectives, evaluation criteria and metrics for assessing the readiness of firefighters. The evaluation scenarios identify weaknesses in training and provide assurance that personnel are ready to respond appropriately.

Although first responders have used common criteria guidelines for decades to assess the readiness of their personnel, the notion is in its infancy for cyber professionals. Current training evaluation relies primarily on exam-based certifications. This method of evaluation, however, is not sufficient given the responsibilities associated with national critical infrastructure protection.

A cyber-based attack against the nation's critical infrastructure could have devastating consequences that directly impact public safety. There is a growing awareness of the threats posed by cyber-based attacks and the implications; however, little is being done to ensure the competency and preparedness of the cyber professionals that will be called upon to detect, respond to and recover from an attack.

2.1.1 Assessing Readiness.

It is imperative that first responders are continually evaluated against realistic scenarios that may be encountered. Firefighters undergo extensive training and evaluation that mirrors real-world situations to ensure an individual will respond adequately when called upon. A common set of evaluation criteria helps prepare firefighters for such responses and helps identify training deficiencies that need attention. Unfortunately, this same set of criteria and rigor is severely lacking for the cyber security professionals associated with responding to a cyber-based attack against the nations critical infrastructure.

2.1.1.1 Standard on Training for Emergency Scene Operations.

Fire department personnel engaged in emergency scene operations use the NFPA 1410 evolutions standard for training evaluation [3]. This standard specifies criteria and metrics that can be adapted to local conditions and serves as a mechanism for evaluating minimum acceptable performance during training activities.

Figure 1 shows a representative evolution training standard for a handline-forward lead out operation. This example simulates a response to a typical structure fire where the company must secure a hydrant and lay supply lines towards the building on fire. The firefighters are evaluated on the ability to correctly apply the forward lay water supply tactic to obtain the appropriate water pressure to suppress a fire.

The example highlights the various criteria the team is evaluated on and specifies the maximum time to complete the objective. The NFPA 1410 provides numerous scenarios and criteria for evaluation that are based on tactics that relate to real-world scenarios. It is important to note that the guidelines and criteria can be adapted to meet local and scenario-specific requirements.

2.1.1.2 Cyber First Responders.

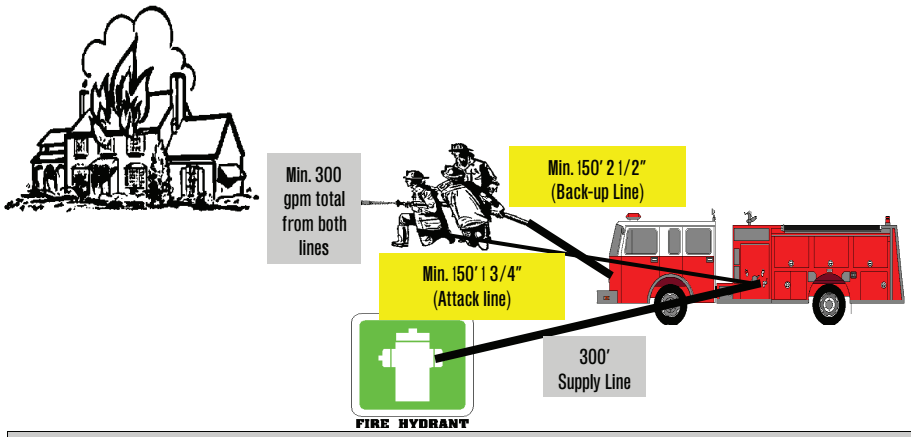
Historical events have demonstrated the susceptibility to disruptive cyber-based attacks against critical infrastructure systems [31]. Attacks against ICS are on the rise as they target operational capabilities within power plants, factories and refineries [11]. As an example, ICS-CERT has issued alerts for multiple campaigns (e.g., Havex RAT [16] and BlackEnergy [18]) aimed at targeting critical systems by exploiting vulnerabilities in products from GE, Advantech/Broadwin and Siemens [17]. Similarly, a recent SANS report claims that a cyber attack was responsible for a power outage in Ukraine [23]. According to the report, hackers likely compromised control systems and installed malware to trip breakers to cut power and prevent technicians from detecting the attack.

Attacks targeting national critical infrastructure can result in devastating consequences. As a first line of defense, organizations spend increasing amounts of money to train and hire cyber security personnel to prevent, identify and mitigate attacks [29]. From a maturity standpoint, however, the ability to evaluate the readiness of

NFPA 1410 Evolutions

Standard on Training for Initial Fire Attack

NFPA 1—Offensive Single Engine: Handline—Forward Lead Out



Objective To place a inital attack line (1 3/4) of min. 150' and a back-up line (2 1/2:) of min. 150' in-service, using units and staffing of the average number of personnel that ordinarily respond.

EVOLUTION DESCRIPTION:

A forward lay using one engine and one supply line. Deploy 300' of 5" hose from hydrant to fire scene. Crew shall deploy 2 hoselines (1 attack and 1 back-up) capable of flowing a minimum of 300 GPM within 3 minutes from start of evolution. Engine shall be permitted to charge the initial attack line with tank water, hydrant supply shall be established **before** back-up line is in place.

EVALUATION CRITERIA:

- All lines shall be completely deployed from hosebeds.
- All nozzles shall be flowing minimal acceptable pressures. Solid tips; 50psi Combo tips; 100 psi
- Time begins at signal from training officer until water is flowing at required pressure from both lines and supply line has been established.

RECOMMENDED MAXIMUM TIME: 3 MINUTES

Reference: NFPA 1410, 2000 Edition; Training for Initial Emergency Scene Operations
Department SOG's

NOTE: Instructors / officers should substitute their department standard hose sizes, manpower, and procedures for this evolution. The evolution provided is a guide to help you set up an initial attack evolution.

Figure 1. Example NFPA 1410 evolution training standard [6].

cyber first responders is in its infancy. Training is disparate and the requisite skill sets have not been standardized [21]. Much attention has been given to frameworks for system security and organizational risk (e.g., the NIST Framework for Improving Critical Infrastructure Cybersecurity [20]); however, organizations do not have a standardized means to evaluate if personnel in a cyber first responder role are adequately prepared to respond to an incident.

Current evaluation for ICS cyber security skill-sets relies primarily on professional certifications. The International Society of Automation (ISA), a professional association, developed a knowledge-based certificate program designed to test the security standards described in ISA99 through a multiple choice exam[13]. The ISA99 standard provides guidelines in areas such as requirements for ICS security management, security risk assessment and system design, and technical security requirements for ICS components. Similarly, the Global Information Assurance Certification organization offers the Global Industrial Cyber Security Professional (GICSP) certification that tests ICS security professionals on essential ICS security related knowledge areas [7]. The topics for the test questions include access management, cybersecurity essentials for ICS, ICS architecture, ICS modules and elements hardening and ICS security monitoring. The Information Assurance Certification Review Board offers a Certified SCADA Security Architect (CSSA) certification for individuals that pass a 100 question exam on knowledge relating to securing a Supervisory Control and Data Acquisition (SCADA) system [4].

The primary concerns with the certification programs are a lack of evaluation criteria against a common set of standards and assessing the ability to apply knowledge, concepts, or experiences to real-time situations associated with an actual exploitation of ICS [10]. In a study performed by the European Union Agency for Network and Information Security (ENISA) that examined existing ICS certification programs,

a key recommendation was the development of a framework for standardizing and evaluating certified ICS security personnel [21].

In addition to certification programs, United States Government organizations have implemented various critical infrastructure response efforts to include the Cyber Defense Initiative (CDI) and Cyber Storm. The CDI is sponsored by the Federal Emergency Management Agency (FEMA) and offers training courses to prepare technical personnel and managers associated with critical infrastructure protection [15]. The training uses lectures, lab exercises and online material to help students prepare for and respond to a cyber-based terror attack.

Similarly, Cyber Storm is a DHS-sponsored exercise initiated in 2006 that tests and evaluates the plans, policies and procedures for cyber security response professionals [19]. Primarily intended to evaluate coordination and information sharing, Cyber Storm focuses on policies and procedures associated with responding to a cyber-based attack against the nations critical infrastructure.

Both government-sponsored efforts highlight the need for a standardized evaluation framework for cyber first responders. Indeed, a common evaluation criteria is needed that can be tailored to an organizations respective environment.

2.2 Evaluation Environment

An evaluation environment including real ICS is necessary to provide real-time situations that evaluation criteria can be applied within. In most cases, the direct use of live ICS is not always feasible due to high loss caused by down time and potential damage for evaluation. Responding to this shortfall, many types of ICS testbeds were developed as solutions for the cyber security research including functionality tests between control systems and education for the responders.

2.2.1 Existing Testbeds.

In order to provide a realistic ICS environment, large-scale testbeds in places like Idaho National Labs and Sandia National Labs recreate the real-world control systems, networks and physical processes [14]. Mississippi State's ICS testbed presents a real-world control system and real-world physical processes to support its cyber security research and education [12]. Others fully or partially simulate their desired ICS environments with or without the real-world equipment. Reaves *et al.*'s [5] testbed fully simulate its ICS environment with virtual devices and simulator to replace the control systems and physical processes, respectively. Wertzberger [32] *et al.*'s testbed simulates physical processes and network while employing real-world control systems. This research focuses on creating the ICS environment through the simulation of physical processes. The simulation of physical processes in this research is designed to satisfy the following attributes:

- Accessible: The physical processes are not geographically limited and cost much less than the full suite of equipment.
- Expandable: The physical processes may be expanded to reflect a complex ICS environment.
- Compatible: The physical processes may be connected to the different types of real-world control systems.
- Separable: The physical processes may be monitored separately from the control system interface.

The current solutions to the physical processes in their testbeds are summarized according to attributes in Table 1.

While the physical processes in National SCADA Test Beds (NSTB) and Mississippi State could be ideal, they are constrained by geographic location and are quite

Table 1. Attributes of physical processes in the testbeds.

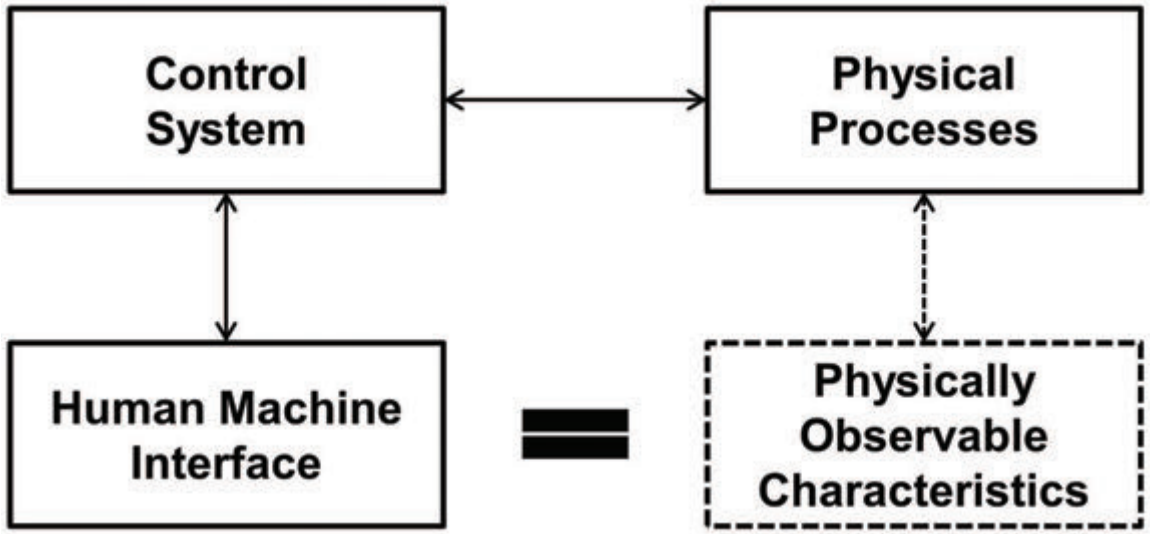
Physical processes	Accessible	Expandable	Compatible	Separable
NSTB		X	X	X
Mississippi State University		X	X	X
Reaves *et al.*	X	X	X	
Wertzberger *et al.*	X	X	X	

expensive to build. Although the testbeds from Reaves *et al.* and Wertzberger *et al.* can be accessible, expandable and connected to the real-world control systems, they do not necessarily separate the views from the physically observable characteristics of physical processes and what are processed by the control systems. The attribute of separable allows the view of physically observable characteristics, which can be used to discern the Human Machine Interface (HMI) under normal operation from maliciously modified or malfunctioning HMI as seen in Figure 2.

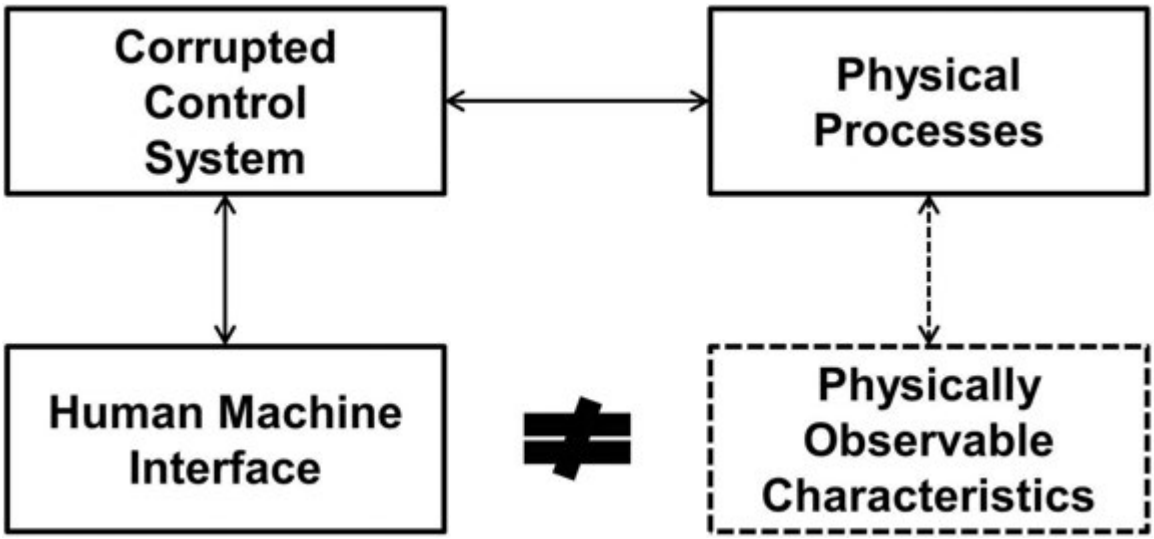
If a museum wanted to replicate the movie scene discussed in Section 1.1 as an exercise to test their defensive capabilities, the exercise coordinators might be tempted to use the security cameras to monitor the progress of the thieves and to evaluate the response of the guards. Were the thieves to execute the same camera attack, the coordinators would be as blind as the guards themselves. Sadly, this is exactly how cyber exercises are conducted today; the coordinators rely on the same view of the exercise as the defenders. If attackers manipulate the view of the defenders, the coordinators are unable to identify what the attackers have done and why the defenders were unable to detect the changes. A view that can't be altered by attackers is necessary for effective control and evaluation by the coordinators.

2.3 Industrial Control Systems and Physical Processes

The evaluation environment is primarily consisted of ICS and physical processes.



(a) HMI under normal operation.



(b) Maliciously modified or malfunctioning HMI.

Figure 2. Comparison of HMIs to the views of physically observable characteristics of physical processes.