Categorization of cyber training environments for industrial control systems

Evan Plumley, Mason Rice, Stephen Dunlap, John Pecarina

Chapter 13

CATEGORIZATION OF CYBER TRAINING ENVIRONMENTS FOR INDUSTRIAL CONTROL SYSTEMS

Evan Plumley, Mason Rice, Stephen Dunlap and John Pecarina

Abstract First responders and professionals in hazardous occupations undergo intense training and evaluation to enable them to efficiently and effectively mitigate risk and damage. For example, helicopter pilots train with multiple simulations that increase in complexity before they fly real aircraft. However, in the industrial control systems domain, where incident response professionals help detect, respond and recover from cyber incidents, there is no official categorization of training environments, let alone training regimens. To address this gap, this chapter provides a categorization of industrial control training environments based on realism. Four levels of environments are proposed and mapped to Bloom's Taxonomy. The categorization enables organizations to determine the cyber training environments that best align with their training needs and budgets.

Keywords: Industrial control systems, incident response, training environments

1. Introduction

In the evening of April 17, 2013, an act of arson at a fertilizer plant in West, Texas resulted in an explosion that killed fifteen people, including ten first responders who were fighting the fire [10, 19]. The first responders were not trained to handle a chemical fire and did not fully comprehend the explosive hazards posed by the materials in the plant. The U.S. Emergency Planning and Community Right to Know Act requires all companies to report hazardous chemicals stored in their facilities. However, there are no legal requirements for local first responders to be trained adequately based on the hazard reports.

To avoid disasters like the Texas explosion, it is imperative that incident responders receive training in environments that teach them the required incident response knowledge and skills as well as help assess the extent of the acquired

knowledge and skills. Processes in an industrial environment are managed using industrial control systems that have limited or weak cyber security protections and can pose physical threats to personnel and equipment. The first responders tasked to respond to incidents in industrial control environments must be properly trained and prepared to deal with the complexity and diversity of cyber incidents.

This chapter proposes a framework for identifying and mapping industrial control system cyber incident response knowledge and skills to training environment components. This chapter also proposes a categorization of training environments based on practicality and realism. The categorization assists organizations in determining the cyber training environments that best align with their training needs and budgets.

2. Incident Response Training Environments

The lack of industrial control system defenses is a cause for concern in the community. Contributing factors include cost, system diversity, long lifecycles and organizations that are reluctant to make changes to their operational systems [28]. Generally, the personnel employed at industrial control facilities do not have the skills to properly collect, analyze and examine the command and control traffic in their networks and they find it difficult to differentiate cyber attacks from non-cyber-induced malfunctions [9]. While most organizations are unable to provide high levels of training to their cyber response teams, they can support effective – albeit lower levels of – training that balance organizational goals and budgets. This section discusses the current state of industrial control system training and training environments at U.S. Government, industry and academic entities.

2.1 U.S. Government

The U.S. Department of Homeland Security Department is the U.S. Government entity that provides the vast majority of training programs in the area of industrial control systems. The training efforts primarily focus on the effects of attacks and the development of mitigation strategies as opposed to emergency incident response.

Training courses offered by the Industrial Control System Cyber Emergency Response Team (ICS-CERT) leverage a partial industrial control system to demonstrate exploits and their impacts; the courses culminate in a red and blue team exercise where participants attack and defend an industrial control system [14]. While the training environment is by no means a full-scale system, it incorporates realistic hardware and displays real physical effects. Participants in the advanced course are expected to have prior knowledge of information technology as well as industrial control systems. The advanced course encourages discussion between information technology and industrial control system professionals, which enhances the development of contextual knowledge in both communities. In a real incident response setting, profession-

als from the two communities must communicate efficiently and effectively to avoid system damage and ensure successful recovery.

However, the exercises and training environment fall short in creating a complete and complex system; moreover, they lean heavily on traditional information technology attacks and defenses instead of focusing intensely on the industrial control domain. Participants must travel to the Idaho National Laboratory facility in Idaho Falls, Idaho for the five-day course. Idaho National Laboratory claims to be able to replicate the control system specifications of any participant, to conduct simultaneous attacks on multiple systems and to perform customized full-scale cyber attacks on an exact replica system [12].

Sandia National Laboratories, which operates as a part of the U.S. Department of Energy National Nuclear Security Administration, is a leader in providing industrial control systems education and training to industry, government and academia [22]. Sandia offers a supervisory control and data acquisition (SCADA) assessment training course that covers the systems and devices in the critical infrastructure and industry. The primary purpose of the course is to provide methodologies and tools for assessing the security of industrial control systems. However, the course is only offered at Sandia's discretion to individuals on an invitation-only basis [22].

Several U.S. research laboratories have leveraged their expertise and capabilities in developing the National SCADA Test Bed [27]. The testbed incorporates full-scale realistic systems and is designed to support research and educational activities. While the emphasis on realism and fidelity ensure that the testbed emulates a real environment, the facility is not currently used to train cyber defenders or incident response teams [27].

2.2 Industry

Industry-provisioned training conducted by vendors is similar to government training; the courses primarily cover industrial control system fundamentals, security audits and assessments of vendor equipment and products. The environments typically provide hands-on laboratory experiences designed to familiarize trainees with programmable logic controllers that are networked to emulate real industrial control environments. The vendors often travel to various locations and offer specific courses to individuals and organizations [3]. The classes are not tailored to train security experts; instead, they are designed for individuals who intend to operate or administer industrial control systems. While these courses are useful, they do not expose potential cyber responders to the complexity of complete systems.

Industry training environments also exist in the form of software simulations of industrial control systems. An example is the LogixPro-500 PLC Simulator that incorporates the RSLogix 500 engineering environment and the ProSim-II programmable process simulation that emulates a programmable logic controller [26]. While this simulation software is not security focused, it provides valuable hands-on experience to novices that advances their understanding of

industrial controllers, with the goal of ultimately gaining expertise in industrial control systems security and first response.

2.3 Academia

Academia also uses assorted testbeds for education and research. Mississippi State University maintains a cyber security testbed that emulates a real-world industrial control system with physical processes [16]. Other academic entities have constructed industrial control system environments with fully- or partially-simulated controllers and processes. Reaves et al. [20] have created a testbed that fully simulates an industrial control system environment, including control systems and physical processes. Wertzberger et al. [29] have implemented a training environment that combines real-world control hardware with simulated physical processes and networking that is a step beyond full simulation. While these environments are adequate for introductory training, they lack the complexity of a full-scale system that is required to impart expertise related to emergency response procedures.

The SANS Institute, a cooperative research and education organization, provides training through online courses and in-class and mentored settings around the world. It has created the SANS CyberCity, a scaled model of a small city that incorporates computers, networks, control hardware and embedded devices that emulate infrastructure assets such as a power grid, water system, traffic system and heating, ventilation and air conditioning (HVAC) systems [23]. This model city is used in an on-site course conducted in Austin, Texas, which exposes trainees to industrial control systems and their components, including human-machine interfaces, industrial protocols and data historians. The model city training environment enables trainees to view the physical effects of their cyber actions while operating realistic vendor-supplied technology. The course covers common security flaws and techniques for thwarting attacks on industrial control systems.

3. Bloom's Taxonomy

Educational frameworks have been created to provide insights into the cognitive value acquired from educational activities (e.g., assigned projects and homework). An educational psychologist named Benjamin Bloom (1913-1999) sought to classify educational goals and objectives based on cognitive complexity [11]. The resulting Bloom's Taxonomy, which was revised in 2001, is widely used by teachers and professors for structuring courses that encourage students to learn, apply knowledge and develop an array of cognitive skills.

Bloom's revised taxonomy comprises the six major categories of educational goals listed in Table 1; the categories range from the least complex category (1) to the most complex category (6). The taxonomy illustrates the progression of cognitive complexity from basic understanding to the creation of original ideas and concepts. It provides a means for aligning an educational tool to the level of skill and complexity that the tool is meant to invoke.

Table 1. Bloom's Taxonomy (revised) [11, 15].

1. Remembering	Retrieving, recognizing and recalling relevant knowledge from long-term memory.
2. Understanding	Constructing meaning from oral, written and graphic messages through interpreting, classifying, summarizing, inferring, comparing and explaining.
3. Applying	Carrying out or using a procedure through executing or implementing.
4. Analyzing	Breaking material into constituent parts, determining how the parts relate to one another and their overall purpose through differentiating, organizing and attributing.
5. Evaluating	Making judgments based on criteria and standards through checking and critiquing.
6. Creating	Putting elements together to form a comprehensive view; reorganizing elements into a new pattern or structure through generating, planning or producing.

4. Relating the Taxonomy to Training Platforms

Bloom strongly recommended the acquisition of concrete knowledge before increasing the intricacy of a training environment presented to students. In many fields, especially those with a high risk of incurring damage to property or injury, a form of training simulation is often used to gradually introduce trainees (or students) to additional variables of complexity before attempting an authentic hazardous task.

Simulations have been used in several hazardous and highly technical professions (e.g., military weapons and vehicle operation, aircraft piloting and astronautics) to build a base of knowledge and comfort for trainees. The U.S. Army uses multiple tank simulators to qualify gunnery soldiers and drivers before they operate real tanks [1, 2]. The Army also uses simulations for generic marksmanship training for soldiers called the Engagement Skills Trainer. To take the training a step further, the Army uses a training tool called the Virtual Convoy Operations Trainer, which enables collective training to be practiced in a virtual environment and multiple soldiers to train together with increasing realism [4].

Several categories of simulations, called flight simulation training devices (FSTDs), are available for private helicopter pilot training. The European Aviation Safety Agency (EASA), a certifying authority for flight simulation training environments, has developed specifications that define each environment level. The specifications cover the exact capabilities that each level is required to provide for certification (e.g., form factor of the cockpit and auditory feedback to trainees) [7]. The categories are:

- **Flight and Navigational Procedure Trainer (FNPT):** A fixed-based generic system that is primarily used for initial and refresher helicopter training, including basic and safety procedures, emergencies, navigation, instrument rating and multi-crew cooperation.

- **Flight Training Device (FTD):** A fixed-based system that simulates a specific type of helicopter. In addition to the flight and navigational procedure trainer capabilities, a flight training device is designed for rating pilots on specific helicopter types. This flight simulation training device has limited checking/testing capabilities because it does not include a motion or vibration system.

- **Full Flight Simulator (FFS):** A motion-based system that provides, in addition to a flight training device, motion and vibration cues. It has the highest level of technical complexity and training capability and can be used for proficiency evaluation.

- **Other Training Device (OTD):** A training aid for which a complete cockpit or flight deck is unnecessary. No regulations cover other training devices, which can vary from desktop computers to helicopter dashboards. These training devices are often used to drill pre-flight tasks or familiarize a pilot with a single cockpit instrument.

Each category serves a different purpose by introducing new variables and increased realism. The simulation categories with increasing levels of realism were created to ensure that pilots demonstrate mastery of the equipment and procedures during training to reduce risk during real flights.

NASA houses numerous training simulators that familiarize its trainees with a variety of environments and situations (e.g., launch, landing, payload and rendezvous activities) [17]. The simulations include fixed-based and motion-based simulators. Astronauts train for 300 hours in the simulators to qualify for real operations. NASA training also extends outside the virtual environment to space environments that are recreated using special aircraft and pools. This training is necessary for the astronauts to gain confidence before operating in the hazardous and unpredictable environment of space.

Every training environment provided by these organizations is intended to gradually assimilate trainees into a real, complex and diverse environment. Each environment serves a different purpose and is tailored to the needs of trainees. With every step forward in the training process, a new training platform is introduced that provides new concepts and builds the strong base of knowledge needed to operate in an unpredictable real environment.

5. Training Environment Development

The framework presented in this section identifies industrial control system first response training environment components that facilitate skill acquisition. The skills are divided into overarching phases of a cyber incident response

based on the National Institute of Standards and Technology (NIST) Incident Response Lifecycle [5]. The skills presented in each phase of the lifecycle are the result of the analysis and consolidation of multiple sources, including several NIST and U.S. Department of Homeland Security publications.

5.1 Preparation

When considering incident response preparation for an industrial control system, a defense-in-depth strategy is not always appropriate for a response team that, in most cases, will interact with the system only after an incident has occurred. Time-sensitive responses in unfamiliar environments require the preparation phase to focus on the acquisition of general knowledge about industrial control systems that can be used in a variety of environments.

The following skills are deemed to be necessary for incident response preparation:

- **Risk and Recovery Prioritization:** The ability to prioritize components that pose the principal security risks to a system as a whole and determine the components that should be addressed.

- **Attack Vector Assessment:** The ability to understand the attack path that an intruder may take when attempting to compromise a system. A responder must understand how an attacker can gain access and the techniques that could be used to manipulate and pivot in the system.

- **Communication with Asset Owners:** The ability to communicate with an asset owner and employees is essential to gain an understanding of system operation. It enables responders to gain insights into system and network layouts, the scope of the damage and the limitations of a response effort. This skill enables the execution of all other skills required during the preparation phase.

- **Competence with Control System Components:** The ability to understand the functions of control system components and how the components (e.g., engineering software, control hardware and control interfaces) operate in order to be able to identify irregularities, malfunctions and manipulations.

Preparing for cyber responses to an industrial control system requires training components that represent the system in a realistic manner.

The following components are deemed to be necessary for assessing preparation skills:

- **System Familiarization Components:** Examples of system familiarization components include descriptions of the devices that guide risk and recovery prioritization in a response plan and network maps that assess the ability of a trainee to understand the role of operational technology.

- **Control Hardware:** Physical industrial control devices that manage the operation of a physical process include programmable logic controllers and remote terminal units.

- **Engineering Software:** This software is used to program and configure industrial control system hardware. The software is often proprietary and is provided by the control hardware vendor.

- **Human Machine Interface (HMI) Software:** This software supports the monitoring and control of a physical process. It enables a human operator to monitor, analyze and control the operational status of the process.

- **Real Control Process:** A realistic process is one that is encountered in an industrial setting and that provides trainees with opportunities to interact and experiment with the process and understand the physical effects.

- **Varied Industrial Control Vendor Exposure:** It is important to expose trainees to multiple proprietary control technologies in a single training environment. This enables the trainees to grasp the similarities and differences between proprietary control components.

5.2 Detection and Analysis

One of the most challenging aspects of incident response is to accurately detect an attack and determine the scope of the problem [5]. This phase is complicated by the wide range of detection technologies that may provide conflicting, inaccurate and/or incomplete information. Assets may also have malfunctions that were not necessarily caused by malicious activities. While an industrial control system response team is normally not the primary detector of an incident, the response team must be able to identify the potential signs of the problem and confirm, by applying detection and analysis methods, that the problem was caused by malicious activity. The team must be able to engage all sources of incident indicators, including intrusion detection systems, anti-virus systems, security information and event management systems (SIEMs), and network-based and operating-system-based logging systems.

While traditional detection devices are valuable, an industrial control system response team should be able to apply its industrial control knowledge to detect malicious effects that may be physically visible or inherent in control software. This adds a layer of complexity over and above traditional information technology intrusion detection systems.

The following skills are deemed to be necessary for detection and analysis:

- **Anomaly and Event Detection:** The ability to use software and hardware detection systems to pinpoint anomalies and events that impact system operation.

- **System Component Monitoring:** The ability to monitor control components and their logical execution to analyze their functionality and detect abnormalities. This includes monitoring via physical means and software.

- **Traffic Monitoring and Analysis:** The ability to monitor and filter traffic in order to track malicious behavior in an industrial control system and the ability to analyze and understand network traffic in the industrial control system.

- **Log Analysis:** The ability to forensically analyze system logs to trace an incident to its cause and track an attacker.

Assessing detection and analysis skills requires components that implement detection technologies, physical effects and realistic network activity.

The following components are deemed to be necessary for assessing detection and analysis skills:

- **Physical Component Effects:** These include the physical operations involved in a process (e.g., pumping of water in a wastewater treatment plant).

- **Anomaly Detection Tools:** These software and hardware tools enable the detection of anomalies in a control system and network via analyses of the physical process and network traffic (e.g., Grassmarlin and Symantec anomaly detection systems for industrial control systems).

- **Realistic Industrial Network Traffic:** It is important to provide realistic industrial control network traffic corresponding to various industrial protocols (e.g., Modbus, EtherNet/IP and DeviceNet). This provides trainees with practical industrial control protocol exposure to perform analysis and monitoring.

- **System Logging:** Components such as network logging tools and data historians must be available to log interactions and industrial process data. These components enable trainees to conduct forensic analyses of industrial control systems.

5.3 Containment, Eradication and Recovery

The containment, eradication and recovery phase focuses on the ability of a responder to select and apply appropriate strategies for isolation, evidence handling, source identification, threat eradication and restoration [5].

Containment strategies include the complete disconnection of an attacker (or source of activity), sandboxing and network filtration. Implementing a temporary solution that decreases malicious activity and prevents further damage is also included in containment. A strategy for containing a threat must consider the possible consequences (e.g., internal damage and solution duration) [5].

In an industrial control system environment, disconnection can lead to catastrophic effects to the control process, where components may depend on each other for interoperability. The same problem can arise during an attempt to filter traffic. It is important for an industrial control system incident responder to understand system operations before making any isolation or containment decisions.

Evidence must be gathered to document an incident and pursue legal proceedings. The evidence should also include all identifying information, information about the personnel who collected, handled and analyzed the evidence, the times and dates of occurrences and the evidence storage locations [5].

To facilitate recovery, a responder or response team must accurately assess the cause of the problem and apply the proper fixes. After the threat has been completely eradicated and system operations are restored, a series of tests must be conducted to ensure the return to system normality.

The following skills are deemed to be necessary for containment, eradication and recovery:

- **Return of a System to the Operational State:** The ability to rapidly return a system to an operational state, mitigate physical and financial losses, and conduct tests to ensure that the system is restored properly.
- **Attacker Identification:** The ability to identify the source of the incident through a forensic investigation.
- **Attacker Disconnection or Sandboxing:** The ability to isolate an attack source from a network and ensure that no further damage can be done by the attacker.
- **Identification and Mitigation of Exploited Vulnerabilities:** The ability to identify the vulnerabilities that were exploited in an attack and mitigate the security weaknesses.
- **Evidence Gathering and Handling:** The ability to gather and handle evidence in a manner that does not compromise the investigation.

To assess the ability to mitigate, eradicate and document attacks, a training environment must include elements that enable a responder to perform actions that stop attacks while keeping the system functional to the extent possible.

The following components are deemed to be necessary for assessing containment, eradication and recovery skills:

- **Emergency Backup Operation Equipment:** This enables the deployment of manual backup operations that prevent a critical process from failing completely. This enables a trainee to prioritize system operations.
- **Real Malware and Attack Scripts:** These help produce realistic attack scenarios and genuine effects on a system that help trainees to detect and defend against attacks.

- **Physical Disconnection or Isolation Options:** These enable the physical disconnection of portions of a system or the isolation of a portion of the system using some form of sandboxing.
- **Filtering Capabilities:** These involve the deployment of filtering technology (e.g., firewalls) in an effective manner.
- **Acceptance Test Execution:** The execution of acceptance tests helps determine whether or not a system has recovered.

5.4 Post-Incident Activity

The post-incident activity phase involves the synthesis of conclusions from the gathered evidence.

The following skills are deemed to be necessary for post-incident activity:

- **Malware Handling and Analysis:** The ability to understand the effects of malware and the proper way to analyze malware.
- **Incident Documentation:** The ability to synthesize conclusions from evidence and knowledge for accurate documentation and response justification.

In order to assess post-incident activity performance, a training environment must include elements that enable the responder to further analyze and properly document the incident in accordance with organizational standards.

The following components are deemed to be necessary for assessing post-incident activity skills:

- **Malware Analysis Tools:** This software is used to dissect and analyze malware (e.g., IDA Pro, OllyDbg and WinDbg).
- **Documentation Standards:** These formalize the documentation process and ensure that it is performed as required by the organization.

5.5 Training Administration

Every environment should provide effective training as well as feedback to trainees. While it is not part of the incident response lifecycle, proper administration of training is vital to the educational experience of participants. Several components are necessary to ensure the complete monitoring of a training environment.

The following skills are deemed to be necessary for training administration:

- **Real-Time View of Physical Signal Exchange:** The ability of a training administrator to view the input and output signals at system endpoints (e.g., sensors and actuators). This helps ensure that the administrator can assess an accurate representation of an environment even when the integrity of the system monitoring components has been comprised and the components are untrustworthy for assessment purposes [31].

- **Remote Administrative Monitoring:** The ability of a training administrator to assess trainees and control an exercise from a different physical location than the exercise environment.

- **Remote Participation:** The ability of a training administrator to administer exercises to trainees at remote physical locations.

6. Training Environment Levels

This section describes the different levels of industrial control system training environments based on their realism and the fidelity of their components and capabilities. While each level has varying capabilities, the primary delimiter between levels is the increased realism that the environment at the higher level provides in the context of a real industrial control system.

6.1 Level 1 Training Environment

A Level 1 training environment is completely software-based and simulates an industrial control device or control system. This type of environment can provide simplified education and training to inexperienced individuals in the areas of controller operations and process control logic.

Example environments are the LogixPro-500 programmable logic controller simulator [26] and the Honeyd programmable logic controller interaction software [30]. These environments do not provide real physical interactions, just software-defined capabilities. While basic interaction and programming features are supported, the simulation programs may not mimic the exact behavior of real control hardware and software. For example, the Honeyd simulation software supports 2,000 TCP requests per second with 65,536 hosts compared with real programmable logic controllers that support significantly fewer connections [30]. Level 1 environments are also limited by their inability to provide realistic defensive response interactions. Additionally, they do not allow for physical disconnection options that are available to defenders in a real environment.

6.2 Level 2 Training Environment

A Level 2 training environment is an emulated system that manifests real physical effects, but does not incorporate genuine control system hardware and software. This type of environment can be constructed using embedded devices (e.g., Arduino, Raspberry Pi and BeagleBone) or other computing devices that can be programmed to control physical sensors and actuators using common programming languages (e.g., C and Python).

Level 2 environments are used as training platforms and research testbeds by many organizations. Researchers at the Air Force Institute of Technology (AFIT) have created a Level 2 environment that emulates an automobile CAN bus, which is controlled by a BeagleBone Black (Figure 1). The environment, which serves as a research testbed, is used to test the effects of CAN

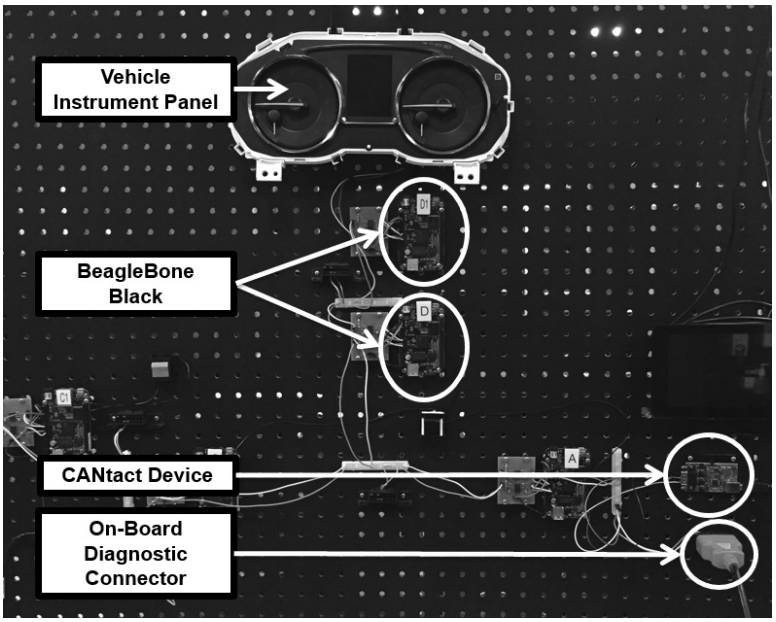

Figure 1. Automobile CAN bus emulation testbed.

bus attacks on vehicular control. The U.S. Industrial Control System Cyber Emergency Response Team (ICS-CERT) uses portable Level 2 training platforms to conduct basic industrial control system classes and exercises. The CybatiWorks Level 2 training kits incorporate Raspberry Pi control emulation devices representing stoplights that use mounted light-emitting diodes (LEDs) as acuators [6]. Siaterlis et al. [24] have created a Level 2 industrial control system simulation testbed for assessing the effects of attacks on networked control systems. While Level 2 environments can manifest physical effects and emulate process control systems, the environments are restricted by the code that executes on the embedded devices. Thus, the environments cannot be guaranteed to mirror the exact behavior of real industrial control systems.

6.3 Level 3 Training Environment

A Level 3 environment comprises genuine process control hardware and software corresponding to a partial industrial control system. In the case of a wastewater treatment plant, an example Level 3 environment comprises the hardware and software that control the lift station portion of the wastewater treatment process. While a Level 3 environment is not fully realistic, it provides a scaled form of realism. Such an environment familiarizes trainees with vendor equipment, industrial networks, process control logic and portability, eliminating the need to construct and maintain a complete and expensive facility.

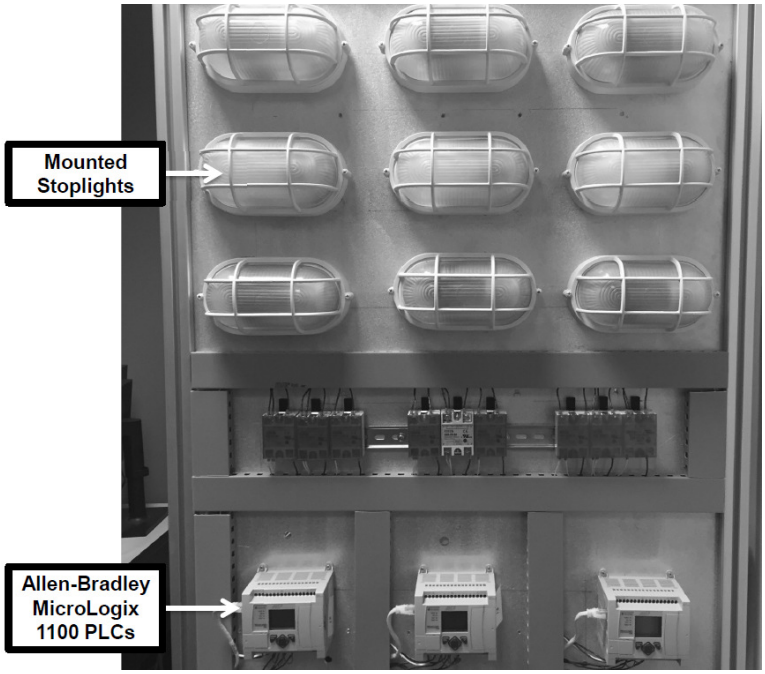

Figure 2. Mounted stoplight control system.

Level 3 environments are used for a variety of security-related activities. The Sandia SCADA Security Development Laboratory, which is considered to be a Level 3 environment, is used to create and evaluate security practices, programs and protocols [21]. Other examples include the Air Force Institute of Technology stoplight system with Allen-Bradley MicroLogix programmable logic controllers that is used to teach industrial control system defense classes (Figure 2). The SANS CyberCity combines Level 2 and Level 3 components in a compact environment that provides robust learning experiences [23].

A Level 3 environment may have genuine hardware and software components, but it still lacks the realism of a production system. This type of environment would not impart an in-depth understanding of a real-world system, especially scenarios where attacks have cascading effects due to interconnections with other systems [3].

6.4 Level 4 Training Environment

A Level 4 training environment is a genuine industrial control facility with functioning processes. Sample Level 4 training environments are located at the Atterbury-Muscatatuck Urban Training Center (MUTC) near Butlerville, Indiana. The training center, which is operated by the Indiana National Guard, is used for military and first responder training. The center houses multiple

Table 2. Mapping of the training environment levels to Bloom's Taxonomy.

Bloom's Taxonomy	**Training Environment Levels**			
	Level 1	**Level 2**	**Level 3**	Level 4
1. Remembering	✓	✓	✓	✓
2. Understanding	✓	✓	✓	✓
3. Applying	–	✓	✓	✓
4. Analyzing	–	✓	✓	✓
5. Evaluating	–	–	✓	✓
6. Creating	–	–	–	✓

industrial facilities, each of which is a separate Level 4 environment. The facilities include a power plant, prison, hospital, subway station, power distribution system and wastewater treatment plant [13]. The cyber portions of some of the Level 4 training environments are still under development.

7. Mapping Training Environment Levels

As the level of a training environment increases, so does the level of cognitive complexity and thinking that can be assessed in the environment. The complexity of training scenarios that can be presented in an industrial control system environment depends on the amount of realism of observations and interactions. Bloom's Taxonomy can be mapped to the different levels of industrial control system training environments for training defenders. The taxonomy is hierarchical in nature and, therefore, an environment that can support exercises at the higher levels of Bloom's Taxonomy can also support exercises at the lower levels. Table 2 shows the mapping of the training environment levels to Bloom's Taxonomy.

A Level 1 fully-simulated industrial control system training environment can present exercises and problems that address the first two cognitive levels of Bloom's Taxonomy, specifically "remembering" and "understanding." The simulated training environment can help evaluate a trainee's ability to recall and retrieve facts that have been programmed into the simulation. The trainees can also interpret meanings from the lessons and make references and comparisons based on the presented facts. A simulation that provides simple programmable logic controller interactions can impart basic programmable logic controller concepts and behavior. However, there is no guarantee that the learnings will directly carry over to a real system. This constrains the ability of a Level 1 environment to support assessments at the higher levels of Bloom's Taxonomy. Another constraint is the limited ability of a trainee to implement realistic security measures. Since a simulated environment can only offer what it is programmed to do, a trainee cannot manipulate a network or make unanticipated configurations to control systems.

A Level 2 training environment in which emulated devices perform physical controller functions can help assess the "applying" and "analyzing" levels of Bloom's Taxonomy. In this type of environment, a trainee can dissect the environment, understand the components and control strategies, and implement external defenses (e.g., firewalls and network isolation). However, since a Level 2 environment does not incorporate real industrial control components, it cannot help evaluate a trainee at Bloom's "evaluating" level.

A Level 3 environment comprises vendor-supplied industrial control hardware and software, but it is not a comprehensive production system. Therefore, it supports training and exercises up to the "evaluating" level of Bloom's Taxonomy. This level of thinking is characterized by making judgments and critiques based on criteria and standards. Evaluative thinking in a Level 3 environment is accomplished by comparing data and observations against the standard operational criteria of control components. The real data enables participants to perform realistic defensive evaluations of the implemented industrial control systems. However, a Level 3 environment struggles to assess trainees at the "creating" level – the highest level of Bloom's Taxonomy.

A Level 4 environment can assess trainees at the highest "creating" level. This level of thinking is characterized by the ability to generate a comprehensive view of a situation. In the context of industrial control system defense and incident response, this type of cognitive complexity cannot be achieved without a complete functioning system. A Level 4 environment provides a trainee with opportunities to view and manipulate every possible element of a real industrial control system. Modifications to existing solutions and new solutions to defense problems can be applied and evaluated. A Level 4 environment also helps trainees discover, analyze and address real-world problems in a creative manner and to observe the ramifications of their actions (e.g., resilience and cascading effects).

8. Example Training Environments

This section presents example training environments at each of the four levels.

8.1 Level 1 Training Environments

The LogixPro-500 PLC simulator enables a trainee to create and manipulate ladder (control) logic, and to view the execution of the logic on simulated sensors and actuators [26]. Consider a scenario where a first responder must be able to analyze a ladder logic program in an industrial controller and determine if it has been tampered with. The trainee would have to understand how to read and write the logic to make these observations. A simulated environment can support the training of basic logic functions and controllers. The training scenarios in the simulated environment provide assessments up to the "understanding" level of Bloom's Taxonomy. They enable trainees to learn facts about control system operation and construct visual meanings

and interpretations through the execution of the simulations. The LogixPro-500 PLC simulation training environment is available for user download at `www.thelearningpit.com/lp/logixpro.html`.

Ladder Logic Engineering Scenario.

- **Objective:** Given engineering specifications for controlling a garage door with open and closed sensors in an industrial control environment, develop the logic that enables the control hardware to execute the specifications.
- **Description:** Create a ladder logic program that enables a programmable logic controller to control a garage door with sensors that indicate when the door is opened or closed. The simulation should execute the logic provided by the trainee and visualize the physical response in the garage door simulator.
- **Type:** Understanding the functionality and relationships between the control hardware and logic software.
- **Evaluation Criteria:** Correctly engineer the required functionality within three hours.
- **References:** Engineering specifications for garage door logic, LogixPro-500 software help menu and Rockwell Automation RSLogix user guide.

LogixPro-500 Environment Components. The environment comprises a single computer system with the LogixPro-500 simulation software installed.

- **Control Hardware:** The control hardware comprises a simulated programmable logic controller that executes the ladder logic program developed by a trainee.
- **Engineering Software:** The engineering software is a version of the Allen-Bradley RSLogix500 programming tool.
- **Human-Machine Interface Software:** The human-machine interface is a software simulation that presents an interactive visual representation of the sensors and actuators. The interface displays how the sensors and actuators react to the ladder logic program in the simulated control hardware.
- **Physical Component Effects:** The physical effects of the system are presented on the computer screen.

8.2 Level 2 Training Environments

Raspberry Pi emulation devices can be programmed to emulate a network of stoplights using LEDs. Consider a scenario where a controller is compromised

in order to interfere with the timing of the lights. In this scenario, a trainee would have to determine the relationships between the components and identify the cause of the incident. This would correspond to the "analyzing" level of Bloom's Taxonomy. The cost of the training environment with four stoplights is approximately $200.

Stoplight Logic Manipulation Scenario.

- **Objective:** Given a network of emulated stoplights that are out of sync, return the lights to normal functionality and find the compromised device.
- **Description:** Monitor network traffic and analyze to determine which devices were impacted and find the source of the attack.
- **Type:** Understanding the functionality and relationships between the control hardware and logic software, and applying response skills to mitigate the effects of the attack and return the system to normal functionality.
- **Evaluation Criteria:** Return the system to normal functionality within three hours and find the source of the attack within one hour.
- **References:** Network and system logs and code on the Raspberry Pi devices.

Stoplight Network Environment Components. The hardware required is a Raspberry Pi development platform that executes a logic program that controls LED lights.

- **Control Hardware:** The control hardware comprises a network of Raspberry Pi emulation controllers.
- **Human-Machine Interface Software:** The human-machine interface software is programmed to view and communicate with the Raspberry Pis.
- **Physical Component Effects:** The physical effects in the stoplight network are represented by LEDs.
- **System Logging:** Logging is implemented in the network by the Rasberry Pi platforms and passive network monitoring software (e.g., Grassmarlin).
- **Physical Disconnect or Isolation Options:** The physical separation of controllers supports network segmentation and physical network disconnection.
- **Filtering Capabilities:** Firewall filtering capabilities are built into the scenario to isolate the stoplight network from outside connections.

8.3 Level 3 Training Environments

Two examples of Level 3 environments are described: (i) wastewater treatment plant; and (ii) prison facility. All the components for each environment fit in a Pelican 1610 case (62.76 cm × 49.73 cm × 30.3 cm). The environments were created to be as cost effective as possible while incorporating genuine control devices. The scenarios support the assessment of thinking skills up to the "evaluating" level of Bloom's Taxonomy. Note that the descriptions of the environments are more detailed than the other levels to demonstrate that high levels of interaction with genuine industrial control components can be achieved at a relatively low cost while maintaining portability.

1. Wastewater Treatment Plant Environment. The Level 3 wastewater treatment plant environment models a wastewater aeration basin. If the oxygen levels are too high or low, alarms are triggered by two red lights in the exercise environment. The oxygen levels are adjusted by modifying the valve openings and the speed of blower fans. The closed loop control of oxygen level uses an Allen-Bradley programmable logic controller and an Allen-Bradley PowerFlex 40 AC variable frequency drive (VFD). The programmable logic controller controls the valve dilation and computes the oxygen levels while the variable frequency drive adjusts the fan speed based on the programmable logic controller calculations. The cost of this training environment is approximately $16,500.

An example training scenario involves a cyber attack on the wastewater treatment plant, which causes the programmable logic controller in the aeration basin to malfunction. This results in fluctuating oxygen levels.

Wastewater Treatment Aeration Basin Failure Scenario.

- **Objective:** Restore the aeration basin to full functionality and find the source and cause of the incident.
- **Description:** By monitoring network traffic, the human-machine interface and the physical devices, the trainee must recognize when the system fails and effect system recovery by blocking attacker access. Also, the trainee must implement emergency procedures to restore the failed control hardware to its normal functionality.
- **Type:** Evaluating the loss of system control and functionality.
- **Evaluation Criteria:** Return the system to normal functionality within three hours and find the source of the attack within one hour.
- **References:** ControlLogix programmable logic controller manual, PowerFlex 40 AC variable frequency drive manual, control hardware vulnerability reports and control network map.

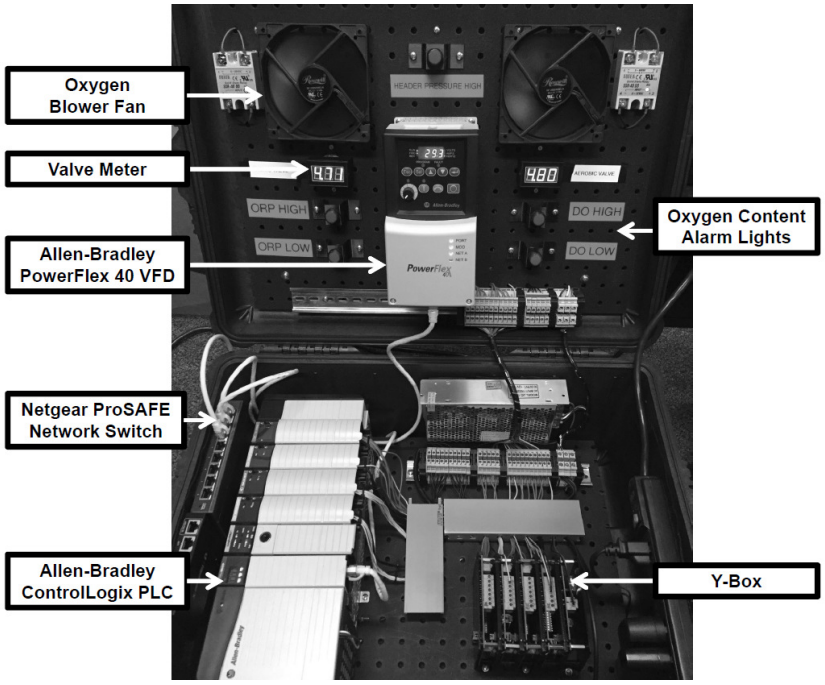

Figure 3. Level 3 wastewater treatment plant training environment.

Wastewater Treatment Plant Environment Components.

- **Control Hardware:** The control hardware comprises an Allen-Bradley ControlLogix programmable logic controller and an Allen-Bradley PowerFlex 40 AC variable frequency drive (Figure 3).
- **Engineering Software:** The engineering software used for programming and configuring the Allen-Bradley programmable logic controller is an RSLogix 5000 system (Figure 4).
- **Real Control Process:** The control process for the environment is modeled after a wastewater aeration basin. It controls oxygen diffusion in two zones using two valves and blower fans.
- **Vendor Exposure:** The environment exposes trainees to the use of a programmable logic controller and variable frequency drive.
- **Physical Component Effects:** The physical effects are presented as voltmeter readings that indicate the extent of valve opening (controlled by the programmable logic controller) and the speed of the fans (controlled by the variable frequency drive).
- **Realistic Industrial Network Traffic Generation:** Traffic generated by the human-machine interface workstation, engineering workstation,

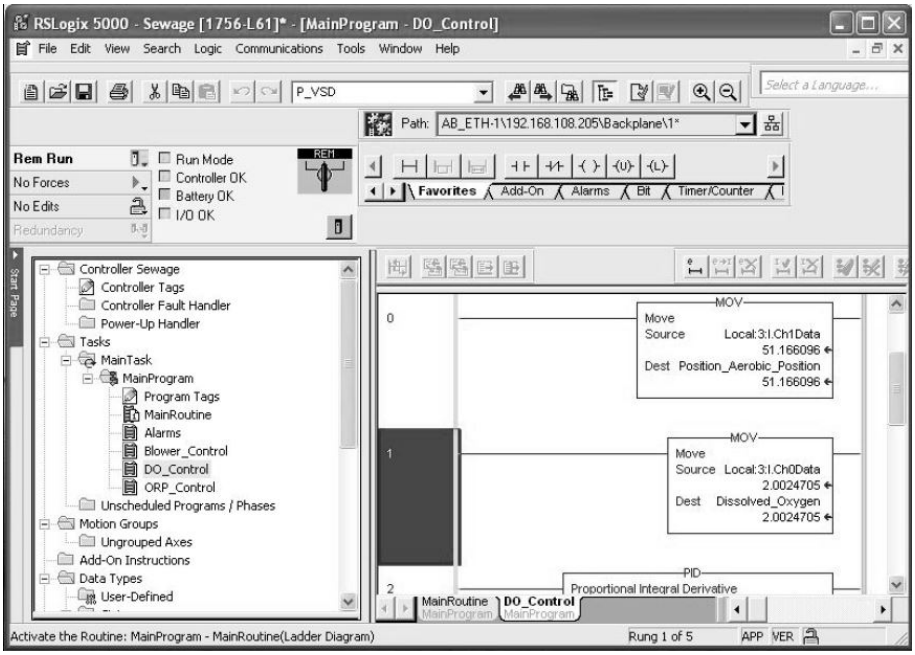

Figure 4. RSLogix 5000 engineering workstation software.

programmable logic controller and variable frequency drive is visible in the network. The realistic network traffic comprises industrial protocol communications, including EtherNet/IP and Common Industrial Protocol (CIP) traffic.

- **Real Malware or Attack Scripts:** Attack scripts that leverage insecure configurations of the control components are incorporated in the training environment.

- **Physical Disconnection or Isolation Options:** All the machines in the network can be physically disconnected from their Ethernet ports and network isolation can be achieved via whitelisting and blacklisting by a Netgear ProSAFE network switch.

- **Filtering Capabilities:** Filtering by an Ubiquiti EdgeRouterX router can be performed using simple firewall rules for network connections in the environment.

- **Real-Time View of Physical Signal Exchange:** Y-Box technology [32] enables an exercise administrator to view the operation of process control endpoints and the human-machine interface to track an ongoing attack (Figure 5).

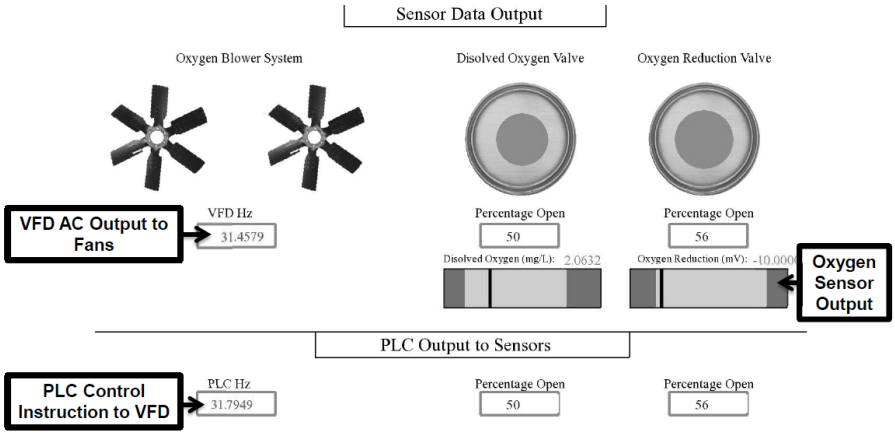

Figure 5. Administrative interface for real-time viewing of attack and defense effects.

- **Remote Administrative Monitoring:** The administration interface for the environment can be viewed using virtual network computing technology; this enables an exercise administrator to evaluate the status of the hardware and software.
- **Remote Participation:** Remote participation is accomplished using remote access tools; this does not hinder the physical manipulation capabilities.

2. Prison Facility Environment The Level 3 prison facility training environment is modeled after a prison cell block containing three prison cells with door lock controls and a mantrap access control system. An Omron programmable logic controller controls the operation of the locks, buttons, security lights and alarm. This equipment costs approximately $1,400.

An example training scenario involves the prison facility experiencing a cyber attack that causes a programmable logic controller to malfunction. This results in the prison door locks being opened.

Prison Control System Failure Scenario.

- **Objective:** Restore the prison to full functionality and find the source and cause of the incident.
- **Description:** By monitoring network traffic, the human-machine interface and the physical devices, the trainee must understand when the system fails and effect system recovery.
- **Type:** Evaluating the loss of system control and functionality.
- **Evaluation Criteria:** Return the system to normal functionality within three hours and find the source of the attack within one hour.

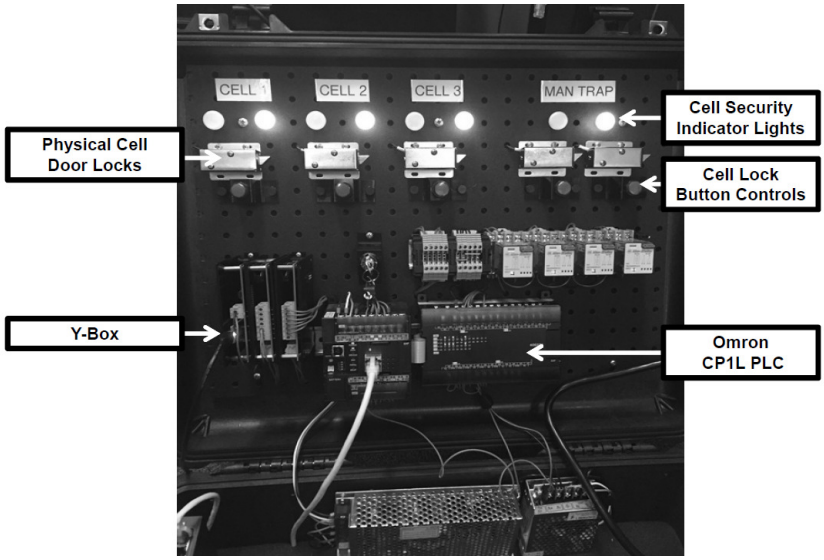

Figure 6. Level 3 prison training environment.

- **References:** Omron CP1L programmable logic control manual, control hardware vulnerability reports and control network map.

Prison Facility Environment Components.

- **Control Hardware:** The control hardware comprises an Omron CP1L programmable controller that controls the prison door locks, buttons, security lights and alarm (Figure 6).
- **Engineering Software:** The engineering software comprises the Omron CX-Programmer.
- **Human-Machine Interface:** The human-machine interface for controlling the prison environment (Figure 7) was created using the Schneider Electric IGSS Free50 software.
- **Real Control Process:** The control process for the environment is modeled after a cell block in a prison in the United States.
- **Physical Component Effects:** The locks and lights are operated using the human-machine interface controls and by physically pressing the lock control buttons in the Pelican case housing the control equipment.
- **Realistic Industrial Network Traffic Generation:** Traffic generated by the human-machine interface workstation, engineering workstation and programmable logic controller is visible in the network. The realistic

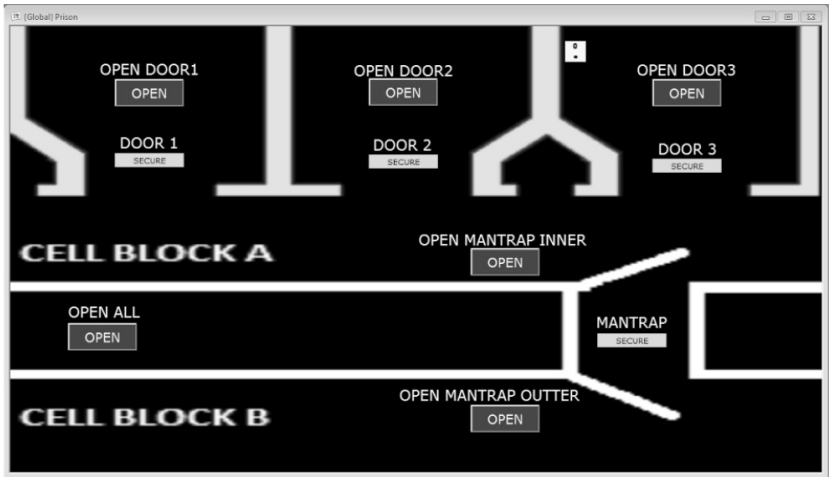

Figure 7. Human-machine interface.

network traffic comprises industrial protocol communications, including EtherNet/IP, Common Industrial Protocol and proprietary Omron protocol traffic.

- **Real Malware or Attack Scripts:** Attack scripts that leverage insecure configurations of the control components are incorporated in the training environment.

- **Physical Disconnection or Isolation Options:** All the machines in the network can be physically disconnected from their Ethernet ports.

- **Filtering Capabilities:** Filtering by an Ubiquiti EdgeRouterX router can be performed using simple firewall rules for network connections in the environment.

- **Real-Time View of Physical Signal Exchange:** Y-Box technology enables an exercise administrator to view the operation of the process control endpoints and the human-machine interface to track an ongoing attack (Figure 8).

- **Remote Administrative Monitoring:** The White Cell interface for the environment can be viewed using virtual network computing technology.

- **Remote Participation:** Remote participation is accomplished using remote access tools; this does not hinder the physical manipulation capabilities.

Figure 8. Administrative monitoring view.

8.4 Level 4 Training Environments

A Level 4 training environment functions at the "creating" level of Bloom's Taxonomy. It presents a trainee with a fully-realistic scenario that enables the trainee to use all the available skills and knowledge to arrive at new solutions to complex problems.

In the case of a power distribution plant, a suitable scenario for a Level 4 environment is the appearance of unusual traffic accompanied by unexplained power fluctuations. Given the complexity of the environment with its many components and connections, a trainee would have to appropriately plan a response by prioritizing components in the network, narrow down the root cause of the anomaly and apply fixes to manage the incident and ensure system recovery. If the incident results from cascading effects in a real system, it can be difficult to determine the root cause and craft an appropriate response. This is because most industrial systems are unique environments and the response of a trainee has to be tailored to the specific environment.

The components used to construct a Level 4 power plant environment are similar to those in a real power plant; however, significant additional engineering tasks would be necessary to implement exercise control and monitoring. A Level 4 training environment may not be suitable to train beginners due to the risk of facility damage if an exercise does not go as intended. Instead, a Level 1 or Level 2 environment could be used as a safe sandbox for beginners to make mistakes and learn from their mistakes.

Failsafe plans should also be considered when designing a Level 4 environment for unpredictable situations during exercises that could lead to facility damage. The cost of constructing a Level 4 power plant can be in the millions of dollars or more. While such a Level 4 training environment would certain not

be mobile, it would provide remote access as in the case of a real infrastructure asset.

9. Conclusions

This chapter has specified four classes of training environments that are mapped to Bloom's Taxonomy, thus covering the various levels of cognitive complexity required in training programs for industrial control system first responders. Level 1 environments are appropriate for average plant operators while Level 4 environments are needed to prepare industrial control system first responders to handle genuine emergencies. The categorization of environments in terms of progressive complexity is necessary to ensure adequate training and readiness of first responders. The proposed categories also help determine the training environment levels that best align with the training goals and budgets of organizations. Well-designed exercise regimens that properly leverage the appropriate levels of training environments will greatly reduce the likelihood of tragic incidents like the explosion at the fertilizer plant in West, Texas that killed fifteen people, including ten first responders.

Note that the views expressed in this chapter are those of the authors and do not reflect the official policy or position of the U.S. Air Force, U.S. Army, U.S. Department of Defense or U.S. Government.

Acknowledgement

This research was partially supported by the U.S. Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team (ICS-CERT).

References

[1] C. Baltos, Soldiers prepare on tank simulators for Saber Guardian exercise, U.S. Army, Washington, DC (www.army.mil/article/171603/soldiers_prepare_on_tank_simulators_for_saber_guardian_exercise), July 15, 2016.

[2] D. Beckstrom, Tank gunnery simulator: Getting back to basics, U.S. Army, Washington, DC (www.army.mil/article/143185/Tank_Gunnery_Simulator__Getting_Back_to_Basics), February 19, 2015.

[3] J. Butts and M. Glover, How industrial control system security training is falling short, in *Critical Infrastructure Protection IX*, M. Rice and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 135–149, 2015.

[4] H. Chang, Simulators always valuable in military training, U.S. Army, Washington, DC (www.army.mil/article/19599/simulators-always-valuable-in-military-training), April 13, 2009.

[5] P. Cichonski, T. Millar, T. Grance and K. Scarfone, Computer Security Incident Handling Guide, NIST Special Publication 800-61, Revision 2, National Institute of Standards and Technology, Gaithersburg, Maryland, 2012.

[6] Cybati, CybatiWorks, Bloomington, Illinois (cybati.org/cybatiworks-one), 2015.

[7] European Aviation Safety Agency, Certification Specifications for Helicopter Flight Simulation Training Devices, CS-FSTD(H), Annex to ED Decision 2012/011/R, Cologne, Germany, 2012.

[8] European Helicopter Safety Team, Teaching and Testing in Flight Simulation Training Devices (FSTD) for Helicopter Pilots, Instructors and Examiners, Training Leaflet, Cologne, Germany, 2016.

[9] M. Fabro and E. Cornelius, Recommended Practice: Creating Cyber Forensics Plans for Control Systems, Idaho National Laboratory, INL/EXT-08-14231, Idaho Falls, Idaho, 2008.

[10] M. Fernandez, Fire that left 15 dead at Texas fertilizer plant is ruled intentional, *New York Times*, May 11, 2016.

[11] M. Forehand, Bloom's Taxonomy, Emerging Perspectives on Learning, Teaching and Technology, University of Georgia, Athens, Georgia (epltt.coe.uga.edu/index.php?title=Bloom%27s_Taxonomy), 2005.

[12] Idaho National Laboratory, INL Cyber Security Research: Defending the Network Against Hackers, Fact Sheets: 21st Century Science and Technology, Idaho Falls, Idaho (www.inl.gov/research/inl-cyber-security-research), 2014.

[13] Indiana National Guard, Atterbury/Muscatatuck, MUTC Overview, Edinburgh, Indiana (www.atterburymuscatatuck.in.ng.mil/Ranges/MuscatatuckUrbanTrainingCenter/MUTCOverview.aspx), 2017.

[14] Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), Training available through ICS-CERT, Idaho Falls, Idaho (www.ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT), 2017.

[15] D. Krathwohl, A revision of Bloom's Taxonomy: An overview, *Theory into Practice*, vol. 41(4), pp. 212–218, 2002.

[16] T. Morris, A. Srivastava, B. Reaves, W. Gao, K. Pavurapu and R. Reddi, A control system testbed to validate critical infrastructure protection concepts, *International Journal of Critical Infrastructure Protection*, vol. 4(2), pp. 88–103, 2011.

[17] National Aeronautics and Space Administration, Johnson Space Center: Training for Space, Astronaut Training and Mission Preparation, FS-2006-03-011-JSC, Washington, DC (www.nasa.gov/centers/johnson/pdf/160410main_space_training_fact_sheet.pdf), 2006.

[18] National Training and Simulation Association, Air Force Training 2015, Arlington, Virginia (www.trainingsystems.org/publications/AirForce.pdf), 2010.

[19] M. Pell, R. McNeill and J. Roberts, Unprepared: Texas blast shows failure of emergency planning law, analysis shows, *NBC News*, May 22, 2013.

[20] B. Reaves and T. Morris, An open virtual testbed for industrial control system security research, *International Journal of Information Security*, vol. 11(4), pp. 215–229, 2012.

[21] Sandia National Laboratories, National Supervisory Control and Data Acquisition (SCADA) Test Bed, Albuquerque, New Mexico (`energy.sandia.gov/energy/ssrei/gridmod/cyber-security-for-electric-infrastructure/scada-systems`), 2015.

[22] Sandia National Laboratories, SCADA Training Courses, Albuquerque, New Mexico (`energy.sandia.gov/energy/ssrei/gridmod/cyber-security-for-electric-infrastructure/scada-systems/education-and-training`), 2015.

[23] SANS Institute, SEC562: CyberCity Hands-on Kinetic Cyber Range Exercise, Bethesda, Maryland (`www.sans.org/course/cybercity-hands-on-kinetic-cyber-range-exercise`), 2017.

[24] C. Siaterlis, B. Genge and M. Hohenadel, EPIC: A testbed for scientifically rigorous cyber-physical security experimentation, *IEEE Transactions on Emerging Topics in Computing*, vol. 1(2), pp. 319–330, 2013.

[25] K. Stouffer, J. Falco and K. Scarfone, Guide to Industrial Control Systems (ICS) Security, NIST Special Publication 800-82, National Institute of Standards and Technology, Gaithersburg, Maryland, 2011.

[26] The Learning Pit, LogixPro 500 PLC Simulator, Whitby, Canada (`www.thelearningpit.com/lp/logixpro.html`), 2016.

[27] U.S. Department of Energy, National SCADA Test Bed, Enhancing Control Systems Security in the Energy Sector, NTSB Fact Sheet, Washington, DC (`www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/NSTB_Fact_Sheet_FINAL_09-16-09.pdf`), 2009.

[28] U.S. Department of Homeland Security, Recommended Practice: Developing an Industrial Control Systems Cybersecurity Incident Response Capability, Washington, DC, 2009.

[29] N. Wertzberger, C. Glatter, W. Mahoney, R. Gandhi and K. Dick, Towards a low-cost SCADA testbed: An open-source platform for hardware-in-the-loop simulation, *Proceedings of the International Conference on Security and Management*, pp. 555–561, 2011.

[30] M. Winn, M. Rice, S. Dunlap, J. Lopez and B. Mullins, Constructing cost-effective and targetable industrial control system honeypots for production networks, *International Journal of Critical Infrastructure Protection*, vol. 10, pp. 47–58, 2015.

[31] J. Yoon, Framework for Evaluating the Readiness of Cyber First Responders for Industrial Control Systems, M.S. Thesis, Department of Electrical and Computer Engineering, Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio, 2016.

[32] J. Yoon, S. Dunlap, J. Butts, M. Rice and B. Ramsey, Evaluating the readiness of cyber first responders responsible for critical infrastructure protection, *International Journal of Critical Infrastructure Protection*, vol. 13, pp. 19–27, 2016.