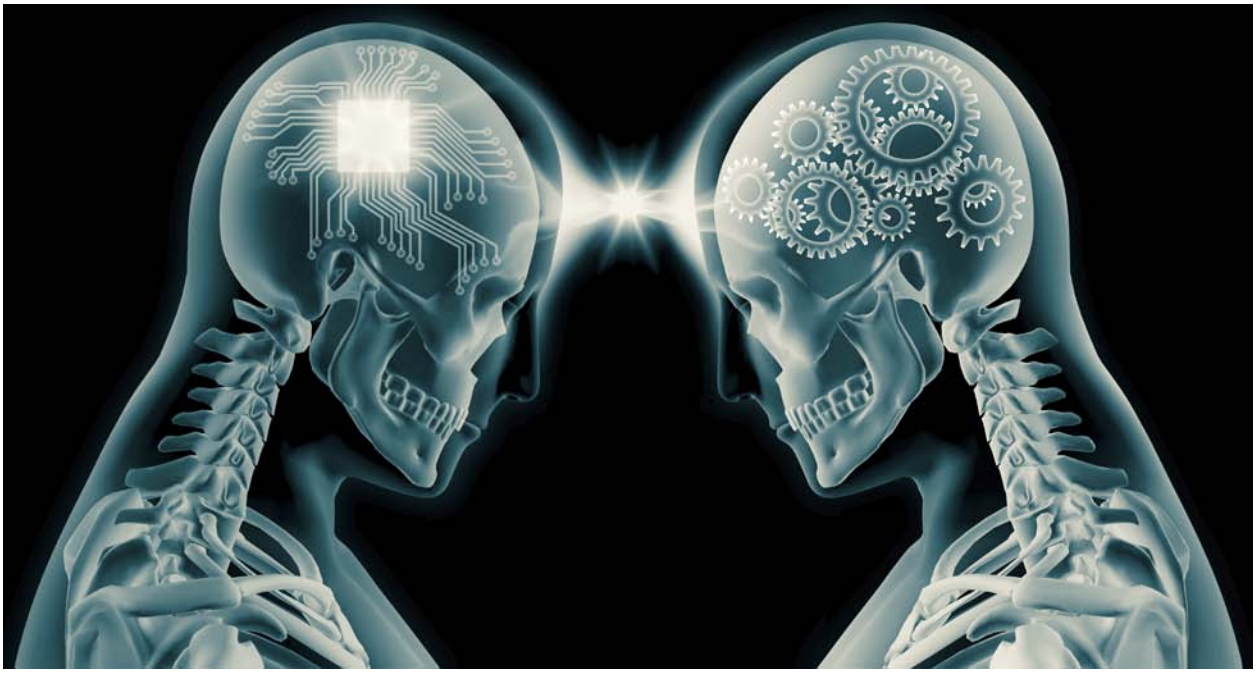
Developing a Tactical Environment Cyber Operations Training Program

January 2015



Prepared for U.S. Government Distribution

Disclaimer: Our conclusions are based exclusively on unclassified, open source information derived from Fox Three observations. None of the information in this report involves access to or confirmation by classified intelligence.

McKeller Corporation was tasked by the Office of the Under Secretary of Defense for Personnel and Readiness to identify gaps between training requirements and current existing capabilities for tactical environment cyber operations (TECO). The study is intended to provide a training strategy and investment roadmap for the Department of Defense to support TECO objectives. This document provides actionable information for developing TECO training curriculum and the associated environment for training delivery and execution. The study was conducted by McKeller Corporation in conjunction with Fox Three Research LLC, primarily at Fox Three's offices in McKinney, Texas.

Executive Summary

There is a growing realization that the military must prepare for operations that blend cyber and traditional capabilities at the tactical level. Indeed, various entities at DoD, Joint, and Service Component levels have expressed an interest in the tactical integration of cyber capabilities.

Traditional cyber operations focus primarily on information and communications technology (ICT) at the operational and strategic levels of war. From a tactical perspective, the integration of cyber capabilities with traditional force employment is not well developed. The intent of this study is to set the stage for the development of a pilot training program that blends various areas of cyberspace and tactical operations into a new skill-set. In the context of doctrinal terminology, this skill-set is yet to be defined and will be referred to under this study as Tactical Environment Cyber Operations (TECO). This study introduces the TECO concept, identifies shortfalls in current training efforts, and provides a way-ahead for developing a pilot training program to meet DoD TECO requirements.

The TECO concept is different from the traditional employment of cyber capabilities. TECO focuses on the integration of cyber capabilities in relation to other tactical military capabilities for creating coordinated battlefield effects. The TECO environment necessitates a rigorous and tailored training program. As military forces begin to integrate cyber capabilities into the tactical environment, the attacks will no doubt face the same scrutiny and concerns as traditional kinetic weapons; perhaps even more so. The TECO training program must incorporate military principles of warfare and mission sets with the understanding that tactical cyber initiated actions may equate to lethal force.

Findings from this study indicate that available training is not adequate for developing the necessary skill sets required for the TECO environment. The primary gap is the need for a robust training facility that incorporates real-world critical infrastructure. The training facility must enable hands-on training, integration with other tactical forces, and evaluation of mission operations across the range of TECO core activities. The study also identified a significant shortfall in adequate supervisory control and data acquisition (SCADA) training for military personnel. Current training focuses primar-

ily on defending and exploiting traditional ICT systems and does not sufficiently incorporate the physical components and processes associated with SCADA systems. Military cyber professionals need a training facility that consists of real-world SCADA to gain an in depth understanding of the effects that cyber initiated actions have on the physical processes.

As part of the analysis for this report, a site survey was performed at the Atterbury-Muscatatuck Urban Training Center (MUTC) to determine the feasibility of providing capabilities to meet TECO training requirements. MUTC is a 1,000 acre urban training center located near Butlerville, Indiana that is operated by the Indiana National Guard and provides a training environment for civilian first responders, the Foreign Service Institute, joint civilian/military response operations, and military urban warfare. MUTC is the largest megacity in the DoD and consists of self-contained, operational water/wastewater, building automation, electric, and dam facilities that can provide students actual hands-on experience in an environment tailored to TECO training requirements. Although the core physical systems are in place, an investment is needed to fully develop the infrastructure to meet TECO mission requirements. However, the unique assets that MUTC affords provides an ideal landscape for developing skill-sets in a real-world environment.

The recommendations in this report provide a roadmap for developing a pilot training program that meets military TECO requirements. As the initial step, an engineering study should be performed for MUTC facilities to specify functionality, design, and automation enhancements required to meet TECO training objectives. Additionally, SCADA training curriculum should be developed based on the knowledge areas and skill sets recommended in this report. Finally, an evaluation should be performed to determine how enhancements to MUTC can be integrated into field training exercises.

The realization of the TECO training program requires an investment that couples curriculum development to a real-world training environment. Once developed, the program will provide an advanced training ground to prepare students for tactical scenarios in a realistic environment.

Table of Contents

Figures and Tables

Figures

Tables

1 Introduction

Cyberspace, through its inextricable connection with individuals and technology, pervades all aspects of human endeavor – business, government, military operations, and societal functions. With the emergence of modern warfare, the United States has maintained military superiority by ensuring tactical advantages across the full spectrum of operations. However, the lack of specialized training and inability to execute cyber capabilities in the tactical environment may result in missed opportunities that could provide decisive advantages.

1.1 Background

The employment of cyber capabilities at the tactical level of war provides both advantages and challenges. The ability to reverse effects, remain anonymous, and launch attacks from virtually anywhere at anytime are appealing attributes. Additionally, cyber attacks are generally not constrained by weather conditions and can be an effective tool for creating psychological effects. Alternatively, understanding system implementations and configurations, gaining appropriate access, leveraging cyber-physical correlations, and coordinating effects are significant challenges.

Department of Defense (DoD) cyber professionals provide advantages within the cyberspace domain through DoD information network operations (DoDIN

> ***Since the early days of warfare, tactical advantages on the battlefield have translated into military victories. ``In the traditional sense, the various operations that make up a campaign are themselves made up of maneuvers, engagements, and battles. From this perspective, the tactical level translates potential combat power into success in battles and engagements through decisions and actions that create advantages when in contact with or in proximity to the enemy.”*** *– Excerpt from Three levels of War,* USAF College of Aerospace Doctrine, Research and Education (CADRE) *Air and Space Power Mentoring Guide*, Vol. 1
> Maxwell AFB, AL: Air University Press, 1997

Ops), defensive cyber operations (DCO), and offensive cyber operations (OCO) [1]. Operations are unified under USCYBERCOM through Cyber Mission Forces that include Cyber Protection Forces that defend the DoD networks, Combat Mission Forces that support Combatant Commanders as they plan and execute military missions, and National Mission Forces that counter cyberattacks against the United States [2].

Despite advancements, a gap exists in the ability to employ cyber capabilities during tactical military operations. Currently, cyber operations focus primarily on information and communications technology (ICT) consistent with a traditional network environment at the operational and strategic levels of war [3]. From a tactical perspective, the integration of cyber capabilities with traditional force employment is not well developed.

Various entities throughout the DoD and service components have expressed the need for delivery of cyber capabilities at the tactical level. The intent of this study is to set the stage for the development of a pilot training program that blends various areas of cyberspace and tactical operations into a new skill-set. In the context of doctrinal terminology, this skill-set is yet to be defined and will be referred to under this study as Tactical Environment Cyberspace Operations (TECO). The TECO concept is different from the traditional employment of cyber capabilities. TECO focuses on the integration of cyber capabilities in relation to other tactical military capabilities for creating coordinated battlefield effects.

1.2 TECO Study

The tactical level of war focuses on the employment and ordered arrangement of forces in relation to each other [4]. There is a growing realization that the military must prepare for operations that blend cyber and traditional capabilities at the tactical level. This study introduces the TECO concept, identifies shortfalls in current training efforts, and provides a way-ahead for developing an extensive and effective training program to meet DoD TECO requirements.

The ability to effectively execute cyber operations in the tactical environment requires: (i) developing trained TECO specialists and (ii) organizing TECO capabilities for force employment. Training should emphasize the development of specialized skill sets in a real-world environment that integrates traditional forces and operational mission sets. Considerations for how to organize TECO specialists requires an analysis of force structure, mission objectives, and capability execution. For example, is it best to embed TECO specialists with ground units, or should TECO specialists provide a reach-back capability similar to air support that can be called upon when the situation warrants? Should the TECO specialist be a designated career field? What is the role and command authority of USCYBERCOM for TECO employment? Decisions surrounding the organization and how TECO specialists are incorporated into the force structure are critical to the realization of the TECO concept. Indeed, Service Component and DoD leadership must evaluate how best to integrate TECO specialists to meet mission requirements. As the organization decisions are being vetted, however, it is imperative that the military starts evaluating requirements for developing trained personnel, regardless of the determination on how to best employ the capabilities – the military can ill afford to wait on developing trained personnel.

This study focuses on the training requirement for TECO specialists. Based on a gap analysis, the study provides recommendations for developing a pilot TECO training course. The training course is intended for tactical forces of a Joint, Interagency, Intergovernmental, Multinational (JIIM) nature. With assistance and guidance from the Directorate for Training Readiness and Strategy at the Office of the Secretary of Defense, the intent of TECO training is to provide a force multiplier that enables tactical forces to understand and achieve effects using cyber capabilities across the full range of operations.

1.3 Implications

The TECO environment necessitates a rigorous and tailored training program. As military forces begin to leverage cyberspace in tactical operations, the effects will no doubt face the same scrutiny and concerns as traditional force employment; perhaps even more so. The TECO training program must incorporate military principles of warfare and mission sets with the understanding that cyber initiated actions may equate to lethal force.

A gap analysis was performed to examine TECO requirements and existing capabilities for delivering TECO training. Shortfalls in training capabilities were identified for the following:

- Training Facilities. The primary shortfall for developing TECO capabilities is the lack of an appropriate training facility. A training facility is needed that comprises real-world systems to prepare students for the situations they will face during actual military missions and engagements. This notion is in keeping with the long-held military philosophy that troops should organize and train as you would fight. Current training either simulates or provides systems with scaled-down models of physical processes. A requisite training facility is often overlooked or considered impractical due to extensive costs associated with developing full-scale systems and physical processes. As a result, it is only possible to develop an abstract understanding of principles and not an in-depth technical knowledge and comprehension of capabilities and effects. It is imperative that the military develops a training program that affords hands-on experience and student emersion into the actual TECO environment. Without the incorporation of actual physical processes and full-scale systems into a training program, it is impossible to develop the skill-sets needed to understand the actual effects associated with the TECO environment.

- SCADA Training Curriculum. The military does not have a comprehensive training program that offers the curriculum to develop the skill-sets for tactical cyber operations. The primary gap in curriculum is associated with supervisory control and data acquisition (SCADA) systems that control and monitor critical infrastructure (e.g., electric power, transportation, oil and gas, and water/waste water). Historically, military campaigns have considered these systems as hard targets that are attacked using kinetic weapons. With the evolution of technology and network interconnections associated with SCADA systems, cyberspace brings opportunities and challenges to the battlefield that previously did not exist. Indeed, SCADA systems are likely to play a significant role in the TECO environment. Often, the military relies on commercial training for cyber professionals to develop skill sets and fill capability gaps for SCADA systems. Commercial training, however, is geared towards certifications for information technology specialists; the training does not meet the special requirements needed for the TECO environment. Additionally, inherent military training for cyber operations does not incorporate the physical systems or effects associated with exploitation of SCADA systems.

- Force Integration. Force integration is critical to fully developing TECO capabilities. The TECO concept is intended to provide battlefield capabilities and course of action (COA) options to military commanders. As such, TECO operations must be exercised in a joint environment that incorporates real-world systems and provides integration of capabilities with other tactical forces. Current exercises that integrate cyber capabilities focus on information networks and primarily use simulation environments for training objectives. A real-world environment is required to exercise full-spectrum military operations that emphasizes hands-on training, identifies training and capability gaps, and enables coordination of tactical effects.

Findings from this study demonstrate a need to develop the necessary training facilities and build a training program tailored to the unique skill sets required for the TECO specialist. This report provides a training strategy and investment roadmap for developing TECO training curriculum and the associated environment for training delivery and execution. Due to the costs and complexity, it is recommended the training is jointly sponsored by service and combatant components.

2 Tactical Environment Cyberspace Operations

To understand the training requirements, it is first necessary to explore the TECO concept. The TECO concept focuses on integrating cyber capabilities with tactical forces. The current focus of cyber operations centers on information networks and providing a force multiplier that can affect tactical operations. The TECO concept, however, is intended as a force capability that is integrated into battlefield tactics executed at the Brigade level and below. As the TECO concept is in its infancy, there are myriad questions that remain to be answered, particularly those associated with organizing TECO capabilities for force employment.

2.1 Effects

A TECO specialist, either embedded with other tactical forces or through reach-back capability, provides battlefield effects through the manipulation of computing systems. At the tactical level, coordinated cyber effects target two primary categories of computing systems: (i) traditional information and communication technology (ICT) and (ii) cyber-physical systems. Note that although the fundamental principles for exploiting the two categories of computing systems may overlap, the resulting effects of cyber-initiated actions are quite different.

2.1.1 Information and Communications Technology

ICT includes systems or applications associated with computer and network hardware, software, and communication medium [5]. The technology encompasses computers, enterprise software, middleware, and data storage, which enable users to access, store, transmit, and manipulate information. Military cyber operations (DoDIN Ops, DCO, and OCO) focus primarily on ICT systems and their integration with military operations [1]. Exploitation of ICT systems can result in loss of intelligence and proprietary information, degraded communication, loss of data processing and computing systems, and manipulation of data. Indeed, compromise of ICT systems effects the confidentiality, integrity, and availability of data that command and control decisions and daily operations depend on.

2.1.2 Cyber-Physical Systems

Cyber-physical systems consist of embedded devices and are system-of-systems often associated with the critical infrastructure. Cyber-physical systems are designed for “seamless integration of computational algorithms and physical components” [6]. Example cyber-physical systems include SCADA, cellular phones, and weapon systems. Indeed, the electric power grid, oil and gas pipelines, railways, and other critical infrastructure are cyber-physical systems that comprise viable military targets. Attacks on these systems disrupt communications, hinder logistical support, create confusion, and achieve psychological effects. For the first time in history, non-kinetic tactical actions can achieve direct kinetic effects that result in the loss of human life.

2.1.3 Tactical Considerations

Questions remain on how TECO capabilities will be integrated on the battlefield with other tactical forces. Lines of authority, command and control decisions, responsibilities, and legal considerations are some of the issues that still need to be addressed. Regardless of the decisions on how to integrate and execute TECO force capabilities, however, tactical advantages exist on the battlefield.

The core activities associated with TECO are yet to be defined. However, based on mission requirements and capabilities, the following list provides examples of core activities that can be realized through TECO:

- Intelligence, Surveillance, and Reconnaissance. Activities that synchronize and integrate sensors, assets, and processing to provide information and intelligence to make informed, timely and accurate decisions [7].

- Special Reconnaissance. Operations conducted in hostile, denied, or politically sensitive environments to collect or verify information of strategic or operational significance [8].
- Military Information Support Operations (MISO). Operations to help influence emotions, motives, objective reasoning, and behavior of foreign governments, organizations, groups, and individuals [9].
- Military Deception. Actions executed to deliberately mislead adversary decision makers and create conditions that contribute to accomplishing US objectives [10].
- Civil-Military Operations. Activities to establish, maintain, influence, or exploit relations between military forces, governmental and nongovernmental civilian organizations and authorities, and the civilian populace in a friendly, neutral, or hostile operational area in order to achieve US objectives [10].
- Unconventional Warfare. Activities conducted to enable a resistance movement or insurgency to coerce, disrupt, or overthrow a government or occupying power by operating through or with an underground, auxiliary, and guerrilla force in a denied area [8].
- Joint Electromagnetic Spectrum Operations. Activities that involve the manipulation of the electromagnetic spectrum to exploit, attack, protect, and manage resources within the electromagnetic operational environment to achieve commander's objectives [11].
- Stability Operations. Operations conducted outside the United States to maintain or reestablish a safe and secure environment, provide essential governmental services, emergency infrastructure reconstruction, and humanitarian relief [12].

TECO can support the core activities by providing tactical advantages at the physical, informational, and cognitive dimensions of the information environment [10]. Additionally, TECO capabilities provide both covert and overt options. From a covert standpoint, the ability to remain anonymous, delay effects, attribute effects to other actors, mask effects, or provide a distraction are appealing attributes. Overt operations are consistent with traditional force employment where the enemy can readily identify the effects. Note that the fundamental principle of the TECO concept is integration with other tactical force capabilities. As such, capabilities and effects associated with the core activities are intended as components of tactical engagements and are not specifically intended as stand-alone capabilities.

2.2 Challenges

Integration of cyber capabilities into the tactical environment requires consideration of the challenges associated with TECO capability employment. Creating a specific, desired effect initiated through cyber means must consider the following constraints:

- Time. Due to the complexity of the environment and the targeted systems, preparing an attack may require substantially more time than traditional force employment. Time is required to gain access to the intended target, identify system components and architecture, develop exploits for the intended target if none exist, and determine attack parameters [13].
- Access. Access to the intended target is determined by network interconnections/topology and communications medium. Due to security mitigations or system configuration, local proximity to the target may be required to gain access (e.g., inserting thumb drive into a system or compromising a local wireless access point). Alternatively, remote access may be possible if the system can be compromised through system weaknesses or through targeted actions (e.g., phishing emails to gain access to a targeted network).
- Containment. Creating targeted effects requires understanding and preparing for second and third order effects. For cyber-physical systems, it is imperative to understand the underlying physical process and how the manipulation of one process cascades to create system-wide effects. In addition, malware can unintentionally spread to systems beyond the intended target. Because of the highly interconnected nature of computing systems, the propagation can result in effects beyond the theater of operation and spread quickly.
- Change in the Environment. Cyberspace is a complex environment that is continually changing and adapting. Changes in system configuration, architecture, applications, or users can drastically alter the targeted landscape. For example, upgrading an operating system may patch a vulnerability that provided access to the system, rendering potential exploits useless against that target. Additionally, enhancements to systems or

introduction of new technology can greatly affect the operating characteristics.

- Gain/Loss. Unique to cyber capabilities is the half life of a developed exploit. Although traditional munitions are constantly upgraded to incorporate newer technologies, the capabilities of a weapon generally remain consistent (e.g., a Mark 84 bomb can penetrate up to 11 feet of concrete depending on the altitude from which it is dropped [14]). For cyber, however, once an exploit is used there is a risk that it will no longer be a viable capability. If discovered, similar systems can be patched to prevent another compromise. Additionally, an adversary could discover the exploit, reverse engineer it, and use the capability for itself. As such, discerning if the situation warrants using an exploit and exposing it to discovery is a significant challenge at the tactical level.
- Coordination. Coordinating TECO effects with traditional force employment requires extensive planning and exercising of capabilities. The dynamic nature of targeted systems, insufficient knowledge of targets, and uncertainty of cascading effects can impact predictability and effectiveness.

These challenges seem to be some of the main considerations for why cyber capabilities have not been fully integrated into tactical operations. To overcome the challenges, an environment is needed that provides the ability to vet capabilities and train for operations using integrated, real-world scenarios. By evaluating TECO capabilities in a real-world environment, the limitations, characteristics, functional capability, and execution requirements will be understood and documented. Such analysis will provide commanders with defined parameters and assurances for the vetted capabilities.

2.3 Core Knowledge Areas

A TECO specialist must be able to provide capabilities across the range of operations that are likely to be encountered during mission sets. To provide viable options for the TECO environment, TECO specialists should have an in-depth understanding of the following core knowledge areas:

- Traditional ICT
- Physical processes
- Cyber-Physical correlation
- Communications
- Potential Attack Vectors
- Cyber Attack/Protection Tools

The core knowledge areas provide the fundamental skill sets initially identified for developing TECO capabilities. As the TECO concept materializes, the core knowledge areas will likely expand to incorporate other technical areas.

Note that understanding the technical intricacies associated with the knowledge areas is critical. However, the TECO specialist must also comprehend how the skill sets apply to battlefield tactical operations. Tactics, techniques, and procedures (TTPs) for cyber operations typically focus on altering system configurations for defending against a cyber attack or manipulating system parameters to achieve a desired effect on a targeted system. For TECO, TTPs include the integration of effects with other combat forces and creating coordinated battlefield impacts.

2.4 Remarks

The TECO concept is in its infancy. Developing a robust capability while aligning force structure and doctrine will take time. Nevertheless, the US military must start developing the technical skill sets associated with tactical cyber operations.

3 Gap Analysis

The intent of this study is to set the stage for the development of a pilot training program that provides capabilities for the TECO environment. As was discerned throughout the course of this study, the primary gap that exists is a robust training facility to enable training, force integration, and research and development associated with TECO objectives. For training curriculum, the study also identified a significant shortfall in adequate SCADA system training for military personnel. The gap analysis examines requirements and existing capabilities of training facilities, training curriculum, and force integration.

3.1 Training Facilities

A robust training facility is the key to developing TECO specialists. The training facility must consist of real-world SCADA systems and provide the ability to evaluate mission operations across the range of TECO core activities. The training facility must enable hands-on training, the ability to evaluate integration with other tactical forces, and the means to foster research and development of capabilities. Note that testbeds and simulation environments do not adequately reflect real-world system implementations.

One of the primary challenges with developing a training facility for TECO requirements is the integration of full-scale SCADA systems. Real-world SCADA systems are comprised of varying vendors, protocols, configurations, and instrumentation. Indeed, the costs associated with designing and building a training facility that consists of real-world SCADA systems is significant. However, training on real-world SCADA systems helps prepare students for the configuration and deployment intricacies that will be seen in an actual environment. Additionally, the use of real-world SCADA systems emphasize the importance of physical safety override systems and how they can impede successful execution of the intended effect. Note that Appendix A provides an overview of SCADA systems and their functionality.

3.1.1 Requirements

A training facility that consists of real-world SCADA systems is needed that enables cyber military professionals the ability to gain an in depth understanding of SCADA systems and the effects that cyber initiated actions have on the physical processes. Simulated environments and small-scale testbeds do not provide the functionality, processes, or physical components that are needed to adequately train personnel. The training facility must be modular to allow reconfiguration for differing mission objectives and provide the ability to integrate with other tactical forces for tactics evaluation and assessment of TECO capabilities.

3.1.2 Analysis of Existing Capabilities

Current military, government, and commercial training facilities were evaluated to assess capabilities for supporting the TECO training objectives. Table 1 provides a summary of the findings. The letter ‘X’ indicates available training facilities adequately cover the requirement. The letter ‘Z’ indicates the requirement is partially covered.

Current training facilities lack real-world systems and the ability to manipulate physical processes and measure effects. To meet TECO training requirements, students must be exposed to a hands-on training that incorporates actual physical systems. Current training facilities primarily use individual components, simulated environments, or small-scale testbeds. The training varies amongst the different groups, with the majority of training facilities using only individual subcomponents. Some of the more advanced training facilities incorporate simulations for traffic generation and to provide notional targets for students to exploit. A few training offerings include small-scale testbeds that model real-world SCADA systems. The small-scale testbeds provide students the opportunity to manipulate physical devices and observe minor effects. It is important to note, however, that the test-

Table 1. Training environment.

	Military	Government	Commercial
Individual Cyber-physical Subcomponents	X	X	X
Interconnected Cyber-physical Subcomponents	Z	Z	Z
Real-world Cyber-physical Systems			
Ability to Assess Multiple Access Points	Z		Z
Ability to Manipulate Physical Processes	Z	Z	Z
Ability to Measure Effects	Z	Z	
Remote Control Center		Z	
Modular Training Environment			
Multiple Vendor Exposure			Z
Multiple Communication Mediums	Z		Z
Interactive Training Capability	Z	Z	Z
Ability to Integrate with other Tactical Forces			
Research and Development Capability			

*X indicates requirement adequately covered; Z indicates requirement partially covered.

beds provide only a fraction of the functionality and do not adequately replicate the processes, inter-workings, or sophistication associated with a fully operational system. At even the most basic level, students need exposure to functional systems to observe the physical processes and to gain insight into the complexity of the systems. It is quite common that graduates of existing training courses have never seen an actual SCADA system in operation.

The majority of training courses use single SCADA subcomponents and virtualized applications for training. For example, students are often assigned individual PLCs for the duration of the training. The PLCs are typically isolated with little-to-no interconnection to other SCADA subcomponents. Additionally, the training does not incorporate a remote control center, which is a core subcomponent for targeting and exploiting a SCADA system. In many instances, the training facility failed to include many of the SCADA applications (e.g., HMI, Historian, and I/O Server). The training facility should also incorporate a variety of common access points to expose students to the various ways to gain access to the SCADA system. For example, a primary training requirement should be the ability to identify SCADA systems from the corporate network and understand how to pivot and gain access to the control system network.

Communication mediums provide different attack vectors and can alter the operating characteristics of SCADA systems. Students should train in a facility that incorporates the range of different mediums that are likely to be observed during actual mission sets. The training facility should provide modularity to allow different configurations to meet training objectives, advance student skill sets, and replicate the myriad environments a TECO specialist is likely to encounter. Current training that use simulations or test-beds focus on single, isolated instances of systems. It is important that TECO training provides students the ability to train on multiple system types and sectors.

For the TECO environment, it is essential that a trained expert is knowledgeable in how cyber actions can manipulate physical processes as well as how altering physical processes affect the cyber components. As an example, achieving a desired effect to shut down power to a targeted area may have various cyber options depending on available access, type of field device manufacturers, operating system/applications, available exploits, and system configuration. Based on the scenario, it may be a better option for ground forces to physically trip a circuit breaker or use munitions to destroy the entire sub-station. However, constraints or mission objectives may negate the presence of ground troops or munitions, and a more effective option may be manipulation of the system via cyber to shut down the power. Indeed, an interactive training facility and ability to integrate tactical options are essential requirements for the TECO training environment.

Another important requirement is the ability to perform research and development. Due to the lack of access to real-world SCADA systems, the military currently does not have an environment to perform detailed research and development. This is a significant challenge throughout the research community. Indeed, access to real-world SCADA systems for research is difficult due to concerns over potential impact to an operational system that cannot suffer from downtime or performance issues [15]. Alternatively, building an operational SCADA system specifically for research is cost prohibitive. As a result, research communities have difficulty obtaining real-world traffic and evaluating solutions in real-world environments. Although organizations such as AFIT, AFRL, and ARL are performing critical infrastructure and SCADA research in lab environments, the results do not necessarily translate to full-scale operational systems. A real-world research and development environment enables operational testing and evaluation, evaluation of TTPs, capability development, and supports rapid acquisition. Coupled with the training environment, research efforts can help identify shortfalls in capabilities and evaluate solutions during 'live fire' training.

3.2 Training Curriculum

Training curriculum for the TECO environment must prepare specialists for the range of operations that are likely to be encountered during actual mission sets. Findings from the study indicate that available training is not adequate for developing the necessary skill sets required for the TECO environment. Current training focuses primarily on defending and exploiting traditional ICT and does not sufficiently incorporate the physical components and processes associated with SCADA systems. To correct this deficiency, a training program is required that emphasizes the physical aspects and effects associated with SCADA systems.

An expert trained in system processes and cyber capabilities has the ability to identify the range of options, comprehend the implications, articulate the strengths and weaknesses of each option, and provide actionable courses of actions. From a defensive perspective, understanding how a cyber attack can alter the physical processes provides the necessary insight to develop strategies to protect against system manipulation. If a physical process is altered, the trained TECO specialist can discern if the physical effect was cyber initiated, identify attack vectors, determine risks to other systems/components, modify configuration/parameters to minimize operational impact, and remove the threat. From an offensive perspective, the TECO specialist must understand the implications of their actions and how they integrate with other battlefield options.

3.2.1 Requirements

To meet TECO training requirements, it is necessary to have a comprehensive knowledge of the cyber components and physical processes. Indeed, it is not sufficient to understand just the cyber components or physical processes to create and defend against targeted attacks. In the SCADA environment, cyber professionals and engineers have (historically) been segregated to focus on their specific area of expertise. This separation of duties and responsibilities, however, has created a void in individuals that understand the holistic functionality of SCADA systems. With the emergence of technology and its incorporation into the automation of physical system processes, there is no ability to draw definitive lines between engineering aspects of the physical processes and the cyber correlation. The notion is similar to a modern-day automobile technician that, due to advancements in technology, must have knowledge of and capabilities for the car's electrical and mechanical, and the interaction between the two.

To be effective, TECO specialists must have the ability to evaluate a targeted system (for attack or defense), understand system functionality, realize how to achieve the desired effect, determine the options, understand the risks, evaluate secondary effects, and articulate options to the commander. The core principles associated with traditional networks has been the military's primary focus for cyber training efforts. As such, initial training curriculum development should focus on cyber-physical systems associated with TECO requirements. Specifically, the military does not have a robust training program that provides the necessary skill sets for SCADA systems.

The core knowledge areas for the TECO training program to fulfill these requirements can be divided into three categories: (i) SCADA system principles, (ii) cyber manipulation, and (iii) targeted effects. Note that from a training perspective, offense and defense TECO specialists require the same technical expertise and knowledge.The following list outlines the associated knowledge areas for the three core categories:

- SCADA System Principles
  - System functionality
  - Principles of control theory
  - System architecture and operating requirements
  - Instrumentation devices
  - Field device components
  - Control and data acquisition
  - System applications
  - Communications and interconnections
  - Real-world configurations and deployment
- Cyber Manipulation
  - Differences between traditional ICT and SCADA systems
  - Access vectors
  - Asset enumeration and identification
  - Field device, application, and operating system analysis
  - Communication and protocol analysis
  - Vulnerability analysis
  - Confidentiality, integrity, and availability attack considerations
  - Exploitation
  - Pivoting
  - Implanting malware
  - Manipulate physical process
  - Network protection mechanisms
  - Forensics
  - Hardening strategies
- Targeted Effects
  - Exploit and Attack
    - Determine what physical system changes are required to achieve desired effect
    - Determine means to manipulate system via cyber capabilities
    - Evaluate exploitation options
    - Identify LIMFACS
    - Develop attack options

    - Prioritize options and articulate associated gain/loss factors
    - Execute mission
    - Evaluate mission success
  - Defend and Recover
    - Prioritize system components
    - Identify attack
    - Determine system impact
    - Minimize impact
    - Eradicate malware
    - Recover from attack
    - Determine root cause
    - Implement safeguards to prevent reoccurrence
    - Examine attack to obtain intelligence
    - Evaluate defense strategies

The knowledge areas were derived from skill-sets required to understand principles associated with defending against and creating targeted attacks on SCADA systems. The trained TECO specialist should understand: system operating principles; components and functionality; underlying physical processes; cyber-physical correlations; means for gaining access to cyber-physical systems; implications of cyber actions on the physical processes; how to leverage cyber capabilities to achieve physical effects; how to evaluate second order and cascading effects; limitations of cyber capabilities; and how cyber-kinetic actions are incorporated into military requirements, planning, and operations.

3.2.2 Analysis of Existing Capabilities

For this report current military, government, and commercial cyber SCADA training courses were evaluated. Military training included reviews of Army, Air Force, Navy, Marine, and USCYBERCOM courses. Government training included reviews of DHS ICS-CERT and Department of Energy courses. Commercial training included reviews of industry leading vendor courses.

The current military, government, and commercial training curriculum were mapped to core knowledge areas to identify shortfalls in existing training. Table 2 provides a summary of the findings . The letter 'B' indicates available training covers the requirements at a basic level with no practical application. The letter 'I' indicates available training covers the requirements at an intermediate level with practical application. The letter 'A' indicates available training covers the requirements at an advanced level with in-depth technical application. To meet the rigors of the TECO environment, training should equate to 'A' for each of the requirements.

The findings revealed little variance in the training courses for SCADA system fundamentals and cyber manipulation. Not surprisingly, the military courses provide some focus on targeted effects relating to military operations and planning; whereas, the government and commercial courses focus on enterprise security. The primary gaps for all training courses included the lack of emphasis and material relating to physical controls, instrumentation, safety systems, and system effect analysis. From a skills and knowledge perspective, the course material ranged primarily from beginner to intermediate.

The common theme identified during the curriculum analysis was the focus on a traditional ICT penetration testing (assessment) mentality. Traditional ICT assessments rely on network focus, freedom of maneuver to discover vulnerabilities, a known environment (e.g., Windows operating system), and common vulnerabilities discovered via network assessment tools. Although SCADA systems are comprised of some traditional ICT systems, understanding how targeted, physical effects are achieved requires evaluation of the composite system-of-systems architecture beyond just the cyber aspects. The current training focuses on individual subcomponents examined in isolation and does not adequately incorporate the holistic system. This notion is important, as it is imperative that trainees understand the interactions amongst subcomponents and how manipulating parameters in one device cascades throughout the system.

Table 2. Training curriculum.

	Military	Government	Commercial
Fundamentals of SCADA Systems	B	B	B
Control Theory			B
SCADA System Architecture	B	B	B
Physical Controls			
Instrumentation			
Field Device Operations and Programming	B	B	I
Control and Data Acquisition	B	B	B
SCADA System Applications			I
Communications Media and Protocols	I	B	I
Implications of Safety Systems			B
System Effect Analysis			
Fundamentals of SCADA Exploitation vs. ICT	I	B	I
Asset Enumeration and Identification	B	B	I
Identifying Access Vectors	B	B	B
Field Device, Application and Operating System Analysis	B	B	B
Vulnerability Analysis	I	B	I
Exploitation	I	I	I
Pivoting	B	B	B
Implanting Malware	B		B
Physical Process Manipulation	B	B	B
Forensics	B	B	B
Hardening Strategies	I	I	I
Military Operations Planning	I		
Intelligence Preparation of the Operational Environment	B		
Asset Prioritization	B		
Time Factors			
Second Order Effects			
Gain/Loss Determination	B		
Course of Action Determination	B		

*B indicates Basic Level; I indicates Intermediate Level; A indicates Advanced Level.

Current training does not extend beyond the basic programming and functionality of SCADA system subcomponents. Similarly, communications protocols are analyzed at a functional level and only a few protocols are incorporated into the training. As a result, a major gap in the training includes the implications of the cyber-physical correlation and the effects cyber actions have on the physical controls and instrumentation. The government and commercial training is geared towards ICT professionals and focuses on material that primarily exposes individuals to SCADA systems and security threats. Although the curriculum provides foundational training to develop awareness and basic knowledge, it is not tailored for advanced skill sets. The military training offers block courses that are coupled with other training as part of a broader cyber curriculum. Similar to the government and commercial training, the military training focuses on the ICT aspects of SCADA systems and fails to incorporate the knowledge-level associated with advanced cyber tactics that manipulate physical processes. As a result, the available training prepares individuals with the knowledge and skills to protect against ICT focused attacks but does not adequately prepare for sophisticated, targeted attacks.

As a perspective on the degree of training, it is imperative that TECO training equates to the advanced skill-sets required of an elite tactical force entrusted with lethal capabilities. Currently, available training equates to basic rifle school; whereas, an advanced sniper's course is needed to fulfill requirements associated with TECO missions.

3.3 Force Integration

Critical to military operations is the integration of TECO capabilities with other tactical forces. As TECO training focuses on developing tactical specialists, it is imperative that trainees understand how their roles integrate with other tactical operations.

3.3.1 Requirements

A large-scale environment is required to exercise TECO training in conjunction with other traditional tactical forces and capabilities. The primary means for integrating and evaluating tactical capabilities is through coordinated field training exercises. Field training exercises provide realistic scenarios that help prepare trainees for actual combat roles. Additionally, field training exercises highlight deficiencies in training and capabilities. As the TECO concept evolves into a military capability, field training exercises are necessary for coordinating effects (e.g., timing, synchronization, and impacts), identifying training gaps, and evaluating combat capabilities.

3.3.2 Analysis of Existing Capabilities

In current military exercises, cyber capabilities are typically exercised in isolation from other tactical forces. Although some exercises have expanded to incorporate joint force operations, cyber efforts focus on traditional ICT effects and lack full-scale training facilities. The most relevant training exercises include Cyber Flag, Cyber Guard, Cyber Shield, and Red Flag.

Cyber Flag is USCYBERCOM's primary exercise for evaluating cyberspace capabilities [17]. The exercise provides integration with air, land, and sea operations and evaluates command and control of cyber capabilities. The exercise is conducted at Nellis AFB, Nevada and uses closed networks that are designed to simulate DoD and adversary information networks. Although Cyber Flag provides tailored training opportunities in the joint environment, the focus is on capabilities for the Cyber Mission Force and information networks. Additionally, Cyber Flag is an annual exercise and only a fraction of cyber forces are able to participate. As specified by Army Brig. Gen. Paul Nakasone, commander of the Cyber National Mission Force, "A persistent training environment (PTE) would meet a growing and urgent need for small team events as well as supplement individual training, incorporating physical locations for on-site or distributed training with live networks. A PTE would include a progressive and evolving curriculum tailored to individual and team-level training to complement larger exercises and incorporating cyberspace into military operations."

Cyber Guard is a combination of elements from the National Guard, Reserves, National Security Agency, and USCYBERCOM in a joint exercise in support of the Department of Homeland Security and FBI responses to foreign-based attacks on simulated critical infrastructure networks [18]. Cyber Guard provides an environment where multiple cyber incidents could affect a variety of targeted locations and facilities. Cyber Guard 14-1 took place in July 2014 at the National Academy in Quantico, Virginia. It was a two-week effort with over 500 participants collaborating as an interagency team promoting critical information sharing in support of a whole-of-nation effort. Participants responded to a variety of scenarios including cyber attacks against critical infrastructure such as water treatment facilities, a gas pipeline, and the electrical grids. As stated by Greg Touhill, deputy assistant secretary of homeland security for cybersecurity operations and programs, "Exercises like Cyber Guard help us develop and refine key information sharing and coordination processes, understand each other?s capabilities and authorities, and operate in a manner that keeps us in the right formation to present the best national response."

Cyber Shield is a National Guard training exercise that focuses on defending critical infrastructure networks [19]. The exercise is geared specifically towards cyber operations and training for Cyber Network Defense Teams. The annual exercise brings together over 300 soldiers, airmen, and civilians to train on scenarios representative of what network defenders face in the real world. In addition to training for guard personnel, the exercise helps identify challenges associated with coordination of different federal and state organizations. As the training is focused on National Guard capabilities and defense of critical infrastructure against cyber attacks, the exercise does not incorporate other tactical force capabilities. Additionally, the exercise does not use real-world SCADA systems and relies on simulations for training scenarios.

Red Flag is a US Air Force combat training exercise hosted at Nellis AFB, Nevada [20]. Red Flag started in 1975 in response to fighter pilot performance during the Vietnam War. It was determined that a pilot's survival rate increased dramatically after the first ten combat sorties. As a result, Red Flag was created so pilots could fly realistic combat missions in a safe training environment to prepare for wartime situations. Cyber was incorporated into Red Flag in 2007 through simulated mission sets and has grown to include the Joint IO Range as a training ground for cyber assets. The Joint IO Range provides the ability to tailor mission sets and configure targets associated with traditional information networks; however, the Joint IO Range does not provide the ability to incorporate real-world facilities and full-scale SCADA systems. As such, the primary mission sets focus on effects associated with compromise of adversary information networks and implications of attacks on joint force operations.

Force integration of cyber capabilities is primarily focused on ICT through exercises that use modeling and simulation training environments. For TECO, tactical capabilities must be exercised in an environment that incorporates real-world systems to include functional SCADA systems. In addition, exercises incorporating the TECO concept must fully integrate TECO capabilities as coordinated combat options. Currently, cyber capabilities are viewed as a force multiplier that can affect tactical operations. Alternatively, the TECO concept is intended as a force capability that is integrated into battlefield tactics. Indeed, TECO effects should be incorporated into military planning and operations, and TECO capabilities should be presented as actionable COAs that are measured against or coordinated with other tactical options. A key to the integration of TECO capabilities with other tactical forces is a persistent training facility that provides the ability to exercise TECO concepts and evaluate the coordination of effects. No current training environment provides the facilities or capabilities to meet these requirements.

Even though some exercises include coordination of federal, state, and local authorities where the DoD collaborates with various levels of government, there is a lack of participation by the private sector that actually owns and operates the nation's critical infrastructure. One of the major concerns with the lack of coordinated efforts is the establishment of command and control during an actual incident. Indeed, the limited insight into the operations of a particular privately-owned facility may prohibit the DoD's ability to respond to the event.

4 Strategic Initiatives

The strategic initiatives are based on delivering a training program that meets the rigorous requirements of the TECO environment. The recommendations provide the next steps for developing a pilot training program that blends various areas of cyberspace and tactical operations into a new skill-set.

An economical and mission effective means for creating the TECO training program is to leverage the existing infrastructure at MUTC and to develop curriculum from the ground up based on the unique TECO mission requirements. In addition to training facility and curriculum requirements, the recommendations for investment extend to encompass DoD capabilities associated with force integration, research and development, and organization requirements for force employment. The strategic initiatives listed below detail efforts to help transition the TECO concept into practice.

4.1 Training Facility

The primary gap for developing the TECO concept is a training facility that incorporates real-world SCADA systems. Developing a facility with real-world SCADA systems enables delivery of meaningful hands-on training curriculum where students observe real effects, provides the ability to exercise force integration, and fosters research and development efforts. The other strategic initiatives are important for realizing the TECO concept; however, the investment for developing a training facility should be a priority.

- Requirements:
  - Training facility with real-world SCADA systems.
  - Ability to configure training facility to meet operational and training requirements.

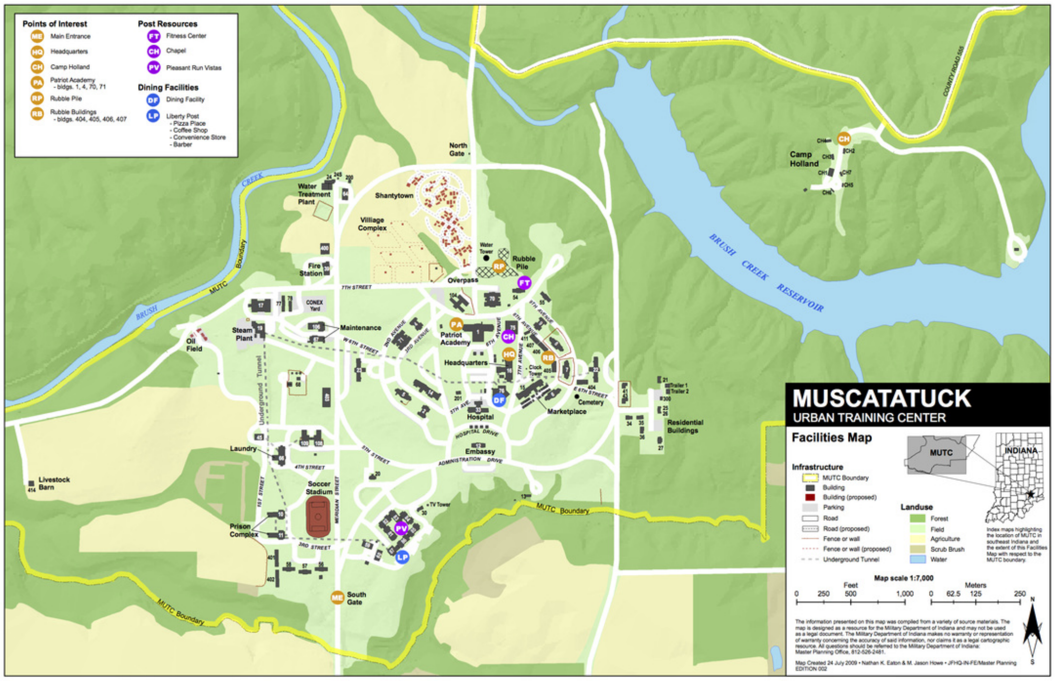
Muscatatuck Urban Training Center.

  - Persistent training facility that is readily available for TECO training and field exercises.

- Recommendations for next steps:
  - Engineering study of MUTC facilities to specify functionality, design, and automation enhancements required to meet training and research objectives.

A consideration for this study was the evaluation of MUTC and the ability to leverage existing facilities for TECO training. The 1,000 acre MUTC site was turned over to the Indiana National Guard in July of 2005 and has been continually evolving into a full-immersion contemporary urban training environment [21]. MUTC is a consortium of governmental, public, and private entities that pool their unique capabilities in order to provide realistic training and pre-operational testing. In accordance with studies by DoD's Test Resource Management Center, the continually-expanding site will meet and exceed pre-operational testing requirements as well as those required by military, governmental, and first-responder agencies.

A site survey was accomplished to evaluate the current MUTC infrastructure and determine the feasibility of automating systems to meet TECO training requirements. Note that the specific details from the site survey are provided in Appendix B. MUTC has the core infrastructure of physical processes and systems in place to support a robust TECO training program. The training environment consists of approximately 180 buildings including a school, hospital, prison, dormitories, light industrial structures, single-family type dwellings, a dining facility, administrative buildings, and a vacant schoolhouse. Additionally, the training area has existing critical infrastructure to include a water treatment facility, waste water treatment plant, coal-fired electric power generation plant, single valve dam, electric substation, traffic control systems, and building automation and access control. The core infrastructure in place at MUTC provides the foundation for a one-of-a-kind TECO training environment.


Points of Interest
ME Main Entrance
HQ Headquarters
CH Camp Holland
PA Patriot Academy - bldgs. 1, 4, 70, 71
RP Rubble Pile
RB Rubble Buildings - bldgs. 404, 405, 406, 407
Post Resources
FT Fitness Center
CH Chapel
PV Pleasant Run Vistas
Dining Facilities
DF Dining Facility
LP Liberty Post - Pizza Place - Coffee Shop - Convenience Store - Barber
North Gate
Water Treatment Plant
Shantytown
Villiage Complex
Fire Station
Water Tower
Rubble Pile
Overpass
7TH STREET
CONEX Yard
Maintenance
Steam Plant
Oil Field
Patriot Academy
Headquarters
Hospital
Marketplace
Cemetery
Residential Buildings
Embassy
Laundry
Underground Tunnel
Livestock Barn
Soccer Stadium
Prison Complex
TV Tower
South Gate
Camp Holland
BRUSH CREEK RESERVOIR
BRUSH CREEK
MUTC Boundary
MUSCATATUCK
URBAN TRAINING CENTER
Facilities Map
Infrastructure
MUTC Boundary
Building
Building (proposed)
Parking
Road
Road (proposed)
Fence or wall
Fence or wall (proposed)
Underground Tunnel
Landuse
Forest
Field
Agriculture
Scrub Brush
Water
MUTC
INDIANA
Index maps highlighting the location of MUTC in southeast Indiana and the extent of this Facilities Map with respect to the MUTC boundary.
Map scale 1:7,000
Feet 0 250 500 1,000
Meters 0 62.5 125 250
N
S
The information presented on this map was compiled from a variety of source materials. The map is designed as a resource for the Military Department of Indiana and may not be used as a legal document. The Military Department of Indiana makes no warranty or representation of warranty concerning the accuracy of said information, nor claims it as a legal cartographic resource. All questions should be referred to the Military Department of Indiana: Master Planning Office, 812-526-2481.
Map Created 24 July 2009 • Nathan K. Eaton & M. Jason Howe • JFHQ-IN-FE/Master Planning EDITION 002

MUTC facilities map.

MUTC affords the ideal location because of the existing infrastructure and ability to incorporate training with other tactical forces. Indeed, MUTC provides the ability for cyber and ground forces to work in a collaborative effort during real-time exercises. This type of environment provides the ability to evaluate the complexities associated with integrating cyber and traditional tactical forces (e.g., communication, coordination, and prioritization) in actual wartime situations. Having a proving ground for coordination and evaluation of ground forces, cyber effects, and command and control, is critical to supporting TECO mission objectives.

Although the core physical systems are in place, an investment is needed to fully develop the infrastructure to meet TECO mission requirements. However, the unique assets that MUTC affords provides an ideal landscape for developing skill-sets in a real-world environment. Indeed, it is estimated that tens to hundreds of millions of dollars in cost savings are realized by using the existing core infrastructure and physical processes already in place. An engineering study is required to specify the functionality, design, and automation upgrades necessary to expand the current capabilities for TECO training objectives. Decisions on system upgrades should be considered in context with the training curriculum to ensure the environment fully aligns with operational needs and training objectives.

4.2 Training Curriculum

The military needs a formal and extensive training course focused on SCADA systems that incorporates actual physical systems. The military-focused training for SCADA systems is required to assess predictability and obtain assurances similar to those employed for kinetic methods. Formal training ensures that strategies translate to tactical capabilities and helps facilitate proper force employment. Defining the courses of action, identifying shortfalls in capabilities, articulating possible outcomes, and examining the feasibility of attacks are dependent on analytical reasoning prior to engagement. As cyberspace becomes a capability on the battlefield with the potential of initiating kinetic strikes, it is imperative that the military has extensive training programs in place that are equivalent to the rigors of traditional force employment.

- Requirements:
  - Training curriculum for SCADA that emphasizes cyber and physical correlations.
  - Training objectives that incorporate military principles and integrates tactical effects.
- Recommendations for next steps:

- Development of SCADA training curriculum tailored to TECO mission requirements.

The training curriculum should be aligned to the three core requirements: SCADA system principles, cyber manipulation, and targeted effects. SCADA system principles and cyber manipulation are divided into specific training blocks aligned to required knowledge and skill sets. The targeted effects areas focus on practical application of knowledge gained in the SCADA system principles and cyber manipulation cores. The following outline shows the primary course topics:

CORE I: SCADA System Principles
Block I: Fundamentals
Block II: Physical Systems and Instrumentation
Block III: Field Devices
Block IV: SCADA System Software
Block V: Communications
Block VI: Advanced Control

CORE II: Cyber Manipulation
BLOCK I: Familiarization
BLOCK II: System Profile
BLOCK III: Vulnerability Analysis and Exploitation
BLOCK IV: Defending Against Attacks and Recovery

CORE III: Targeted Effects
Exploit and Attack
Defend and Recover
Mission Sets

Part of this study included providing a way-ahead for curriculum development. The curriculum details, including knowledge and skill sets, are provided in Appendix C. The training curriculum is tailored specifically to meet tactical DoD mission requirements. Each of the training modules are intended to incorporate a classroom learning environment coupled with hands-on labs. Students start with modules designed to teach the principles of SCADA systems and provide exposure to actual systems and subcomponents. Students will become proficient in SCADA engineering principles and learn control theory, system design, instrumentation, programming, and configuration of SCADA field devices, applications, and interfaces. Students will then study the intricacies associated with cyber attacks on SCADA systems. The techniques associated with exploiting SCADA subcomponents will be explored in detail. Students will learn how to achieve targeted effects using cyber initiated actions to manipulate physical processes. The training covers prioritization of assets, defense strategies, and how to recover from attacks. The training will culminate in mission sets that apply principles to real-world situations tailored to military operations. The training is designed to provide familiarization in the classroom with individual labs and then applying the knowledge in the real-world SCADA training environment.

4.3 Force Integration

Force integration is dependent on training facilities and exercises that provide real-world scenarios. Service components need a persistent training environment to complement larger exercises and incorporate TECO capabilities. Additionally, a persistent training environment provides continual training options to help develop TECO specialists.

- Requirements:
  - Persistent training environment.
  - Integration of TECO capabilities and MUTC training facility with existing exercises.
  - Development of field training exercises to incorporate TECO capabilities.
  - Execution of TECO training objectives with other tactical forces .
- Recommendations for next steps:
  - Evaluation of how MUTC can be incorporated into existing exercises.

An evaluation should be performed to determine how the MUTC infrastructure and SCADA systems can be incorporated into existing exercises (e.g., Cyber Flag, Red Flag, and Cyber Shield). Integration of MUTC provides the ability to evaluate actual effects in a real-world environment. Note that the evaluation should be performed in conjunction with the MUTC engineering study to identify upgrades to current capabilities that meet exercise training objectives.

4.4 Research and Development

Research and development efforts are needed to help identify shortfalls and evaluate solutions in TECO capabilities, operational effectiveness, suitability, and mission capability. Additionally, research questions exist on how to best configure and use the training facility to optimize training efforts and capability evaluation.

- Requirements:
  - Environment to support operational testing and evaluation, evaluation of TTPs, capability development, and rapid acquisition.
  - Ability to optimize training facility to support training and research efforts.
- Recommendations for next steps:
  - Research studies to maximize training and research environment.

The research and development environment must incorporate real-world SCADA systems. Similar to training facility requirements, MUTC has the core infrastructure in place to support research and development efforts. Enhancements to MUTC that support training efforts align with requirements for the research and development environment. As such, considerations for the facility as a dual-purpose environment should be taken into account when developing the strategic plan for MUTC facility enhancements.

The incorporation of functional facilities that contain large scale, real-world SCADA systems and multiple critical infrastructure sectors for cyber training and research has never been done. Coordinating system interoperability for planned operations and test evaluation brings new technical challenges. The following list provides select research questions that help maximize the training and research environment.

- Prioritization of enhancements
  - Based on MUTC enhancement requirements and military needs, what should the order of priority be for the facilities that will be upgraded for training and research?
  - Which vendor devices should be incorporated into the training facility based on military requirements and utilization?
- Instrumenting the environment for training and test evaluation?
  - How should data be captured and where should sensors be placed to optimize data collection?
  - What data is required for analysis?
  - What configuration optimizes data collection?
- Remote connectivity
  - How should remote connectivity be incorporated into the training environment?
  - What organizations should have remote access?
- Scenario development
  - What training scenarios incorporate military requirements, TECO training, and force integration at MUTC facilities?
  - How should manipulation of the physical processes be evaluated?
- System Configuration
  - How should configuration control be implemented?
  - What should the baseline system functionality be?
  - What operator controls and parameters are required for training execution?
- Incorporating modular system functionality
  - How should system modularity be designed into training and test configurations?

  - What are the challenges associated with integrating multiple SCADA systems and sectors into one coherent, interconnected environment?
  - How can system functionality be incorporated into the training and research environment as new facilities are brought online?

- Research and development capability
  - What research can be realized through the real-world environment that cannot be accomplished in a lab setting?
  - How can research be incorporated into training scenarios?
  - How will new capabilities be evaluated in the environment?
  - How will operational, test, and evaluation be performed in the MUTC environment?

4.5 Organization for Force Employment

Considerations for how to organize TECO specialists requires an analysis of force structure, mission objectives, and capability execution.

- Requirements:
  - Develop DoD and service component investment strategy.
  - Determine force structure, mission objectives, and capability execution strategy.
  - Define TECO core activities.
- Recommendations for next steps:
  - Perform a capabilities-based assessment using the Joint Capabilities Integration and Development System (JCIDS) process.
  - Familiarize TECO concept with service components.
  - Establish chief architect to manage the design, development, and operation of SCADA systems at MUTC.

The JCIDS process identifies capability shortfalls and considers operational gaps in the context of all service components. An Initial Capabilities Document (ICD) summarizes the results of the Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, and Facilities (DOTMLPF) analysis and defines gaps in terms of the functional area, the relevant range of military operations, desired effects, timeframe, and recommendations. Based on TECO training requirements and total force implications, it is recommended that the Directorate for Training Readiness and Strategy at the Office of the Secretary of Defense provide the strategic direction for furthering the TECO concept.

Appendix A: Overview of SCADA Systems

SCADA systems are a type of industrial control system that manage, direct, and monitor the behavior of large-scale, distributed systems in the critical infrastructure sectors. As demonstrated in Figure A1, an operator located in a control center monitors for alarm conditions (e.g., pressure increase) and controls remote processes (e.g., closing a valve) for thousands of miles of pipeline and hundreds of field sites that are spread throughout the United States.

Figure A2 shows a more detailed representation of a SCADA system architecture and associated components. The control system network connects the operator workstation and application workstations located in the control center to remote field sites via various communication media (e.g., radio frequency, Internet and telephone lines). Field sites consist of specialized embedded devices such as remote terminal units (RTUs) or programmable logic controllers (PLCs) that convert digital control messages into physical actions such as opening and closing valves and breakers, collecting data from sensor systems, and monitoring the local environment for alarm conditions. A remote access capability enables engineers to perform remote diagnostics and repairs over a separate dial up modem or network. Process data for trend analysis and accounting are stored in the Historian server located in the demilitarized zone (DMZ). A segmented corporate network allows communication to the Historian server to facilitate business operations (e.g., billing, auditing, and trend analysis).

SCADA systems are integrations of cyber computational components and instrumentation devices [22]. Functionally, cyber components include the hardware, software, networks, and communications protocols that enable process automation. Instrumentation devices measure the physical system processes (e.g., flow rate) and provide signals to manipulate the physical

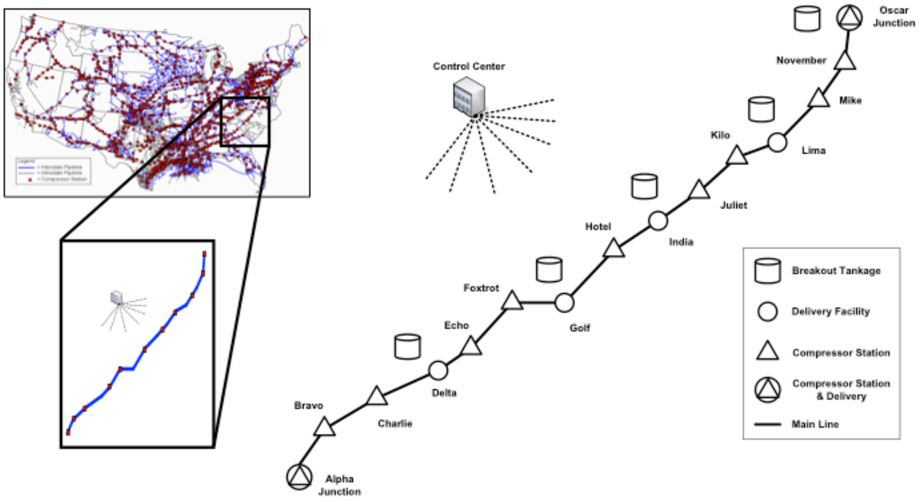


Figure A1. Notional SCADA system for a gas pipeline.

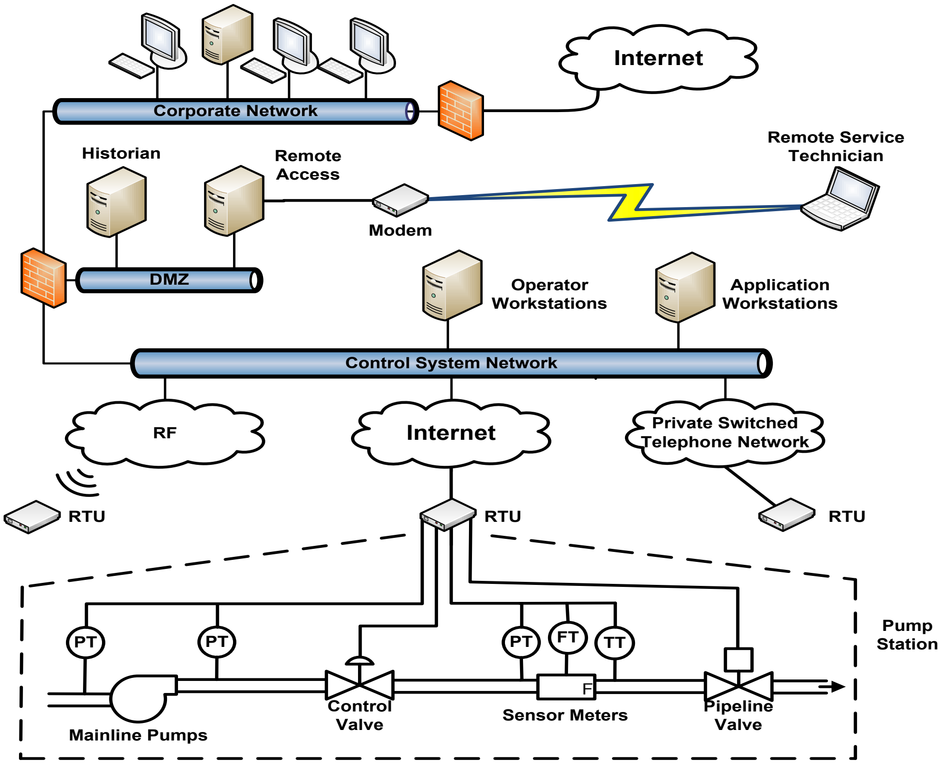


Figure A2. Representative SCADA architecture.

process (e.g., closing a valve). Note that the field devices, such as PLCs, are the primary interlink between the cyber and physical domains. As specified in the NIST Special Publication 800-82, the following list details the primary subcomponents associated with SCADA systems [22]:

- Control Server. The control server hosts the supervisory control software that communicates with lower-level control devices. The control server accesses subordinate control modules over a SCADA network.

- Human-Machine Interface (HMI). The HMI is software and hardware that allows human operators to monitor the state of a process under control, modify control settings to change the control objective, and manually override automatic control operations in the event of an emergency. The HMI also allows a control engineer or operator to configure set points or control algorithms and parameters in the controller. The HMI also displays process status information, historical information, reports, and other information to operators, administrators, managers, business partners, and other authorized users. The location, platform, and interface may vary a great deal. For example, an HMI could be a dedicated platform in the control center, a laptop on a wireless LAN, or a browser on any system connected to the Internet.

- Data Historian. The data historian is a centralized database for logging all process information within a SCADA system. Information stored in this database can be accessed to support various analyses, from statistical process control to enterprise level planning.

- Input/Output (IO) Server. The IO server is a control component responsible for collecting, buffering and providing access to process information from control sub-component field devices. An IO server can reside on the control server or on a separate computer platform. IO servers are also used for interfacing third-party control components, such as an HMI and a control server.

- Field Devices. Field devices control local operations such as opening and closing valves and breakers, collecting data from sensor systems, and monitoring the local environment for alarm conditions.

  - Remote Terminal Unit. The RTU, also called a remote telemetry unit, is a special purpose data acquisition and control unit designed to support SCADA remote stations. RTUs are field devices often equipped with wireless radio interfaces to support remote situations where wire-based communications are unavailable. Sometimes PLCs are implemented as field devices to serve as RTUs; in this case, the PLC is often referred to as an RTU.
  - Programmable Logic Controller. The PLC is a small industrial computer originally designed to perform the logic functions executed by electrical hardware (relays, switches, and mechanical timer/counters). PLCs have evolved into controllers with the capability of controlling complex processes, and they are used substantially in SCADA systems. Other controllers used at the field level are process controllers and RTUs; they provide the same control as PLCs but are designed for specific control applications. In SCADA environments, PLCs are often used as field devices because they are more economical, versatile, flexible, and configurable than special-purpose RTUs.
  - Intelligent Electronic Device (IED). An IED is a ‘smart’ sensor/actuator containing the intelligence required to acquire data, communicate to other devices, and perform local processing and control. An IED could combine an analog input sensor, analog output, low-level control capabilities, a communication system, and program memory in one device. The use of IEDs in SCADA systems allows for automatic control at the local level.

- Safety systems. SCADA systems are designed to be fault-tolerant systems with significant redundancy built into the system architecture. Safety systems are protective hardware and software controls that provide fail-safe protections when unacceptable or dangerous situations occur.

The integration of networking technologies has enabled remote monitoring and control of physical processes. As specified in the NIST Special Publication 800-82, the following list details the primary subcomponents of a SCADA network [22]:

- Fieldbus Network. The fieldbus network links sensors and other devices to a PLC or other controller. Use of fieldbus technologies eliminates the need for point-to-point wiring between the controller and each device. The devices communicate with the fieldbus controller using a variety of protocols. The messages sent between the sensors and the controller uniquely identify each of the sensors.
- Control Network. The control network connects the supervisory control level to lower-level control modules.
- Communications Routers. A router is a communications device that transfers messages between two networks. Common uses for routers include connecting a LAN to a WAN, and connecting field devices to a long-distance network medium for SCADA communication.
- Modems. A modem is a device used to convert between serial digital data and a signal suitable for transmission over a telephone line to allow devices to communicate. Modems are often used in SCADA systems to enable long-distance serial communications to remote field devices. They are also used in SCADA for gaining remote access for operational and maintenance functions such as entering commands or modifying parameters, and diagnostic purposes.
- Remote Access Points. Remote access points are distinct devices, areas and locations of a control network for remotely configuring control systems and accessing process data. Examples include using a personal digital assistant (PDA) to access data over a LAN through a wireless access point, and using a laptop and modem connection to remotely access a SCADA system.
- Communication Protocols. Communication protocols used in the SCADA environments for field device control and intra-processor communication

are typically different from the traditional ICT environment and are often proprietary.

The operating parameters and security principles associated with traditional ICT systems do not readily translate to the SCADA environment; security solutions for ICT systems focus primarily on protecting the confidentiality of system and user data. Alternatively, SCADA systems must adhere to strict safety and reliability requirements and rely extensively on system availability. As demonstrated by Stuxnet, the ability to create a desired, targeted effect requires a high degree of sophistication and an in-depth knowledge of the underlying physical system.

STUXNET

The Stuxnet virus represents a targeted cyber attack on SCADA systems. The virus targeted control systems running a Siemen's Programmable Logic Controller (PLC). It utilized four different Windows zero-day exploits to gain access to computers and search for the Siemen's PLC software [23]. It has been described as "the most technologically sophisticated malicious program developed for a targeted attack".

Stuxnet spread using traditional security vulnerabilities in commercial operating systems, and then propagated to two ICS applications (with hard-coded passwords) to inhibit the functioning of Variable Frequency Drives (VFD) made by specific vendors. To remain hidden, the worm displayed the last program sent to the VFDs while running its own code, similar to running a closed circuit television (CCTV) in a loop. The worm was designed to increase and decrease centrifuge speeds causing the aluminum housing to expand and contract, ultimately coming into contact with other centrifuges.

"There are so many different types of execution needs that it's clear this is a team of people with varied backgrounds, from the rootkit side to the database side to writing exploits. And from the SCADA side of things, which is a very specialized area, they would have needed the actual physical hardware for testing, and [they would have had to] know how the specific factory floor works," - O Murchu [24].

It is impractical to assume that a desired physical effect can be achieved with only the understanding of cyber vulnerabilities and exploits for a SCADA system. A calculated, target effect that results in the desired physical reaction requires an in-depth understanding of the physical processes and components. Only then can cyber capabilities be leveraged to create meaningful impacts on the battlefield. Additionally, defending against and recovering from cyber attacks that target SCADA systems requires a detailed understanding of the cyber-physical correlations.

Appendix B: MUTC

A site survey was accomplished to identify current MUTC infrastructure that could be incorporated into the TECO training environment. For each facility, the existing capabilities were documented along with required enhancements to meet TECO training objectives.

The MUTC infrastructure provides an ideal training ground because it affords functional systems that are isolated specifically to the MUTC site and are not interconnected to public utilities. As a result, training efforts and impacts are constrained to the local MUTC environment. An investment is required to fully automate and instrument the core infrastructure to meet TECO training requirements. However, there are substantial cost savings in enhancing the existing infrastructure as opposed to fully developing a new training environment.

Water Treatment Facility

At the water treatment facility, raw (untreated) water is withdrawn from either a surface water supply (e.g., the Brush Creek Reservoir) or from a holding tank/circular system. There are simple, automated control systems that control and monitor the water flow to the central treatment facility. As water is withdrawn from the source, it passes through steel bar screens to prevent large objects such as logs or fish from entering the treatment facility. The water is pretreated and held in a large pre-sedimentation basin to allow time for sand and larger silt particles to settle out. A basic process that includes coagulation, flocculation, sedimentation, filtration, and disinfection is used for treatment of the water. The treated water is pumped under pressure into the distribution system, or a network of pipes (water mains) interconnected with ground level or elevated storage facilities (reservoirs).

Although the water treatment facility at MUTC no longer provides services to the site, the core system functionality is in place and upgrades/modifications can be made to make the system operational to meet training objectives. Upgrades to existing flow meters, pressure transmitters, ground storage tank level instrumentation, control valves, and water quality instrumentation are required. Further automation enhancements are needed, to include integration of field devices and remote control and monitoring capabilities.

Waste Water Treatment Plant

There are three typical stages used in waste water treatment: influent flow and primary clarification; secondary biological treatment; and tertiary disinfection and effluent flow. The primary clarification stage uses a series of screens to remove suspended and floating solids from the raw sewage. Secondary biological treatment removes organic materials by using microbes that consume the organic matter as food, and convert it to carbon dioxide, water, and energy. The wastewater then flows to settling tanks where the bacteria clarifies and the remaining solids are removed. The third stage use chemicals to remove additional phosphorous and nitrogen from the water. Chlorine is added to the water to kill any remaining bacteria, and the water is discharged. The MUTC waste water treatment plant has system functionality for stage one and stage two. Instrumentation and automation includes the ability to measure and control water flow, tank levels, pressures, temperatures, pH, conductivity, turbidity, and basic wastewater analysis functionality.

The facility provided waste water treatment capabilities for the MUTC campus until it was decommissioned in 2014.The core system functionality is still in place and upgrades/modifications can be made to make the system operational to meet training objectives. Mechanical, civil, and electrical work is required to modify the existing infrastructure. Note that the intent is not to retrofit the facility to a condition suitable for sanitary waste treatment, but to create a real-world training environment that uses actual processes observed in real-world waste water treatment plants. As such, system modifications can be made to bring the waste water treatment facility to an operational status that meets the intent of TECO training. Upgrades are required for existing flow meters, pressure transmitters, ground storage tank level instrumentation, control valves, and water quality instrumentation. Further automation enhancements are needed, to include integration of field devices and remote control and monitoring capabilities.

Coal-Fired Electric Power Generation Plant

Coal-fired power generation plants turn water into steam, which drives turbine generators to produce electricity. Coal is pulverized and mixed with hot air and placed into the firebox of the boiler. Purified water is pumped through pipes inside the boiler which turns to steam as a result of the intense heat. The steam can reach temperatures of up to 1,000 degrees Fahrenheit and pressures up to 3,500 pounds per square inch. The steam is piped to the turbine and pushes against a series of giant turbine blades which turns the turbine shaft. The turbine shaft is connected to the generator, where magnets spin within wire coils to produce electricity. The steam is then drawn into a large condenser chamber where it is cooled by water that is pumped through tubes in the condenser. The process converts the steam back into water so that it can be recirculated and used over and over again in the plant.

The facility at MUTC does not provide electric power generation; however, a small-scale control system is used at the local facility for monitoring and controlling the system processes. Engineering modifications are required to incorporate the existing infrastructure into the TECO training environment. Architecture design changes are required to retrofit the current control system with automation and instrumentation to enable remote control and monitoring at the training master control center. The modifications require major engineering and installation efforts to ensure training objectives do not interfere with daily operations. Additionally, due to the nature of the coal-fired electric power generation processes, there is a high degree of safety concerns relating to the manipulation of physical processes through cyber initiated actions that must be evaluated.

Single Valve Dam

There is a single valve dam located on the Brush Creek Reservoir. The dam is used for flood control for North Vernon. The valve uses a manual process for opening and closing the dam. To provide a real-world environment to meet TECO training objectives, the dam should be retrofitted with an automated process for integration of field devices and remote control and monitoring capabilities to include opening and closing of the valve, water flow rate, valve position sensor, and ultrasonic level sensor to measure leaking water. Additionally, radio communication is needed to facilitate remote control and monitoring.

Prison Security and Monitoring Systems

MUTC contains a prison training facility that consists of prison cells. Currently, there is a centralized command center that allows guards to monitor inmates through a closed-circuit TV system. Typical prisons are equipped with integrated intercom, closed-circuit TV, and cell door locking systems. Prisons use a door control protocol that ensures that doors are locked and unlocked in the right order and only at the appropriate time. Security zones have designated posts with cameras located throughout the facility that are systematically scanned to display officers and inmates. Officer posts are also equipped with an intercom that enables communication between the post and the command center. To provide a real-world environment to meet TECO training objectives, the prison should be upgraded to an automated process for remote control and monitoring at the prison command center for the cell door locks, intercom system, and closed circuit TVs. The required enhancements include:

- Building modification
- Operator workstations

- Overhead monitoring screens
- Dedicated SCADA System Servers
- SCADA control software
- Client workstations
- Network and communications upgrade

Electric Substation

A substation is a part of an electrical generation, transmission, and distribution system . A substation includes transformers to step up voltage to higher levels or step down voltage to lower levels. Substations generally have switching, protection, transformers, and control equipment. Circuit breakers are used to interrupt any short circuits or overload currents that may occur.

The MUTC electric substation provides training opportunities to evaluate effects of manipulating SCADA systems in the electrical sector (e.g., opening circuit breakers, changing tap settings, and equipment failure indication). Engineering modifications are required to incorporate the existing infrastructure into the TECO training environment. Architecture design changes are required to retrofit the current control system with automation and instrumentation to enable remote control and monitoring at the training master control center. Additionally, modifications may be required to isolate the substation to ensure training activities objectives do not interfere with daily operations.

Traffic Control Systems

Modern-day traffic lights incorporate automated control technologies to execute multiple timing plans and communicate in real time with networked sensors to efficiently manage traffic flow. Traffic lights use sensors that are typically connected via wireless networking technologies to nearby access points and repeaters, which then send the data to a traffic management system located in a centralized traffic management center. The MUTC facility currently has operational traffic lights that are not automated or controlled via a traffic management center. To provide a real-world environment to meet TECO training objectives, the traffic lights should be automated to enable remote control and monitoring. Additionally, radio communication and network architecture is needed to facilitate interconnection of the lights and the master control center.

Building Automation

Building automation systems are designed to monitor and control the mechanical, security, fire and flood safety, lighting, HVAC, humidity control, and ventilation systems in a building. The majority of commercial, institutional, and industrial buildings built after 2000 include building automation capabilities. Control centers provide remote monitoring and control of building automation for multiple facilities.

Buildings within the MUTC complex have HVAC systems that allow engineers to remote in and control climate systems. The buildings also have fire alarm and suppression systems that can be remotely monitored. Additionally, security systems for access control are installed at various buildings. The security system is strictly for access control and uses standard RFID technology to grant users with authorized cards access to buildings. The security system does not provide a monitoring capability that alarms for unauthorized access or if someone attempts to break into the facility.

The building facilities require upgrades to existing HVAC systems to enhance remote control and monitoring. The mechanical systems should be retrofitted with an automated process for integration of field devices and remote control and monitoring capabilities. The existing HVAC infrastructure requires upgrades for automation to existing chillers, boilers, air handling units, fan coil units, heat pump units, and variable air volume boxes. Engineering modifications are also required to incorporate the existing fire alarm and suppression systems into the TECO training environment. Processes and procedures are required to ensure coordination with responders are incorporated appropriately to meet training objectives. Additionally, further automation enhancements are needed for the security system to provide remote monitoring capabilities. The building automation systems should be interconnected and remotely monitored and controlled at the master control center.

Communications Infrastructure

SCADA operations will be monitored and controlled at the centralized Master Control Center with all facilities interconnected via fiber optic cable and last-mile radio frequency (RF) communications. The fiber optic interconnectivity has been previously established within MUTC and is available for integration of the SCADA systems. Wireless radio RF interconnectivity will be established using Motorola Canopy components of the GRANITE System currently available at MUTC. The following list details some of the existing communications infrastructure at MUTC.

- Approximately 5,000 strands of fiber scattered throughout the campus
- Radio shot to COB panther (at the airport)
- Several point-to-point and point-to-multipoint air fiber shots across the campus
- Wireless umbrella on campus that can used cover current existing dead spots
- Two VHF radio repeaters and six UHF radio repeaters
- Three outgoing circuits – Guardnet, JAWS (the ISP for MUTC), and another ISP for Atterbury
- Available server room with redundant power, and battery backups

The facilities that will be incorporated into the TECO training environment have existing communications or can be readily upgraded to support the requirements for enhancing MUTC.

Master Control Center

The master control center is the centralized hub that provides real-time system control and monitoring. The control center integrates the MUTC operational SCADA systems into one location for remote control and monitoring. Students can train on designated HMIs and observe real-time SCADA system processes. The control center also provides students the ability to evaluate effects of cyber-initiated actions on physical processes.

Currently, there is no centralized, master control center at MUTC. As a major subcomponent in SCADA systems, a master control center is necessary for the TECO training environment and should be a priority when considering investment strategies. To facilitate the training environment, the master control center should be separated in to several control pods that allow simultaneous monitoring of different SCADA systems. Overhead display monitors should provide real-time views of associated processes and systems, therefore enabling instructor evaluation and to facilitate student learning. SCADA system control should be configured for each training pod to align with current training objectives. Note that control could be isolated to allow individual control pods access to specified SCADA systems. The control center should utilize a combination of virtual servers to allow modular back-end systems and virtual desktops for the modular operator/engineering workstations. This will increase the economy of the systems while creating a flexible training environment, increase system stability, and decrease training delays for system changes. Figure B1 shows a notional representation of the master control center with four control pods and overhead display examples.

MUTC currently has a designated building containing fiber and network communications with storage space to house a data center. The building requires upgrades to meet the TECO training objectives.

Figure B1. Master control center representation.

Appendix C: Training Curriculum

The TECO training will consist of classroom learning that emphasizes hands-on labs to facilitate student learning. Curriculum development should be accomplished using a phased approach to ensure development and delivery of training in an efficient manner. The initial phase involves course material development for the knowledge and skill sets requirements associated with the three core knowledge areas. A mission set analysis should be performed to map operational requirements to training scenarios associated with the capabilities of the training environment. As MUTC SCADA systems are upgraded to incorporate more facilities, curriculum revisions are required to align labs and scenarios to integrate the expanded real-world training environment.

SCADA System Principles

The SCADA system principles core emphasizes the requisite knowledge for understanding physical system attributes and the cyber-physical relationship. System functionality includes operating principles, common vernacular, and details on implementation throughout the various sectors. Control theory provides the fundamental knowledge of basic processes, controls, system engineering, and dynamic behavior for understanding system function and design specifications. System architecture and operating requirements detail the types of configurations and parameters for supporting system functionality. Note that system functionality is dependent on the underlying physical process. For example, a liquid pipeline has strict timing requirements because liquid does not readily compress and an increase in pressure due to a blockage could result in a pipeline rupture; whereas, a gas pipeline has less restrictive timing requirements because gas has greater compressibility.

Understanding these types of system properties is critical when planning to defend against or execute an attack.

Instrumentation devices measure the physical system attributes to include temperature, pressure, flow, and level. It is important to understand how the current and voltage input/output signals to/from the field devices impact the sensors and actuators that instantiate the physical changes in the system process. Understanding the programming languages and field device system architecture (i.e., hardware, firmware, and software) provides the ability to manipulate system control through device exploitation. Control and data acquisition provides the fundamentals for system interaction and incorporates how data is processed and used throughout the system. Applications include the SCADA system specific programs for managing functionality, providing process visualization, and enabling the operator interface. Understanding the communication protocols, network design, and topology is critical for determining access capabilities and how network traffic is routed throughout the system.

Cyber Manipulation

The cyber manipulation core emphasizes the ability to exploit cyber vulnerabilities to affect the physical process. First, it is important to understand the differences in traditional ICT systems and SCADA systems. Fundamentally, the methods for identifying a vulnerability in hardware, software, or system configuration do not change; however, the application to the environment and impact of exploiting a vulnerability is dependent on the targeted system. For example, performing a routine network scan on a traditional ICT system provides identification and details of workstations connected to the network. Performing this same action on a SCADA system network, however, may cause a field device to malfunction and render it inoperable. It is important for the TECO specialist to understand how to obtain system configuration and parameters, as well as the capabilities and limitations of available tools.

Understanding access vectors provides insight to leveraging intercommunication, access points, and various medium to gain access to the SCADA system. Note that the access vector may change depending on desired effects and mission parameters. Asset enumeration and identification provides the ability to discern what components are in the system, to include device manufacturers and the associated network interconnections. This information is used for field device, application, operating system, communication, and protocol analysis to determine system configuration and software revision information. A vulnerability analysis reveals weaknesses in system configuration, design, and implementation for system exploitation and implanting malware. Confidentiality, integrity, and availability attack considerations are used in determining how to execute the attack and manipulate the physical processes. Pivoting involves using obtained access from one system to compromise other systems. For SCADA systems, pivoting enables access to the appropriate subcomponent to achieve the desired effect. Once appropriate access is obtained, determination of second order and cascading effects must be examined. Defensive capabilities ensure appropriate configurations and safeguards are implemented to prevent compromise or minimize damage with respect to the physical process should an attack occur. Forensics capabilities help determine how the attack occurred, determine extent of damage, identify preventative measures to prevent future compromise, and discern intelligence about the attack.

Targeted Effects

The targeted effects core emphasizes military planning and operations for executing a tactical mission. Exploiting and attacking a SCADA system requires a detailed understanding of how to achieve the desired affect, identify limitations, develop courses of actions, evaluate gain/loss factors, execute the mission effectively, and evaluate the outcomes. Defending systems against an attack and recovering from an attack requires prioritization of assets to ensure the physical processes continue to operate as required. The defender should have safeguards in place prior to an attack and perform routine assessments to identify weaknesses. Once an attack is identified, the system impact must be discerned to minimize and prevent further damage. Recovering from the attack requires the ability to determine the root cause, eradicate the malware, and prevent recurrence of the attack. An extensive knowledge of forensics capabilities provides the ability to understand the attack and provides the ability to gain intelligence regarding the attack and attacker.

The targeted effects core synthesizes the SCADA system principles core and cyber manipulation core for the military TECO environment. Understanding targeted effects is best realized through mission-set training by immersion of trainees into environments that mirror real-world scenarios. The TECO specialist must be able to apply knowledge of SCADA systems and cyber manipulation to tailored missions that emphasize considerations for combined effects, determination of second order effects, and integration with other tactical forces/capabilities for military operations.

CORE 1: SCADA SYSTEM PRINCIPLES

BLOCK 1: Fundamentals	
Concepts	Knowledge and Skill Sets
Introduction to SCADA	• Definition of SCADA • Applicable processes • Elements of a SCADA system • Operating principles • Common vernacular • Sector specific implementation overview
Control Theory	• Basic processes • Process dynamics • Basic control • Discrete control • Sequential control • Hazard analysis methodologies • Risk analysis • Safety system design • Process Industry Practices (PIP) • Ergonomics • Interpreting design specifications and system requirements
System Design	• Understanding process control • Fundamentals of schematic diagrams • Basic pressure units • Basic flow units • Basic conversions • Manufacturer specifications • Interpreting P&ID symbols • Interpreting loop diagrams • Interpreting mechanical and electrical drawings • Interpreting complex technical documents • Identifying abnormal variations in data or readings • Identifying malfunctions in equipment and possible causes • Identifying abnormal operating conditions • Manipulating inputs to a device • Interpreting output readings
Codes, Standards, and Regulations	• American National Standards Institute (ANSI) • Factory Mutual (FM) • Institute of Electrical & Electronics Engineers (IEEE) • International Society of Automation (ISA) • National Electrical Code (NEC) • National Electrical Manufacturers Association (NEMA) • National Fire Protection Association (NFPA) • Occupational Safety and Health Administration (OSHA) • Underwriter Laboratory (UL) • Equivalencies to international codes and standards

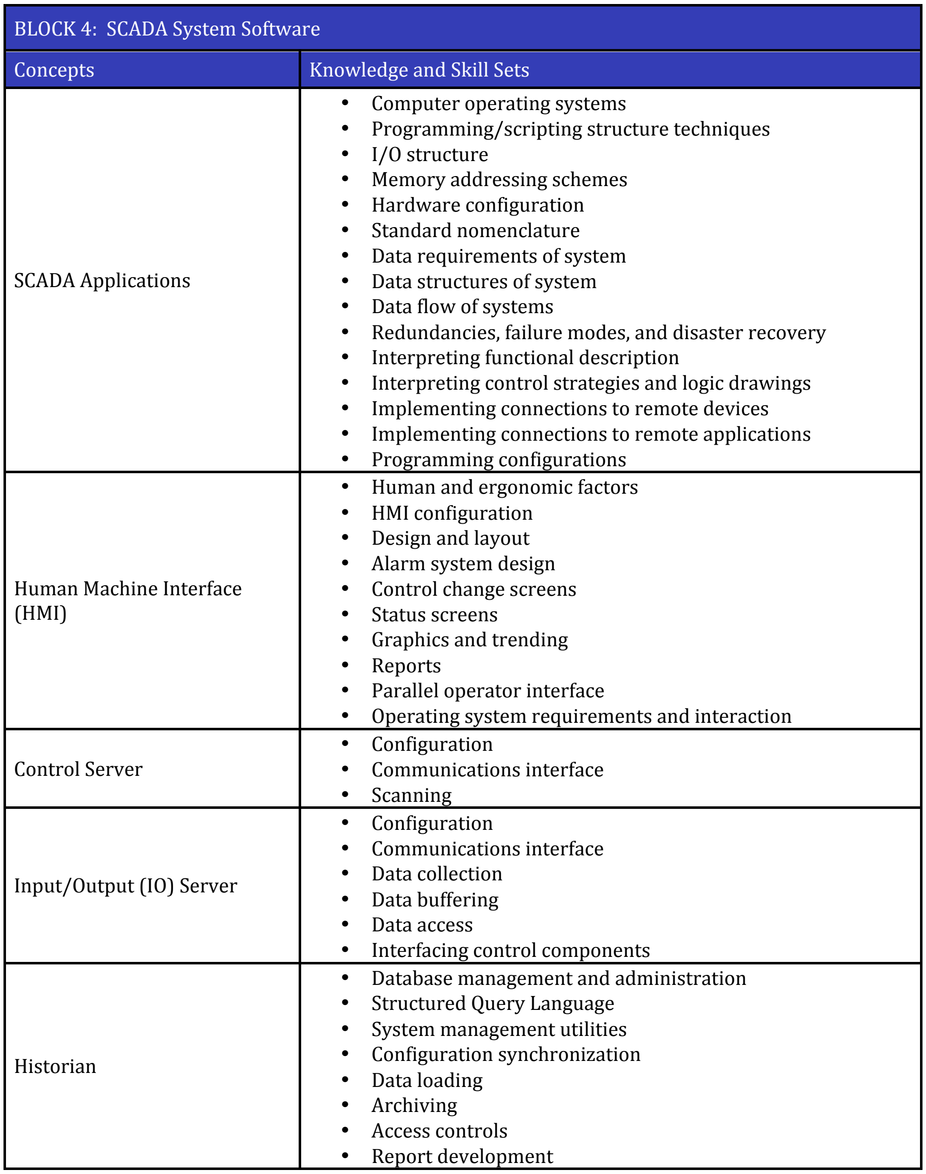
CORE 1: SCADA SYSTEM PRINCIPLES

BLOCK 2: Physical Systems and Instrumentation	
Concepts	Knowledge and Skill Sets
Sensor Technology	• Sensor characteristics • Sensor technologies applicable to desired measurement • Analog and digital input/output • Calculations involved in sensor technologies
Pressure Relieving Devices	• Types • Characteristics • Functionality • Calculations • Rupture discs
Control Valves	• Types • Characteristics • Functionality • Calculation • Applications of fluid dynamics • Accessories • Environmental constraints
Motor Driven Control Elements	• Types of motors • Types of motor controllers or drives • Drive and motor characteristics • Functionality

CORE 1: SCADA SYSTEM PRINCIPLES

BLOCK 3: Field Devices	
Concepts	Knowledge and Skill Sets
Devices	• Remote terminal units • Programmable logic controllers • IEDs • Characteristics
Architecture	• Hardware layer • Firmware layer • Programming layer • Communications interface • Discrete control and monitoring • Analog control and monitoring • Pulse control and monitoring • Serial control and monitoring
Programming	• Methods of representing logic, Boolean algebra, instruction code and graphical presentation • Comparison of different manufacturers, memory, data representation and instruction code • Using ladder logic o Rules o Comparison of relay ladder diagrams o Scan concept o Infinite fan-out o Contact normal states o Positive and negative logic o Basic Boolean functions o Usefulness of DeMorgan's Law • Using registers (words) o Number systems o Timers o Types of register data o Counters o Bit shift and rotate o Table functions o Register (Matrix) logic functions
Management Software	• Comparison of different manufacturers • Version control • Device updates and patching • Digital signatures for firmware

CORE 1: SCADA SYSTEM PRINCIPLES



BLOCK 4: SCADA System Software	
Concepts	Knowledge and Skill Sets
SCADA Applications	• Computer operating systems • Programming/scripting structure techniques • I/O structure • Memory addressing schemes • Hardware configuration • Standard nomenclature • Data requirements of system • Data structures of system • Data flow of systems • Redundancies, failure modes, and disaster recovery • Interpreting functional description • Interpreting control strategies and logic drawings • Implementing connections to remote devices • Implementing connections to remote applications • Programming configurations
Human Machine Interface (HMI)	• Human and ergonomic factors • HMI configuration • Design and layout • Alarm system design • Control change screens • Status screens • Graphics and trending • Reports • Parallel operator interface • Operating system requirements and interaction
Control Server	• Configuration • Communications interface • Scanning
Input/Output (IO) Server	• Configuration • Communications interface • Data collection • Data buffering • Data access • Interfacing control components
Historian	• Database management and administration • Structured Query Language • System management utilities • Configuration synchronization • Data loading • Archiving • Access controls • Report development

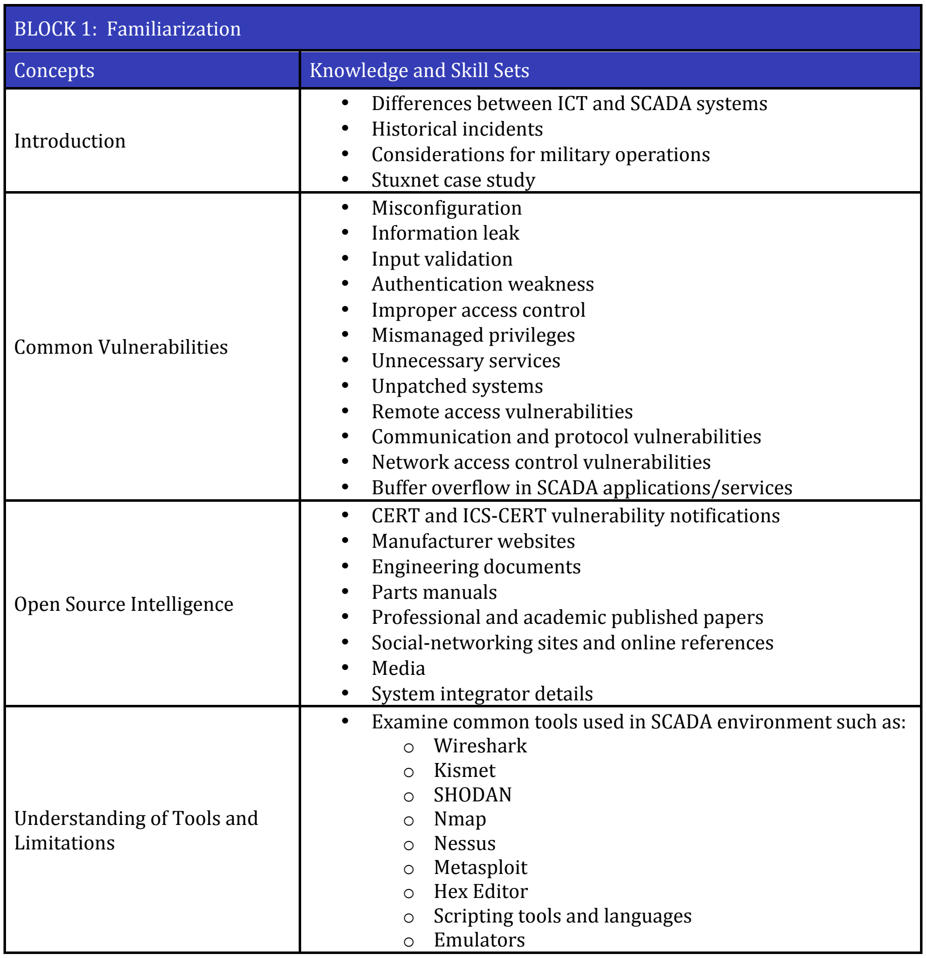
CORE 1: SCADA SYSTEM PRINCIPLES

BLOCK 5: Communications	
Concepts	Knowledge and Skill Sets
Topology	• Types • Physical topology rules and limitations • Design decisions • Analog to digital conversion • Long distance communication • Communications system components • Synchronous and asynchronous communications
Protocols	• Messaging protocol fundamentals • RS-232 and RS-485 interface standards • Common SCADA protocol specifications o Modbus, DNP3, Fieldbus, CIP, HART, Profibus, etc. • Protocol analysis • Packet inspection
Medium	• Radio Frequency o Simplex and duplex o Turn-on time o Frequencies o Path studies and seasonal variations o Solar variations o Reliability and maintenance o Spread-spectrum o Wi-Fi o Satellite communications o Cell phones • Background to cables • Noise and interference on cables • Twisted pair cables and fiber optic cables • Wide Area Network o Digital hierarchies o T1 and E1 o Packet switching o Frame relay o ATM o SDH/sonnet • Local Area Network o Ethernet networks o Industrial Ethernet o TCP/IP o LAN connectivity: bridges, routers, and switches o Redundancy options o Web based industrial SCADA o OPC • Public network provided services • Modems • Secure communications

CORE 1: SCADA SYSTEM PRINCIPLES

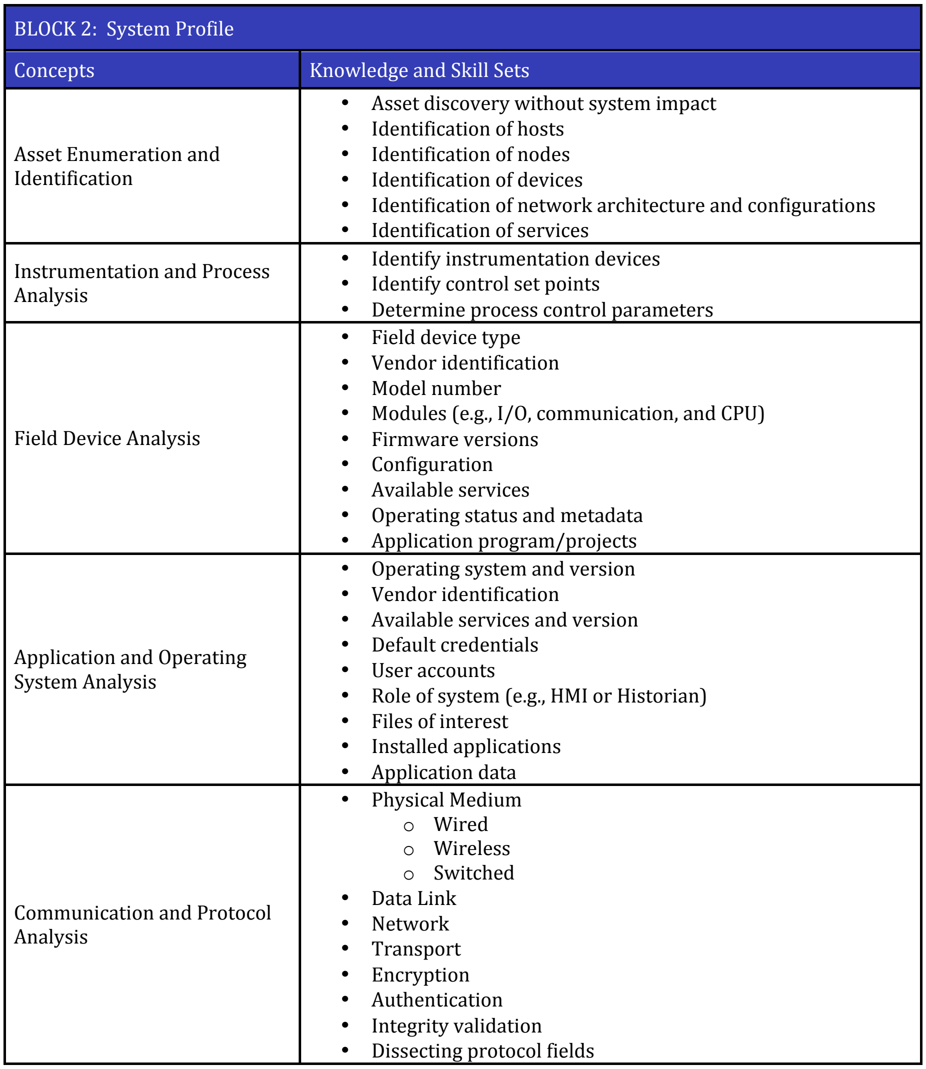
BLOCK 6: Advanced Control	
Concepts	Knowledge and Skill Sets
Logic	• Concept of reusable logic • Drive logic and alarm handling • Use of advanced programming functions • Matrix logic • Table functions and indirect addressing
Bath Processes and Sequential Control	• Remembering the program state • Creating a 'stepper' • Step advance • Fault detection and recovery • Operator intervention • Multiple recipes or alternative paths • Sequential function charts
PID Control	• Timing and scan time • Intermittent measurements • Long transport delays
Safety Systems	• Physical safety devices • Programmable electronic logic solvers • Safety certification • Certified programming systems • Application examples • Networked safety devices and certified networks • Integrated safety systems

CORE 2: CYBER MANIPULATION



BLOCK 1: Familiarization	
Concepts	Knowledge and Skill Sets
Introduction	• Differences between ICT and SCADA systems • Historical incidents • Considerations for military operations • Stuxnet case study
Common Vulnerabilities	• Misconfiguration • Information leak • Input validation • Authentication weakness • Improper access control • Mismanaged privileges • Unnecessary services • Unpatched systems • Remote access vulnerabilities • Communication and protocol vulnerabilities • Network access control vulnerabilities • Buffer overflow in SCADA applications/services
Open Source Intelligence	• CERT and ICS-CERT vulnerability notifications • Manufacturer websites • Engineering documents • Parts manuals • Professional and academic published papers • Social-networking sites and online references • Media • System integrator details
Understanding of Tools and Limitations	• Examine common tools used in SCADA environment such as: ○ Wireshark ○ Kismet ○ SHODAN ○ Nmap ○ Nessus ○ Metasploit ○ Hex Editor ○ Scripting tools and languages ○ Emulators

CORE 2: CYBER MANIPULATION



BLOCK 2: System Profile	
Concepts	Knowledge and Skill Sets
Asset Enumeration and Identification	• Asset discovery without system impact • Identification of hosts • Identification of nodes • Identification of devices • Identification of network architecture and configurations • Identification of services
Instrumentation and Process Analysis	• Identify instrumentation devices • Identify control set points • Determine process control parameters
Field Device Analysis	• Field device type • Vendor identification • Model number • Modules (e.g., I/O, communication, and CPU) • Firmware versions • Configuration • Available services • Operating status and metadata • Application program/projects
Application and Operating System Analysis	• Operating system and version • Vendor identification • Available services and version • Default credentials • User accounts • Role of system (e.g., HMI or Historian) • Files of interest • Installed applications • Application data
Communication and Protocol Analysis	• Physical Medium ○ Wired ○ Wireless ○ Switched • Data Link • Network • Transport • Encryption • Authentication • Integrity validation • Dissecting protocol fields

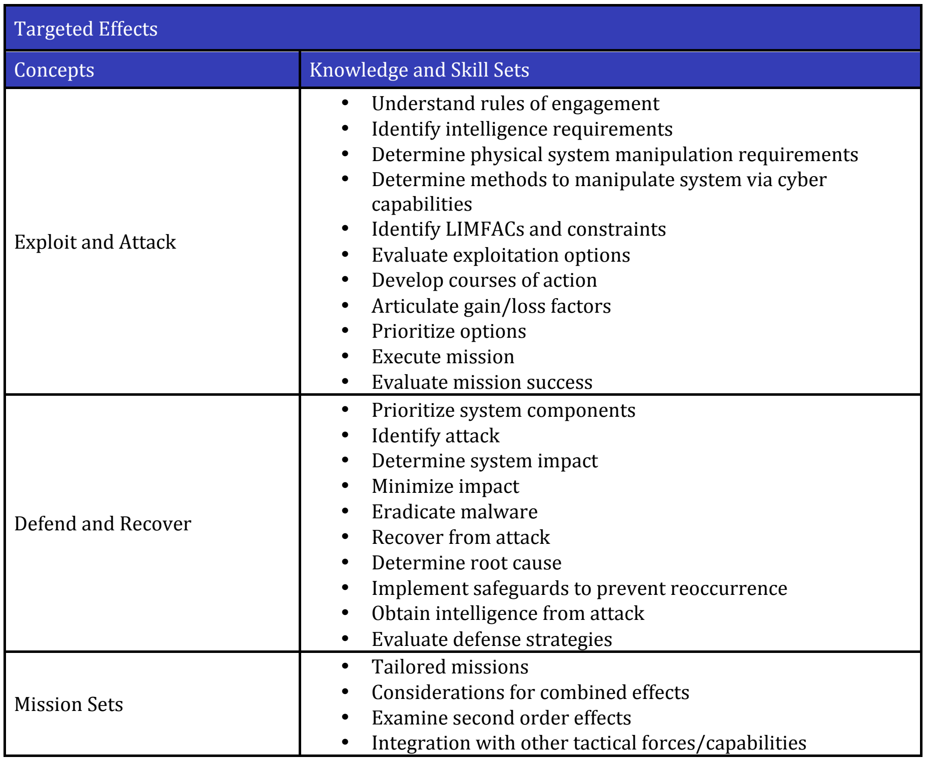
CORE 2: CYBER MANIPULATION

BLOCK 3: Vulnerability Analysis and Exploitation	
Concepts	Knowledge and Skill Sets
Access Vectors	• Communications Medium • End-User • Credentials • Public Certs • Exposed Connections • Supply Chain Compromise
Vulnerabilities	• Identify existing vulnerabilities o Operating Systems o HMIs and User Interfaces o Control Servers and Applications o Field Devices Vulnerabilities o Networking Equipment o Communications Medium and Protocols o Security Systems • Evaluate for new vulnerabilities o Fuzzing Techniques o Protocol Analysis o Application Analysis o End-User Analysis
Gaining Access	• Determine Required Access • Exploit Trust Relationships • Exploit Code Vulnerabilities • Elevating Privileges • Pivoting
Attack Types	• Payload Analysis o Persistent and Non-Persistent o Timing Considerations • Create Desired Effects o Confidentiality o Integrity o Availability • Coordinated Effects
Attack Execution	• Installing Malware • Attack Triggers • Manipulating Physical Processes • Covering Tracks • Assessing Impacts and Success

CORE 2: CYBER MANIPULATION

BLOCK 4: Defending Against Attacks and Recovery	
Concepts	Knowledge and Skill Sets
Traditional ICT Security in the SCADA Environment	• Data Classification • Access Controls • Network Architecture • Cryptography • ICT Security Devices
Defending SCADA Subcomponents	• Defending SCADA Servers and Workstations o SCADA Servers and Workstation Technologies o System and Security Updates o Enforcing Security Policy o System Processes and Services o Logs and Log Management o Databases and Historians • Defending SCADA Networks and Devices o Communication Medium o Controlling Access o Field Devices
Evaluation	• Vulnerability Assessments • Security Architecture and Design • Incident Response Plans • Minimizing Attack Surfaces
Identifying Cyber Attacks	• Identifying Cyber Attacks • Determining Extent of Compromise • Evaluating System Impact • Factoring Potential Implications
Recovery	• System Prioritization • Minimizing Effects to Physical Processes • Containing Malware • Forensics and Eradication

CORE 3: TARGETED EFFECTS



Targeted Effects	
Concepts	Knowledge and Skill Sets
Exploit and Attack	• Understand rules of engagement • Identify intelligence requirements • Determine physical system manipulation requirements • Determine methods to manipulate system via cyber capabilities • Identify LIMFACs and constraints • Evaluate exploitation options • Develop courses of action • Articulate gain/loss factors • Prioritize options • Execute mission • Evaluate mission success
Defend and Recover	• Prioritize system components • Identify attack • Determine system impact • Minimize impact • Eradicate malware • Recover from attack • Determine root cause • Implement safeguards to prevent reoccurrence • Obtain intelligence from attack • Evaluate defense strategies
Mission Sets	• Tailored missions • Considerations for combined effects • Examine second order effects • Integration with other tactical forces/capabilities

Appendix D: Acronyms

COA	Course of Action
DCO	Defensive Cyber Operations
DMZ	Demilitarized Zone
DoD	Department of Defense
DoDIN Ops	DoD Information Network Operations
DOTMLPF	Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, and Facilities
HMI	Human-Machine Interface
ICT	Information and Communications Technology
IED	Intelligent Electronic Device
IO Server	Input/Output Server
JCIDS	Joint Capabilities Integration and Development System
JIIM	Joint, Interagency, Intergovernmental, Multinational
MISO	Military Information Support Operations
MUTC	Muscatatuck Urban Training Center
OCO	Offensive Cyber Operations
PDA	Personal Digital Assistant
PLC	Programmable Logic Controller
PTE	Persistent Training Environment
RF	Radio Frequency
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
TECO	Tactical Environment Cyber Operations
TTPs	Tactics, Techniques, and Procedures

Appendix E: References

[1] United States Department of Defense, Joint Publications 3-12, Cyberspace Operations, February 5, 2014.

[2] United States Department of Defense, Quadrennial Defense Review, 2014.

[3] A. Metcalf and C. Barber, Tactical Cyber: How to Move Forward, Small Wars Journal, September 14, 2014.

[4] United States Department of Defense, Joint Publications 1, Doctrine for the Armed Forces of the United States of America, March 25, 2013.

[5] United States Department of Defense, Instruction 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks, November 5, 2012.

[6] National Science Foundation, NSF 14-542, Cyber-Physical Systems, (http://www.nsf.gov/pubs/2014/nsf14542/nsf14542.htm), 2014.

[7] North Atlantic Treaty Organization, Joint Intelligence, Surveillance and Reconnaissance (http://www.nato.int/cps/en/natolive/topics_111830.htm), October 20, 2014.

[8] United States Department of Defense, Joint Publication 3-05, Special Operations, July 16,2014.

[9] United States Department of Defense, Joint Publication 3-13.2, Military Information Support Operations, December 20, 2011.

[10] United States Department of Defense, Joint Publication 3-13, Information Operations, November 20, 2014.

[11] United States Department of Defense, Joint Publication 6-01, Joint Electromagnetic Spectrum Management Operations, March 20, 2012.

[12] United States Department of Defense, Instruction 3000.05, Stability Operations, September 16, 2009.

[13] G. Rattray and J. Healey, Categorizing and Understanding Offensive Cyber Capabilities and Their Use, Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy, 2010.

[14] S. Tucker, Persian Gulf War Encyclopedia: A Political, Social, and Military History, ABC-CLIO, 2014.

[15] T. Morris and W. Gao, Industrial Control System Traffic Data Sets for Intrusion Detection Research, J. Butts and S. Shenoi (eds.), Proceedings of the 8th International Conference on Critical Infrastructure Protection, March 2013.

[16] M. Naedele, Addressing IT Security for Critical Control Systems, Proceedings of the 40th Hawaii International Conference on System Sciences, January 2007.

[17] United States Department of Defense, DoD News, Cyber Flag Exercise Tests Mission Skills (http://www.defense.gov/news/newsarticle.aspx?id=123621), November 12, 2014.

[18] United States Department of Defense, DoD News, Cyber Guard Exercise Tests People, Partnerships (http://www.defense.gov/news/newsarticle.aspx?id=122696), July 17, 2014.

[19] K. Green and K. Key, Cyber Warriors Flex Digital Muscle at 2014 Cyber Shield Exercise (http://www.nationalguard.mil/News/ArticleView/tabid/5563/Article/8972/cyber-warriors-flex-digital-muscle-at-2014-cyber-shield-exercise.aspx), National Guard, May 20, 2014.

[20] J. Carr, Cyber: The New Red Flag Battleground (http://www.af.mil/News/ArticleDisplay/tabid/223/Article/503204/cyber-the-new-red-flag-battleground.aspx), United States Air Force, October 2, 2014.

[21] Atterbury-Muscatatuck Urban Training Center, MUTC Overview (https://www.atterburymuscatatuck.in.ng.mil/Ranges/MuscatatuckUrbanTrainingCenter/MUTCOverview.aspx), 2014.

[22] K. Stouffer, J. Falco and K. Scarfone, Special Publication 800-82, Guide to Industrial Control System Security, National Institute of Standards and Technology, June 2011.

[23] A. Matrosov, E. Rodionov, D. Harley and J. Malcho, Stuxnet Under the Microscope, Revision 1.31, ESET, 2011.

[24] G. Keizer, Is Stuxnet the Best Malware Ever?, Computerworld, September 16, 2010.