JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

11100 Johns Hopkins Road • Laurel, Maryland 20723-6099

AOS-16-0917

August 2016

CONTROL SYSTEM (CS) / PLATFORM INFORMATION TECHNOLOGY (PIT) WORKFORCE DEVELOPMENT FINAL REPORT

Prepared for:

ENERGY, INSTALLATIONS AND ENVIRONMENT

Office of the Assistant Secretary of Defense for Energy, Installations, and Environment

Prepared by:
The Johns Hopkins University Applied Physics Laboratory
Julie L. Marble, PhD
Willie Stewart

Task No.:	CI103XXX
Contract No.:	N00024-13-D-6400

This Page Intentionally Left Blank

CONTENTS

Page

Figures v

Tables v

1. Introduction 1

2. Method 2
   - 2.1 Facilities Visited 2
   - 2.2 Representative Processes, Activities, and Outcomes for Vulnerability Assessment 3
   - 2.3 Facility Operation Roles 4
   - 2.4 Training Assessment and Competencies Derivation 6
   - 2.5 Qualitative Analysis of Observations 7
   - 2.6 Development of What If Scenarios 7
   - 2.7 Assumptions 7

3. Human Error Classification and Assessment 8
   - 3.1 Classifying Error 8
   - 3.2 Other Considerations in Assessment of Human Error in Cybersystems 9

4. Human Factors Analysis and Classification System 10
   - 4.1 Applying HFACS to Workforce Cyber 10
     - 4.1.1 HFACS First Order Effect – Organizational Influences (Organizational Level) 11
     - 4.1.2 HFACS First Order Effect Supervision (Supervisory Level) 13
     - 4.1.3 HFACS First Order Effect Preconditions for Unsafe Acts (Operational Effects) 15
     - 4.1.4 HFACS Outcomes: Unsafe Acts 17

5. Findings 18
   - 5.1 Vulnerabilities Derived from Site Visits 18
   - 5.2 Analysis 18
     - 5.2.1 Quartile Analysis 19
     - 5.2.2 Assessing Vulnerabilities within HFACS 21
   - 5.3 Competencies, Skills, and Education for Facility Roles 32
     - 5.3.1 ICS and Cybersecurity Competencies 32
     - 5.3.2 Gaps in Competencies 37
   - 5.4 Assessment of Training Materials 41
     - 5.4.1 Training Derived from Government Sources 41

5.4.2 Training Provided by Industrial and Commercial Entities 42

6. 'What If' Scenario Examples 45

7. Mitigating Cyber Workforce Vulnerabilities 51
7.1 Organizational Cyber Awareness 51
7.2 Improving the Technological Environment 52
7.3 Integrating Cybersecurity and Operations 53
7.4 Recommendations 54
7.4.1 Cost Benefits 55

8. Acronyms / Abbreviations 56

9. References 58

APPENDIX A. Training List for Facility Managers and Facility Engineers A-1

APPENDIX B. Competencies by Vulnerabilities by Roles B-1

FIGURES

Page

Figure 1. Facility Internal Mission Areas 4
Figure 2. Reason's Taxonomy of Error 9
Figure 3. Organizational Levels 1, 2, and 3 13
Figure 4. Supervisory Levels 1, 2, and 3 15
Figure 5. Operational Levels 1, 2, and 3 17
Figure 6. Quartile 1 Error Precursors 19
Figure 7. Quartile 2 Error Precursors 20
Figure 8. Quartile 3 Error Precursors 20
Figure 9. Quartile 4 Error Precursors 21
Figure 10. HFACS Cyber Level 1 Vulnerabilities 22
Figure 11. HFACS Cyber Level 2 Effects (key: Green – Organizational, Red – Supervisory, Dark Blue – Operational, Light Blue – Positive observations) 23
Figure 12. Level 2 Organizational Cyber Awareness Level 3 26
Figure 13. Operational Level 2 Effects 29
Figure 14. Technological Environment Error Precursors 29
Figure 15. Competencies and Available Training 36
Figure 16. Competencies, Training, and Vulnerabilities 37

TABLES

Table 1. EI&E Processes, Activities, and Outcomes for Roles Interviewed 5
Table 2. Observations of Technological Environment and Un-integrated Systems 25
Table 3. Example Organizational Cyber Awareness Vulnerabilities 26
Table 4. Example Observations of Technology Vulnerable to External Influence 30
Table 5. Example Vulnerabilities, Competencies and Related Training Available for Facility Operation Roles 34
Table 6. Competency Gaps 38
Table 7. What if Scenario 1 46
Table 8. What If Scenario 2 47
Table 9. What If Scenario 3 49
Table 10. Base Access by Unauthorized Personnel 50

1. INTRODUCTION

Cyber threats to Control Systems (CS) and Platform Information Technology (PIT) will not occur solely through Internet connections. CS/PIT include supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control systems such as the Programmable Logic Controllers (PLCs) often found in the industrial sector and critical infrastructures. CS/PIT are often installed piecemeal using commercial off-the-shelf components or subsystems, which may be installed by different contractors using equipment from different manufacturers. CS/PIT may be a loosely connected system of systems, typically consisting of a multi-facility front end, an installation-wide Internet Protocol (IP) network, and multiple subsystems. Malicious actors wishing to gain access to these facilities may realize that not all CS/PIT connect to external data connections. Therefore, to access the controls of these types of facilities, malicious actors may need to gain physical access to the facility, or socially engineer a response from inside the facility. Facility managers and operators are trained in their fields but are not trained in securing systems from cyber threats or differentiating normal events from events related to cyberattacks or facility phishing events. They may not be aware that actions taken to achieve their work-related goals may create cyber vulnerabilities that can be leveraged by an adversary. Facility management personnel have multiple roles within a facility that do not primarily focus on prevention or detection of cyber threats to the facility. In addition, protection against cyberattacks is seen as the goal of the information technology (IT) specialists, independent from facility management. To ensure facility security, it is necessary to integrate cybersecurity awareness into facility management roles.

Beyond the roles and responsibilities fulfilled by technical personnel dedicated full-time to cybersecurity and other IT-related activities, there is an increasing need for recognition and understanding among facility management staff of potential degradation or interruption of building operations caused by cyberattacks on buildings and energy delivery system CS/PIT. Fuel storage and distribution systems, fixed and tactical microgrids, physical access control systems, building control systems such as HVAC, lighting, and vertical transport controllers, and life safety systems such as fire alert and suppression systems are examples of building CS/PIT that are vulnerable to attacks that impact mission and the operability, reliability, and safety of the Department of Defense (DoD) facilities. It is shortsighted to assume that all cyber-based vulnerabilities to DoD facilities will be handled entirely through staff dedicated to cybersecurity; rather IT security and cyber awareness should be integrated throughout facility management. Traditional Military Site management roles must expand to include the capability to recognize and deal with such threats, and remain prepared to mitigate any impacts. Additionally, an understanding of what information the traditional IT professionals know regarding connecting and protecting CS/PIT is required to prescribe the proper balance among Military Site management and IT professionals in securing those systems.

Other industries centered around complex critical systems, such as aviation and nuclear power, have recognized the critical role in system safety of roles of facility management staff [i.e., facility managers (FMs) and facility engineers (FEs), safety managers (SaMs) and security managers (SeMs), facility energy managers (FEMs), and logistics managers (LOG)] on potential degradation or interruption of plant operations. The concept of Human Reliability Analysis

(HRA) reflects an understanding that people and systems are not error-proof, and that improved reliability and increase system resilience requires an understanding of error problems, leading to improved mitigation strategies.

The Office of the Assistant Secretary of Defense for Energy Installations & Environment [OASD(EI&E)] tasked the Johns Hopkins University Applied Physics Laboratory (JHU/APL) to assess the potential for cyber vulnerabilities to be caused by or potentially prevented by facility management personnel at DoD facilities. The purpose of this project was to identify vulnerabilities in facility cyber operations and the associated competencies, training, and changes to the workforce that could be added to the DoD's traditional FM/FE/SaM/SeM/FEM/LOG management staff to improve cybersecurity and situation awareness in facility management and to identify cost effective techniques to mitigate cyber vulnerabilities in facility operations.

2. METHOD

The objective of this task was to assess cyber vulnerabilities centered on facility operations, building automation systems, and workforce cyber training and competencies and recommend mitigations to improve facility cyber security. The method used to conduct research on DoD facility CS/PIT vulnerabilities focused on the Workforce consisted of the following steps:

- Selection of facilities visited
- Selection of representative processes, activities, and outcomes (PAOs) for vulnerability assessment
- Selection and observation of facility operation roles
- Qualitative analysis of observations
- Training assessment and competencies derivation as a function of observed vulnerabilities
- Identification and prioritization of recommended management processes and gaps, and the development of mitigation strategies
- Development of 'what if' scenarios for training

2.1 Facilities Visited

JHU/APL worked with OASD(EI&E) to select a representative set of facilities at which to perform interviews and observations of a variety of facility management roles and processes, activities, and outcomes. The sites selected were chosen based on proximity to the Washington, DC, area; visiting a variety of facility types supporting different mission areas; and their use of Internet Protocol (IP) systems such as building automation systems.

The following sites were visited:

- Defense Fuel Supply Point, Craney Island, Virginia
- Fort Belvoir, Virginia
- Mark Center, Arlington, Virginia

- Fort Detrick, Frederick, Maryland

In addition, relevant facilities at the JHU/APL campus in Laurel, Maryland, were visited. Information relevant to workforce analysis was also obtained from the Defense Supply Center in Columbus, Ohio, and Patrick Air Force Base, Florida.

2.2 Representative Processes, Activities, and Outcomes for Vulnerability Assessment

Based on the PAOs available at the facilities visited, JHU/APL identified a set of representative PAOs to recognize and respond to CS/PIT cyberthreats that covered both non-crossover of information, planning, and roles between DoD and non-DoD personnel, and crossover activities, in which responsibility for completion of an activity is transferred between DoD and non-DoD personnel. Based on the observation of these PAOs, JHU/APL identified a set of workforce centric cyber vulnerabilities with respect to organizational, supervisory, or operational source of the vulnerability.

JHU/APL categorized the possible PAOs for all facilities into seven Facility Mission Areas, as shown in Figure 1. The PAOs used for the analysis included management and control of, access to, and maintenance of operational energy, vehicle operations, environmental monitoring, utility services, and health and safety systems such as fire alert and suppression, Real Property Support and IT services. To the extent possible, facility personnel from the relevant facility mission area were interviewed and their interactions and knowledge of their cybersystems was assessed. Initial plans were to assess vulnerabilities based on near miss events and procedures for operations at these locations were proposed. While facility management staff was very helpful during this assessment, these sources of data were not available for assessment.

Figure 1. Facility Internal Mission Areas

2.3 Facility Operation Roles

Personnel in the roles assigned to the PAOs of interest at each facility visited were interviewed with respect to their knowledge of the cyber connections within their systems, their experience with cybersecurity, and whether that experience varied between DoD and non-DoD personnel. JHU/APL was especially interested in procedures and processes for sharing information between DoD and non-DoD personnel during off-normal events and identification of communication pathways for off-normal events, including other roles contacted, how contact is initiated, whether and how follow up is ensured after contact or off-boarding of responsibility for an action or task.

JHU/APL interviewed personnel in similar roles across facilities to awareness of vulnerabilities to cyber-based threats at each facility. Personnel were interviewed about the cybersecurity training they received for the systems with which they interacted, and observed (to the extent possible) interacting with these systems. These observations and interviews were used to drive a comparison of experience and training levels of performers in similar roles but with different backgrounds. These interviews covered both facility management staff and traditional IT professionals. Personnel and roles selected considered those technologies that could be influenced by outside cyber manipulations, and those PAOs that could allow physical access to the facility.

Table 1 presents the EI&E focused facility PAOs and personnel roles interviewed. To the extent possible, JHU/APL interviewed personnel at multiple levels of management within each PAO (e.g., supervisors, operators, facility workers). Due to the security needs of the facilities, it was not possible to job shadow personnel at facilities. However, personnel were interviewed in their work areas whenever possible. JHU/APL personnel were typically able to view the systems used to perform tasks and complete internal facility PAOs. The focus of the interviews and observations was to assess how personnel interacted with all systems in performance of their jobs in order to identify human-cyber system vulnerabilities in the processes and activities performed. Focusing on vulnerabilities helped identify needed competencies and gaps in competencies for varying PAOs or differing facility operations roles.

Table 1. EI&E Processes, Activities, and Outcomes for Roles Interviewed

GSA – Building Act Defined Role	Roles	PAOs	Facility Personnel Interviewed
Facility Management	FMs	Provide operational vehicles	Not available
	Safety personnel	Health & safety	Fire Chief Fire Marshall Emergency dispatch personnel Police SaMs
Operations and Maintenance	FEs	Utility services environmental monitoring	Public Works and Water & Sewage Treatment plant personnel Fuel handling engineers Public works water contractor personnel Medical waste incineration plant personnel
	Logistics personnel	IT services Utility services	Emergency dispatch personnel Navy Shore Operations Center personnel IT services personnel Computer intrusion detection staff SCADA system engineers and operators (water & electric)
	Security personnel	Physical security	Police Physical security Security engineer SaMs
Energy Management	Energy personnel	Provide operational energy	Automation and Energy personnel Master planner Facilities and energy SCADA system engineers and operators (electrical)

With respect to cyber security, JHU/APL was interested in determining whether personnel had accurate mental models of system interconnections and vulnerabilities. All systems were the focus of interview questions, not just standard computer systems or business systems. JHU/APL asked personnel about communication platforms, WiFi-enabled systems in the work environment, and use of personal electronic devices. Personnel were asked how their systems connected to one another as well as to the Internet. To the extent possible, personnel were asked to demonstrate the systems and asked how the systems interconnected or connected to the Internet. During the interviews, JHU/APL inquired whether there were procedures and protocols for use of personal devices or using personal electronic devices. Early in the assessment, JHU/APL determined that procedures to ensure cybersecurity within CS/PIT systems were rare.

2.4 Training Assessment and Competencies Derivation

JHU/APL initially proposed to perform a quantitative human reliability analysis (HRA) on workforce operations with operational technology systems. HRA techniques are based on the ability to perform a step by step breakdown of a given task, then calculate the probability of human error at each step as a function of the performance environment. The performance environment includes consideration of the sufficiency of information provided from the human-machine interface (HMI), the workload of the performer, support for the task from supervisory roles such as through the provision of procedures for complex tasks, and organizational support such as emphasis on safety over mission in communications. Procedures for operations were not common at the facilities identified. Therefore, a quantitative HRA technique could not be used. Instead, a qualitative human error classification system was modified from other literature to provide insight into the Organizational, Supervisory, and Operational influences on workforce performance and cyber vulnerabilities. While this technique allows insight into the causes of workforce vulnerabilities, given the lack of procedures it was not possible to definitively analyze observations of vulnerabilities as a function of role or PAO. Rather, vulnerabilities were assessed as a function of whether they would be best mitigated at the Organizational, Supervisory, or Operational Levels.

JHU/APL initially proposed to review available training materials for the PAOs and roles identified in the previous tasks. During the site visits, training materials, procedures, and processes for cybersecurity and cybersystems were requested. Materials obtained were typically usage and user manuals, which had limited information on maintaining cybersecurity of the systems, and little or no information about the process within which the system itself was used. Training for cybersecurity primarily referred to basic cybersecurity training common to all Government facilities, such as the Defense Information Systems Agency (DISA) provided Cyber Awareness Challenge, which focuses on cybersecurity for office and business systems. (See Appendix A for an example list of cybersecurity training provided by one facility.) Based on this lack of information, JHU/APL, with sponsor approval, identified and assessed alternate sources for training, and relevance of available training to facility management needs. These sources were also used to identify needed cybersecurity and facility operations competencies across the roles of interest.

2.5 Qualitative Analysis of Observations

JHUAPL identified and modified the Human Factors Aviation Classification Systems (HFACS) for organization and analysis of the vulnerabilities identified during the site visits. A discussion of HFACS assumptions is provided in Section 3, which also describes the definitions used during this analysis. The use of HFACS allowed identification of common causes of a diverse set of observed vulnerabilities independent from the PAOs, facilities, or workforce roles involved.

2.6 Development of What If Scenarios

Based on the observations from the facility visits and interviews, as set of 'what if' scenarios was developed which could be used to test facility managers' understanding of the interaction between systems and indicators of vulnerabilities, and how these systems could be manipulated externally through cyber channels. These what if scenarios are based on the most common vulnerabilities observed across facilities for PAOs. The purpose of the 'what if' scenarios is to allow consideration of the interaction between a set of real world vulnerabilities.

2.7 Assumptions

The intent of this work was to assess human sources of cyber vulnerability in processes used by facility management personnel. JHU/APL hypothesized that within cybersystems, vulnerabilities can arise from five sources:

1. Malicious entity introduced through removable media
2. Co-opted insider threat
3. Unwitting insider threat
4. Malicious entity introduced through supply chain
5. Unknown system or software flaw exploited through connected network

For the purpose of this task, JHU/APL did not explicitly consider Co-opted insider threats. Insider threats were not directly considered because the actions taken to reduce vulnerabilities within the network relevant to facility personnel (such as training, cybersecurity tools, or provision of information about the network) could be used by a malicious insider to best determine where to affect the system. Further, increased Organizational Cyber Awareness, which we will discuss later, should reduce the possibility of a malicious insider being able to take action on the system because of increased awareness by co-workers.

In the remaining cases, cyber vulnerabilities identified in this report are caused, essentially, by human error, as they are the unintended consequence of action or failures to take actions by facility management personnel.

3. HUMAN ERROR CLASSIFICATION AND ASSESSMENT

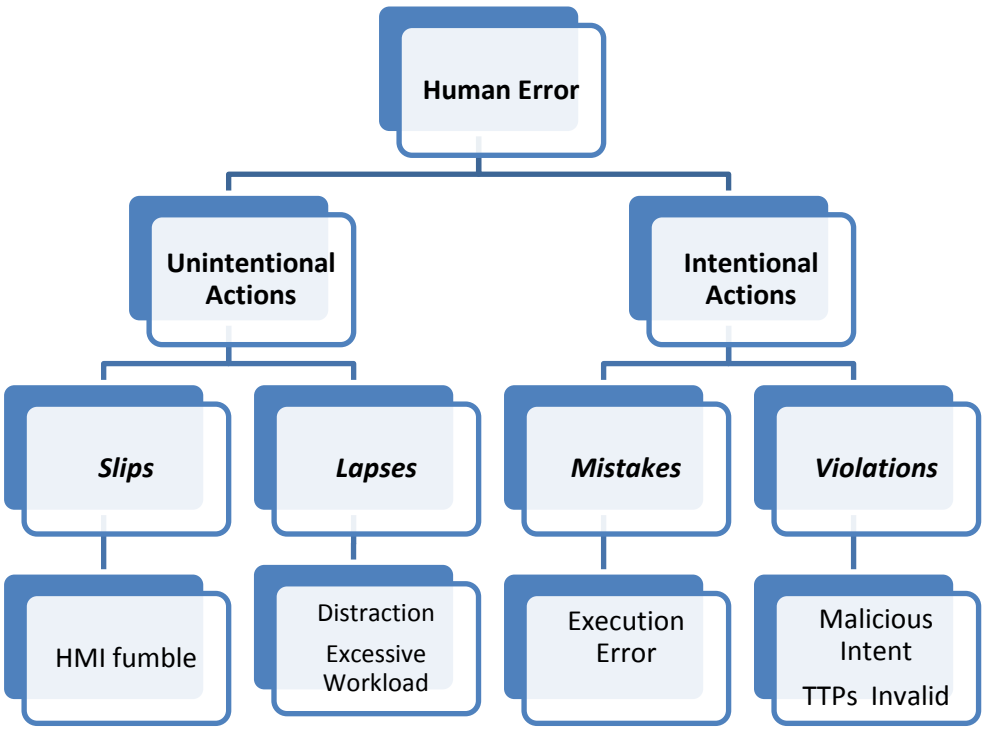
Cyber vulnerabilities with operational technology and building automation systems arising from workforce actions are a function of human error. With the exception of malicious intent, people do not act with the intent to err. Human error implies a consequence to an action was not intended or desired by the person performing the action or an external observer or that the action pushed the task or system beyond acceptable bounds. Actions where a plan is followed, but the plan itself is flawed, leading to an undesired consequence are called mistakes. In contrast, the plan could be correct, but the execution of the act is flawed leading to the undesired consequence; these errors are called slips or lapses.

3.1 Classifying Error

The most commonly accepted model of human error was proposed by James Reason [1]. Reason hypothesized that most accidents can be traced to one or more of four levels of failure: Organizational influences, unsafe supervision, preconditions for unsafe acts, and the unsafe acts themselves (see Figure 2). Reason made the comparison of the actions an organization takes to prevent errors to a series of barricades, but because of weaknesses (or holes) of varying size in the barricades due to poor implementation or actions of individuals, there would be a potential for an error to slip through. Human errors occurred on "a trajectory of accident opportunity," in which all the vulnerabilities in a task lined up so that an error event slipped through all the defenses, yielding a failure [1].

Models of human error define active failures and latent failures. Active failures are the unsafe acts (error precursors) that can be directly linked to an event, such as such as clicking on a malicious link in an email. Latent failures are defined as factors in the system that may have lain dormant for a long time (days, weeks, or months) until they finally contributed to the accident; these can include excessive workload (which leads to poor decisionmaking) or lack of training (so that the potential of a cyber vulnerability is not known). Latent failures span the first three levels of failure in Reason's model. A third latent failure, organizational influences, are defined as characteristics of the organization that set up the potential for unsafe acts, such encompass such things as reduction in expenditures on training or software tools to save costs.

Classification of human error has been used on many complex, critical systems to identify vulnerabilities and techniques to eliminate those vulnerabilities. These analyses have been done for aviation (including space), nuclear power, and medicine. An example of a latent failure is the design of the e-shifter in 2016 Jeeps (which has been linked to deaths). In this case, the design of the e-shifter obscured whether the car was in park, because the mode was not a function of shifter position. As a result, drivers would manipulate the shifter, believe the car was in park and exit the vehicle – at which point the vehicle would roll because it was actually in reverse or neutral. This failure has be a contributory factor in several vehicle accidents. For cybersystems, an example of a latent failure would be a case where the software updates failed to install because the computer was unavailable when the patch was pushed through the system. The failure to update would yield a vulnerability that was unknown to the system users. Research on human error has led to the realization that errors are the result of flaws within the system rather than a character defect, and that the blame, shame, and retrain mantra does not reduce vulnerabilities.



TTP= Tactics, Techniques and Procedures

Figure 2. Reason's Taxonomy of Error

3.2 Other Considerations in Assessment of Human Error in Cybersystems

Facility management underlies the mission of the facility. In addition to typical business software (email, office computers linked to the Internet), facility management personnel interact with a variety of energy management and building automation systems which are interconnected and may also connect to the Internet. Facility management interactions with cyber-enabled systems are different from typical office or business focused cyber-enabled systems. Failures of control systems within the facilities can have cross cutting impacts on mission performance. In DoD facilities, building automation and facility management may focus on more than just HVAC, water chillers or heater, and fire/safety alarms. The sites visited for this project included fuel supply points, medical waste incineration, closed and classified areas (with somewhat unique security and access needs), or required coordination between multiple buildings.

Most building automation networks consist of a primary and secondary bus, which connect high-level controllers (generally specialized for building automation, but may be generic PLCs with lower-level controllers, input/output devices, and a user interface. Energy management systems (EMS) and building automation systems (BAS) serve two different functions. The EMS allows the users to see all the controls and understand how all components are operating. BAS are control systems that allow modification of set points of various systems. In addition, BAS have alarm capabilities, which can be sent out to computers, cell phones, pagers or other systems. Alarms can immediately be sent if there is a deviation from 'normal' or when alarms build to some threshold. Good BAS are aware of overrides and complex failure conditions. When BAS

are poorly configured, they can send out an alarm for every alert, and may not recognize any manual, fire or electric or fuel safety override. In this case, alarms become ineffective and operators ignore them. In that case, these false alarms become an error precursor, in which a real alarm is dismissed as a false alarm, or a vulnerability that within the cybersystem that a malicious actor could exploit by covering an actual event with a set of false alarms. When poorly architected, or when connections between systems within the network architecture are obscured, control systems represent a vulnerability to business systems when servers are shared, as demonstrated in the hack of Target Corporation [2]. Training, tools, and procedures, as well as support from specialized IT resources, should exist to allow understanding of the complex interactions between OT and IT systems. However, these training, tools, procedures, and specialized resources are few at the current time.

4. HUMAN FACTORS ANALYSIS AND CLASSIFICATION SYSTEM

To serve as a basis for classification of vulnerabilities in cybersystems for facility management, JHU/APL adapted The Human Factors Analysis and Classification System (HFACS) developed by Shappell and Wiegmann (2001) [3], see also [4]. HFACS is a human error framework that was originally used by the U.S. Air Force to investigate and analyze human factors aspects of aviation. HFACS is heavily based upon James Reason's model of human error, discussed previously. The HFACS framework is a tool to assist the investigation of aviation errors and accidents; the focus of HFACS is to target training and prevention efforts to prevent future errors. HFACS is used to identify active and latent failures within an organization that led to an accident. Its purpose is to define the causes that led to an event and provide techniques and tools to defend against future events. HFACS identifies factors that make humans vulnerable to error arising from the individual, supervision, and the organization.

4.1 Applying HFACS to Workforce Cyber

JHU/APL applied HFACS to assist in the identification of vulnerabilities at the sites visited. HFACS, because it was developed for aviation, contained a few assumptions that were violated within the facility environment; most notably, all personnel in aviation environments undergo constant training. The most notable modification of HFACS arose because we were assessing facilities independent from assessment of actual cyber or infiltration events, which meant that information about actual errors was not available; JHU/APL instead assessed for potential causes of errors. Therefore, the Outcomes Level Unsafe Acts category was not applied. However, for clarity in outlining the Human Factors Classification System, it is described below. Because of these differences, the definitions used by HFACS were relaxed or modified as noted in the following sections. In addition, definitions within Levels 2 and 4 were added to reflect organizational workforce acceptance, perception, and understanding of risk. HFACS defines First Order Effects (Organizational, Work Planning, and Contextual Effects), which are then subdivided into Second Order effects. Second Order Effects provide sufficient levels of identification to classify all levels of errors, incidents, and accidents. The Third Order factors provide the greatest utility for error-type preventative measures and trend analysis. The most effective way to define and display the relationship of First, Second, and Third error categories is to examine each First Order Category independently. Following the guidance derived from the applications of HFACS to aviation maintenance systems [5], we have modified the HFACS First

and Second Order Effects, and derived common Third Order effects for classification of cyber vulnerabilities in Facility Management. In application, HFACS is used to allow an analyst to drill down into the actual origins of an event or vulnerability. HFACS defines First Order effects into Organizational Influences, Unsafe Supervisions, and Preconditions for Unsafe Acts, which may independently or in aggregate yield a vulnerability, that is, a Violation or Unsafe Act. First Order Effects are further broken down into Second Order factors that define workable categories for error classification and prevention. Second Order Effects are further broken down to Third Order Effects, to provide sufficient levels of identification to classify all levels of errors, incidents, and accidents. The Third Order factors provide the most utility for error-type preventative measures and database trend analysis.

Modifications to the HFACS architecture were made to adapt to the facility operations environment. These modifications address differences in the two environments. For example, cyber security is a threat environment wherein systems should always be considered vulnerable to attack, while aviation maintenance (especially for commercial airlines) is not. Aviation workforces are highly trained on all the systems they use, and operations are highly dependent on procedures; facility workforce operations are not. Finally, and potentially most critically, resources needed for aviation operations are integrated into their workforce. Facility operations focuses on maintenance and performance of buildings and support systems at the facility; it is funded separately from information technology (IT), and IT security. Consideration of cyber security within these operational technology systems is a new responsibility for facility operations personnel and not all needed resources or organizational structures yet exist for these new missions. The modifications to the definitions, supplied below, focus on the vulnerabilities seen within site visits and observations. While there are potentially many more level 3 error precursors that could be included, only those that were assigned observations are included below.

4.1.1 HFACS First Order Effect – Organizational Influences (Organizational Level)

One advantage to HFACS for categorization of error precursors is its well-defined categorization of Organizational Influences. A premise in the study of human error is that people do not set out on purpose to make mistakes. Rather, factors within the organization and performance environment influence their behavior in negative ways, predisposing them to err. HFACS details the multiple levels of influence of the Organization into three categories. Organizational First Order Effects are used to characterize the organization's processes and resources; regulations; and outside influences (e.g., manufacturers' guidelines, bulletins, procedures, or design issues). Organizational Influence is comprised of the Second Order Effects of Resource Management, Organizational Cyber Awareness, and Operational Processes (see Figure 3). The Second Order Effects are defined below, and their Third Order Effects are listed after each.

- **Resource Management**: Factors arising from priorities in the organization on the allocation, coordination, and maintenance of organizational assets (e.g., human resources, monetary/budget resources, equipment/facility recourse). In this case, we included availability of software, management of patches, and ease of interaction between facility management and IT support. For the purpose of this report, we included organizational factors that increased use of personal electronic devices in the course of job performance.
  - Management of patches/maintain updates
  - Lack of equipment
  - Inappropriate training
  - Insufficient tools for situation awareness
  - Inconsistent procedures
- **Organizational Cyber Awareness**: The working atmosphere within the organization influences performance and operators' decisions. In HFACS, the definition of the original category, Organizational Climate, was expanded to include the factors that reflect communications between groups, divisions, or organizations (e.g., Government and civilian employees). Organizational Cyber Awareness is the value given to and incorporation of cyber hygiene practices at the organizational level to reduce vulnerability, such as accurate understanding and representation of risks. It also includes design of cybersystems to account for human activities and operator actions – from mandating two people in control rooms (to reduce the potential for insider threats) to promoting assessment of risk during task performance. The category emphasizes the idea that the organization must prioritize cyber security and demonstrate a value for cyber security equal to or greater than that of performance of the operational mission. If the organization does not value cyber security at the level of the operational mission then the workforce will sacrifice cyber security in order to get the job done. Vulnerability classifications included:
  - Downplaying risk at the level of the organization
  - Lack of tracking/awareness of cybersystems or use
  - Lack of communication of vulnerabilities between divisions
  - Lack of coordination between IT and other groups
  - Over reliance on physical barriers as a source of cyber security
- **Operational Processes**: Organizational decisions or policies for activities within an organization (can include procedures, oversight).
  - Lack of clear procedures for use of outside equipment
  - Use/adherence to procedures
  - Failure to test procedures

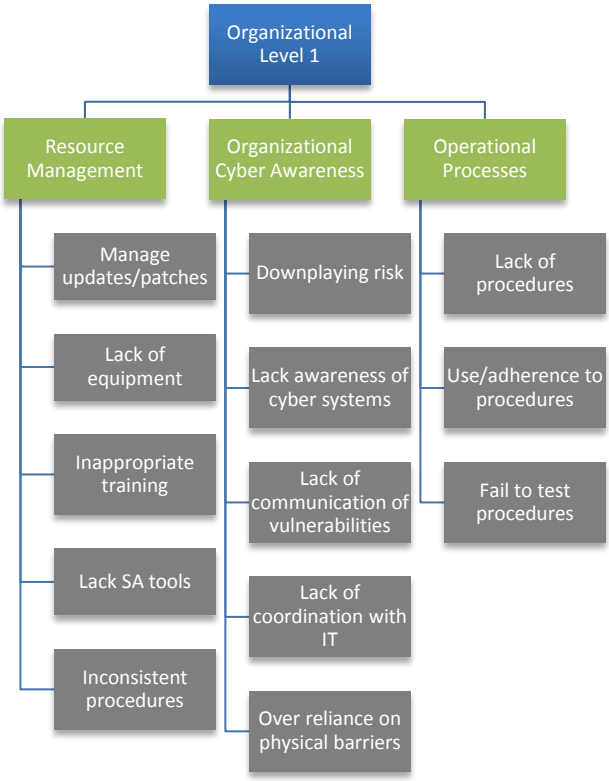


Figure 3. Organizational Levels 1, 2, and 3

4.1.2 HFACS First Order Effect Supervision (Supervisory Level)

In order to integrate cybersecurity awareness into facility workforce activities, the role of supervision will be critical. HFACS divides Unsafe Supervision divided into four Second Order Effects: Inadequate Supervision, Planned Inappropriate Actions, Failure to Correct Known Problem, and Supervisory Violation (see Figure 4). HFACS defines these categories as follows [3], [4]:

- **Inadequate Supervision**: This factor reflects the degree to which supervisory roles provide sufficient guidance, training, leadership, oversight, or incentives to ensure the task is performed safely and efficiently. The definition was expanded to include lack of acknowledgement or lack of knowledge of cyber vulnerabilities/risk. If the supervisor is not knowledgeable of a cyber vulnerability, it becomes less likely that the operations level personnel will look for the issue.
  - Lack of guidance on cyber hygiene
  - Lack of knowledge of cyber vulnerabilities
- **Planned Inappropriate Actions**: Within organizations, it may be accepted to rely on shortcuts or workarounds to complete the mission of the facility. This could include placing equipment on the network without involving IT. A common example that we call out because it reflects a violation of basic cyber hygiene would be use of common passwords or displaying login information. In addition, HFACS differentiates between

operations, policies and procedures that can be acceptable and different during emergencies, but unacceptable during normal operation. In the case of workforce response to cyber events, the converse can be critical – would normal operations be sufficient during off normal events?

  - Display of credentials/passwords or use of common credentials
  - Procedure or policy ineffective (does not prevent cyber vulnerability)
  - Reliance on workarounds

- **Failure to Correct Known Problem**: This factor is representative of the degree to which supervisors are responsive to reports of cyber vulnerabilities. It indicates deficiencies are known at supervisory levels, but are allowed to remain (e.g., use of unapproved software or personal electronic devices, software patches not updated).
  - Unauthorized/illegal software systems – use of systems that have not been vetted or approved for use, or use of systems that should have been phased out due to known vulnerabilities
  - Fail to correct known system problems – acceptance of known vulnerabilities or systems that induce errors
  - Technology poorly designed focused on systems that were not well designed to support the task, such as enforcing single logins when systems needed to be used in conjunction
- **Supervisory Violation**: Refers to those instances when cyber hygiene best practices (e.g., clicking on links in unexpected email, use of unauthorized electronic devices) occur by supervisory personnel.
  - Cyber hygiene violation – this referred to an instance of known poor cyber hygiene at the supervisory level as a failure to model good practices.

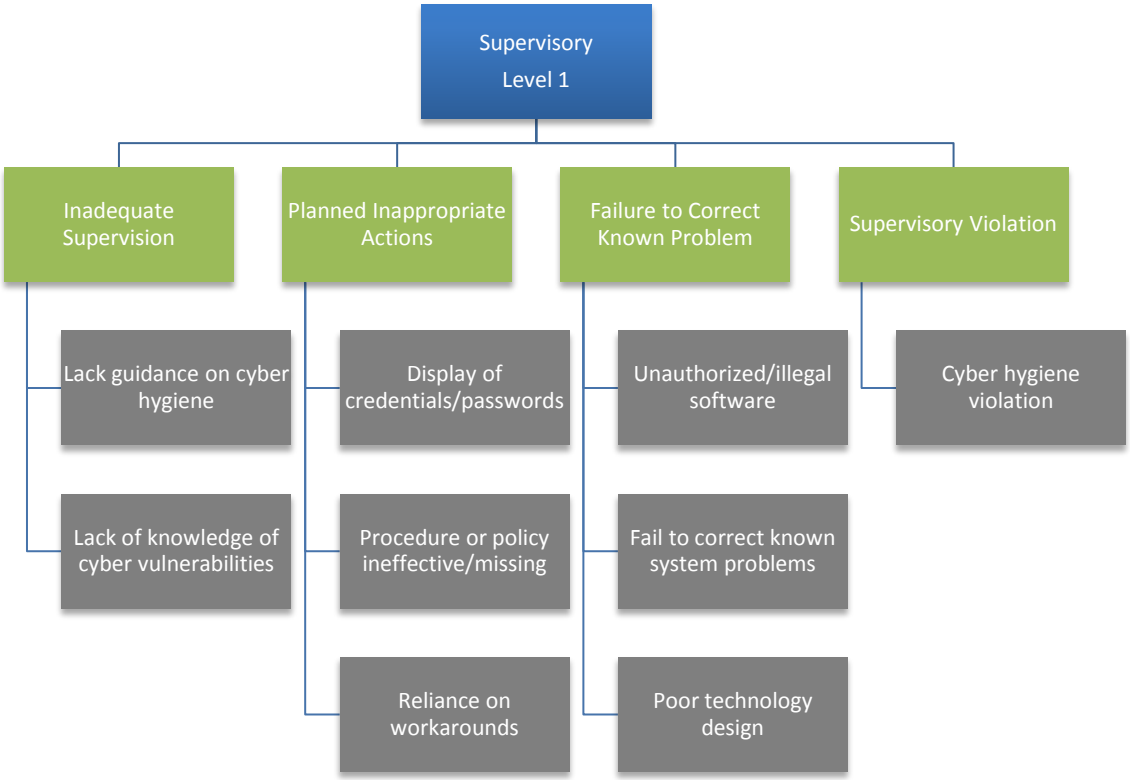


Figure 4. Supervisory Levels 1, 2, and 3

4.1.3 HFACS First Order Effect Preconditions for Unsafe Acts (Operational Effects)

The First Order Effect: Preconditions for Unsafe Acts is comprised of factors that have immediate impact on the decision at the operational level, that is, by the workforce. These factors reflect immediate influences on action, because they shape the information available to the operation at the time of the decision. Preconditions for Unsafe Acts level allows for influences arising from environmental and technological factors, the condition of operators, and personnel factors (see Figure 5). Each of these three categories is then further defined in the Second Order effects, as follows:

- **Physical Environment** factors include the ambient environment (e.g., noise). This category was expanded to include physical set ups, such as allowing cabling to run out of closed spaces or lack of redundancy between critical lines (e.g., telephone).
  - Physical set up
  - Lack of redundancy between critical systems
- **Technical Environment** refer to things that impact human-machine interaction, such as the integration of systems that are used together, the degree to which the system was designed to support the tasks for which is was used (e.g., sufficient available phone lines). This included use of systems that could be vulnerable to external influence. Lack of sufficient equipment was included because it can influence workers to use un-approved systems. Similarly, systems that are to be used together on a task should be integrated to all sharing of information, otherwise risk of error or poor decisionmaking is

increased. Training and Education was called out as a factor at this level. In the original HFACS structure, training is assumed to be very high quality, appropriate and timely because of the nature of the aviation environment which is not the case in the cyber context.

  - Technology vulnerable to external influence
  - Un-integrated systems
  - HMI missing information; overly complex
  - Insufficient or inappropriate technology for the task

- **Crew Resource Management** refers to issues of communication, team coordination and teamwork, and planning that affect practices, conditions or actions of individuals, and result in human error or an unsafe situation. We included within this category communication between individuals within parallel organizations, such as communication between a facility manager and IT personnel.
  - Over reliance on expertise
  - Workload, stress, fatigue due to insufficient coordination, staffing, etc.
- **Training and Education** reflects training on system vulnerabilities and vulnerabilities due to the hybrid nature of control systems. Training should include training on the physical impacts of the cybersystems and cyber influences on physical systems. Operators should have awareness of cyber connections (at least know that their system has or does not have a cyber connection), and its vulnerabilities. Training should be appropriate for the type of system interactions operators have in the course of their tasks.
  - Lack awareness of cybersystems in use
  - Lack of training/education on cyber vulnerabilities

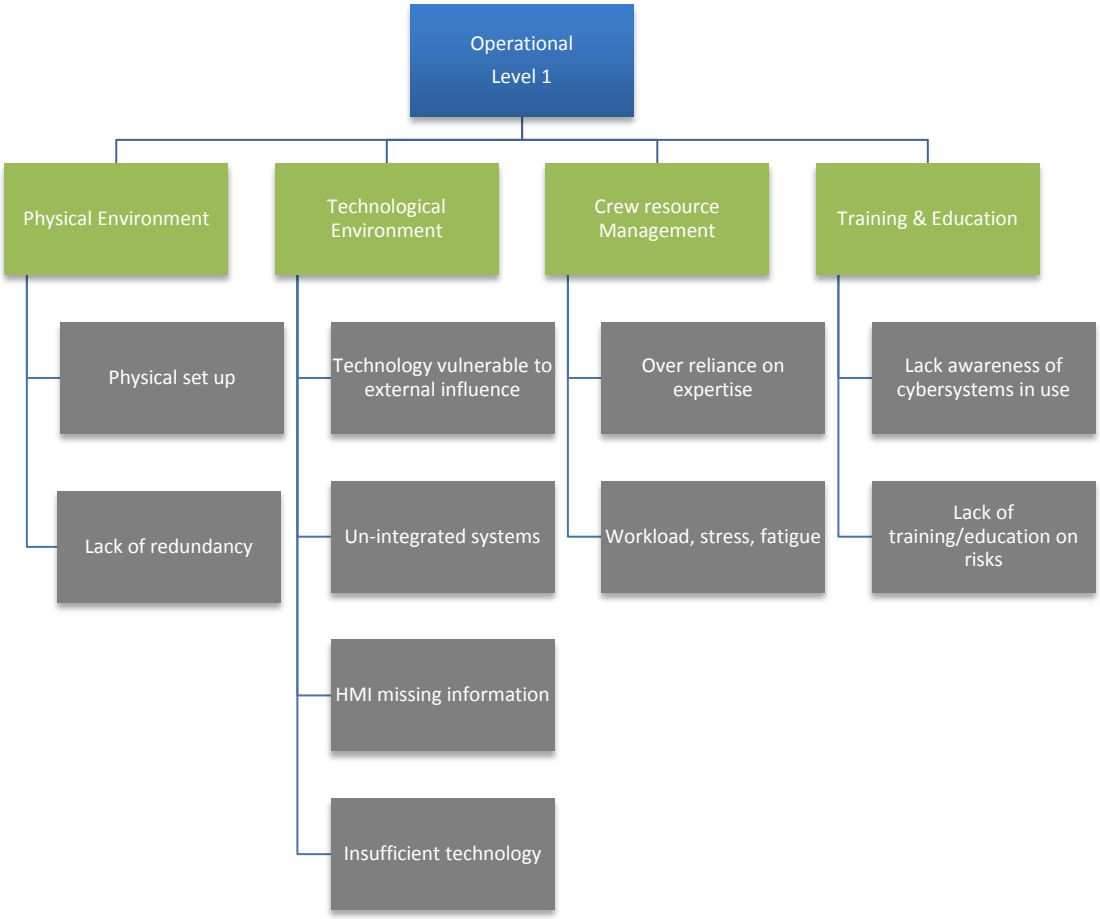


Figure 5. Operational Levels 1, 2, and 3

4.1.4 HFACS Outcomes: Unsafe Acts

Unsafe Acts consist of errors and violations, which are divided into subcategories. Errors are unintentional behaviors, while violations are a willful disregard of the rules and regulations. Errors are divided into skill-based, decision errors, and perceptual errors. For the purpose of this report, we did not use the Errors category as we were reporting on potential vulnerabilities. Violations are comprised of Routine violations (habitual operator actions that are outside of rules of the task but which are tolerated by management) and exceptional violations (isolated departures that are neither typical or condoned). We did not use the Violations category, unless we were able to state that an act occurred even though we were aware of a policy or procedure existed at that site that would have prevented it. Therefore, no unsafe act or violations are reported here.

5. FINDINGS

In Section 5, we first discuss the observed vulnerabilities identified through the site visits, their classification within the HFACS Cyber framework, and assessment of common themes and issues derived from the classification. We begin with an overall analysis of the quartiles of vulnerabilities, and then discuss the most common HFACS Cyber factors. After the analysis of the observed vulnerabilities, we discuss our assessment of training sources, identification of competencies, and gaps between training, competencies, and vulnerabilities observed.

5.1 Vulnerabilities Derived from Site Visits

Interviews and interactions at the sites focused on workforce PAOs focused on the performance of the facility. Vulnerabilities were defined as an interaction within the physical facility (not the network proper) that could be exploited to allow access to cybersystems or data or allow interruption of the mission of the facility by a malicious actor. While the focus of the assessment was on interaction with cybersystems, some vulnerabilities arising in physical systems (which could affect the performance of the facility or cybersystems) were also identified. Examples of cyber vulnerabilities identified include things such as an unlocked touch screen in a utility area. An example of a physical vulnerability with cyber implications included network cabling running outside a locked switch cabinet; such cabling could give a malicious actor access to data or systems. For the purpose of this assessment, while the physical vulnerabilities are discussed, the primary focus of the statistical analysis is on the cybersystem vulnerabilities.

Results of site visits and interviews were analyzed in several ways. Findings were analyzed with respect to facility, mission area (e.g., health and safety), and personnel role (e.g., facility manager vice SCADA engineer) from which they were derived. While facility information was obtained, to maintain the privacy of the facilities visited, site information is not associated with particular vulnerabilities or positive lessons learned. Data were analyzed with respect to HFACS to identify common Unsafe Acts and Error Precursors across PAOs, and roles. Based on the findings, the HFACS category definitions were expanded and modified to cover the types of vulnerabilities seen in these cyber physical systems. Findings were assigned up to three HFACS categories by the analysts. Three category levels were assigned to assist in the determination of effectiveness of mitigations across sites and error precursors. This was done to determine the gaps in training or personnel that would be most effective in reduction of potential cyber violations. HFACS provided a framework to assess common vulnerabilities across sites regardless of differences in facility mission, PAO assessed, and cybersystem used.

5.2 Analysis

Observations were idiosyncratic to each facility, as a function of personnel roles observed, the OT systems in use, and differences in PAOs (dispatch emergency services) and missions (e.g., provide health and safety services) observed at each facility. While a few similar missions or PAOs were observed at multiple facilities, there were significant differences in the process between facilities, which prevented collapsing vulnerabilities and observations across mission, role, or PAO. Therefore, JHU/APL instead analyzed across role, mission, PAO, and facility. Observations are not identified by location within this report, and efforts have been made to remove location identifying information from observations and vulnerabilities.

Across the facilities visited, 167 observations were made, 41 of which were positive cybersecurity factors. The remaining 126 observations were categorized within the HFACS Cyber framework. Each observation was assigned to not more than three HFACS cyber categories, for a total of 227 vulnerabilities. Primarily two raters performed HFACS classifications. Inter-rater reliability was very high (κ = .81) for these two raters, indicating common assignment of observation to HFACS category. All disagreements between raters were resolved by discussion, and discussion was used to clarify the HFACS Cyber definitions. Given the small numbers of vulnerabilities and observations for each PAO, role or facility (on average 21 observations per facility, but in actuality one facility had primarily positive observations); vulnerabilities were condensed across these categories. Once findings were categorized with respect to HFACS, the vulnerabilities were organized into quartiles of common vulnerabilities, condensing across PAO, role, and facility.

5.2.1 Quartile Analysis

Error precursors were assessed across the HFACS Level 1 and 2 categories to define quartiles of impact for these precursors. Quartiles are defined with respect to the HFACS classifications seen most frequently. The results are shown in Figures 6 through 9. There are several trends that can be identified at this lowest level of analysis. First, insufficient training, downplaying risk, IT integration, and communication of vulnerabilities accounted individually for the largest number of vulnerabilities identified. Second, there appears to be repetition in vulnerability categories (especially with respect to lack of training and procedures) when they are presented independently of the Level 1 and Level 2 effects.

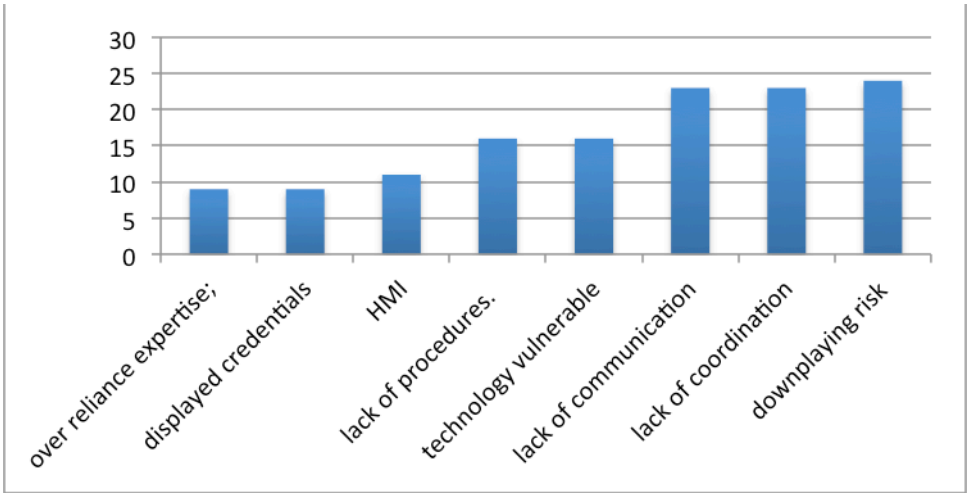


Figure 6. Quartile 1 Error Precursors

Differentiation of Error Precursors by quartile is slightly misleading because the raw number of instances was relatively low for over half of the precursor types. It is more useful to begin by exploring the trends of co-occurrence between error precursors, and trends in the first and second level effects.

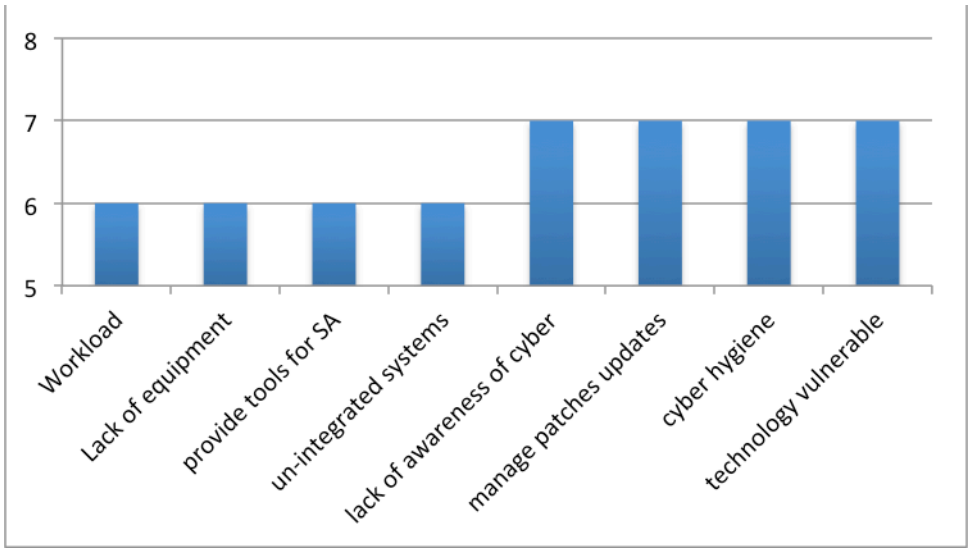


Figure 7. Quartile 2 Error Precursors

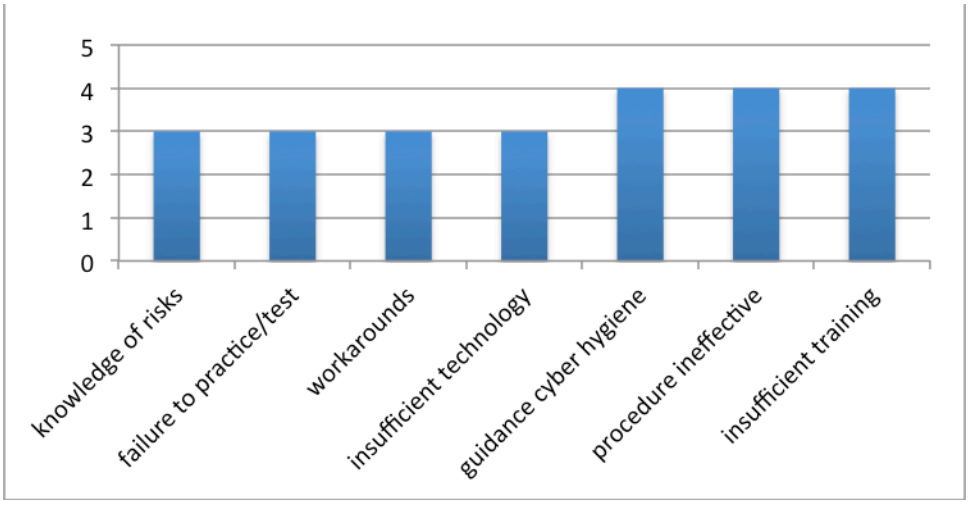


Figure 8. Quartile 3 Error Precursors

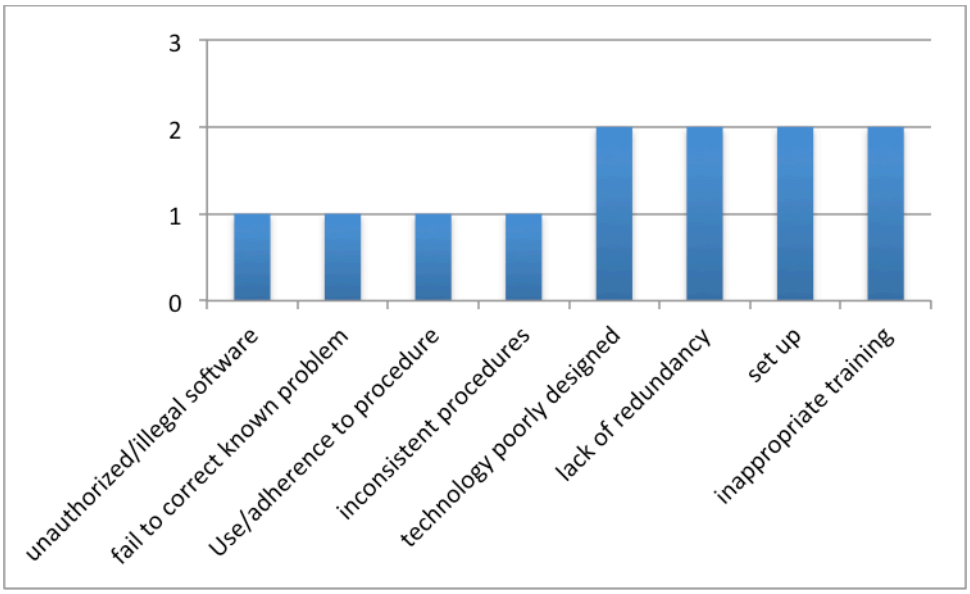


Figure 9. Quartile 4 Error Precursors

5.2.2 Assessing Vulnerabilities within HFACS

While breaking the vulnerabilities into quartiles, as presented above, does provide some insight into the types of vulnerabilities identified, the use of HFACS as a framework is to allow understanding of the potential best mitigation of these vulnerabilities. As discussed in Section 4, HFACS further breaks down Level 1 factors in to Levels 2 and 3. Organization Level 1 factors were divided into three categories: Organizational Level, Supervisory, and Operational, Factors. Figure 11 summarizes the vulnerabilities seen across these Level 1 factors. As shown in Figure 11, the greatest number of vulnerabilities could be tied to an Organizational cause. Organizational factors break into Resource Management, Organizational Cyber Awareness, and Operational Processes. Of interest, the majority of error precursors associated with Organizational level decisionmaking reflected vulnerabilities in Organizations Cyber Awareness (see Figure 12), a function of its safety culture – the emphasis that an organization devotes to safety considerations. Safety Culture is frequently assessed as a function of the Resources devoted to training, tools, and techniques as well as the presence and absence of procedures to guide decisionmaking. However, during the interviews a common theme emerged from Facility Management with respect to the known need for better funding for cyber safety considerations.

Organizational Cyber Awareness. JHU/APL next assessed at which Organizational tier vulnerabilities were most attributable. What stood out in the analysis was that a large portion of vulnerabilities appeared to have connections to organizational and operational factors. Of the 267 error precursors assigned, 127 were associated with decisions and actions occurring at the Organizational level, while 66 were associated with Operations, and 34 were assigned Supervisory Category precursors (see Figure 10). From a mitigation standpoint, this would imply that mitigations aimed at the manner in which the organization addresses cybersecurity would

have the greatest impact, while those aimed at the operations level would have a greater effect than changes made in supervision of the work.

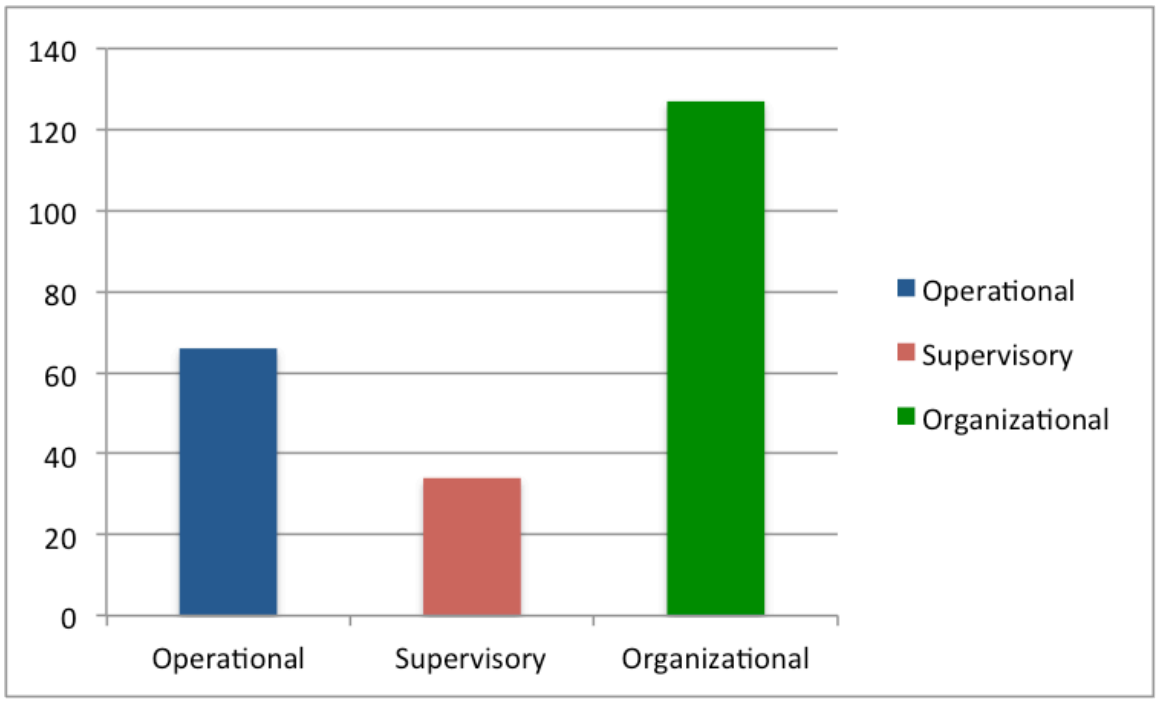


Figure 10. HFACS Cyber Level 1 Vulnerabilities

The Organizational Level 1 effects were broken down and assessed at Level 2 effects. Based on the assessment of Level 2 Effects, the Organizational Cyber Awareness category, which was assigned to 85 vulnerabilities, was further examined (see Figure 11). The error precursors assigned to Organizational Cyber Awareness included Downplaying risk, Lack of communication of cyber vulnerabilities, Lack of integration between IT and other groups, and Coordination with external organizations.

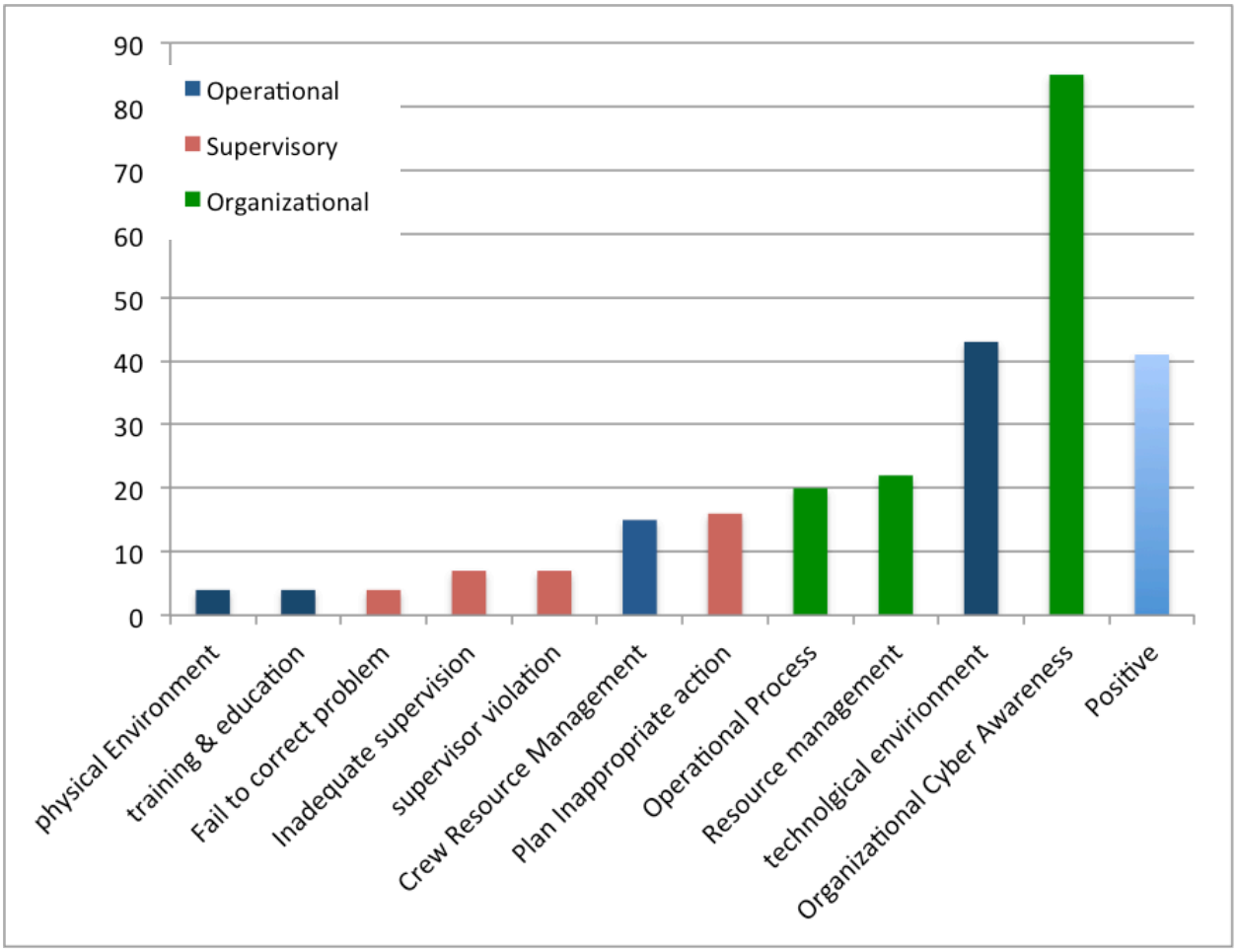


Figure 11. HFACS Cyber Level 2 Effects

Lack of coordination between IT and other groups was associated with the greatest number of vulnerabilities. (For clarification, the term IT is used to encompass all groups who perform network monitoring and information technology support, including the Network Enterprise Center (NEC) and Information Technology Security Division (ITSD), but who are not part of facility management or facility operations.) However, this category did show differences for varying processes, activities, and outcomes. Lack of coordination with external organizations arose from different causes for different activities. A recurring theme in interviews with Health and Safety personnel reflected difficulties in assigning calls to emergency services depending on whether the calls came in from landlines or cell phones. At the facilities where we spoke with Health and Safety personnel, we learned that calls to 911 are answered by the county in which the cell phone tower is located. Landline calls from on facility are routed to the facility emergency services (if the facility has emergency services). If the county emergency services determine that a cell-based call is on the facility, county emergency services transfers the call to the facility emergency services. The vulnerability arises when county emergency services fail to remain on line to provide the information that they have already obtained to facility emergency services. In addition, there is no automated function that can transfer this information between the emergency services dispatcher systems. The facility emergency services dispatcher must then again collect much of the same information previously provided to county emergency services, which can delay responding.

Lack of integration between IT and other groups lead to vulnerabilities for all PAOs of interest and across most roles interviewed. Vulnerabilities that arose from lack of integration between IT and other groups were associated with conflicts between requirements and system capabilities, or systems that were poorly designed for the task to be performed. Examples included the finding of a requirement to use common access card (CAC) authentication for closed restricted networks but the central authentication server is inaccessible from the closed restricted networks (to NEC). A second example was seen again in emergency services at one facility. Multiple systems (ANI/ALI, Kingfisher, and CAD) were used to identify the location from which a call for assistance arose. Because one system was run by NEC while other systems were owned by emergency services, emergency dispatch was required to correct the origin location of calls in the NEC-owned system; however, that update was not stored in the system. If another call came from the same location, the emergency dispatcher would again need to update the location information. At a second facility running the same systems, NEC has worked with facility management for several months to update all incorrect location information to avoid delays in emergency response. This update was done as part of an upgrade to the emergency response system at that facility. Because of the siloed nature of facility management and IT, resources were not available to correct this vulnerability at the first site.

Table 2. Observations of Technological Environment and Un-integrated Systems

IT Services for Facility Management	Facility Engineer	Long turnaround on ICS network maintenance (10–30% uptime)
Emergency Services	Emergency Dispatch	NEC does not update the corrections to Kingfisher when they are input into CAD and Intergraph. Corrections to addresses need to be made each time a call comes from that location.
Emergency Services	Emergency Dispatch	ANI/ALI system 'upgrade' reduced concurrent call management capability to 1 active call.
Facility Management	Facility Engineer	Requirement to use CAC authentication is recognized for closed restricted networks but the central authentication server is inaccessible from the closed restricted networks (to NEC).
Facility Management	Facility Manager	VLAN seemed to be used as a security feature. They are an ineffective way of providing security.
Facility Management	Facility Engineer	ICS servers connect to NIPRNet for patches - possible attack vector; some patches have to be moved manually and installed - CD is possible attack vector

Exploring co-assignment of Organizational Cyber Awareness as a potential error precursor indicated that when it was assigned to a vulnerability, it co-occurred with another category. This would be expected because of the nature of safety culture. When an organization does not emphasize safety, behaviors manifest at the level of operations and supervision. In the assessment of vulnerabilities, Organizational Cyber Awareness was co-assigned most often with Training & Education (9), Technological Environment (8), and Supervisory Violations (6). More than one Organizational Cyber Awareness precursor was co-assigned 9 times to a single vulnerability. These findings are in keeping with the definition of Organizational Cyber Awareness. Co-occurrence of Organizational Cyber Awareness with Technological Environment emphasized the lack of coordination between IT and other organizations. Examples of observations associated with un-integrated systems are provided in Table 2.

Organizational Cyber Awareness error precursors also included Lack of Communication between groups, which were assigned to 22 vulnerabilities (see Figure 12). Lack of communication led to several exploitable vulnerabilities that could be used by a malicious actor to gain access to a facility or disrupt the functioning of the facility. Examples of Lack of Communication were:

- Poor communication between groups. ICD, Emergency Services, and Physical Security groups do not communicate directly but each get different pieces of information. There are no systems that commonly show alerts.
- Poor communication paths between Government and civilian agency that both require access common location. Solution was to leave the common location unlocked.

Interactions between Government and civilian agencies were observed at 3 of the 6 sites visited by JHU/APL. Overall, interactions between facility and civilian agencies were well coordinated. However, as noted above, at one facility there appeared to be communications difficulties

between two agencies, for reasons that were not ascertained. However, because of this communication difficulty, access to the keys to an electrical system that was critical to both the local government utility and the Federal Government facility would be left open and unattended.

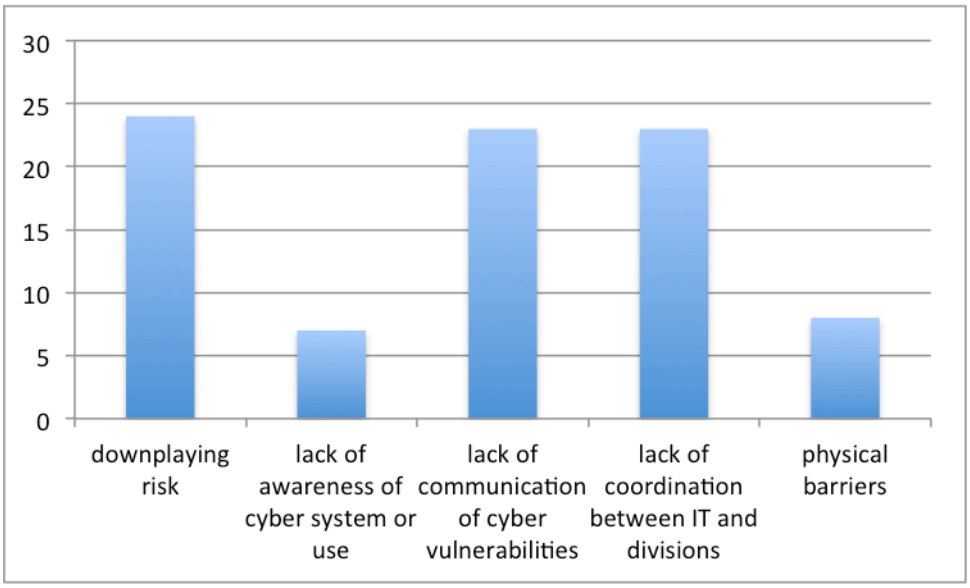


Figure 12. Level 2 Organizational Cyber Awareness Level 3

Organizational Cyber Awareness vulnerabilities were seen across multiple personnel roles interviewed and facility PAOs of interest. Table 3 lists a subset of Organizational Cyber Awareness associated vulnerabilities identified across sites.

Table 3. Example Organizational Cyber Awareness Vulnerabilities

Process, Activity, Outcome	Personnel Role	Vulnerability Seen	HFACS-Cyber Level 2	Level 3
Emergency Services	Health and Safety	Public relations would not send out the notification of 911 down and to call new numbers	Organizational Cyber Awareness	Coordination with External Organizations
Facility management	Facility Engineer	BAS Vendor has same level of access as on site administrator, can create authorized users	Organizational Cyber Awareness	Lack of communication of risk
Emergency Services	Emergency Management	EMS personnel are aware of the RF null points and issues (as shown by the coast guard story) but they do not know how to protect their communications and do not see the need to protect their communication. They know that there are radio dead spots within the	Organizational Cyber Awareness	Downplaying risk

Process, Activity, Outcome	Personnel Role	Vulnerability Seen	HFACS-Cyber Level 2	Level 3
		base -- at those points they use personnel electronic devices		
Facility Management	Facility Managers Facility Engineers	Personnel had limited awareness of cyber connections within facility; were not aware that VOIP was cyber	Organizational Cyber Awareness	Lack of communication of risk
Environmental monitoring	Facility Engineer	Access control, CCTV and barrier control system can be controlled via business systems	Organizational Cyber Awareness	Lack of integration of IT with other divisions
Facility management Utility (Energy) Services	Facility Engineer Energy System Personnel Environmental Services Utility services	4 separate observations of login/passwords displayed at workstations (3 of 4 were for cyber connected systems).	Organizational Cyber Awareness	Downplaying risk
Facility Management	Facility Engineer	User name and password never changed. Easily guessable	Organizational Cyber Awareness	Downplaying risk

Active development of a positive Organizational Cyber Awareness was found at two of the facilities, while there were indications of development of a positive Organizational Cyber Awareness at two other facilities. Indicators of positive safety culture seen at two different facilities were:

- Evaluation of cyber vulnerabilities of new systems by NSA before integration into building systems.
- Contractors and vendors were required to use facility equipment or allow the facility to approve any equipment used. The process for equipment approval was documented; staff in several roles (facility manager, facility engineer, security personnel) knew the procedure and the contact point to initiate an approval. The process was seen as a positive act, and personnel performing the approval worked with facility engineers to assess equipment as quickly as possible.
- ITSD staff regarded IT as a service agency to all other divisions. They would actively market their capabilities (as a slide show presentation) to other divisions.
- Procedure/regulation exists to allow external laptop to be attached to network -- procedure was known and followed.

An example of poor Organizational Cyber Awareness stood out at a third site. In multiple buildings (including the building housing the electrical SCADA system, the pumphouse for a water tower, and the waste incineration plant) a WiFi-enabled monitoring system was observed. Facility managers had a general awareness of the system, as it had been approved by a previous

facility manager. However, no facility engineer or manager interviewed was aware of the purpose of the system, nor did IT services have information on the system. One facility manager interviewed said that the system was no longer used, but he did not know whether it still sent information, where that information would be sent, or who would have access to the information.

Downplaying risk was initially combined with lack of awareness of risk or vulnerabilities within Organizational Cyber Awareness but because it had a different underlying cause, it was later separated. In the case of lack of awareness of vulnerability, personnel did not appear to be aware that there was a potential risk from the technology or process that they were applying or were not aware of cyber connections within their system. (For example, at one facility, personnel were unaware that their phone lines were VoIP.) Downplaying risk was defined as personnel indicated that they knew (or could be assumed to know) that the technology or process that they used contained risk, but felt that the risk was not significant enough to change the technology or procedure. Since risk is a function of probability of an event multiplied by its impact, personnel were either underestimating the risk or the impact should the vulnerability be exploited. Examples of downplaying risk included:

- Access control not being used widely for areas where ICS systems are in use. (Vault protected by old locked door). No logical access controls on HMI.
- No logical controls on HMI touch screen in water tower. Touch screen active.
- Use of personal electronic devices (cameras) for fire scene investigation (in part due to lack of equipment).
- Emergency Services are aware of the vulnerabilities in RF coms (anecdotal evidence) but either do not know how to protect their communications and/or do not see the need to protect their communications. They know that there are radio dead spots within the base —at those points they use personnel electronic devices if Government-issued phones are not available.
- Unencrypted WiFi.

In some cases, downplaying risk seemed to occur because the system had been installed by a trusted agent or because that type of system had “always” been present. The security of the system was not questioned later when vulnerabilities were known. In both cases, changes to the education and training that personnel receive would reduce these vulnerabilities, but more importantly, programs to emphasize questioning attitudes about system, ability to query IT experts about system vulnerabilities, and emphasis of personal responsibility for system risk would be as or more effective, as personnel may have sufficient information about vulnerabilities but not sufficient power or responsibility to act.

Operational Level Effects. Continuing with the assessment, Level 1, Operational Effects also demonstrated significant effect on vulnerabilities. Operational Effects focused on factors affecting performance of the decision maker at the point of performance. Operational Level effects were subdivided into Crew Resource Management, Technological Environment, Physical Environment, and Training & Education (Figure 13). Within the Operational Effects, Technological Environment was associated with the greatest number of vulnerabilities. Technological Environment is broken down to its associated Error Precursors (Figure 14).

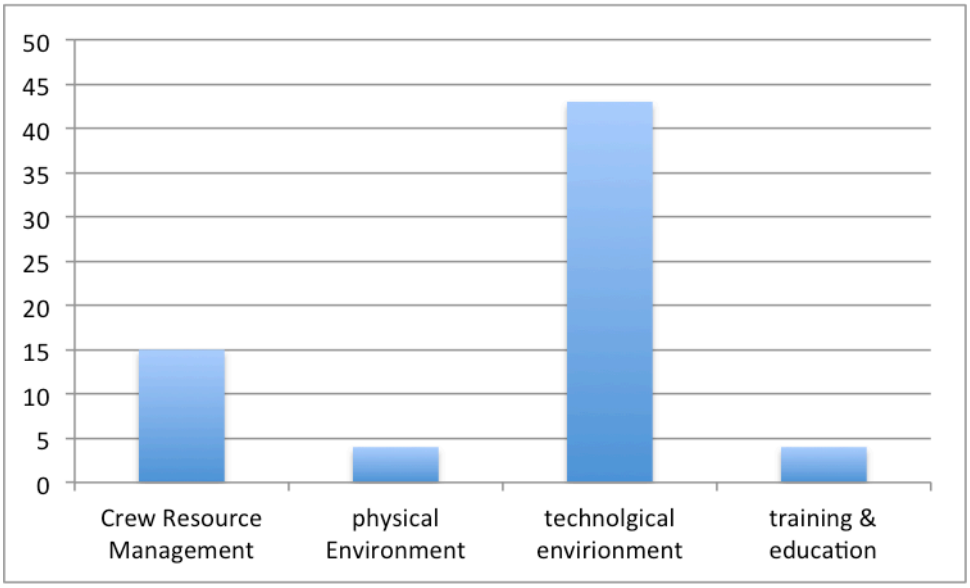


Figure 13. Operational Level 2 Effects

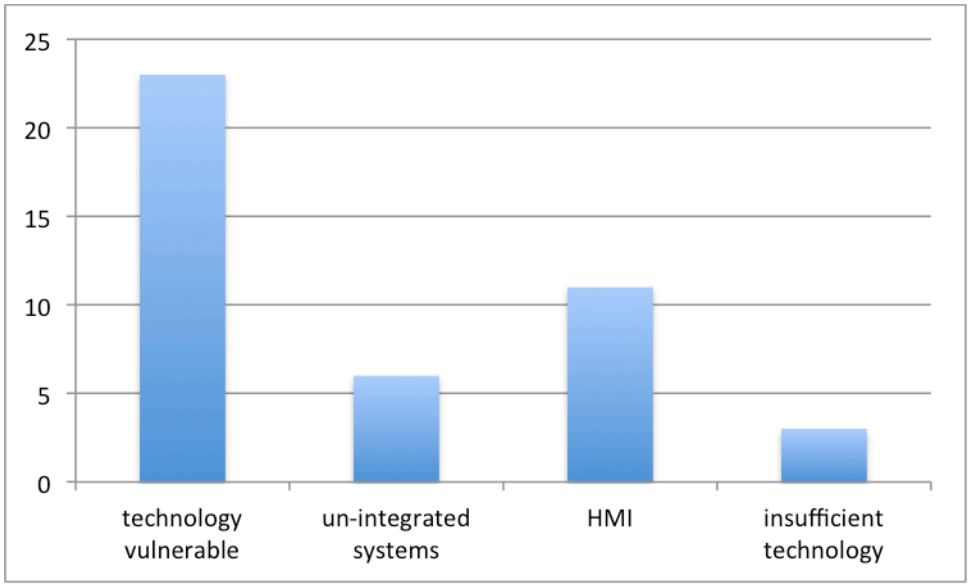


Figure 14. Technological Environment Error Precursors

The greatest factor within the Technological Environment was use of systems or technology that could be vulnerable to external influences. Table 4 lists a selection of vulnerabilities associated with Technology Vulnerable to External Influence as a function of PAO and Personnel Role interviewed.

Table 4. Example Observations of Technology Vulnerable to External Influence

Process or Activity	Personnel Role	Vulnerability Seen	HFACS-Cyber Level 2	Level 3
Facility maintenance	Facility engineers	Maintenance laptops have intermittent direct connection to the closed, restricted ICS networks.	Technological Environment	Technology vulnerable to external influence
Utility Services	Water and Sewage Engineering	Base water distribution uses RF communications for C2 for the primary and only control path.	Technological Environment	Technology vulnerable to external influence
Safety and Health Emergency Services	Emergency Dispatch	Autodialers and marketers can call emergency services.	Technological Environment	Technology vulnerable to external influence
Facility Management Physical Security	Facility Managers Security Personnel IT Services	Cameras, Metering and HVAC, and LENEL system are on separate VLANs but one ICS network. VLANs are not a security measure and the unsecure metering, HVAC, and camera systems provide the potential to pivot between VLANs and access sensitive data.	Technological Environment	Technology vulnerable to external influence
Utility Services	Utility Engineer	Water facility system accessible remotely (password protected).	Technological Environment	Technology vulnerable to external influence

Technological environment issues were common to all sites visited. Analysis of Technological Environment Error Precursors also indicated issues with poor HMI and un-integrated systems. The majority of issues with un-integrated systems arose primarily from discussions with Emergency Management personnel, but was also seen as an issue for facility management systems, and systems used for physical security. In these cases, the cause of the vulnerability was need to integrate new systems together to more easily support the work or avoid confusion; but because IT is a separate division, resources were not available to support the integration. In other cases, CS systems were not integrated with the NEC topology. In some cases, requirements for system authorization conflicted with the design of the network due to the lack of integration. At one site, there was a requirement to use CAC authentication recognized for closed restricted networks but the central authentication server was inaccessible to the NEC from the closed restricted networks. However, if IT (NEC) capabilities were integrated within facility operations, ensuring that operational functional requirements were included in the development of systems and integration of systems would be simplified.

As with Organizational Cyber Awareness, there were positive Technological Environment instances identified:

- Building to building communication is discouraged... All building systems are designed to talk to servers.
- Less secure hardware are typically installed behind more secure panels to avoid vulnerability
- Operations center has a centralized, integrated system for awareness of BAS performance, which can monitored by multiple people, simultaneously
- Other internet services were not available from CS workstations (email, Internet, etc.), must go to another workstation

One ***lesson learned*** from the exploration of technological environment was that integration of IT services with development of tools, procedures, and protocols for monitoring the facility led to the strongest cybersecurity posture.

Crew resource management. At the operational level, vulnerabilities associated with staffing, workload, and personnel issues were seen. These issues were primarily associated with over-reliance on expertise and workload. An example of over-reliance on expertise included lack of procedures for responding to off-normal events, or failure to practice procedures for off-normal events. Emergency Dispatch systems were seen which receive hundreds of false alarms within a shift; these false alarms are ignored based on the expertise of the dispatcher rather than improving the system. Other systems for remote monitoring of facilities include dwell alarms which also had high false alarms, and which were ignored by operators based on experience. In addition, Emergency Response systems did not identify where within a building an alarm was occurring; rather the Emergency Dispatcher or Response Personnel knew from experience with what location the alarm was associated (e.g., the location of a pump). Similarly, knowledge of the locations of SCIFs within buildings relied Dispatcher experience, rather than being included within building information. At several facilities, maintenance personnel would call in to physical security and voice identify if they had set off an alarm; the person receiving the call would identify them by voice, and at some locations via caller ID. Both over-reliance on expertise and workload issues were tied to technology issues, in that the technology typically did not well support the task to be performed.

Education and Training. In this section, we discuss those observations that were attributed to an issue with the training received by the facility operations personnel. (An assessment of training sources follows.) Training did not receive as many attributions as was initially expected. This was not because training was particularly good, but rather because training at an operator level did address basic cybersecurity issues – facility operations personnel were aware of the need for cyber security, and aware of some actions they could take. However, their training was focused on business systems, not cyber vulnerabilities for the operational technology systems with which they interacted most frequently. They did not receive training on assessing risk to their systems, or connections and interactions between their systems. Actions for securing systems were generally seen as activities that were the responsibility of the IT division. For example, at one facility, WiFi was present and unencrypted. However, the facility operator

whom we interviewed did not know how to shut off the WiFi or how to encrypt it (though he may have understood the need for encryption).

Need for training and education to increase competency was seen at the supervisory and organizational levels, and was reflected in error precursors at those levels. One training list obtained from a facility list is included in Appendix A. Interviews at all facilities included questions about training received. For the majority of the workforce, the training list in Appendix A was typical. Interviews with facility management at JHU/APL indicated that facility management also takes a course for the building automation system office by its BAS vendor. However, investigation of the curriculum did not show any discussion of cyber vulnerabilities or cybersecurity. Due to the separation between control system engineering (and facility management) and cybersecurity, there has been a distinct lack of training, education, or course work. At JHU/APL, the IT Security Division actively countered this lack of training and integration by frequently going to other departments and divisions (including facility management) to present an overview of security considerations relevant to that division and to advertise the types of support that they could provide, actively seeking to raise awareness. As discussed earlier, one characteristic of poor Organizational Cyber Awareness is lack of knowledge and downplaying of risks. Risks are downplayed when the consequences (or severity) of a decision are not well understood. This led to a ***second lesson learned***: Cyber security is increased with an active stance toward interactions between IT and other divisions.

5.3 Competencies, Skills, and Education for Facility Roles

5.3.1 CS and Cybersecurity Competencies

Cybersecurity competencies specific to IT have been defined and are readily available from various sources (e.g., National Initiative for Cybersecurity Careers and Studies [18]); however limited work has been done to establish cybersecurity competencies specific to CS personnel. Therefore, JHU/APL began with a review of the available competencies already identified to further refine them to meet the needs of CS personnel. (See Appendix B for a complete list of the competencies identified.) Below is a partial list and description of the sources reviewed:

- **National Initiative for Cybersecurity Careers and Studies (NICCS),** which developed the National Cybersecurity Workforce Framework provides a blueprint to categorize, organize, and describe cybersecurity work into Specialty Areas, tasks, and KSAs. While numerous cybersecurity competencies are identified few covered specific CS job requirements.
- **The Federal Buildings Personnel Training Act 111-308**, released a resource that outlines Core Competencies and Recommended Curriculum for CS personnel. Within the 207 performance areas that fall within the 12 competency areas identified, only 1 performance area highlighted cybersecurity as a required competency.
- **Facility Workforce Requirements for Cyber Securing Industrial Control Systems** document developed by EI&E Business Enterprise Integration Directorate and the Operational Energy Plans and Programs Directorate expanded on the 12 competencies established in the Core Competencies and Recommended Curriculum created by the

Federal Buildings Personnel Training Act by establishing specific cybersecurity requirements for CS that fit within the 12 competency areas.

Many of these sources provide competencies at a very high level, and do not provide detail about the type of KSAs that are needed in a cyber operations role. For example, the Department of the Navy released the Cyberspace Information Technology and Cyber Workforce Management and Qualification Manual [19]. The qualifications for Authorized User, Enhanced User, and Core IT/CS User are very generalized, as can be seen below:

A. Authorized User: Requires general computer skills and a baseline understanding of cybersecurity

B. Enhanced User: Authorized Users who require detailed knowledge of Cyber IT and/or cybersecurity to support work in the development, maintenance, and operations of multiple DON systems including weapons, tactical, electronic and electrical services, navigation, and engineering. These personnel require an advanced knowledge of Cyber IT/CS, but their knowledge and abilities are centered on their professional area.

C. Core Cyber IT/CS User: Authorized Users who require KSAs in the technical and managerial aspects of Cyber IT/CS. This group is focused on delivering cyber capabilities to the DON and includes those who design, develop, operate, maintain, and defend data, networks, network centric capabilities, computing capabilities, and communications. It also includes personnel who manage risk and protect DON networks and IS.

Given the high level of competencies available from these sources, JHU/APL compiled competency areas and compared these areas to the types of vulnerabilities identified during the site visits and interviews to identify needed knowledge, skills and abilities for differing facility operations roles.

Competencies, Training, Personnel Roles & Vulnerabilities

In order to understand how those vulnerabilities could have been prevented an analysis was performed of the cyber specific CS competencies CS personnel should have, the training currently available to obtain those competencies and the observed vulnerabilities that could have been prevented if personnel where trained appropriately.

Twelve aspects of facility operations and 44 competencies were identified. Facility operations were defined in this manner to maintain consistency with the operations areas defined in the FBTA 111-308. They were:

1. Management of Facilities
2. Performance of Facilities
3. Technology
4. Energy Management
5. Safety

6. Design
7. Sustainability
8. Water Efficiency
9. Project Management
10. Business, Budget and Contracting
11. Leadership and Innovation
12. Management of Cybersecurity for Critical Facility Systems

Analysis of the competency areas and available training varied by the role of the facility personnel. Appendix B provides a detailed view of facility personnel roles, competencies and suggested training. A subset of the table is presented in Table 5.

Table 5. Example Vulnerabilities, Competencies and Related Training Available for Facility Operation Roles

Vulnerabilities	Competencies	Training Opportunities	Roles
Can't identify where within a building an alarm occurs	Demonstrate knowledge of Continuous Monitoring of CS systems	isa.org: Cybersecurity for Automation, Control, and SCADA Systems (IC32E)	Facility Engineers Logistics Personnel Health and Safety Personnel Security Personnel
Poor communication between groups. ICD and Security groups don't talk but each get different pieces of information.	Demonstrates knowledge and ability to ensure cybersecurity requirements are established and standard operating procedures are in place for the operation of control systems, water treatment, ventilation systems and fire prevention systems. Gap: Does not discuss sharing of information	isa.org: Cyber Security for Automation, Control and SCADA Systems infosec: SCADA/ICS Security Boot Camp WTSS580 Managing Security of Control Systems UTSA: Security of cyber physical systems faculty research laboratory	Facility Engineers Logistics Personnel Security Personnel Health and Safety
Have lighting controls for one building connected to the HVAC network	Demonstrates knowledge and understanding of the potential cybersecurity vulnerabilities of	*No Training available Not focused on 'high performance buildings' but may be relevant: AFIT: Cyber Attack, ICS/SCADA Lab &	Environmental Services Facility Operations Facility Management

Vulnerabilities	Competencies	Training Opportunities	Roles
	the technology used to build and maintain "high performance buildings."	Civil Engineering WTSS580 Managing Security of Control Systems UTSA: Security of cyber physical systems faculty research laboratory	
There is WiFi in the plant but the operator could not remember how to turn it on/off. Staff were not aware of the purpose of the profile systems, the location of the systems, the capabilities of the systems. Power system in use is several decades old, to the point where few people have the knowledge to run it.	Demonstrate familiarity with building systems, subsystems, sensors and other components. GAP: Maintain configuration management of CS; maintain awareness of vulnerabilities to older systems (due to age); ensure workforce training and procedures for operation of critical equipment	ICS-CERT: Intro to Control Systems Cybersecurity NPS: CS Lab, CISR Lab, CS4558 Network Traffic Analysis USMA: Network Lab	Facility Managers Utility Services Health and Safety

The greatest numbers of competencies were associated with personnel who were responsible for the management of facilities and for the management of cybersecurity for critical facility systems. Personnel who were responsible for energy and water efficiency also had a high number of associated competencies. In contrast, competency areas in safety, project management, and leadership and innovation showed the least number of relevant competencies. These findings imply that facilities managers and disciplines that require unique expertise as it relates to CS and cybersecurity have the highest numbers of competencies.

Analysis of available cyber training for CS indicates that training for Management of Facilities and Management of Cybersecurity for Critical Facility systems competencies show the highest amount of available training. This finding is likely due to the high number of competencies but could also be due to the organizations that provide training targeting facility managers and the training that is designed to address numerous CS disciplines. The findings also demonstrate the need for cyber training in competency areas that deal with unique jobs such as sustainability and water efficiency where no relevant cyber training was identified in competency areas such as energy management, safety, project management, business, budget and contracting, and leadership and innovation, see Figure 15.

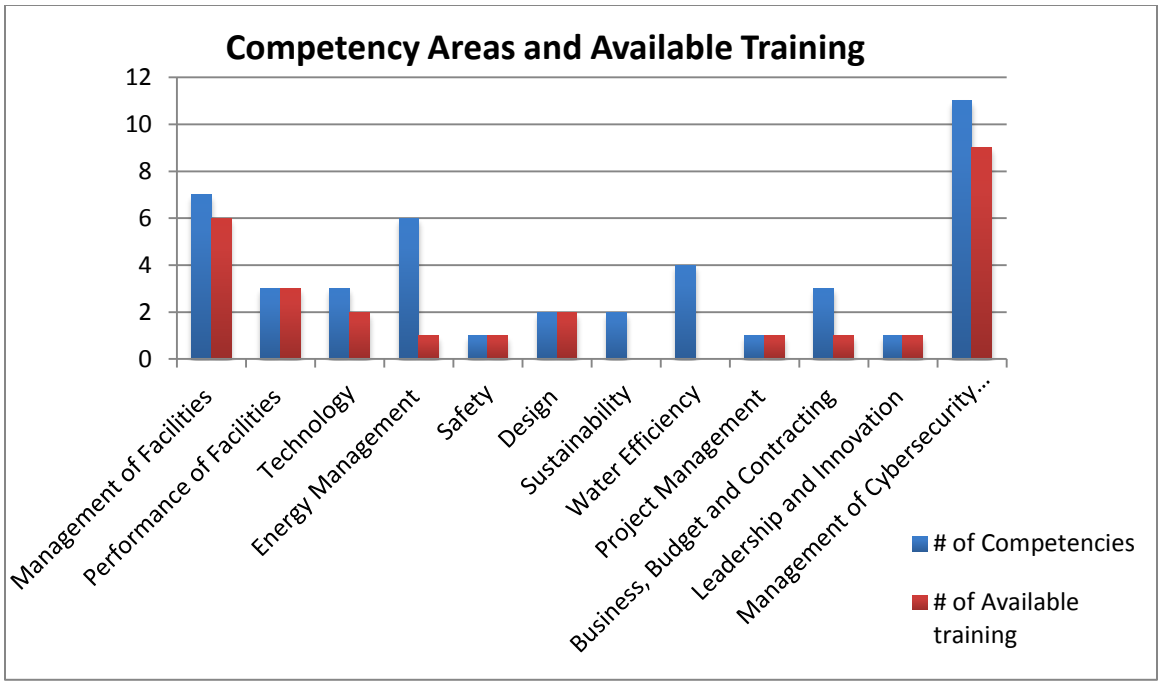


Figure 15. Competencies and Available Training

Competencies, Training and Vulnerabilities

An analysis of the cyber vulnerabilities that were identified during the site visits to the facilities with respect to the competency areas was performed. Consistent with the competency and training findings, the results indicate that the highest number of vulnerabilities were found for the following areas: Management of Facilities, Energy Management and Management of Cybersecurity, Performance of Facilities, and Technology (see Figure 16). The least number of vulnerabilities were identified for competency in areas of water, efficiency, project management, sustainability, and leadership, and innovation. This in part is a function of the accessibility of these areas to JHU/APL. JHU/APL had limited interactions with personnel focused on sustainability, leadership, or innovation.

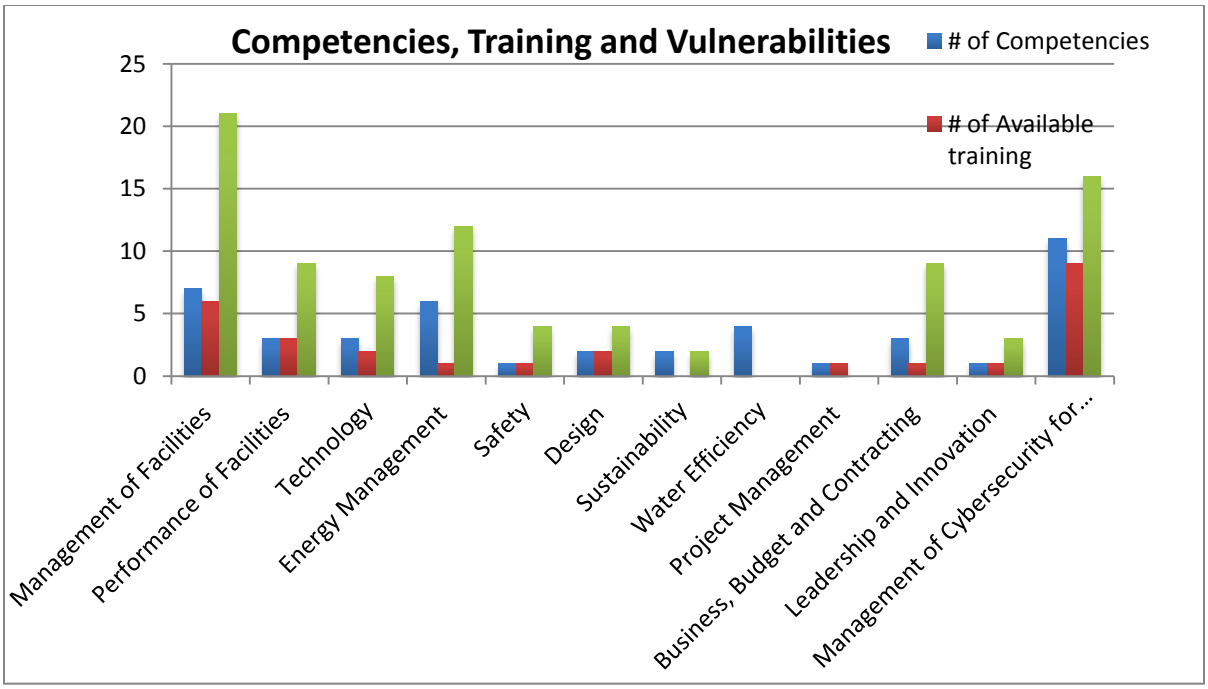


Figure 16. Competencies, Training, and Vulnerabilities

In summary, facilities were found to be most vulnerable to cyberattacks for tasks that management roles were responsible for, but in contrast, those management roles indicated the most relevant training. This finding is consistent with JHU/APL observations of limited access to cyber training specific to CS. The findings also indicate that facility staff responsible for the day-to-day operation of facilities have limited cyber training available specific to their job roles, which indicates a need for the development of additional training.

5.3.2 Gaps in Competencies

Given the limited combined training for cybersecurity and facility operations, it is not surprising that there has been limited identification of competencies needed. JHU/APL began by assessing previously identified competency areas, and then to those areas mapped the vulnerabilities seen at facilities in order to identify gaps in competencies. For a large portion of previously identified competencies, simply including the cyber environment or 'information technology' to the application areas was sufficient to make the competency applicable to the types of vulnerabilities seen. However, for a significant portion of competencies, the vulnerabilities indicated gaps in competencies or skills that would be need in each operational area. These competencies were especially present for identification of vulnerabilities of cyber-physical systems; that is points at which the physical system could be used to impair cyber performance or cybersystems could be used to impair the physical performance of the facility (such as identification that network cabling run out of a locked closet invalidates the security of the closet lock).

Other gaps focused on communication of vulnerabilities between facility groups, or gaps in system design that lead to vulnerabilities in coordination of group response to vulnerabilities. In addition, the ability to integrate human factors or cybersecurity considerations into design stood

out. Table 6 provides an overview of competency gaps by operational area. This table provides a subsection of the information that is included in Appendix B.

Table 6. Competency Gaps

Facility Management	**Competency:** Demonstrate familiarity with building systems, subsystems, sensors and other components. GAP: Maintain configuration management of CS; maintain awareness of vulnerabilities to older systems (due to age); ensure workforce training and procedures for operation of critical equipment
	Competency: Demonstrate familiarity with condition and cybersecurity assessments for building systems. GAP: Maintain network awareness; provide institutional knowledge of system purpose and architecture; Provide for identification of new vulnerabilities
	Competency: Demonstrate ability to work with Facilities Team to establish practices and procedures, including procedures for intercepting and responding to cyber threat alerts, and application of system patches/updates. GAP: Establish procedures to minimize social engineering vulnerabilities
	Competency: Demonstrate familiarity with governance (policy, ownership, vendor arrangements), terminology, and general function of facility control systems. GAP: Ensure external vendors and contractors follow cyber hygiene requirements
	Competency: Demonstrate knowledge and ability to perform Continuous Monitoring of CS systems, identify system instability due to potential exploits and/or malware infection, implement cyber incident response, and recovery procedures. GAP: Ensure that monitoring policies allow for identification of anomalous behaviors during workforce down times
Performance of Facilities	**Competency:** Demonstrate knowledge of Continuous Monitoring of CS systems. GAP: Provide for coordination of information from cybersystems
	Competency: Demonstrate knowledge of what to do when a cybersecurity threat alert affecting one or more facility control systems is received. GAP: Provide policies and procedures for early response off normal conditions; minimize false alarms
	Competency: Demonstrate knowledge of normal operations of facility electrical and mechanical systems, and when (and to whom) to report abnormal operations. GAP: Provide for continuous assessment of normal and off-normal operations

Technology	**Competency:** Demonstrate ability to manage corrective, preventive, and predictive maintenance, including application of cybersecurity patches. GAP: Provide support for use of known vulnerable systems (when vulnerabilities cannot be avoided).
	Competency: Demonstrate knowledge of physical and cybersecurity requirements that must be included in procurement specifications for new systems and upgrading/modification specifications for existing systems. GAP: Ensure for integration of systems during requirements specification
	Competency: Demonstrate understanding of how to respond to alerts regarding threats to cybersecurity. GAP: Maintain awareness and active, valued communication between workforce groups about on-going vulnerabilities and newly discovered threats
Energy Management	**Competency:** Demonstrate knowledge of Energy Management Systems (EnMS) and Energy Information Systems (EIS), associated cybersecurity requirements, and identification of subsystems, sensors, and other component devices. GAP: Provide for identification of vulnerabilities as systems age or new systems are integrated
	Competency: Demonstrate knowledge of how to determine baseline energy consumption patterns and trends, and how to use that information to identify anomalies. GAP: Ensure that maintenance procedures or workarounds do not void anomaly detection
	Competency: Demonstrate knowledge of the Energy Savings Performance Contracting (ESPC) procedures and requirements, including how to respond to cyber threat alerts affecting EPSC systems, subsystems, sensors, and other component devices. GAP: Ensure that regulations do not engender cybersecurity gaps.
	Competency: Demonstrate knowledge and ability to ensure cybersecurity requirements are appropriately addressed in Utility Energy Service Contract (UESC) and ESPC projects. GAP: Ensure conflicting or competing regulations do not create vulnerabilities in cyber physical systems
Design	**Competency:** Demonstrate knowledge and ability to “design in” cybersecurity requirements during design of facilities and associated control systems. GAP: Ensure cybersecurity in design does not impact ability to perform work.
Water Utilities	**Competency:** Demonstrate knowledge of utility meters – location, reading, cybersecurity requirements, and data management. GAP: Identify cyber physical system interactions

Critical Systems	**Competency:** Demonstrate knowledge and ability to identify Critical Systems - those information systems, building automation systems, facility control systems, and communications systems that need to be maintained for operation of the facility, so that these systems can be secured. GAP: Ability to identify cyber connections to critical physical systems; ability to identify physical impacts of minor systems on critical cybersystems
	Competency: Demonstrate ability to conduct periodic assessments of risk, including the magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the organization. GAP: Ability to update vulnerabilities and identify changes in vulnerabilities
	Competency: Demonstrate ability to deliver security awareness training to inform personnel (including contractors and other users of information systems that support the operations and assets of the organization) of the information security risks associated with their activities and their responsibilities in complying with organizational policies and procedures designed to reduce these risks. GAP: Identify limitations in training
	Competency: Demonstrate ability to implement a process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in the information security policies, procedures, and practices of the organization. GAP: Develop process to identify remedial technology and cybersystems
	GAP: Demonstrate ability to implement procedures for detecting, reporting, and responding to cybersecurity incidents.

5.4 Assessment of Training Materials

As stated above, facility operations personnel received little if any training tailored to cybersecurity for their operational technology systems. Training for cybersecurity focused on business systems, rather than on the more embedded cyber capabilities of the systems with which they dealt. Traditionally core competencies and relevant training for Federal facility management personnel has focused on the facility personnel primary performance areas while little attention has been given to cybersecurity. Across the variety of personnel interviewed, the majority responded that the only cybersecurity training that they received was the standard, Cyber Awareness Challenge, provided by DISA for DoD employees. It addresses threats associated with spyware, malicious code, phishing, identity theft, and malicious insiders (see http://iase.disa.mil/eta/Pages/online-catalog.aspx). The DISA training provides an overview of cybersecurity appropriate for a general audience but doesn't address the cybersecurity competencies required to protect against cyber events in operational technology, or detection of cyber threats and risks to these systems..

5.4.1 Training Derived from Government Sources

Given the lack of training materials available from the facilities, JHU/APL explored the training available from various sources to assess what training, if any, was focused on issues relevant to facility management or the human element in cybersecurity.

Several Federal agencies have made efforts to address the needs of CS personnel to be more cyber aware. JHU/APL began by exploring the training available from various sources to assess what training, if any, was focused on issues relevant to facility management or the human element in cybersecurity.

General Service Administration (GSA) implemented The Federal Buildings Personnel Training Act 111-308 (FBPTA). The Federal Buildings Personnel Training Act 111-308 (FBPTA) attempts to standardize facility personnel competencies by focusing on Facility Management, Energy Management and Facility Operations and Maintenance Roles by identifying of 12 competency areas, 42 core competencies and 207 performances indicators (see https://www.fmi.gov/fbpta). Of the competency and core competencies identified by the Act, none possessed a cyber component. The only cyber component included (Demonstrate knowledge and ability to manage cybersecurity for critical Facility Management technologies and systems) was within one of the 207 performance areas within Technology. In addition the cyber performance area focused on Facility Management and not Energy Management and Facility Operations & Maintenance Roles. The FBPTA also identified relevant training for the competency and performance areas and again a limited number of courses identified addressed the needs of personnel to have a working knowledge of cybersecurity concerns.

The Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS –CERT). The Department of Homeland Security's component ICS-CERT is a component within a larger effort within the United States Computer Emergency Readiness Teams which focus on improving cybersecurity awareness and responding cyber threats for Government users, Home and Business users and Control System's Users. ICS-CERT's a division of the National Cybersecurity and Communications Integration Center (NCCIC) works

with industry groups and the Federal Government to improve cybersecurity awareness of control systems operators. In addition, ICS-CERT provides free regional in person training and workshops as well as web based training targeted at facilities personnel [11] . ICS-CERT's training is comprised of both Web-based training and instructor led training. The Web-based training focuses on Operational Security for Control Systems and Cybersecurity for Industrial Control Systems (ICS). Instructor-led training comprises three courses:

- Introduction to Control Systems Cybersecurity
- Intermediate Cybersecurity for Industrial Control Systems
- ICS Cybersecurity

National Institutes of Standards and Technology's (NIST) Risk Management Framework (RMF). The 'NIST Risk Management Framework (RMF), which was created in response to the Federal Information Security Management Act (FISMA), requires federal agencies and develop, document and implement information security programs. The NIST RMF focuses on the selection and specification of security controls for information systems with the goal of managing risk to the organization and risk to the individual who perform a job role within the organization. The RMF also presents security standards and guidance for ICS. NIST has provided the following Workshops in line with its goal for ICS (as of July 2016, additional training and workshops were not currently planned):

- ICS Security Workshop
- NIST Workshop on Applying NIST Special Publication (SP) 800-53, Revision 2 to Industrial Control Systems (ICS)
- NIST Workshop on Applying NIST Special Publication 800-53, Revision 1:Recommended Security Controls for Federal Information Systems, to Industrial Control Systems.

5.4.2 Training Provided by Industrial and Commercial Entities

In addition to Government entities, JHU/APL reviewed the standards and training of private organizations, including:

- SCADAhacker: Cybersecurity for Critical Infrastructure Protection
- Global Information Security Certification
- National Institute of Building Sciences

SCADAhacker: Cybersecurity for Critical Infrastructure Protection. SCADAhacker.com provides information sharing and knowledge development for industrial security related to understanding and securing Supervisory Control and Data Acquisition (SCADA), Distributed Control (DCS) and ICS. SCADAHacker provides basic and introductory curriculum on assessments, penetration, security controls, and audits focused in ICS technologies (available at https://www.scadahacker.com/index.html).

Global Information Security Certification. GIAC (Global Information Association Certification) Information Security Certification identifies minimum standards needed for cybersecurity and information security professionals to perform their job. They provide professional certifications in Industrial Cybersecurity. GIAC collaborates with SANS Institute on an ICS/SCADA Security Essentials curriculum (available at https://www.sans.org/course/ics-scada-cyber-security-essentials#results). The curriculum provides an ICS Overview; a course on ICS Attack Surfaces; industry specific regulations on protection of CS systems; defense of CS servers and workstations; and ICS network defense.

National Institute of Building Sciences provides for the construction of safe, affordable structures for housing, commerce and industry in the United States. NIBS has recently developed an Introductory and Advanced curriculum for ICS and cybersecurity (available at http://www.nibs.org/). They also offer an advanced course that focuses on best practices for implementing cybersecurity throughout the facility lifecycle.

The International Society of Automation (ISA) is a nonprofit professional society that provides standards, training, and certifications for improving the management, safety, and cybersecurity of control systems and critical infrastructure. ISA offers four certificate programs for IT and control system security professionals which provides a combination of training and exams to ensure individuals have an awareness of ANSI/ISA 99 standards (https://www.isa.org/training-and-certifications/isa-certification/isa99iec-62443/isa99iec-62443-certificate-program-requirements/).

InfoSec Institute offers both training and certifications that target IT Professionals, Information Security Professionals, Control Systems Engineers, and SCADA System Operators. InfoSec' training focuses on educating students on best practices for security SCADA networks and systems, field-based attacks and how to defend networks against internal and external cyberattacks.

Finally, in 2015, the Idaho National Laboratory compiled a white paper comparing the training needed and available training to meet the demands of Control System Cybersecurity [10]. Their paper identified a set of skills relevant to cybersecurity engineering of ICS and identified training available to provide those skills where possible. Competencies were defined for each role and PAO, focusing most specifically on the PAOs and roles identified during the site visits. Available training and any gaps in training for each competency was assessed. Finally, JHU/APL associated the vulnerabilities identified during the site visits with each set of competencies to better determine whether gaps in training remain. The full table of Competencies by Vulnerabilities by Roles can be found in Appendix B. A subset pertaining to the vulnerabilities most frequently seen during the site assessments are discussed below as a function of 'what if' scenarios. This training consists primarily of two courses; the first is a 1-hour course, the second consists of 12 modules on different topics relevant to preventing cyber threats in CS/PIT. Based on an assessment of the curriculum, the 1-hour course is a good start for facility managers and the workforce, but is not sufficient by itself because it does not delve into details unique to the systems, components, and PAOs at each facility. The curriculum on identifying vulnerabilities and risks within a facility should be tailored to the facility to allow a facility manager or engineer to identify vulnerabilities similar to some of those that we saw, such as the presence of the

forgotten wireless Profile system in multiple buildings but might be sufficient to identify that WiFi was enabled in a building. If the ICS-CERT training course did trigger a facility manager to identify Profile or WiFi as a vulnerability, the course does not provide information to identify how to mitigate the threat (other than remove the vulnerable system). The curriculum of the 1-hour course does not address how to mitigate a vulnerability in a system for which there is not a valid alternative, such as using RF because there are few/no alternatives. The longer course is better for facility managers and engineers, but should still be supplemented by training on the particular components of the facility (or by creation of that hybrid IT/Operational Technology (OT) role who could support vulnerability assessment and mitigation of a particular facility). As with the 1-hour curriculum, the components that are specific or unique to a facility may not be discussed. With respect to the workforce beyond facility managers, the detail provided by the long course appears to go beyond what is needed by a SCADA system engineer or other non-facility manager. At the same time, these non-facility manager roles would benefit from training specific to their systems. Such tailored training should provide an overview of the components and connections within the OT, the known system and component vulnerabilities and mitigations, and discussion of risk assessment and encouragement of a questioning attitude with respect to system functioning and vulnerabilities.

The above is a representative, not exhaustive, list of the types of cybersecurity training, certifications, and resources available to facility engineering personnel. While not comprehensive, the resources represent the types of training and certifications available to facilities staff to attain the cybersecurity competencies specific to CS.

Consistent with the recommendations of US-CERT, JHU/APL also recommends that training should incorporate the importance of smart Internet browsing practices, and that all employees and vendors or contractors who interact with Government systems should be cautioned that visiting suspicious websites (and even legitimate websites via watering holes) may expose computers systems to malware embedded on the site. US-CERT provides the following training, which may be useful for facility management personnel:

- Avoiding Social Engineering and Phishing Attacks (US-CERT)
- Recognizing and Avoiding Email Scams (US-CERT)
- Securing Your Web Browser (US-CERT)
- Incident Handling: Preparing for Incident Response (ICS-CERT)

The US-CERT training, while useful does not focus on operational technology, and by itself leaves significant gaps in vulnerability assessment, prevention, and mitigation. We recommend that this training be supplemented as a function of workforce roles and responsibilities.

6. 'WHAT IF' SCENARIO EXAMPLES

A set of scenarios was created to use as the basis for training facility personnel. The purpose of the scenarios is to provide real world instances that can be used to allow facility personnel to assess vulnerabilities within their cyber physical systems. The set of scenarios listed in Tables 7 through 10 utilize examples from the top quartile of vulnerabilities defined as facility exploits for training of facility managers, engineers, and other roles. The scenarios describe vulnerabilities that could be exploited by a malicious actor. The scenarios address the most common and most critical vulnerabilities seen for the different roles and PAOs interviewed.

It is important to note that not all vulnerabilities identified in a scenario may be needed to impact the mission of the facility. In addition, not all vulnerabilities described in a scenario may have been found within a single facility; however, all vulnerabilities were observed at one or more facilities. The vulnerabilities are categorized within the scenario according to HFACS Cyber, and the mitigation(s) of the scenarios (as well as the questions for consideration) tie back to the classification.

For each scenario, a severity basis and rating was created. The rating system was based on the recently released United States Federal Cybersecurity Center Severity Rating Schema [11], which rates cyber risks on a scale of 0 (Baseline: unfounded or inconsequential) to 5 (Emergency: Imminent Threat), as a function of impact to public health and safety, national or public security, or confidence. It is difficult to rate a potential vulnerability independent of the systems on which the vulnerability is present. The vulnerabilities presented were found within sites, and the systems described in the vulnerabilities are similar to the systems known to be associated with the vulnerabilities seen. However, if the named vulnerabilities were present on other systems, severity could be increased or decreased. Due to the nature of the assessment process, it is possible that similar vulnerabilities were present on more critical systems but were not identified during this project.

Table 7. What if Scenario 1

What If Scenario 1: Disrupt Emergency Services by Jamming Dispatch			
Severity Basis: Potential impact to health and safety, potential loss of information Severity Rating: Medium			
Description	**Vulnerabilities Exploited**	**Roles Effected**	**Critical competency or gap**
Using an autodialer, a malicious actor ties up the 6 phone lines to emergency services dispatch – each call must be answered. In the building of interest, the malicious actor pulls the fire alarm. Physical security is notified of the fire alarm and assumes any intrusion alarms are people exiting the building. The jamming of phone lines delays the response of emergency services to the building of interest. The malicious actor uses the delay to access a closed area or a system (e.g., gas, fire suppression) that gives off significant 'false alarms.'	Organizational Cyber Awareness: communication and coordination between divisions: ICD and Security get different pieces of information but do not communicate. Technological Environment: Vulnerable systems – Emergency services has 1 active line, and 6 total; frequently gets robo-calls. Technological environment: un-integrated systems.	Emergency services Health & Safety (Public Affairs) IT services (Design) Physical Security	Identify system instability due to potential exploits; Familiarity with building systems, subsystems, sensors Demonstrate knowledge and ability to "design in" cybersecurity requirements during design of facilities and associated control systems Competency gap: Awareness of overlap in response to threats Competency gap: Ensure communication between threat responders (Emergency response, CID, Physical Security)
Training questions: • How do Physical Security, Emergency Services, and Cyber Intrusions Divisions communicate at your facility? • How do Physical Security, Emergency Services, and Cyber Intrusion Divisions coordinate response to secure facilities? • What tools are in place to allow Emergency services to maintain awareness of cyber-physical interactions? • What tools are in place to allow back up contact of emergency services? • If an emergency occurs at a classified facility, what actions occur automatically or what procedures are in place to guard against spillage? • How does Emergency services notify the facility if there is an issue with their dispatch system? How quickly does that information get shared? Which groups are notified?			
Mitigations: *Organizational Cyber Awareness:* Ensure coordinated information paths between groups both through personnel communications and technological integration. Ensure cybersecurity requirements as well as task based functional requirements are included in design. *Technological Environment:* Design in coordination as a functional requirement through awareness that a communications gap can yield a cyber gap.			

Table 8. What If Scenario 2

What If Scenario 2: Exploit of HVAC System via Maintenance Contractor			
Severity Basis: Potential Loss of physical systems, Potential risk to public health and safety (Low), potential risk to facility information Severity Rating: High			
Scenario	**Vulnerabilities Exploited**	**Roles Effected**	**Critical competency or gap**
Malicious actors hack the HVAC service vendor. Contractor is either allowed to use own equipment, or is ignorant of, forgets or ignores the policy to use facility supplied equipment because of a preference for their own equipment. Malicious software downloads into the facility servers. Objective of the attack is to take out a specific server by manipulating the temperature in the server room over a weekend. Malware allows malicious actor to watch & disseminate active times of the BAS (patterns of life at the facility). Would allow identification of long holiday weekend if needed. Malware could also migrate to Government systems that are attached and then attached to business systems (on different servers). The goal here would be to allow the malware to migrate to a building with critical HVAC systems (e.g., a medical or biological studies building).	Resource Management: Provide tools for situation awareness. Facility engineers lack ability to monitor energy usage, or do not have information on anomalies. Plan inappropriate action: Workarounds. Facility engineers sometimes remotely adjust HVAC ventilation settings rather than physically adjusting them (which creates problems in other areas). Organizational Cyber Awareness: Lack of awareness of risk. BAS vendors have remote access and administrative control to create new users and adjust systems. Vendors and contractors may bring their own equipment (at some locations) or are only prevented from using their own equipment by policy. Technological Environment: missing information; BAS not monitored 17:00 Friday to 05:00 Monday.	Facility Manager Facility Engineer IT Professional	Knowledge of physical and cybersecurity requirements for new systems, upgrades, modifications to existing systems . Ability to ensure cybersecurity requirements are appropriately addressed in UESC and ESPC projects. Ability to determine baseline energy consumption patterns and trends, and how to use that information to identify anomalies. Knowledge of how to respond to cyber threat alerts affecting EPSC systems. Gap: Tools for identification of anomalies; monitoring may not occur 24/7. Gap: Institutional knowledge of system installation and configuration management.

What If Scenario 2: Exploit of HVAC System via Maintenance Contractor			
Severity Basis: Potential Loss of physical systems, Potential risk to public health and safety (Low), potential risk to facility information Severity Rating: High			
Scenario	**Vulnerabilities Exploited**	**Roles Effected**	**Critical competency or gap**
Training Questions: • What policies are in place with respect to contractors' use of external equipment on facility systems? • What tools are in place to detect external systems in contact with facility equipment? • What tools are in place to allow monitoring of facility energy consumption and HVAC systems? How are anomalies detected? How is normal use identified? Who is notified of an anomaly and how? How reliable (prone to false alarms) is this system? • How are facility CS isolated from business systems? How is this segregation maintained? • What tools do facility operations personnel have that allow them to maintain awareness of the current configuration of the network? How often is network configuration assessed? • Do facility operations personnel have appropriate training to manage these systems? What training is needed to manage these system? • What support from IT personnel exist within the facility management to support these assessments?			
Mitigations *Resource management:* Provide tools to allow 24/7 monitoring of building automation and network traffic. *Technological Environment:* If it is not cost effective to monitor the building 24/7, alerts and summary statistics should be available on demand, preferably sent to print rather than stored. *Planned inappropriate Action/Workarounds:* Building monitoring systems should indicate when manual action versus logical actions have been taken on building performance and controls provided to discourage reliance on workarounds. *Organizational Awareness of Risk:* Contractors should be required to use facility provided equipment or equipment should be scanned at the beginning of each maintenance session.			

Table 9. What If Scenario 3

What If Scenario 3: Exploit of Unmanaged WiFi-Enabled Systems			
Severity Basis: Potential loss to utility systems, Potential loss to physical systems, potential risk to public health Severity Rating: Medium			
Scenario	**Vulnerabilities Exploited**	**Roles Effected**	**Critical competency or gap**
A WiFi-enabled system is installed with permission in several buildings at a facility for a project monitoring building lighting and HVAC. The system is forgotten, and while the data is no longer recorded, the system is still powered, still capable of broadcasting and receiving data. The system is forgotten, and a wireless control systems are installed to monitor and control BAS in the some buildings nearby. Malicious actor accesses the forgotten WiFi system in order to send bogus information to the nearby wireless BAS control system. BAS is used to drain the water tower, and close vents at the medical waste incineration facility. These two events trigger a general evacuation of the area.	Organizational Cyber Awareness: downplaying risk, lack of coordination between divisions, lack of awareness of risk. Profile 1900 system installed, operating, and forgotten in several buildings. IT and Facility management unaware of all locations or purpose.	Facility Managers IT and cybersecurity personnel	Familiarity with buildings, systems, subsystems, sensors, and other components. Gap: Institutional knowledge of systems, subsystems, and sensors. Demonstrate ability to develop subordinate plans for providing adequate information security for networks, facilities, information systems, or groups of information systems. Demonstrates knowledge and understanding of the potential cybersecurity vulnerabilities of the technology used to build and maintain "high performance buildings."
Training Questions: • How are new systems betted before they are inserted within the facility? • What tools exist to allow institutional awareness of the systems installed in the facility, their purpose, their capabilities, and who and how they can be accessed? • How are systems phased in and out? How is network configuration managed within the facility? • What tools exist for sharing of institutional knowledge when a person retires or leaves the facility? • What tools or training do facility manages have to allow them to identify potential interactions between wireless systems? What tools or training to facility managers receive to assist in identifying potential cyber vulnerabilities?			
Mitigations: *Organizational Cyber Awareness:* Increase personnel awareness of risk and personal responsibility for cybersecurity through training, interaction between IT and other divisions, and cultivating a questioning attitude. Provide tools to allow situation awareness into network architectures, and review periodically. Ensure integration between IT and facility operations, to allow for record keeping of systems installed within the facility and their capabilities.			

Table 10. Base Access by Unauthorized Personnel

Base Access by Unauthorized Personnel			
Severity basis: potential Access to facilities, potential impact to physical environment			
Scenario	**Vulnerabilities Exploited**	**Roles Effected**	**Critical competency or gap**
A duplicate CAC is obtained (or created) for an unauthorized user. If necessary, the bio chip is spoofed. At a facility where some gates are staffed with personnel with a handheld CAC reader and some gates have the integrated CAC readers, a person with the fraudulent CAC enters the facility at a gate with an integrated reader while at the same time the authorized user enters at the gate with the handheld reader. The use of the same CAC within a short time period will go unnoticed because the two systems update to different databases. If the attempt is made at a high traffic time, the flag could be buried in the text readout of authorized users.	Supervisor violation: cyber hygiene. Staff reported using 2 CAsC issued to the same individual for two weeks before 1 was deactivated (issue found because staff member was looking for vulnerabilities as part of his job). Technological Environment: Un-integrated systems. Possible to use 'same badge' at 2 places simultaneously to access Yard (card reader and human w/CAC reader go to different database, so no alert if doubled).	Physical Security, Security Managers IT Systems	Demonstrate knowledge of physical and cybersecurity requirements that must be included in procurement specifications for new systems and upgrading/modification specifications for existing systems. Demonstrate knowledge and ability to "design in" cybersecurity requirements during design of facilities and associated control systems.
Training Questions: • What tools exist to allow detection of use of duplicate CAC? • How are databases for tools with similar purposes coordinated? • With what timing are these databases coordinated? • How can physical barriers within the facility be exploited to allow access to cybersystems?			
Mitigations *Technological Environment:* Ensure there is not a conflict between cybersecurity and functional requirements by ensuring incorporation of facility operation needs in the design process When multiple systems are used for the same or similar tasks, ensure that information sharing occurs effectively (that there are not security gaps in to the sharing process) *Organizational Cyber Awareness:* When a security issue is found by personnel, the organization should put mitigations in place to close the vulnerability. In addition, provide recognition and positive feedback for the individual who finds the gap.			

7. MITIGATING CYBER WORKFORCE VULNERABILITIES

There are three primary types of mitigations that would address the majority of vulnerabilities observed. These encompass increasing Organizational Cyber Awareness, improving the technological environment primarily through integration of systems, and development of a hybrid OT/IT role within facilities. These mitigations all involve greater coordination and communication between IT and facility operations.

7.1 Organizational Cyber Awareness

Organizational Cyber Awareness (adapted from [9]) would be defined by a commitment to cybersecurity and hygiene in resource management, decisions and behaviors. This includes support for training and development of technology to support cyber situation awareness. Communication should be promoted between agencies and facility divisions. Integration of IT personnel with Facility Management and CS deployment would help ensure that issues potentially impacting cybersecurity are promptly identified, fully evaluated, and promptly addressed and corrected commensurate with their significance (Design-Basis Threat). Integration would improve information sharing of vulnerabilities and exploits between divisions. Integration of IT support would provide the resources to ensure that systems (and system configuration) are constantly assessed. IT integration with facility management would allow for better reduction of vulnerabilities in the development of tools, technologies and process that involve cybersystems. The purpose of integration of IT with facility management would be to demonstrate that all individuals take are responsible for the security of cybersystems. Integration of IT with facility engineering and management would provide for more cost effective identification of cyber risks.

Cybersecurity assessments require competencies to understand the purpose of various operational technology, and assess the network architecture. This in itself could be extremely time consuming. Facility managers are limited in their ability to maintain situation awareness of their network architecture both through training and lack of tools, while simultaneously being responsible for cybersecurity. Facility operations rely on IT staff for this information, but do not always have the resources to get the information that they need (or performance the maintenance and upgrades that are required, by some reports). Because IT and facility operations are separate, information is not easily accessed. As other groups have noted, hybrid training for operational technology (OT) and information technology (IT) is lacking. These gaps were especially apparent for non-electrical systems, for example, water SCADA systems. However, the amount of training suggested to maintain facility operations cybersecurity (as shown in Appendix B) would be time consuming.

Further complicating facility manager training needs is the long life of Operational Technologies. While older systems are typically considered to be more cyber secure than younger systems, simply because they cannot be accessed in the same ways, Operational Technology as it ages may yield more cyber issues in part because the workforce who have expertise on these systems (and knowledge of anomalies in their performance) are also retiring. As this workforce retires, information on the performance of the system is lost. In addition, Facility Managers are faced with the difficulty of finding replacement parts to maintain systems that are no longer supported by the manufacturer. In this case, facility managers may need to use hardware that has not been vetted for use. At the facility that had one of the strongest

cybersecurity stances, NSA would vet all new hardware that had not been previously assessed, but which was necessary for facility operations. In essence, they were acting as hybrid facility operations and IT specialists, providing knowledge and assessment that was not part of facility operations personnel competencies. Tailored training for facility managers or hybrid OT/IT engineers would need to address both assessing risks in new systems, and teach operations personnel how to identify known and unknown risks in aging systems.

7.2 Improving the Technological Environment

CS/PIT have very long life spans, and rather than being replaced, can be upgraded for decades. This presents a unique challenge in cybersecurity first because replacement parts can be difficult to obtain, and second software may cease to be supported. Compared to cybersecurity for IT, cybersecurity of OT is relatively young. The most common cyber defense has been the 'air gap' – physical separation of CS and IT servers and systems. The 'air gap' can be easily violated in any number of ways: USB transfer, vendor systems that intermittently connect to the Internet, or even network bridges and workarounds created by employees focused on their own tasks. Use of SHODAN can reveal to a malicious actor (or just the curious) tremendous numbers of systems that use standard CS protocols.

In addition, CS may support a much wider variety of missions than business based IT systems, and these missions require specialization and training in Operational Technologies by their operators. Some operators, such as Emergency Management Personnel, need access to facility controls in the course of their work. However, none of these groups have IT specialization. In many facilities, IT support is a separate division, and Control System security is not given the weight of business IT security because the vulnerabilities and their impacts are unknown. Cybersecurity training, policies, and tools have typically been developed with (the more common) business systems in mind. However, CS present unique challenges and security techniques applicable to business systems can be awkward to implement or not relevant to the exploits commencing on CS (see [15]).

In light of these issues and others, Horkan [16] and other experts recommend abandoning reliance on air-gaps, and replacing it with the concept of a connected floor plan that supports traditional security software, updates, security patches, and Intrusion Detection System/Intrusion Prevention System (IDS/IPS) alert rule updates. Horkan points out that vulnerabilities are more likely to be introduced through authorized activities of non-malicious users, often because they are not aware of the vulnerability or the threat. As Chipley [12] points out, the human element is as integral to the security of CS as are the cyber and engineered elements. JHU/APL's findings support this assessment.

7.3 Integrating Cybersecurity and Operations

In July 2016, Presidential Policy Directive/PPD-41, "United States Cyber Incident Coordination" [[7], [8]] was issued. It states that all individuals, private sector and Government agencies have shared complementary roles in prevent malicious cyber activity. To instill this shared responsibility, JHU/APL recommends developing and enhancing the Organizational Cyber Awareness at DoD facilities, to increase awareness and ability to respond to cyber acts. JHU/APL recommends integrating Information Technology support and personnel into CS and Facility Management in order to increase Organizational Cyber Awareness across DoD facilities. Integration of IT with Facility Management, especially during the upgrade and installation of BAS and CS will allow consideration of the human user as part of the system. The most common vulnerabilities seen during this assessment arose from a lack of awareness of risk, lack of knowledge of the cybersystem, or use of vulnerable technologies – in part because of the need to meet requirement not defined with BAS and CS in mind. In contrast, the most cybersecurity and positive effects identified arose from integration of IT as a service with Facility Engineering. These positive characteristics included:

- Backups are stored on portable HD; fire proof safe; locked room with limited access
- 4 layers of user privileges on CS systems
- Other services not available from CS control workstations (email, www, etc.), must go to other workstations
- Outside vendors are issued site credentials and site machines, not allowed to connect non-site computers to the network
- BAS is on its own VLAN
- Site security gateway segregates VLANs for machine-machine traffic from VLANs with human-machine traffic. The HMI traffic can be independently disabled if security posture dictates (leaving only machine-to-machine flows).
- GRASSMARLIN - IP address allocation from locally-routable pools only (no externally routable addresses observed)
- Human interaction based weaknesses with system were considered during the design of the building and BAS
- Procedure/regulation exists to allow external laptop to be attached to network -- procedure was known and followed
- Centralized system for awareness of performance monitored by multiple people simultaneously
- NSA evaluates major systems for vulnerabilities before integrating into building systems
- Building to building communication is discouraged but could not be prevented. All building systems are designed to talk to servers.
- Less secure hardware are typically installed behind more secure panels to avoid vulnerability

Integration of IT with CS and Facility management would provide the basis for the critical characteristics (as defined by NIST cited in [12]):

- Creation of reusable cyber physical systems (includes CS/PIT) components and tools to measure and evaluate their performance
- Communication across diverse stakeholder community
- A common lexicon and taxonomy that can apply across cyber physical systems
- Facilitate interoperability between components and systems

7.4 Recommendations

Based on the vulnerabilities seen, JHU/APL proposes the following recommended mitigations:

1. Instantiation of programs to increase Organizational Cyber Awareness. These programs would incorporate the following:
    a. Stress the importance of cybersecurity equivalent to the mission, task or PAO
    b. Resource management to allow greater integration and interaction of IT across all divisions of facility operations
    c. Cultivation of awareness of the connections between systems. Positive feedback for questions about system interactions
    d. Identification of critical systems, with an emphasis on identifying the interactions between cyber and physical system (in both directions)
2. Integration of IT cybersecurity with Facility engineering and the potential development of a hybrid cybersecurity/ Facility management role within DoD facilities.
    a. Use of this hybrid role for the assessment and closure of vulnerabilities within the technological environment
3. Tailored cybersecurity training for other-than-business cybersystems, tailored to the facility, the PAOs, CS/PIT systems and roles. This training should be developed as a supplement to the ICS-CERT 101 and 201 training. Facility management and engineers, energy operations roles, SCADA system engineers, and other roles which interact with critical systems should begin their training with the ICS-CERT 101 and 201 training, which is then supplemented with education on their unique systems.
    a. Development of hybrid training for facility operations/cybersecurity roles. This training should be tailored to address interactions between cyber-physical systems at the facility. This training should address the components, systems and PAOs at that facility. Known vulnerabilities should be addressed. More critically, this training should address assessment of risk, the need to appreciate the potential for exploitation of unknown vulnerabilities, and focus on the need to identify anomalous system performance. The training should include education on processes to engage IT should anomalous system behavior occur, and emphasize that identification of a vulnerability (or violation of a cybersecurity policy, e.g.,

use of external equipment by an external vendor) will yield positive feedback from the organization, similar to processes used by continuous improvement programs.

7.4.1 Cost Benefits

Integration of IT and Facility engineering will not be easy, and may receive significant push back from organizations. A recent SANS institute report indicated that the two roles most commonly responsible for control system cybersecurity are the system owner and the information security officer, indicating a new role for cybersecurity managers. They point out that training a person with an IT background to the management of control systems would require training, as would the operator or facility manager stepping into a cybersecurity role. However, cross training of this type would allow facility operators and security staff to collaborate lead to the creation of a hybrid role such as an Information and Control Security Officer (ICSO) or two individuals working together to fill a control security office. The SANS Institute began trending reports of breaches to SCADA and ICS systems in 2013 [17]. They report that within this time period, suspected security breaches rose 12%. Of the industry's assessed, 26.7% were certain they had a control system breach; only 9% were certain that they had not been breached. Of the 164 unique vulnerabilities identified in this assessment, roughly 1/3 were associated with a lack of Organizational Cyber Awareness, and the severity of these vulnerabilities ran from minor (lack of awareness of VOIP phones) to potentially severe (presence of an unrecorded, unmonitored, WiFi-enabled system in multiple buildings at a site). The cost of a failure to increase Organizational Cyber Awareness then could be as high as 14 breaches, leveraged by their severity.

With respect to training that is available, the ICS-CERT training is available on-line for free; therefore the cost of this training is primarily in the time cost to personnel. The ICS-CERT 101 cost of 1 hour per non-facility manager role per year is reasonable. As discussed previously, this training should be supplemented by education tailored to systems, components, and PAOs of the facility. The greatest cost will be in the development of this training at each facility. It may be possible to develop some of this training as common elements which are then modified to unique aspects of the facility. While the majority of competencies were associated with training sources, curriculum from universities would be expensive in terms of tuition and time cost (on average 9 hours per week for 13 weeks) for facility managers and engineers. However, personnel with an IT background would have completed this type of coursework. Therefore, the integration of IT with facility management could be a cost effective solution.

8. ACRONYMS / ABBREVIATIONS

BAS	Building Automation System
CAC	Common Access Card
COTS	Commercial Off-the-Shelf
CS	Control Systems
DCS	Distributed Control System
DFSPs	Defense Fuel Supply Points
DISA	Defense Information Systems Agency
DLA	Defense Logistics Agency
DoD	Department of Defense
EIS	Energy Information System
EMS	Emergency Management System
EnMS	Energy Management System
ESPC	Energy Savings Performance Contracting
FBPTA	The Federal Buildings Personnel Training Act 111-308
FE	Facility Engineer
FEM	Facility Energy Manager
FISMA	Federal Information Security Management Act
FM	Facility Manager
GISC	Global Information Security Certification
GSA	General Service Administration
HFACS	Human Factors Analysis and Classification System
HMI	Human Machine Interface
HRA	Human Reliability Analysis
HVAC	Heating, Ventilation and Air Conditioning
IC32E	Cybersecurity for Automation, Control, and SCADA Systems
ICS	Industrial Control System
ICS–CERT	Industrial Control Systems Cyber Emergency Response Team
ICSO	Information and Control Security Officer
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
ISA	International Society of Automation
IT	Information Technology
ITSD	Information Technology Security Division
JHU/APL	Johns Hopkins University Applied Physics Laboratory
KSA	Knowledge, Skills and Abilities
LOG	Logistics Manager

NEC	Network Enterprise Center
NIBS	National Institute of Building Sciences
NICCS	National Initiative for Cybersecurity Careers and Studies
NIST	National Institutes of Standards and Technology
OASD(EI&E)	The Office of the Assistant Secretary of Defense for Energy Installations & Environment
PAO	Processes, Activities, and Outcomes
PIT	Platform Information Technology
PLC	Programmable Logic Controller
RMF	Risk Management Framework
SaM	Safety Manager
SCADA	Supervisory Control and Data Acquisition
SeMs	Security Manager
SP	Special Publication
TTP	Tactics, Techniques and Procedures
UESC	Utility Energy Service Contract
VLAN	Virtual Local Area Network
WiFi	Wireless Fidelity

9. REFERENCES

[1] Reason, J. (1990). Human Error. Cambridge Press, pp. 320.

[2] Radichel, T. (2014). *Case Study: Critical Controls that Could Have Prevented Target Breach* GIAC (GSEC) Gold Certification. Available at https://www.sans.org/reading-room/whitepapers/casestudies/case-study-critical-controls-prevented-target-breach-35412

[3] Wiegmann, D. A., & Shappell, S. A. (2003). A human error approach to aviation accident analysis: The human factors analysis and classification system. Burlington, VT: Ashgate Publishing, Ltd.

[4] Shappell, S., & Wiegmann, D. (2000). The Human Factors Analysis and Classification System–HFACS. Prepared under DOT/FAA/AM-00/7U.S. Department of Transportation, Federal Aviation Administration. Available at https://www.nifc.gov/fireInfo/fireInfo_documents/humanfactors_classAnly.pdf

[5] Schmidt, J., Lawson, D., & Figlock, R. Human Factors Analysis & Classification System –Maintenance Extension (HFACS-ME) Review of Select NTSB Maintenance Mishaps: An Update. Available March 2016 at http://www.faa.gov/about/initiatives/maintenance_hf/library/documents/media/hfacs/ntsb_hfacs-me_updated_study_report.pdf

[6] Naval Safety Center School OF Aviation Safety. Human Factors Analysis & Classification System Maintenance Extension (HFACS-ME) – Student Guide. Available March 2016 at http://www.faa.gov/about/initiatives/maintenance_hf/library/documents/media/hfacs/studentguide.pdf

[7] Presidential Policy Directive/PPD-41. "United States Cyber Incident Coordination." Available July 2016 at https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber incident

[8] White House Cyber Incident Severity Scheme. Available July 2016 at http://www.ndia.org/Policy/policyweeklydigest/Documents/1Aug2016/Cyber_Incident_Severity.pdf

[9] Nuclear Regulatory Commission. Safety Culture Trait Talk. Available July 2016 at http://www.nrc.gov/docs/ML1506/ML15062A478.pdf

[10] Foster, R. & Price, J. (2015). Building Skills for Advanced Cybersecurity of Industrial Control Systems. White paper. White paper. Idaho National Laboratory.

[11] Training available through ICS-CERT. Available June 2016 at https://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT#need)

[12] Chipley, M. (2013). Cybersecurity. The Whole Building Design Guide. Available May 2016 at https://www.wbdg.org/resources/cybersecurity.php

[13] GAO-15-6. Federal Facility Cybersecurity: DHS and GSA Should Address Cyber Risk to Building and Access Control Systems Published: Dec 12, 2014. Publicly Released: Jan 12, 2015. Available at http://www.gao.gov/products/GAO-15-6

[14] IAEA. (2009). Development, Use and Maintenance of the Design Basis Threat. Vienna, Austria. Available July 2016 at http://www-pub.iaea.org/MTCD/publications/PDF/Pub1386_web.pdf

[15] Radichel, T. (2014). Critical Controls That Could Have Prevented the Target Breach. The SANS Institute. Available January 2016 at https://www.sans.org/reading-room/whitepapers/casestudies/case-study-critical-controls-prevented-target-breach-35412

[16] Horkan, M. (2015). Challenges for IDS/IPS Deployment in Industrial Control Systems. The SANS Institute. Available May 2016 at https://www.sans.org/reading-room/whitepapers/ICS/challenges-ids-ips-deployment-industrial-control-systems-36127

[17] Luallen. M. (2014). Breaches on the Rise in Control Systems: A SANS Survey. Available July 2016 at https://www.sans.org/reading-room/whitepapers/analyst/breaches-rise-control-systems-survey-34665

[18] National Initiative for Cybersecurity Careers and Studies. https://niccs.us-cert.gov/training/framework/competencies

[19] Department of the Navy (June 2016). Cyberspace Information Technology and Cybersecurity Workforce Management and Qualification Manual (SECNAV M-5239.2) Department of the Navy Chief Information Officer

APPENDIX A. TRAINING LIST FOR FACILITY MANAGERS AND FACILITY ENGINEERS

DoD Cyber Awareness Challenge and Digitally Signing Your AUP
Anti-Terrorism Level 1
Phishing
Portable Electronic Devices and Removable Storage
PKI Overview and Using PKI Certificates
Social Networking v. 1.0
Personal Identifiable Information
Human Trafficking
Accident Avoidance Course

APPENDIX B. COMPETENCIES BY VULNERABILITIES BY ROLES

B.1 COMPETENCY AREA: MANAGEMENT OF FACILITIES

Vulnerabilities	Competencies	Training Opportunities *Training not currently offered	Roles	NIST Cybersecurity Framework Unique Identifier
Single fiber runs from building to building creating single points of failure for each independent system that has its own run. There is WiFi in the plant but the operator could not remember how to turn it on/off. Staff were not aware of the purpose of the profile systems, the location of the systems, the capabilities of the systems. Power system in use is several decades old, to the point where few people have the knowledge to run it.	Demonstrate familiarity with building systems, subsystems, sensors and other components. GAP: Maintain configuration management of CS; maintain awareness of vulnerabilities to older systems (due to age); ensure workforce training and procedures for operation of critical equipment	ICS-CERT: Intro to Control Systems Cybersecurity NPS: CS Lab, CISR Lab, CS4558 Network Traffic Analysis USMA: Network Lab	Facility Managers Health and Safety	ID.AM ID.RA PR.MA
Profile wireless Systems P1900 Series (monitoring HVAC/Lighting) are installed in several buildings and appears to be operating. Staff	Demonstrate familiarity with condition and cybersecurity assessments for building systems. GAP: Maintain network	ICS - CERT: Intermediate Cybersecurity for Industrial Controls Systems, NPS: CS4678 Advanced Cyber Vulnerability Assessment, CS4679	Facility Managers Health and Safety	ID.AM ID.RA

Vulnerabilities	Competencies	Training Opportunities *Training not currently offered	Roles	NIST Cybersecurity Framework Unique Identifier
reported that Profile no longer performs wireless access of the units, but it is still possible to access the units wirelessly.	awareness; provide institutional knowledge of system purpose and architecture; Provide for identification of new vulnerabilities	Advances in Cyber Security Operations, Network Penetration Testing and Computer Networks CS 420 Data Communications ICS-CERT: ICS Cybersecurity Scadahacker: General ICS and Cybersecurity Training NPS: CS Lab, CISR Lab, CS4558 Network Traffic Analysis USMA: Network Lab		
Few written procedures for Facility Managers: reliance on personnel expertise (single point of failure) The hardware was not rated for the temperature of use. The facility had to use it anyway because there were no alternative	Demonstrate knowledge of procedures for maintaining authority to operate building systems within the NIST Risk Management Framework.	*NIST: Industrial Control Systems (ICS) Security Workshop	Facility Managers Health and Safety	PR.AT PR.IP
Response to alerts depends on authenticating responding personnel according to cellular ID or known voice. No explicit authorization protocol.	Demonstrate ability to work with Facilities Team to establish practices and procedures, including procedures for intercepting and responding to cyber threat alerts, and	Infosec Institute: Security Boot Camp, SANS: Defending ICS Servers and Workstations	Facility Managers Health and Safety	PR.AT PR.IP

Vulnerabilities	Competencies	Training Opportunities *Training not currently offered	Roles	NIST Cybersecurity Framework Unique Identifier
Repair personnel were not looking at the actual position of building ventilation settings; instead would use BAS to override setting remotely Communication problems were identified between IT and facilities”	application of system patches/updates. GAP: Establish procedures to minimize social engineering vulnerabilities	ICS-CERT: Intermediate Cybersecurity for ICS SANS: FOR508 Advanced Digital Forensics and Incident Response & MGT535 Incident Response Team Management CS4684 Cyber Security Incident Response and Recovery Tulsa: Malware Analysis and Creation		
Repair personnel were not looking at the actual position of building ventilation settings; instead would use BAS to override setting remotely Contractors are given gov’t login credentials and access to gov’t laptops/desktops for repairs and maintenance. Contractors prefer to use their own equipment	Demonstrate familiarity with governance (policy, ownership, vendor arrangements), terminology, and general function of facility control systems. GAP: Ensure external vendors and contractors follow cyber hygiene requirements	SANS GAIC: ICS Security Governance	Facility Managers Health and Safety	ID.AM
System is so complex that maintenance personnel cannot identify if an individual device is being tampered with	Demonstrate knowledge of how to respond to cyber incidents and alerts regarding threats to the cybersecurity of one or more facility control systems.	Infosec Institute: Security Boot Camp, SANS: Defending ICS Servers and Workstations SANS: FOR508 Advanced Digital Forensics and	Facility Managers Health and Safety	RS.AN RS.RP

Vulnerabilities	Competencies	Training Opportunities *Training not currently offered	Roles	NIST Cybersecurity Framework Unique Identifier
		Incident Response & MGT535 Incident Response Team Management NPS: 260 & 261 Cyber Security Adversarial Techniques Certificate, CS4684 Cyber Security Incident Response and Recovery Tulsa: Malware Analysis and Creation ICS-CERT: Intermediate Cybersecurity for ICS NPS: CS Lab, CISR Lab, CS4558 Network Traffic Analysis USMA: Network Lab		
Building Automation Systems only monitored 5am-5pm On night list, building had emergency access alarm going off all night, no one was able to shut off. Building was identified as visitor center security building. Building Automation Systems in different buildings are monitored based on a tiered approach based on	Demonstrate knowledge and ability to perform Continuous Monitoring of ICS PIT systems, identify system instability due to potential exploits and/or malware infection, implement cyber incident response, and recovery procedures. GAP: Ensure that monitoring policies allow for identification of anomalous behaviors during workforce down	isa.org: Cyber Security for Automation, Control and SCADA Systems (IC32E) NPS: CS Lab, CISR Lab, CS4558 Network Traffic Analysis USMA: Network Lab	Facility Managers Health and Safety	PR.PT PR.AT

Vulnerabilities	Competencies	Training Opportunities *Training not currently offered	Roles	NIST Cybersecurity Framework Unique Identifier
feedback from management	times			

B.2 COMPETENCY AREA: PERFORMANCE OF FACILITIES

Vulnerabilities	Competencies	Training Opportunities *Training not currently offered	Roles	NIST Cybersecurity Framework Unique Identifier
Can't identify where within a building an alarm occurs Every building on campus manages its own physical access controls but does not have access to view or manage ICIIDS alerts/notifications. Monitoring and control responsibilities do not overlap.	Demonstrate knowledge of Continuous Monitoring of ICS PIT systems. GAP: Provide for coordination of information from cyber systems	isa.org: Cyber Security for Automation, Control and SCADA Systems (IC32E) CS4558 Network Traffic Analysis USMA: Network Lab AFIT: ICS/SCADA laboratory ISU: EE 447 Digital Signal Processing NMT: CSE 452 Sensor Networks	Facility Engineers Logistics Personnel Security Personnel	PR.AC
Every building on campus manages its own physical access controls but does not have access to view or manage ICIIDS alerts/notifications. Monitoring and control responsibilities do not overlap. Operators know through experience and expertise which alarms to ignore Dwell alerts are used (high False Alarm rate)"	Demonstrate knowledge of what to do when a cybersecurity threat alert affecting one or more facility control systems is received. GAP: Provide policies and procedures for early response off normal conditions; minimize false alarms	ICS-CERT: Intermediate Cybersecurity for Industrial Control Systems InfoSec: SCADA/ICS Security Boot Camp Scadahacker: General ICS and Cybersecurity Training USMA: Programmable Logic (2 courses), Signal Processing & Control Systems Laboratory, Digital Computer Logic Laboratory ISU: EE 447 Digital Signal Processing NMT: CSE 452 Sensor Networks	Facility Engineers Logistics Personnel Security Personnel	RS.RP

Vulnerabilities	Competencies	Training Opportunities *Training not currently offered	Roles	NIST Cybersecurity Framework Unique Identifier
Wireless monitoring systems was installed in several buildings and appears to be operating. Staff reported that they no longer have wireless access of the units, but it is still possible to access the units wirelessly. System is so complex that maintenance personnel cannot identify if an individual device is being tampered with 94 buildings on base, 20 of which are centrally monitored by Powerlogic HVAC/BAS are not centrally monitored on base providing no SA or common control point	Demonstrate knowledge of normal operations of facility electrical and mechanical systems, and when (and to whom) to report abnormal operations. GAP: Provide for continuous assessment of normal and off-normal operations	ICS-CERT: Operational Security (OPSEC) for Control Systems *NIST: ICS Workshop May also be relevant: AFIT: Cyber Attack, ICS/SCADA Lab & Civil Engineering WTSS580 Managing Security of Control Systems UTSA: Security of cyber physical systems faculty research laboratory	Facility Engineers Logistics Personnel Security Personnel	ID.AM RS.CO DE.CM

B.3 COMPETENCY AREA: TECHNOLOGY

Vulnerabilities	Competencies	Training Opportunities *Training not currently offered	Roles	NIST Cybersecurity Framework Unique Identifier
EMS operators are aware of the vulnerabilities (as shown by the coast guard story) but they do not know how to protect their communications and do not see the need to protect their communication. They know that there are radio dead spots within the base -- at those points they use personnel electronic devices	Demonstrate ability to manage corrective, preventive, and predictive maintenance, including application of cybersecurity patches. GAP: Provide support for use of known vulnerable systems (when vulnerabilities cannot be avoided).	ICS-CERT: Intermediate Cybersecurity for Industrial Control Systems SANS: Defending ICS Servers and Workstations Infosec: Scada Security Online ISA.org: Cyber Security for Automation, Control and SCADA systems.	Facility Managers Health and Safety	PR.IP PR.MA
Kingfisher Emergency Response systems not integrated with CAD Emergency Dispatch Limited physical security on water facility system operations.	Demonstrate knowledge of physical and cybersecurity requirements that must be included in procurement specifications for new systems and upgrading/modification specifications for existing systems. GAP: Ensure for integration of systems during requirements specification	*No Training available May be addressed in part by: NPS: CS4678 Advanced Cyber Vulnerability Assessment, CS4679 Advances in Cyber Security Operations, CS4648 Advanced Cyber Munitions Tulsa: Software Reverse Engineering, Network Penetration Testing and Computer Networks AFIT: Cyber Attack,	Facility Managers Health and Safety	PR.MA PR.AT PR.PT

Vulnerabilities	Competencies	Training Opportunities *Training not currently offered	Roles	NIST Cybersecurity Framework Unique Identifier
		ICS/SCADA Lab & Civil Engineering WTSS580 Managing Security of Control Systems UTSA: Security of cyber physical systems faculty research laboratory		
Every building on campus manages its own physical access controls but does not have access to view or manage ICIIDS alerts/notifications. Monitoring and control responsiblities do not overlap. Response to alerts depends on authenticating responding personnel according to cellular ID or known voice. No explicit authorization protocol. ICS system in the research facility monitors hazardous gas leaks locally (isolated network) and relies on wireless (KF) system for reports to EMS.	Demonstrate understanding of how to respond to alerts regarding threats to cyber security. GAP: Maintain awareness and active, valued communication between workforce groups about on-going vulnerabilities and newly discovered threats	ICS-CERT: Intermediate Cybersecurity for Industrial Control Systems SANS: FOR508 Advanced Digital Forensics and Incident Response MGT535 Incident Response Team Management NPS: 260 & 261 Cyber Security Adversarial Techniques Certificate, CS4684 Cyber Security Incident Response and Recovery Tulsa: Malware Analysis and Creation InfoSec: SCADA/ICS Security Boot Camp Scadahacker: General ICS and Cybersecurity Training:	Facility Managers Health and Safety	RS.CO RS.RP RS.MI

B.4 COMPETENCY AREA: ENERGY MANAGEMENT

Vulnerabilities	Competencies	Training Opportunities *Training not currently offered	Roles	NIST Cybersecurity Framework Unique Identifier
Power system in use is several decades old, to the point where few people have the knowledge to run it.	Demonstrate knowledge of Energy Management Systems (EnMS) and Energy Information Systems (EIS), associated cybersecurity requirements, and identification of subsystems, sensors, and other component devices. GAP: Provide for identification of vulnerabilities as systems age or new systems are integrated	*No Training available Relevant to cybersecurity requirements of energy information systems: AFIT: Cyber Attack, ICS/SCADA Lab & Civil Engineering WTSS580 Managing Security of Control Systems UTSA: Security of cyber physical systems faculty research laboratory	Energy System Personnel	ID.AM ID.GV ID.RA
No way for workforce to identify anomalies in power usage. BAS Techs rely on automation and remote repair capabilities when repairs are needed. Will over ride default settings to adjust temperature, etc., as opposed to physically going to the room to troubleshoot the hardware problem.	Demonstrate knowledge of how to determine baseline energy consumption patterns and trends, and how to use that information to identify anomalies. GAP: Ensure that maintenance procedures or workarounds do not void anomaly detection	*No Training available Not directly focused on anomaly detection and baselining, but may be relevant: ICS/SCADA Lab & Civil Engineering WTSS580 Managing Security of Control Systems	Energy System Personnel	DE.AE DE.DP DE.CM

Vulnerabilities	Competencies	Training Opportunities *Training not currently offered	Roles	NIST Cybersecurity Framework Unique Identifier
Power utility has control of the microgrid by regulations No way for workforce to identify anomalies in power usage. BAS Techs rely on automation and remote repair capabilties when repairs are needed. Will over ride default settings to adjust temperature etc as opposed to physically going to the room to troubleshoot the hardware problem. “	Demonstrate knowledge of the Energy Savings Performance Contracting (ESPC) procedures and requirements, including how to respond to cyber threat alerts affecting EPSC systems, subsystems, sensors, and other component devices. GAP: Ensure that regulations do not engender cybersecurity gaps.	*No Training available	Energy System Personnel	RS.MI RS.IM ID.RM
Wireless monitoring systems was installed in several buildings and appears to be operating. Staff reported that they no longer have wireless access of the units, but it is still possible to access the units wirelessly	Demonstrate knowledge of utility meters – location, reading, cybersecurity requirements, and data management.	*No Training available	Energy System Personnel	ID.AM

Vulnerabilities	Competencies	Training Opportunities *Training not currently offered	Roles	NIST Cybersecurity Framework Unique Identifier
Electric utility has control of microgrid at times because of regulation	Demonstrate knowledge and ability to ensure cybersecurity requirements are appropriately addressed in Utility Energy Service Contract (UESC) and ESPC projects. GAP: Ensure conflicting or competing regulations do not create vulnerabilities in cyber physical systems	*No Training available	Energy System Personnel	ID.RM ID.GV

B.5 COMPETENCY AREA: SAFETY

Vulnerabilities	Competencies	Training Opportunities *Training not currently offered	Roles	
Unencrypted LMR is used for mission-critical coordination between all EMS. Poor communication between groups. ICD and Security groups don't talk but each get different pieces of information. Public affairs failed to send out message regarding down e911 system	Demonstrates knowledge and ability to ensure cybersecurity requirements are established and standard operating procedures are in place for the operation of control systems, water treatment, ventilation systems and fire prevention systems.	isa.org: Cyber Security for Automation, Control and SCADA Systems infosec: SCADA/ICS Security Boot Camp WTSS580 Managing Security of Control Systems UTSA: Security of cyber physical systems faculty research laboratory	Facility Operations Physical Security	ID.GV ID.RA PR.AT PR.IP

B.6 COMPETENCY AREA: DESIGN

Vulnerabilities	Competencies	Training Opportunities *Training not currently offered	Roles	NIST Cybersecurity Framework Unique Identifier
Kingfisher and CAD are not integrated Tokens were required for login to prevent simultaneous logins; however, simultaneous logins were required to optimize performance Positive: Operations center was designed with human operations considered Positive: CAC authentication required Positive: Building to building communication is discouraged but could not be prevented. All building systems are designed to talk to servers.	Demonstrate knowledge and ability to "design in" cybersecurity requirements during design of facilities and associated control systems. GAP: Ensure cybersecurity in design does not impact ability to perform work.	NIBS: Cybersecuring DoD Control Systems Workshop AFIT: Cyber Attack, ICS/SCADA Lab & Civil Engineering WTSS580 Managing Security of Control Systems UTSA: Security of cyber physical systems faculty research laboratory NPS: CS4678 Advanced Cyber Vulnerability Assessment, CS4679 Advances in Cyber Security Operations, CS4648 Advanced Cyber Munitions Tulsa: Software Reverse Engineering, Network Penetration Testing and Computer Networks CS3030 Computing Architecture and Operating Systems, Software Engineering and Architecture, and Information Security Systems Engineering (ISSE)	Facility Managers Health and Safety	ID.RM

B.7 COMPETENCY AREA: SUSTAINABILITY

Vulnerabilities	Competencies	Training Opportunities *Training not currently offered	Roles	NIST Cybersecurity Framework Unique Identifier
Repair personnel were not looking at the actual position of building ventilation settings; instead would use BAS to override setting remotely (short term problem solved but not long term).	Demonstrates knowledge of cybersecurity requirements as it relates to "high performance buildings" that integrates and optimizes all major high-performance building attributes, including energy efficiency, durability, life-cycle performance, and occupant productivity. (The Energy Independence and Security Act (EISA) of 2007.)	*No Training available Not focused on 'high performance buildings' but may be relevant: AFIT: Cyber Attack, ICS/SCADA Lab & Civil Engineering WTSS580 Managing Security of Control Systems UTSA: Security of cyber physical systems faculty research laboratory	Environmental Services	ID.RM ID.RA ID.GV
Have lighting controls for one building connected to the HVAC network	Demonstrates knowledge and understanding of the potential cybersecurity vulnerabilities of the technology used to build and maintain "high performance buildings."	*No Training available Not directly focused on "high performance buildings" but may be relevant: AFIT: Cyber Attack, ICS/SCADA Lab & Civil Engineering WTSS580 Managing Security of Control Systems UTSA: Security of cyber physical systems faculty research laboratory NPS: RES 261 Cyber	Environmental Services	ID.RM ID.RA. ID.GV

Vulnerabilities	Competencies	Training Opportunities *Training not currently offered	Roles	NIST Cybersecurity Framework Unique Identifier
		Security Adversarial Techniques Certificate, CS3030 Computing Architecture and Operating Systems, UI: CS451 Advanced Computer Architecture NPS: CS4678 Advanced Cyber Vulnerability Assessment, CS4679 Advances in Cyber Security Operations, CS4558 Network Traffic Analysis & CS4648 Advanced Cyber Munitions USMA: Information Warfare Analysis Research Laboratory (IWAR) Network Penetration Testing and Computer Networks		

B.8 COMPETENCY AREA: WATER EFFICIENCY

Vulnerabilities	Competencies	Training Opportunities *Training not currently offered	Roles	NIST Cybersecurity Framework Unique Identifier
	Demonstrate knowledge of Utility Energy Service Contract (UESC) cybersecurity procedures and requirements.	*No Training available	Environmental Services	PR.AT
	Demonstrate knowledge of how to respond to cyber threat alerts affecting systems, subsystems, sensors, and other component of a water system, including those provided through privatization or a UESC.	*No Training available	Environmental Services	RS.RP
Water pumps on RF channels	Demonstrate knowledge and ability to identify water consumption trends, baselines, and ability to identify significant water consumption considering operational requirements. GAP: Ability to identify anomalies in usage and trace to cyber activity	*No Training available	Environmental Services	RS.AN
	Demonstrate knowledge of utility meters – location, reading, cybersecurity requirements, and data management. GAP: Identify cyber physical system interactions	*No Training available Some cybersecurity requirements may be derived from: AFIT: Cyber Attack, ICS/SCADA Lab & Civil Engineering WTSS580 Managing Security of Control Systems	Environmental Services	ID.AM

Vulnerabilities	Competencies	Training Opportunities *Training not currently offered	Roles	NIST Cybersecurity Framework Unique Identifier
		UTSA: Security of cyber physical systems faculty research laboratory		

B.9 COMPETENCY AREA: PROJECT MANAGEMENT

Vulnerabilities	Competencies	Training Opportunities *Training not currently offered	Roles	NIST Cybersecurity Framework Unique Identifier
	If Project will be completed by contractors, demonstrate the ability to provide technical support to the organization's procurement process and incorporate cybersecurity requirements and energy and sustainability goals.	NIBS: Cybersecuring DoD Control Systems Workshop	Facility Managers	ID.GV PR.IP

B.10 COMPETENCY AREA: BUSINESS, BUDGET AND CONTRACTING

Vulnerabilities	Competencies	Training Opportunities *Training not currently offered	Roles	NIST Cybersecurity Framework Unique Identifier
.	Demonstrate ability to identify and include technical requirements needed to procure components with appropriate cybersecurity controls and capabilities to ensure the mission of the asset(s).	NIBS: Cybersecuring DoD Control Systems Workshop	Facility Managers, Health and Safety	ID.AM PR.MA
Disconnect of information passing between systems ANI/ALI automated data transfer from base phone system to Intergraph CAD is inconsistent and incomplete.	Demonstrate ability to assess technical requirements needed to ensure delivery, cybersecurity, and quality of services/products.	*No Training available	Facility Managers, Health and Safety	ID.RA
	Demonstrate ability to identify new costs and risks such as those from emerging cybersecurity requirements, and how to use in forecasting.	*No Training available	Facility Managers, Health and Safety	ID.GV

B.11 COMPETENCY AREA: LEADERSHIP AND INNOVATION

Vulnerabilities	Competencies	Training Opportunities *Training not currently offered	Roles	NIST Cybersecurity Framework Unique Identifier
CIDS and Physical Security do not share information. Both get different pieces of alerts and do not share Emergency Services Fire and Police TMS are managed independently. And don't talk well(?)	Demonstrate ability to receive, communicate, and respond to cybersecurity alerts affecting facility systems, sub-systems, sensors, and other components necessary for continuity of operations.	Infosec Institute: Security Boot Camp, SANS: Defending ICS Servers and Workstations ICS-CERT: Intermediate Cybersecurity for ICS NPS: CS Lab, CISR Lab, CS4558 Network Traffic Analysis USMA: Network Lab	Facility Managers	PR.AT RS.CO

B.12 COMPETENCY AREA: MANAGEMENT OF CYBERSECURITY FOR CRITICAL FACILITY SYSTEMS

Vulnerabilities	Competencies	Training Opportunities *Training not currently offered	Roles	NIST Cybersecurity Framework Unique Identifier
Public relations would not send out the notification of 911 down and to call new numbers Large SCIFs on base require fire alarms/PA/etc. that create SCIF penetration challenges for EMS. ICIIDS monitoring stations monitor live sensor feeds (door ajar, etc.) from inside SCIFs. There is a heavy reliance on external physical access controls, without understanding of how those controls could fail.	Demonstrate knowledge and ability to identify Critical Systems - those information systems, building automation systems, facility control systems, and communications systems that need to be maintained for operation of the facility, so that these systems can be secured. GAP: Ability to identify cyber connections to critical physical systems; ability to identify physical impacts of minor systems on critical cyber systems	ICS - CERT: Intermediate Cybersecurity for Industrial Controls Systems NPS: RES 261 Cyber Security Adversarial Techniques Certificate, CS3030 Computing Architecture and Operating Systems, Software Engineering and Architecture, and Information Security Systems Engineering (ISSE) USMA: Computer Architecture UI: CS451 Advanced Computer Architecture ISA.org: Cyber Security for Automation, Control and SCADA Systems NPS: 260 & 261 Cyber Security Adversarial Techniques Certificate, Tulsa: Malware Analysis and Creation AFIT: Cyber Attack, ICS/SCADA Lab & Civil Engineering WTSS580 Managing Security of	Facility Managers, Health and Safety	ID.AM ID.RA ID.RM

Vulnerabilities	Competencies	Training Opportunities *Training not currently offered	Roles	NIST Cybersecurity Framework Unique Identifier
		Control Systems UTSA: Security of cyber physical systems faculty research laboratory		
Unlocked touch screen display observed in water tower control room (unmanned room, key based access, might be possible to access through outside panel) Remote access is available for a system that control burner settings.	Demonstrate ability to conduct periodic assessments of risk, including the magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the organization. GAP: Ability to update vulnerabilities and identify changes in vulnerabilities	isa.org: Cyber Security for Automation, Control and SCADA Systems NPS: CS4678 Advanced Cyber Vulnerability Assessment, CS4679 Advances in Cyber Security Operations, CS4648 Advanced Cyber Munitions USMA: Information Warfare Analysis Research Laboratory (IWAR) Network Penetration Testing and Computer Networks ICS-CERT Cyber Security Industrial Control Systems SANS: FOR508 Advanced Digital Forensics and Incident Response & NPS: 260 & 261 Cyber Security Adversarial Techniques Certificate, Tulsa: Malware Analysis and Creation		ID.RA PR.AT PR.AC PR.PT

Vulnerabilities	Competencies	Training Opportunities *Training not currently offered	Roles	NIST Cybersecurity Framework Unique Identifier
The network has not been tested to ensure that it is actually closed.	Demonstrate ability to implement policies and procedures that are based on risk assessments, cost-effectively reduce information security risks to an acceptable level, and ensure that information security is addressed throughout the life cycle of each organizational information system.	NIBS: Cybersecuring DoD Control Systems Workshop ICS CERT: Intro to Control Systems Cybersecurity		PR.IP RS.RP RS.AN
Over reliance on expertise rather than procedures	Demonstrate ability to develop subordinate plans for providing adequate information security for networks, facilities, information systems, or groups of information systems, as appropriate.	NIBS: Advanced Cybersecuring DoD Control Systems Workshop ISA.org: Cyber Secuiry for Automation, Control and SCADA systems		PR.IP
Cabinets and storage locked to connection points but wires run out of closets Majority of roles interviewed received cybersecurity training focused on business systems, not relevant to the types of OT the were using.	Demonstrate ability to deliver security awareness training to inform personnel (including contractors and other users of information systems that support the operations and assets of the organization) of the information security risks associated with their activities and their responsibilities in complying with organizational policies and	ICS - CERT:Intro to Control System Cybersecurity ICS - CERT:Intermediate Cybersecurity for Industrial Controls Systems, ICS-CERT ICS Cybersecurity ISA.org: Cyber Security of Automation, Control and		PR.IP RS.CO RC.CO

Vulnerabilities	Competencies	Training Opportunities *Training not currently offered	Roles	NIST Cybersecurity Framework Unique Identifier
	procedures designed to reduce these risks. GAP: Identify limitations in training	SCADA Systems		
Staff reported using 2 CACs issued to the same individual for two or more weeks before 1 was deactivated	Demonstrate ability to conduct periodic testing and evaluation of the effectiveness of information security policies, procedures, practices, and security controls to be performed with a frequency depending on risk, but no less than annually.	*No Training available		ID.RA ID.RM
Staff reported using 2 CACs issued to the same individual for two or more weeks before 1 was deactivated Illegal or unregistered software in use Common Passwords in use 4 separate observations of login/passwords visually displayed within proximity of workstations (3 of 4 were for cyber connected systems).	Demonstrate ability to implement a process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in the information security policies, procedures, and practices of the organization. GAP: Develop process to identify remedial technology and cyber systems	*No Training available However, CS4684 Cyber Security Incident Response and Recovery may cover some aspects		ID.RA ID.RM

Vulnerabilities	Competencies	Training Opportunities *Training not currently offered	Roles	NIST Cybersecurity Framework Unique Identifier
Lack of procedures	GAP: Demonstrate ability to implement procedures for detecting, reporting, and responding to cybersecurity incidents.	ICS - CERT: Intermediate Cybersecurity for Industrial Controls Systems ICS - CERT: ICS Cybersecurity Scadahacker: General ICS and Cybersecurity Training SANS: FOR508 Advanced Digital Forensics and Incident Response & MGT535 Incident Response Team Management NPS: 260 & 261 Cyber Security Adversarial Techniques Certificate, CS4684 Cyber Security Incident Response and Recovery Tulsa: Malware Analysis and Creation		PR.IP
Experienced workforce running power distribution is retiring (4 within the last 6 months) and there is limited knowledge management process/procedures in place to capture knowledge Over reliance on expertise	Demonstrate ability to execute plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the organization.	NIBS: Cybersecuring DoD Control Systems Workshop ICS-CERT: ICS Cybersecurity		RS.RP RS.COM RS.MI

Vulnerabilities	Competencies	Training Opportunities *Training not currently offered	Roles	NIST Cybersecurity Framework Unique Identifier
EMS was using personal devices for scene analysis -- pictures via business email or sneaker net to isolated computers (after scanning) Contractors prefer to use own equipment (stopped by policy)	Demonstrate ability to ensure contractors comply with cybersecurity requirements for information systems and control systems (building systems), and connect NO systems to facility communications networks without prior cyber risk assessment and authorization.	NIBS: Cybersecuring DoD Control Systems Workshop NPS: RES 261 Cyber Security Adversarial Techniques Certificate, CS3030 Computing Architecture and Operating Systems, Software Engineering and Architecture, and Information Security Systems Engineering (ISSE) USMA: Computer Architecture UI: CS451 Advanced Computer Architecture		PR.IP PR.PT

Vulnerabilities	Competencies	Training Opportunities *Training not currently offered	Roles	NIST Cybersecurity Framework Unique Identifier
	Demonstrate ability to ensure tenants comply with cybersecurity requirements for information and control systems (building systems), and interconnections with facility communications networks.	NIBS: Cybersecuring DoD Control Systems Workshop ISU: EE 447 Digital Signal Processing NMT: CSE 452 Sensor Networks isa.org: Cybersecurity for automation, control and SCADA systems. NPS: RES 261 Cyber Security Adversarial Techniques Certificate, CS3030 Computing Architecture and Operating Systems, Software Engineering and Architecture, and Information Security Systems Engineering (ISSE) USMA: Computer Architecture UI: CS451 Advanced Computer Architecture		PR.IP PR.PT