DISSERTATION

MEASURING DISAGREEMENT IN SEGMENTS OF THE CYBERSECURITY PROFESSION AS A MEANS OF IDENTIFYING VULNERABILITIES

Submitted by

Aleksandra Scalco

Department of Systems Engineering

In partial fulfillment of the requirements

For the Degree of Doctor of Philosophy

Colorado State University

Fort Collins, Colorado

Spring 2022

Doctoral Committee:

Advisor: Steven J. Simske

James Cale
Daniel Herber
Bryan J. Dik

ABSTRACT

MEASURING DISAGREEMENT IN SEGMENTS OF THE CYBERSECURITY PROFESSION AS A MEANS OF IDENTIFYING VULNERABILITIES

Disagreement exists among different groups of professionals about remediation of control system vulnerability due to discrepancies in engineering practice, paradigms, processes, and culture. Quantification of agreement among professionals is needed to increase understanding of areas where divergence arises. This need to quantify agreement is particularly among control system Operational Technology (OT) and business enterprise Information Technology (IT) professions. The control system OT workforce does not fully understand the relative vulnerability of each element of its system. Likewise, the business enterprise IT workforce does not widely understand control system assets that control critical infrastructure to achieve cybersecurity assurance. This disagreement among professionals leads to misalignment, which results in vulnerability. Similarly, known vulnerability can inform alignment and bring about agreement among professionals. The exposure induced by misalignment may be greater than innate system design vulnerability. This research introduces an analytical model and methodology for measuring multi-concern assurance among different groups of professions through the statistical uncertainty analysis of Likert and semantic differential scales used for interpreting the scores to identify specific areas of vulnerability.

ACKNOWLEDGEMENTS

I am indebted to my husband, Salvatore "Rich" Scalco, without whom this journey would have been much more challenging. As a former Senior Executive Service (SES) technical leader with the National Security Agency (NSA) and former director of the Global Information Assurance Program (GIAP) responsible for the Department of Defense (DOD)'s $3 Billion IA budget, Rich shared his insights about introducing new technology to field operations and sacrificed many hours of family time while I researched this dissertation subject. I thank my mother, Gisela Wiszynski, who believed in me. I extend my appreciation and gratitude to my dissertation advisor Steve Simske for his expertise and generous support of this work. My most sincere appreciation to the Colorado State University Systems Engineering Department faculty and staff, to name but a few (alphabetically): Jim Adams, Ann Batchelor, Thomas Bradley, Ingrid Bridge, James Cale, Chrissy Charny, Dan Herber, Greg ("Bo") Marzolf, Katharyn Peterman, and Teaching Assistants (TA) Harshwardhan Ketkale, Jayesh Narsinghani, and Angie Robinson. What a terrific department to be a part of – Everyone's constant encouragement, shared interest, and advice helped support critical thinking and continuous consideration of perspectives. A piece of your combined wisdom is in this research. Thank you to the Institute of Electrical and Electronics Engineers (IEEE) and International Council on Systems Engineering (INCOSE) Technical Leadership Institute (TLI), coaches, mentors, and colleagues committed to championing the practice of engineering. A special thank you, to name but a few (alphabetically): Patrick Arvidson, Chris Cleary, Michael Dransfield, Dan Ermer, Dave Flanagan, Dave Ford, Mark Hadley, Daryl R. Haegley, Michael Kilcoyne, Sandra Kline, Michael McCarty, Terry Merz, Harley Parkes, Maureen Raley, William F. Reyers, Craig Rieger, Ross Roley, Capt. Wesley S. Sanders (Ret.), William Waugaman, Keith Willett, Neal Ziring, and many others.

PREFACE

This dissertation introduces a mathematical model and methodology to measure disagreement in segments of the cybersecurity profession to identify vulnerabilities through statistical uncertainty analysis of Likert and semantic differential scales. We know that if people disagree on certainty about cybersecurity in the field, that is a source of vulnerability. We also know that people's degrees of attitudes and opinions vary, which is also a source of vulnerability. Therefore, we want to test the hypothesis that there is disagreement among different professionals about cybersecurity, leading to misalignment and vulnerability. A survey tool is used to test the hypothesis. The survey analysis and correlations with other studies about exposure lead to recommendations to address these vulnerabilities.

For example, the cyberattack on the Oldsmar, Florida water treatment facility highlighted the vulnerability of control systems that often use legacy software and hardware and personnel who reuse and share passwords to access network systems. Responsibility for cybersecurity concerns the technology that plays a role and the people interacting with the technology. "This also requires policies to be in place, and that people understand what is required, as we know that unawareness on the part of users can introduce further vulnerabilities; for example, by using weak passwords, installing untrustworthy software, and using insecure devices and applications." (Hans de Bruijn). The continued use of old, unsupported operating systems that contain well-known vulnerabilities means that even if control systems are perceived not internet-facing, they can still be easy targets. That there is vulnerability is already well established. In December 2015, a publicly acknowledged cyberattack on the power system in Ukraine cut electricity to a population of nearly a quarter-million people. (Dubova).

Operators could not regain remote control of more than 50 substations and sent technicians to the substations to take control manually. A further complication was a simultaneous Denial of Service (DoS) attack overloading the utility telephone systems and remotely disabling the control center's Uninterruptible Power Supplies (UPS). (David E. Whitehead). Post analysis concluded that the malicious actors used harvested credentials to access Supervisory Control and Data Acquisition (SCADA) Human-Machine Interface (HMI) servers and substations. (David E. Whitehead). Is it possible to go further? Are there different types of exposure other than brute force attacks on stored passwords or standard remote access tools to access a control system network? Measuring disagreement in segments of the cybersecurity profession can identify different vulnerability types. Evidence-based framing strategies about cybersecurity are needed to communicate a complex problem to avoid misunderstanding and ambiguity. (Hans de Bruijn).

The control system industry is changing fast due to technological changes such as "digitalization" and "automation." This change drives the transformation of context-sensitive critical infrastructure control system dynamic classes. These systems are "*context-sensitive*" as the system variables include the view of the system designer, operator, technician, and the corporate board of governance members; the critical infrastructure sector; the system layer in the architecture; system governance and policies; and system mission. The "*dynamic classes*" set is dynamically classified at the time of operation rather than a static set of classes. There is no compass for "Context-sensitive Critical Infrastructure Dynamic Classes" characterized in a meaningful way while best practices, guidance, standards, and policy "catch up." Responsibilities are distributed across commercial and government entities and diverse stakeholders at federal and local levels. (Hans de Bruijn). Approaches differ by sector (e.g., chemical, government facilities); sub-sector (e.g., education facilities, event facilities); as well as by segment (e.g., government,

commercial). (A. Scalco and S. Simske "Engineering and Development of a Critical Infrastructure Cyber Defense Capability for Highly Context-Sensitive Dynamic Classes — Part 2, Development").

These differences represent transitions that can be confusing and stressful to personnel who operate these systems. Professionals have varying interests, levels of knowledge, and experience. Therefore, it is necessary to ensure the problem is relevant to professionals in their immediate environment so urgent cybersecurity needs are recognized. (Hans de Bruijn).

Professionals and decision-makers tend to be selective to messages and react differently to relevantly equivalent descriptions of the same problem. (Irwin P.Levin). Research shows framing variables affect behaviors such as risk preferences (i.e., choices for risky options), evaluations, and consequences. (Irwin P.Levin). While framing does not rely on risk, it helps understand it for tradeoff discussions necessary for setting priorities. Better cybersecurity requires understanding from multiple disciplines (e.g., computer science, psychology, engineering, organizational behavior, law). It is easy for people to get lost in the technical details even though the problem is as much a nontechnical issue as a technical one. (David Clark). Further, IT capability is, for the most part, created, owned, and operated by the commercial sector, while the public policy perspective is that the government is responsible for controlling system security. (David Clark). Disagreement about investment decisions being the responsibility of the commercial sector or the government is central to cybersecurity policy. "Decision-making under conditions of high uncertainty will almost surely characterize U.S. policymakers responding to the first reports of a significant cyber incident," (David Clark).

The cyber domain is a driver of change for control systems and the careers of those who operate these systems and bring risks. The technological revolution in these sectors can contribute

to the uncertainty of agreement among professionals about asset management and the knowledge, skills, and abilities (KSA) to thrive in changing circumstances. However, how cyber domain challenges are framed is not clearly understood. Cybersecurity requires humans to maintain and update systems. It is difficult to explain and requires policies that people can easily understand. "Cybersecurity has been the domain of specialists and experts who are not trained to communicate about the issues". (Hans de Bruijn). Understanding uncertainty can assist in building the adaptability of professionals, supporting organizational preparedness for the future, and remediating critical infrastructure vulnerability. A key to thriving in a changing world is career adaptability, which refers to adapting to change. (Dik). Industry and career changes can lead to tension and disagreement, which leads to misalignment that leads to vulnerability. "If you don't address the people issues, you're missing the really hard cybersecurity problems. A lot of vulnerabilities that exist in organizations come from the corporate culture we create and practices we have." (Madnick).

Vulnerability induced by misalignment may be greater than innate system design vulnerability. Estimates are that insiders abetted up to 80 percent of all cyberattacks unintentionally. For example, a targeted spear-phishing involving emails containing a link or attachment to open have an open rate of 70 percent. (Madnick). Malware found on the affected Ukrainian utility networks in 2015 that was part of the overall attack plan was infiltrated via such a targeted spear-phishing involving an infected email attachment. (Pultarova). Therefore there is a need to evaluate cyber situational awareness from a human perspective due to the dynamic environment. (Akwetey Henry Matey). Studies show cyber incidents are often a result of employee mistakes and misunderstanding control system information from coordinated attacks on power sector infrastructure. (Akwetey Henry Matey). Measuring disagreement in segments of the

cybersecurity profession is used to identify vulnerabilities. Disagreement exists among professionals due to variances in engineering practice, paradigms, processes, and culture. The most poignant difference is cybersecurity knowledge between IT and OT personnel. (Terry Merz). Understanding the whole picture and what can be done to improve things is a continuous science and engineering challenge. This challenge holds particularly true for systems that control the physical world, such as power systems. Cybersecurity challenges are increasing and becoming more sophisticated and alarming than people think in the power generation sector. (Akwetey Henry Matey). Disagreement produces misalignment, leading to vulnerability. "The assumption that appropriate network cybersecurity can solve the problem has been challenged by two recent issues—one from Russia and another from China—to the point that relying on network cybersecurity alone should now be recognized as a fatal flaw." (Weiss, Stephens and Miller). However, it is possible to measure the uncertainty of agreement through statistical analysis and an analytical model to identify pain points where different stakeholders disagree. The same measure can be walked back to stakeholder sources beginning with a vulnerability assessment to help drive better alignment and, eventually, agreement. It is the disagreement that ends up in vulnerability.

This research describes an analytic model and methodology as a new means of assessing uncertainty and interpreting Likert scores to overcome control system cybersecurity vulnerability. A mathematical model and analytical methodology are used to measure disagreement in segments of the cybersecurity professions to identify vulnerabilities through statistical uncertainty analysis of Likert and semantic differential scales. This model allows the systems engineer to put the finger on where there may be disagreement, which leads to misalignments and vulnerability and walk that back through the model from exposure to alignment to agreement. The analytic approach shows correlation to the agreement, and then lack of agreement is vulnerability.

Control system cybersecurity is poorly understood for process control equipment and field devices, particularly potential vulnerabilities in operational environments connecting with the Internet. On-site control engineers are typically trained from the aspect of the control process, and the combination of a professional with both control system process and IT security expertise is rare. (Graham, Hieb and Naber). Cyber vulnerability assessments methods can vary in depth of analysis and breadth. Assessment techniques and methodologies used in IT do not necessarily apply to control systems and do not easily transfer into SCADA systems. For example, penetration tests involve bypassing security controls and are generally not recommended on production SCADA systems because they might negatively impact the system. (Hahn and Govindarasu). Further, there are gaps in assessments due to the differences in IT and control system environments such as undetectable network protocols that make it difficult to determine what controls are required, undocumented third-party software tools, unknown configuration requirements, insufficient security configuration documentation, and limitations of testing methods that could result in system faults. (Hahn and Govindarasu).

Most exploited vulnerabilities occur due to weak boundary protection and limited or ill-defined security policies. (Kayan et al.). A rapid increase in Internet connectivity during the past twenty years contributes to the lack of professional agreement and understanding. There is a culture gap between IT and control system engineering communities. Cybersecurity is taught in computer science with no courses about control system processes. Similarly, typical engineering curricula do not address cybersecurity in depth. (Weiss, Stephens and Miller). Even though literature about control systems security and the Internet, its diversity makes it challenging to produce unifying taxonomy, implementation techniques, or evaluation metrics. (Kayan et al.). The first publicly known digital weapon targeting equipment and operations that control the physical

world was the Stuxnet Worm in 2010. (Fruhlinger). Stuxnet specifically targeted industrial software and equipment for uranium enrichment. The path to cybersecurity for control systems as a cornerstone of defense remains unclear without putting it in the context of the actual threat to motivate people to protect things from obscure, not well understood, nor agreed upon, threats. Cybersecurity approaches to critical infrastructure protection are not universally accepted. Robert Lewis argued in 2006 that "[the] human element reduces the risk of cyberattack to critical infrastructure." (Lewis). However, since 2010 attacks on control systems have been increasing. People need to recognize a cyberattack and prevent one, which creates the need for championing cultural change in cybersecurity of control systems. (S. S. Aleksandra Scalco). The lack of cybersecurity addressing the lower levels of a control system architecture is a significant gap between IT and operation teams. "The two teams that need to play well together do not even comprehend what the other one knows, and there is no common language." (Weiss, Stephens and Miller).

Control systems are those computing devices that control physical world processes. A typical computer is estimated to have a lifespan of a couple of years, expecting that updates and software fixes are made frequently. However, control systems devices are different. The life cycles can span up to 30 years or more. In addition, the systems often rely on legacy operating systems with meager resistance against standard attack techniques even as conveniences such as remote access are introduced. U.S. House Resolution 1833 (H.R. 1833) "Department of Homeland Security (DHS) Industrial Control Systems Capabilities Enhancement Act" introduced in March 2021 gives greater authority to the Cybersecurity and Infrastructure Security Agency (CISA) to defend critical systems against cyber-attack. (House). Executive Order (E.O.) 14028 Removes barriers to sharing threat information to ensure acceleration of incident deterrence, prevention, and

response efforts. The action also enables more effective defense of agencies' systems and data collected, processed, and maintained by or for the Federal Government. (Biden "Executive Order on Improving the Nation’s Cybersecurity"). S. 1605 National Defense Authorization Act (NDAA) for the Fiscal Year 2022, included SEC. 1505. Operational Technology and Mission-Relevant Terrain in Cyberspace, December 21, 2021. (Congress). On January 19, 2022, President Biden signed a National Security Memorandum (NSM) to improve the cybersecurity of National Security, Department of Defense, and Intelligence Community Systems, as required in his Executive Order (E.O.) 14028, Improving the Nation's Cybersecurity. (Biden "National Security Memorandum to Improve the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems"). The National Security Memorandum establishes voluntary cybersecurity goals for owners and operators of critical infrastructure. This National Security Memorandum requires that, at minimum, National Security Systems employ the same network cybersecurity measures as those required of federal civilian networks in Executive Order 14028. The NSM builds on the Biden Administration's work to protect our Nation from sophisticated malicious cyber activities from nation-state actors and cybercriminals. The Memorandum establishes timelines and guidance for implementing these cybersecurity requirements, including multifactor authentication, encryption, cloud technologies, and endpoint detection services. (Scalco "Months to Minutes - Command and Control (C2) of Control Systems").

In addition to the lack of understanding for process control equipment and field devices, new exposure was introduced by a global pandemic. The start of a worldwide coronavirus crisis in 2020 demonstrated teleworking electro-mobility. Remote access to operations increased significantly. Socio-technical systems engineering and climate goals generated added tensions as significant transformation drivers. (E. P. Aleksandra Scalco). Such drivers can potentially change

existing jobs and create new demands for digital KSA and solutions engineered for the digital environment. More changes lie ahead as Internet connectivity of control systems expands. Systems engineering methodology and practice can offer equilibrium to complex, context-sensitive, dynamic classes of control systems for critical infrastructure. An uncertainty model can provide a valuable tool. The pandemic focused on critical infrastructure as crucial infrastructure sectors underwent a global transformation. The global pandemic caused many workers to quickly and unexpectedly move to online work environments without cybersecurity training, processes, plans, or tools to ensure that fundamental cybersecurity rules followed the remote work transition. (Tasheva). The pandemic's start demonstrated an increased change to the levels of teleworking electro-mobility than previously witnessed. More changes lie ahead as Internet connectivity of control systems expands. Yet, interest tends to focus on incidents after the fact, even though the impact can have broad societal safety and security consequences. (Hans de Bruijn). The information officer leads most organizational cyber policies without engineers or facility representation involvement, demonstrated by the lack of addressing cybersecurity in operational process systems in assessments and an "irrational fantasy" that control systems are "air-gapped.” ,(Weiss, Stephens and Miller). Air gapped is a term used to mean or imply the absence of connection to the Internet by a computer system or other device.

For example, there was an increase reported by OT and Internet of Things (IoT) security company Nozomi Networks by some of its customers in extending remote control access to operations from 9 percent to 60 percent in three months. (Ribeiro "Hackers See Big Bucks in OT Infrastructure, Cloud Adoption Picks Up"). According to Nozomi, ransomware attacks on industrial organizations increased 500 percent between 2018 and 2020. Furthermore, the number of incidents increased by 116 percent between January and May of 2021. (Networks). Predictions

are that global ransomware damage costs will exceed USD 265 Billion by 2031(Braue).

A challenge is that the control system context is different from that of an IT system. As a result, in addition to operating within a diverse environment, OT operators respond to operational anomalies differently than IT users. (A. Scalco and S. Simske "Digital Transformation of Cyber-Physical Systems and Control Systems"). Systems engineering methodology and practice can offer equilibrium to the domain of complex, context-sensitive, dynamic classes of control systems. Therefore, the analytic model can provide a valuable tool to identify disagreement and overcome control system cybersecurity vulnerability. There seems to be insufficient public awareness about cybersecurity for control systems because the concept is complex and challenging to grasp, complicating policy. (Hans de Bruijn). Understanding how cyber introduces vulnerability into control systems and innate vulnerability in the control system functionality and design is helpful to appreciate the value of measuring disagreement among professionals fully.

Another malware example is DarkSide ransomware. DarkSide ransomware is an example of a malware attack deployed in the oil and gas critical infrastructure sector against fuel pipeline company Colonial Pipeline in 2021. (C. a. I. S. A. (CISA) "Alert (Aa21-131a), Darkside Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks"). The headlines read that a ransomware attack led one of the Nation's biggest fuel pipeline operators to shut down its entire network. However, this was a ransomware attack directed at the business enterprise level of the architecture. The attack was not directed at the lower levels of the architecture to do "physical harm" or damage. Instead, the shutdown was a call by the organization to prevent any potential for grave damage. The cyber-attack on Colonial Pipeline can be seen as an example of how disagreement may lead to misalignment that results in vulnerability. The threat actor compromised the network system with a single compromised password. (Turton and

Mehrotra). A compromised password was likely used by a Colonial Pipeline Co. employee on multiple systems, which eventually enabled the credentials to be obtained by the hacker. The threat actor remotely accessed Colonial Pipeline's network system through a Virtual Private Network (or VPN) account using the compromised credentials.

Understanding best practices to protect networks from cyber threats helps the defense strategy. A well-known best practice is to protect the network by protecting remote access (e.g., VPN), protecting wireless access points, and using strong passwords to protect against unauthorized access to the physical system. If engineers believe security controls, or safeguards, to eliminate or reduce the threat or vulnerability are in place, and other personnel such as safety are in misalignment, there is a problem. For example, suppose safety personnel considers access convenience by remote access using shared credentials is valuable. In that case, a misalignment may induce vulnerability to the system that is greater than the system design itself. The vulnerability caused by the disagreement and subsequent misalignment may be greater than any innate system design vulnerability.

Cyber-attacks are caused by criminal actors and hackers, and unintentional insiders. Fifty percent of participants surveyed by an Information Security Breaches Survey indicated the single worst organizational cyber breach was related to human error. (Veiga). Instruments to measure cybersecurity culture are needed to identify actions to influence and promote cybersecurity culture at all levels. (Veiga). Comprehensive password policies need to be established and communicated. In most insider attacks, another employee’s account credentials are used to perpetrate the attack. All employees need to understand organizational policies and be trained in the personal responsibility of protecting passwords and alerting procedures for abnormal system activity. Yet, cases show employees share passwords with coworkers. (Keeney et al.).

There are 16 critical infrastructure sectors identified by the Department of Homeland Security (DHS) (C. a. I. S. A. (CISA) "Securing Industrial Control Systems: A Unified Initiative Fy 2019—2023"; D. o. H. S. D. C. I. S. A. (CISA)). This research about overcoming uncertainty of agreement for achieving cyber security using a model and mechanism for integrating contextual information from context-sensitive critical infrastructure control system dynamic classes into a model applies to any of these 16 sectors, as shown in Table 1. Countries categorize essential infrastructure sectors differently than the United States, adding complexity to the certainty of agreement about critical infrastructure cybersecurity defense. For example, the United Kingdom (UK) Centre for the Protection of National Infrastructure (CPNI) identifies 13 national infrastructure sectors and includes "space" as a category. ((CPNI)). Canada classifies critical infrastructure into ten sectors. (Government).

Table 1 Department of Homeland Security (DHS) 16 Critical Infrastructure Sector

Chemical Sector	Financial Services Sector
Commercial Facilities Sector	Food and Agriculture Sector
Communications Sector	Government Facilities Sector
Critical Manufacturing Sector	Healthcare and Public Health Sector
Dams Sector	Information Technology Sector
Defense Industrial Base (DIB) Sector	Nuclear Reactors, Materials, and Waste Sector
Emergency Services Sector	Transportation Systems Sector
Energy Sector	Water and Wastewater Systems Sector

AUTOBIOGRAPHY

Aleksandra Scalco received an M.ENG. degree in systems engineering from Iowa State University in 2012, an M.B.A. (2009), and a B.J. (1988). She is a Ph.D. candidate in systems engineering at Colorado State University, Fort Collins, CO. She has been an Engineer with the Naval Information Warfare Center Atlantic (NIWC Atlantic), United States Department of the Navy, since 2016. From 2012 to 2016, she was an Information System Security Designer (ISSD) and Client Advocate with the National Security Agency/Central Security Service (NSA/CSS). She is a technical manager for intelligence-informed mitigations of control system vulnerabilities and leads the transition of mitigation capabilities into fielded solutions. Her research interest includes the digital transformation of control systems, Software Defined Networking (SDN), and the development of Tactics, Techniques, and Procedures (TTP) using software orchestration for control systems. Ms. Scalco is a Senior Member of the Institute of Electrical and Electronics Engineers (IEEE). She is an International Council on Systems Engineering (INCOSE) Certified Systems Engineering Professional (CSEP) (Credential ID 30251735) and member of the seventh cohort of the INCOSE Institute for Technical Leadership. She is Information Technology Infrastructure Library (ITIL) Expert Certified in IT Service Management (Credential ID GR761012539AS). In addition, she is certified at the highest Defense Acquisition Workforce Improvement Act (DAWIA) Certification in Engineering Level 3. She is certified in Science & Technology (S&T) Management and Program Management at Level I. She is an Industry Advisory Board Member at Charleston Southern University, Department of Computer Science for the 2021 — 2024 Term. Her honors included the NSA/CSS Crescent Performance Award for Mission Excellence in 2013.

DEDICATION

This dissertation is for those control system operators who participated in the MOSAICS MUA. The "Plank Owners" of the first commissioning of the initial cyber defensive capability for control systems. (Navy). You are the change agents.

And for

Eugene Wiszynski (‡)

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF EQUATIONS

ORGANIZATION OF DISSERTATION

The dissertation is organized into four sections to guide the reader. The research followed the method of asking questions about observations about cybersecurity vulnerability, leading to a hypothesis and experimentation to test the hypothesis, analyze experimental data, and draw conclusions. Each step of the process is described in a section and summarized at the end. The objective is to progress from problem statement observations (i.e., cyber-attacks on control system infrastructure during a global pandemic) to a hypothesis and analytic methodology (i.e., using an analytical model to discover emergent details) to use the model to measure disagreement as a means of identifying vulnerability (i.e., gaining insights and making correlations), to recommendations and future work (i.e., providing repeatable methods that can be applied and reused).

- SECTION I – PROBLEM STATEMENT – Background research is performed about the subject of what is known about disagreement among professionals in the cybersecurity community by literature review and form questions about the observations. This section introduces cybersecurity awareness of control systems gives background and literature review about the operational need and problem fraught by unknowns in a high turbulence environment. In a chaotic context, the relationships between cause and effect constantly shift with no manageable patterns. This absence of manageable patterns leads to disagreement, which leads to misalignment and vulnerability.
- SECTION II – HYPOTHESIS, METHODOLOGY, AND TEST RESULTS – The hypothesis, resulting predictions to be measured based on background research, and test findings are presented in this section. This section provides insights from a workforce

research study and protocol authorization (Colorado State University (CSU) Internal Review Board (IRB) Protocol Number 20-10209H, July 8, 2020).[1] A survey tool is used to understand better the workforce involved in defending control systems from cyberattacks. The study involved the development of 203 questions about cybersecurity for control systems, and subsequent online questionnaires collected responses from 187 professionals. Analysis of the response data identifies key points about attitudes toward cybersecurity and control systems.

- SECTION III – USE OF THE MODEL TO MEASURE DISAGREEMENT AS A MEANS OF IDENTIFYING VULNERABILITY – The method to conduct experiments to test the hypothesis is presented in the previous section, and the data from the experiment analyzed. The next step is to draw conclusions from the experiment data and elucidate how the experiment's output can be used. The effectiveness of the regression approach is demonstrated by two Use Cases, one for a power system and one for a water facility. This section describes how the uncertainty model can be applied to a cybersecurity control system solution deployment to understand conflicting voices better and vulnerabilities discoverable but not immediately apparent to everyone.
- SECTION IV – RECOMMENDATIONS FOR FUTURE WORK AND CONCLUSION – Experiment outcomes that can be applied to control systems are presented. This section provides recommendations using fact-based management for other critical infrastructure vertical(s) integrating cybersecurity into control systems and areas of future work. The approach uses the uncertainty of agreement measures to achieve alignment and agreement to overcome vulnerability.

A new cyber defensive capability must traverse the acquisition gap "valley of death"

at every development phase, separating innovation from milestone realization in another domain. Each transition phase may introduce disagreement, misalignment, and vulnerability greater than the innate system design vulnerability. In addition, the uncertainty of agreement among professionals exists throughout about early prototyping, experimental concepts, operational use, and competition for resources. This research presents an integrative analytic model involving multiple Likert outputs to get an "emergent" picture of the state of agreement and alignment of different sections of the cybersecurity community. An objective system engineering approach deals with the complexity of disagreement to remediate any shortcomings throughout each development phase of the system lifecycle from the customer requirement, systems engineering, subsystem engineering, component design, through component testing, subsystem testing, integration, and verification, as well as each iterative development phase from early novel prototype to mature system and best practices. The approach takes a relatively traditional type of survey and uses it to gain analytical insights about sets of professionals who work in control systems and cybersecurity. As a result, the analytic process makes it possible to focus on uncertainty in an environment likely to create vulnerability.

LIST OF ACRONYMS

2FA	two-factor authentication
ACI TTP	Advanced Cyber Industrial Control System Tactics, Techniques, and Procedures
ACVAM	Air Force Center for Cyberspace Research developed Avionics Cyberspace Vulnerability Assessment and Mitigation Workshop
AFIT	Air Force Institute of Technology
AFRL	Air Force Research Laboratory
AI	Artificial Intelligence
AO	Authorizing Official
AoA	Analysis of Alternatives
API	Application Programming Interface
ATO	Authority to Operate
B2B	Business to Business
BDD	Block Definition Diagram
BES	Budget Estimate Submission
C2	Command and Control
C2SOC	Cyber-security Operations Center
CAE-CDE	Centers of Academic Excellence in Cyber Defense Education
CCB	Change Control Board
CDA	Central Design Authority
CDD	Capability Development Document
CDM	Conceptual Data Model
CIA	Confidentiality, Integrity, and Availability
CIO	Chief Information Officer

CISA	Cybersecurity and Infrastructure Security Agency
CM	Configuration Management
CNDSP	Computer Network Defense Service Provider
CNIC	Commander, Navy Installations Command
CNSSP	Committee for National Security Systems Policy
COA	Course of Action
COCOM	Combatant Command
COI	Critical Operational Issue
CONOP	Concept of Operations
COTS	Commercial-off-the-shelf
COV	Coefficient of Variation
CPD	Capability Production Document
CPNI	Centre for the Protection of National Infrastructure
CPRC	Cyber Planning and Response Center
CPS	Cyber-physical Systems
CPT	Cyber Protection Teams
CS	Control Systems
CSEP	Certified Systems Engineering Professional
CSPE	Cyber Security Physical Enclave
DAWIA	Defense Acquisition Workforce Improvement Act
DB	Database
DCS	Distributed Control Systems
DEI	Diversity, Equity, and Inclusion
DHS	Department of Homeland Security
DIB	Defense Industrial Base
DID	Defense-in-Depth

DIS	Distributed Interactive Simulation
DNP or DNP3	Distributed Network Protocol
DNS	Domain Name System
DOC	Department of Commerce
DOD	Department of Defense
DoDAF	DoD Architecture Framework
DoDI	DoD Instructions
DOE	Department of Energy
DoS	Denial of Service
DOT	Department of Transportation
DOTMLPF-P	Doctrine, Organization, Training, Materiel, Leadership, and Education, Personnel, Facilities, and Policy
DPC	Discrete Process Control
DT&E	Developmental Test and Evaluation
E-ISAC	Electricity Information Sharing and Analysis Center
E.O.	Executive Order
EC NIS2	European Commission Network and Information Systems (EU NIS2)
EIE	Energy, Installations, and Environment
EPA	Environmental Protection Agency
ERP	Enterprise Resource Planning
FBI	Federal Bureau of Investigation
FEC	Facilities Engineering Command
FEC SE	Facilities Engineering Command Southeast
FEC SW	Facilities Engineering Command Southwest
FEOC	Facilities and Energy Operations Center
FEOC	Field Engineering Operations Center

FERC	Federal Energy Regulatory Commission
FFRDC	Federally Funded Research and Development Center
FIPS	Federal Information Processing Standards
FMA-C	Functional Mission Analysis for Cyber
FRCS	Facility Related Control Systems
FSA	Functional Solutions Analysis
FY	Fiscal Year
GERD	Grand Ethiopian Renaissance Dam
GIAP	Global Information Assurance Program
GOTS	Government off-the-shelf
GW	gigawatt
HARM	Hierarchical Attack Representation Model
HBCU	Historically Black Colleges and Universities
HI	Hawaii
HLA	High-level Architecture
HTTP	HyperText Transfer Protocol
HVAC	Heating, Ventilation, and Air Conditioning
IA	Information Assurance
IAP	Independent Assessment Plan
IATO	Initial Authority to Operate
IATT	Interim Authority to Test
ICS	Industrial Control Systems
ID	Implementation Directive
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IIoT	Industrial Internet of Things

IMT	Integrated Management Team
IMT	Integrated Management Team
INCOSE	International Council on Systems Engineering
IoT	Internet of Things
IoTF	Installation of the Future
IP	Internet Protocol
IPS	Intrusion Prevention System (IPS)
IPT	Integrated Product Team
IRB	Institutional Review Board
IRP	Incident Response Plan (IRP)
ISAC	Information Sharing and Analysis Center
ISEA	In Service Engineering Agent
ISO	Information System Owner
ISO	International Organization for Standardization
ISPS	International Ship and Port Facility
ISSD	Information System Security Designer
ISSM	Information System Security Manager
ISSO	Information System Security Officer
IT	Information Technology
ITIL	Information Technology Infrastructure Library
JCIDS	Joint Capabilities Integration and Development System
JCTD	Joint Capability Technology Demonstration
KPI	Key Performance Indicators
KSA	Knowledge, skills, and abilities
kW	kilowatt
kWh	kW hours

LE	Likert Entropy
LSE	Lead Systems Engineer
LV	Logical View
MAC	Mandatory Access Control
MBSAP	Model-Based Systems Architecture Practices
MBSE	Model-Based Systems Engineering
MCCS	Mission-Critical Control Systems
MFA	Multi-Factor Authentication
MIDLANT	Mid-Atlantic
MIT	Massachusetts Institute of Technology
ML	Machine Learning
MOE	Measures of Effectiveness
MOP	Measures of Performance
MOSAICS	More Situational Awareness for Industrial Control Systems
MUA	Military Utility Assessment
MW	megawatt
NASA	National Aeronautics and Space Administration
NAVFAC	Naval Facilities Engineering Systems Command
NCI	National Council of Information Sharing and Analysis Centers
ND-ISAC	National Defense Information Sharing and Analysis Center
NDAA	National Defense Authorization Act
NDS	National Defense Strategy
NIEM	National Information Exchange Model
NIST	National Institute of Standards and Technology
NNN	Net-net-net
NPS	Naval Post Graduate School

NSA	National Security Agency
NSM	National Security Memorandum
NSS	National Security Strategy
OJT	On-the-job Training
OM	Operations Manager
ONG-ISAC	Oil & Natural Gas Information Sharing and Analysis Center
OPM	Office of Personnel Management
OS	Operating System
OT	Operational Technology
OT-SDN	Operational Technology Software Defined Network
OT&E	Operational Test and Evaluation
OUSD	Office of the Undersecretary of Defense
OV	Operational View
OWASP	Open Web Application Security Project
PERA	Purdue Enterprise Reference Architecture (also known as the "Purdue" model)
PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
POC	Point of Contact
POM	Program Objective Memorandum
POR	Program of Record
PV	Physical View
QA	Quality Assurance
QoS	Quality of Service
R^2	R-squared
RA	Reference Architecture

RDP	Remote Desktop Protocol
RMF	Risk Management Framework
ROI	Return on Investment
S&T	Science and Technology
SA	System Architecture
SCADA	Supervisory Control and Data Acquisition
SDN	Software-defined Networking
SECDEF	Secretary of Defense
SECOPS	Security Operations
SES	Senior Executive Service
SIEM	Security Information and Event Management
SLA	Service Level Agreements
SME	Subject Matter Expert
SOA	Service Oriented Architecture
SOAR	Security Orchestration, Automation, and Response
SOS	System of Systems
SoSE	System of Systems Engineering
SQL	Structured Query Language
SSH	Secure Shell
STPA	System Theory Process Analysis (STPA)
SYSE	Systems Engineering
SysML	Systems Modeling Language
TA	Teaching Assistant
TAXII	Trusted Automated Exchange of Intelligence Information
TLI	Technical Leadership Institute
TTA	Transition Technology Agreement

TTP	Tactics, Techniques, and Procedures
TVA	Tennessee Valley Authority
TWh	Terawatt-hours
UAF	Unified Architecture Framework
UARC	University Affiliated Research Center
UC	Utility Control
UK	United Kingdom
UNK-UNKs	Unknown-Unknowns
UNSC	United Nations Security Council
UPS	Uninterruptable Power Supply
USB	Universal Serial Bus
V&V	Verification and Validation
VPN	Virtual Private Network
WaterISAC	Water Information Sharing and Analysis Center
ZT	Zero Trust

SECTION I – PROBLEM STATEMENT

1. Chapter One – Introduction

This chapter addresses observations that lead to the problem examined in the hypothesis that disagreement exists among professionals, which leads to misalignment, which results in vulnerability. A method is to perform background research about the subject. System engineers are tasked with designing, developing, implementing, and managing complex, large-scale systems throughout the project's entire lifecycle. The whole of the system, including the role of the system and the environment in which it will operate, can be impacted by any change to any of the system elements to include the cyber domain for control systems, which may create uncertainty of agreement about how to treat the system security posture. Disagreement exists among professionals about how to treat systems due to discrepancies in engineering practice, paradigms, processes, and culture of critical infrastructure control systems and business enterprise systems. There are no practical constraints to support many decisions that need to be made at cyber speed. Quantification of agreement among OT and IT professionals is required to increase visibility into areas where divergence arises. The OT workforce still does not understand what cybersecurity entails, and the IT workforce does not widely understand the control system assets. There are many "unknowables" in this environment. The convergence of IT and OT, or the Industrial Internet of Things (IIoT), is happening at an accelerated, broader scale. Organizations look for what works now, potentially missing better answers.

The industry creates a cyber capacity affecting all system-level elements used in the operational side of critical infrastructure and Facility Related Control Systems (FRCS). The OT operational context is different from that of an IT system. In addition to operating within a different environment, OT operators respond to functional anomalies differently than IT users. Using

automated attacks, adversaries target critical infrastructure assets (such as power, fuel, water, and critical facilities) through cyberattack vectors. Therefore, systems must be engineered to achieve cyber resiliency in an OT environment. The system engineering approach needs to be formulated and tailored to the unique characteristics of such an environment keeping in perspective all systems-level elements (including people, hardware, software, facilities, policies, documents) that produce results. While innovative methodologies and new technologies are in research and development to address the cyber resiliency challenge, there is a lack in the system engineering community body of knowledge of how to transition those into the characteristics of the OT system successfully. OT operators are used to manual operations. Cyber resilience solutions bring automation to a physical manual world. Not until Artificial Intelligence (AI) is matured and engineered into solutions will cyber resilience be fully realized in Industry 4.0. System engineering principles are needed to discover solutions, moving the problem from a chaotic domain to more manageable context characteristics.

Understanding the whole picture and what can be done to improve things is a continuous science and engineering challenge. This understanding holds particularly true for the Department of Defense (DOD) when concerned about greater energy security, acquiring and disposing real property, constructing and maintaining installations, and overseeing personnel's occupational health and safety issues. All while overseeing environmental protection, planning, and restoration efforts; and leading efforts to conserve cultural and natural resources. (Assistant Secretary of the Navy (Energy). Of course, new complexities are introduced by innovation, new technology, and methodologies. Still, these also present opportunities to achieve climate goals, rethink strategies, and explore new options to ensure infrastructure is resilient in unknown challenges (Blockley and Godfrey).

The DOTMLPF-P is the common acronym broadly used by the DOD for Doctrine, Organization, Training, Materiel, Leadership, and Education, Personnel, Facilities, and Policy to align agreement among professionals to support the materiel solution development process. (Defense "DOTMLPF-P Analysis"). The DOD must unambiguously align the entire ecosystem from strategic guidance to the DOTMLPF-P strategy to achieve objective mission success. (Scalco "Months to Minutes - Command and Control (C2) of Control Systems"). For example, the Navy's Energy, Installations, and Environment (EIE) strategy must intersect in a logical approach within this framework, as shown in Figure 2. Any time something game-changing is introduced, it affects the DOTMLPF-P process and can create uncertainty.

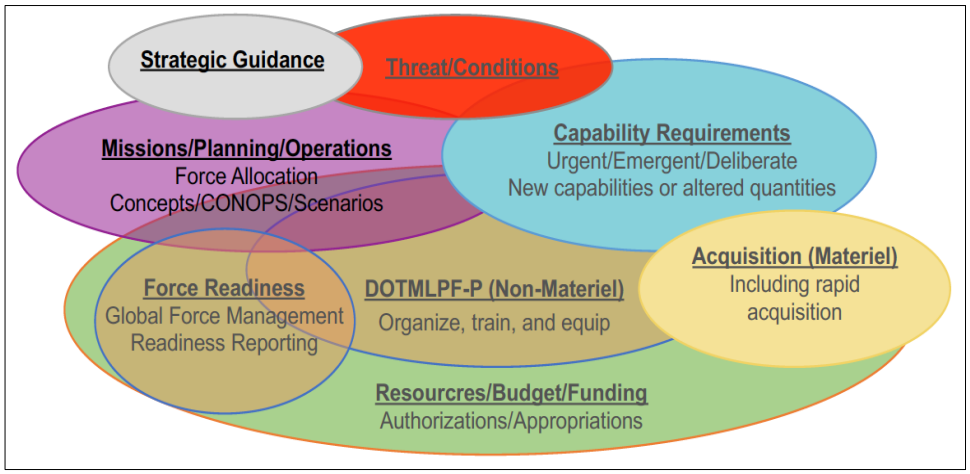

Figure 1 DOTMLPF-P Domains (DOD, 2021)

Connectivity between the physical world and Internet Protocol (IP) based components (i.e., the cyber domain) introduces new capabilities to control systems affecting each domain. However, new capabilities also introduce complexity and uncertainty among professionals as materiel solutions are developed. Uncertainty and lack of agreement among professionals about introducing cyber capability into operations create multi-concern assurance interest. (Scalco "Preliminary Exam"). While there are many efforts and initiatives within the DOD to speed the acquisition

process, the Joint Capabilities Integration and Development System (JCIDS) is the formal process to address capability gaps and define the acquisition and evaluation criteria for solutions. ((DAU)). Therefore, a significant emphasis of DOTMLPF-P is to support the development of a materiel solution. Multi-concern assurance flows between each of the eight domains of a DOTMLPF-P analysis, as shown in Figure 3. The output of the JCIDS analysis defines needed capabilities, guides materiel development, and directs the production of capabilities in coordination with the Joint Staff. Introducing any solutions follows this process.

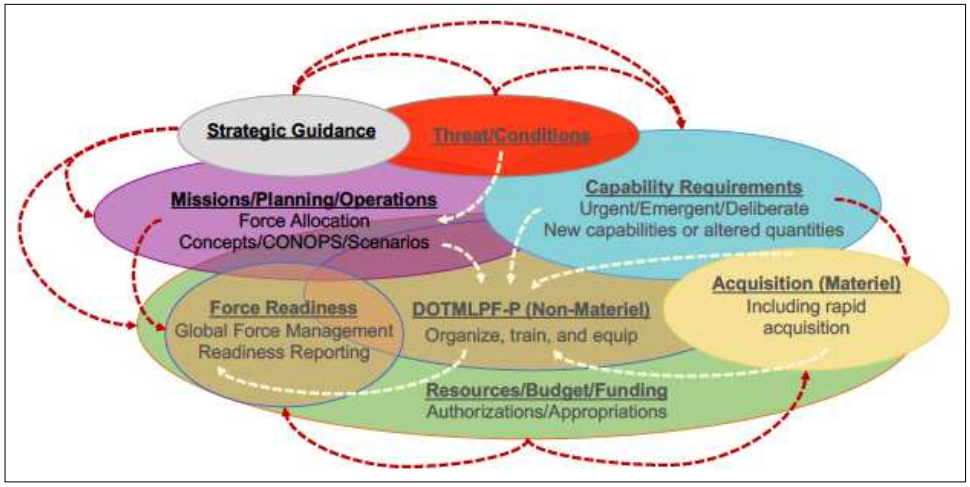

Figure 2 DOTMLPF-P Domains (DOD, 2021) and Multi-Concern Assurance Interest Flow

Command and Control (C2) are information management, decision management, and execution management. Variables include a complex system of people, processes and procedures, technology, and doctrine, coordinated to realize the mission. As a result, the entire system – including its role at the time of operation and the environment in which it will operate – can be impacted by any change. Adversaries use automated cyberattacks to target critical infrastructure control systems such as power, fuel, water, and FRCS. In addition, the DOD operates thousands of networks and millions of computing devices dispersed worldwide that are vulnerable to attack (Haegley and Chipley).

In a chaotic domain, a leader's job is to drive alignment by immediately reestablishing order (e.g., C2). (Snowden and Boone). Combatant Commands (COCOM) identified the urgent need to defend these critical task assets in signed letters to the Secretary of Defense (SECDEF) during the past several years. Nevertheless, most resources continue to be directed to traditional kinetic defenses without acknowledging the Cyber Domain's kinetic role. A challenge is that while the four other doctrinal warfighting domains are well-defined (e.g., Land, Maritime, Air, and Space), cyberspace is still not well understood.

Physical boundaries define the Land, Maritime, Air, and Space Domains. Cyberspace is also a warfighting domain. Cyberspace characteristics and connections control the physical realm in each of the other domains. However, Tactics, Techniques, and Procedures (TTP) for cyberspace at the physical level is still evolving. Resources are needed accordingly, specifically for Cyber-Physical Systems (CPS), also referred to as OT and Industrial Control Systems (ICS). These control systems enable the physical delivery of power, fuel, gas, and water across all domains (e.g., Land, Maritime, Air, and Space) to DOD and private sector customers. Back-ups to physical systems typically are designed to last only a short duration (e.g., diesel, uninterruptable power supply (UPS), battery) to support emergency switchovers.

The DOD is advancing automated solutions such as MOSAICS that remove disagreement about response action to address the cyber resilience requirement for control systems. The MOSAICS capability concept is to automate selected procedures to detect, mitigate and recover from a cyberattack, moving from a chaotic situation to a complex domain. The capability is combined with the best-of-breed commercial technologies related to analytics, visualization, decision support, and information sharing. (M. J. Aleksandra Scalco, Steve Simske). Capabilities such as MOSAICS provide cyber resiliency that supports sustainability and system robustness to

help achieve EIE climate mission objectives. The MOSAICS prototype was successfully demonstrated during a Military Utility Assessment (MUA) in August 2021. During this stage of development, the MOSAICS capability was tested and evaluated in an experiment to confirm that the attributes needed are present in the initial design to ensure that the prototype is in line with the needs identified by the COCOMs. The MOSAICS prototype experiment created an environment that allowed for probing and sensing of ideas and innovative approaches. It is foundational for government and commercial entities to invest in cyber domain solutions (i.e., threat intelligence, automation, and analytics) to protect physical assets, train personnel, and continuously enhance the organizational security posture (i.e., Zero Trust, Defense-in-Depth). (Diogenes and Ozkaya). These are all relatively new concepts. The DOD establishment of cyberspace as an "operational domain" occurred in 2011. Navigating new investment strategies in cyber solutions through the DOTMLFP-P framework can be met by many questions, uncertainties, and unknown unknowns ("UNK-UNKS") while the materiel solution is developed. Therefore, it becomes worthwhile to understand the broad professional agreement or uncertainty throughout the domains and create a strategy that meets each of the eight DOTMLPF-P domains. A model and methodology for measuring multi-concern assurance through the statistical uncertainty analysis of Likert and semantic differential scales can help identify outcomes where different professionals disagree with the current state of cybersecurity readiness and best practices for critical infrastructure control systems. (A. Scalco and S. Simske "Model for Multi-Concern Assurance in the Digital Transformation of Engineering of Critical Infrastructure Control Systems"). The outcome may identify gaps and opportunities that impact the efficacy of the new capabilities' fulfillment of the intended mission and goals and help reduce the uncertainty of agreement among professionals throughout the DOTMLPF-P framework.

This research is necessary because it addresses disagreement in evaluating, transitioning, and assessing joint concepts and requirements and the DOTMLPF-P components that the new capability may affect. DOTMLPF-P is important because it is a critical, authoritative tool in the DOD to deliver an operational capability. It may seem obvious that the development of a new capability should include the value of attention to doctrine, organization, training, the materiel needed to equip operations, leadership and education, personnel, and facilities. However, the speed of transformational revolution in control systems owing to technological drivers of change such as digitalization and automation, telework electro-mobility, social systems engineering, and climate goals generates tensions and uncertainty. This research hopes to help clarify disagreement and misalignment through this transformation through quantitative models and methodology to enable fact-based management.

1.1. Why is this research necessary?

Electric power is the backbone of modern convenience operating appliances such as refrigeration for food preservation and electronics that transmit sounds of voice and music. It operates computers and equipment that ensure national security, such as driving turbines, powering airport runway lights, and providing electricity to the powerful mechanical systems that rotate machinery. Electric power is the backbone of public health and safety. Lifesaving hemodialysis centers depend on it to provide care to patients. Flowing water can produce electricity by putting a dam on a river to store water in a reservoir as the Tennessee Valley Authority (TVA) operates on the Tennessee River system. (("TVA") "A Guide to Information About the Tennessee Valley Authority"). The TVA operates the largest public power system in the United States, supplying power to Alabama, Georgia, Kentucky, Mississippi, North Carolina, Tennessee, and Virginia by

releasing water from the reservoir flows through turbines, spinning and activating electric generators to produce power. In the summertime, TVA releases water, turning still Southeast waterways into magnificent rivers. Millions of people enjoy recreational activities such as fishing, swimming, boating, and kayaking on the water. (("TVA") "Tva Fun"). When a dam bursts, tranquility is interrupted by hazards of far greater impact than any normal flood event. Dam failure can force downstream residents to evacuate their homes, and wide areas may be submerged under a depth of water. Damage to infrastructure can cause loss of human life as a roadway is washed away, carrying people in cars into the flooding waters. As water picks up speed as it plunges uncontrolled over the dam, hazardous material may be spread, carrying raw sewage and other chemicals, wastes, and hazardous materials along with trillions of gallons of water within hours, submerging everything in its way.

Specific critical infrastructure sectors are interrelated so that the decomposition of effects of a collapse affects other sectors. The Dams sector is one such sector. For example, dams provide eight to twelve percent of the nation’s power, give water to concentrated populations, are a source of emergency water supply, and provide irrigation to the Food and Agriculture sector. (Hemme). However, the Dams sector has a poor report card for emergency action plans. (Hemme).

In 2013, malicious actors used a cyberattack to gain control of water levels of the Bowman Avenue Dam in the Village of Rye Brook, New York, USA. (Esposito). The mayor's solution was to take the dam controls off the Internet and have staff operate the dam manually. (Esposito). The mayor acted in response to a chaotic situation. Add the Bowman Avenue Dam cyber-attack mode to feasible attack vectors against Dams sector assets such as land vehicle-borne explosive devices, small arms, water-borne explosive devices, or aircraft impact. ((DHS)). Cyber presents a new attack mode for malicious actors to cause physical damage and harm. In March 2016, a cellular telephone

was used to compromise the Command and Control (C2) system on a New York Dam. (Akwetey Henry Matey).

In 2010, unknown malicious actors detonated incendiary devices on an access road near the Black Rock Dam in Thomaston, Connecticut, USA. ((DHS)). Neither the Bowman Avenue Dam nor Black Rock Dam caused injuries or facility damages. However, other attacks have caused loss of life assets and interrupted water supply. In 2003, suspected rebels fired rocket-propelled grenades at the Kidapawan Reservoir Water Plant in Kidapawan, Philippines, destroying a water pipeline and disrupting the water supply to more than 100,000 residents. ((DHS)). The Bowman Avenue Dam incident shows hackers could have had control of the dam's water flow. A direct external link often connects the industrial management network to the Internet, which can cause physical damage or loss of life.

Further from any reservoir dam, between Tampa and Clearwater is the city of Oldsmar. Oldsmar is like many small towns and cities throughout the United States. The city has a population of slightly more than 15,000 residents. (C. I. S. A. (CISA) "Alert (Aa21-042a) Compromise of U.S. Water Treatment Facility"). On February 5, 2021, someone tried to poison the water supply of the city of Oldsmar, Florida, by a cyberattack. (C. I. S. A. (CISA) "Alert (Aa21-042a) Compromise of U.S. Water Treatment Facility"). By chance, a facility supervisor saw the pointer of the hacker's movements across the screen to make unauthorized changes to settings. The supervisor then prevented an unwarranted and illicit increase in a sodium hydroxide ("lye") used in the water treatment process, making the chemical a caustic hazard to humans. The supervisor happened to be at the right place at the right time, recognized something unusual was in play, and acted. However, serendipity is not security. (Scalco *The Case for Control Systems Cybersecurity Capability*).

Further examination is needed to assess others' preparedness given a similar situation, but serendipity was indeed in play in this case. The Oldsmar water supply event highlights the value of facility workforce training to ensure physical systems' safety and mission assurance. Such attacks have staggering potential to affect human life. Proposed legislation and guidance following this event and others intended to treat networks with a heightened security level to agree about the cyber domain and how tools and people are engaged. As in most communities, the Oldsmar Community treats its water supply to remove contaminants and disinfectants such as lye, which kill disease-causing agents before piping to consumers. Making water safe to drink is generally similar in U.S. municipalities, and water supplies are safe for consumption.

Municipal governments oversee the water treatment process following federal, state, and local laws and regulations. Traditionally, the water facility workforce consists of a concentration of civil, mechanical, or chemical engineering personnel whose primary concern is the availability of safely provisioned, clean potable water, flow and storage of water, and wastewater and sewage disposal. The unidentified actors who gained access to the Oldsmar drinking water treatment plant used weaknesses found in the cyber domain to affect operations. The hacking attempt on Oldsmar was a relatively unsophisticated attack on using the remote-access system to the water treatment plant operational side of the chemical composition. (Elmhorst).

The remote-access system was subsequently disabled, but simple cybersecurity measures should have prevented the hacker's access. (Elmhorst). The cyber domain yields IT capabilities and consists of interdependent networks and infrastructures transporting and storing data. Traditionally, IT is a domain of computer scientists and network administrators whose primary concern is data confidentiality, integrity, and availability (known as "CIA"). (S. S. Aleksandra Scalco). The Oldsmar cyber-attack demonstrated the varying perspectives of the IT and OT

personnel that can lead to vulnerabilities. The facility supervisor's observations and actions, fortunately, averted the attack. Good cyber hygiene is needed to prevent water distribution and chemical treatment disruption and ensure safe drinking supplies. (Elmhorst). The actions highlighted the critical importance of developing a cybersecurity culture among workforce personnel in the OT field and developing an IT knowledge of how physical systems function in the IT field to understand the potential vulnerabilities. (S. S. Aleksandra Scalco). The United States Environmental Protection Agency (EPA) provides resources for implementing cybersecurity best practices and offers a cybersecurity technical assistance provider program to help reduce risks in the Water and Wastewater Sector. DHS CISA provides resources and tools to assist critical infrastructure facilities with cybersecurity. (EPA).

Still, ransomware is a formidable threat to operations. Remote access to functions increased significantly in 2020, induced by the global pandemic. For example, there was an increase reported by OT and Internet of Things (IoT) security company Nozomi Networks by some of its customers in extending remote control access to operations from 9 percent to 60 percent in three months. (Ribeiro "Hackers See Big Bucks in OT Infrastructure, Cloud Adoption Picks Up"). During the same period, cybercrime ransomware attacks were estimated to have increased by 116% between January and May 2020. (Networks). All countries are vulnerable to the potential economic impact of cyber-attacks on crucial infrastructure such as power grids. (Group). DarkSide ransomware is just one example of a malware attack deployed in the oil and gas critical infrastructure sector against Colonial Pipeline’s fuel pipeline in 2021. (T. C. a. I. S. A. (CISA)). Predictions are that global ransomware damage costs will exceed USD 265 Billion by 2031. (Braue). Cyberspace is a warfighting domain. (Defense "National Defense Strategy of the United States of America").

1.2. Motivation to Protect Control System Critical Infrastructure

It is important to understand principles of motivation to protect critical infrastructure from cyber events and why some actors use cyber vectors to attack critical infrastructure. The approach is like how cybersecurity Red Team/Blue Team assessment techniques gauge an organization's security. A Red Team/Blue Team assessment is an ethical approach to attempting real-world attacks. The method uses the red team to act as a threat actor trying to exploit an organization's security defenses. It uses the blue team to play the defensive role in countering the attacks.

Electricity generation, capacity, and consumption are essential terms to understand in the power sector. Generation is a measure of the production of electricity over time. A standard unit of measurement for electricity is the kilowatt (kW), equal to 1,000 Watts. Other units for the measure in the power industry are megawatt (MW), which is equivalent to 1,000 kW, and gigawatt (GW), which is equal to 1,000 (MW). Utility-scale electricity generation is classified as at least one megawatt (MW) of total generating capacity, and small scale includes generators with less than one MW of developing capacity. ((EIA)). In 2019, the electric power industry in the United States generated approximately USD 402 billion in revenue. (Statistica). Electricity sales in the United States in 2020 was distributed by 40 percent (1,462 billion kW hours (kWh)) residential sales, 35 percent (1,276 billion kWh) commercial sales, 25 percent (920 billion kWh) industrial sales, and 0.2 percent (7 billion kWh) in transportation sales. ((EIA)). Hydropower harnessing dams produce eight to 12 percent of power generation needs in the United States. There are an estimated more than 90,000 dams located in the United States. (Officials). Global installed capacity of renewable power such as dams reached approximately 2.84 terawatt-hours (TWh), 1.67 TWh of which were generated through hydropower. (Jaganmohan "Hydropower and Renewable Energy Capacity 2008-2020"). China had the most hydropower capacity of energy generation in 2019. (Jaganmohan "Largest Hydroelectric Power Generating Countries Worldwide in 2019 (in

Terawatt Hours)"). Dams effectively create reservoirs to store water, prevent flooding and erosion, create wildlife habitats and recreation areas, and provide electrical generation from falling or fast-moving water, replacing the need to burn more than "121 million tons of coal, 27 million barrels of oil, and 741 billion cubic feet of natural gas combined," (Officials). Dams are designed to function for decades and to automatically function without human intervention with some maintenance to replace components, clear debris from spillways, and manage water levels for a short period.

Much critical infrastructure in the United States is aging, such as dams. Dropping water levels that feed dams threaten the ability to use the dams to generate power. For example, the Hoover Dam at Lake Mead has generated electric power for California, Arizona, and Nevada for more than 75 years. Years of unrelenting drought, record heat, and increased dependency on use by the growing regional population create concerns about what would happen if Hoover Dam stopped generating electricity. (WOLFF). Dropping water levels at Lake Meade mean less water pressure, which causes problems to the mechanical technologies initially designed for a high-elevation dam, such as air bubbles flowing with the water through the intake pipes that reduce turbine efficiency. (WOLFF).

These concerns may be realized for the first time in 2021. Low water levels of a critical reservoir at Northern California's Lake Oroville in the United States may push its hydroelectric power plant to shut down, ceasing power generation due to lack of sufficient water to turn the plant's turbines. (Meeks). When at total capacity, the power generated from Lake Oroville hydropower generates enough electricity to power 800,000 homes. (Meeks). There is tremendous pressure added to the electrical grid without Lake Oroville's contribution to capacity. In response, the state's governor signed an emergency proclamation to allow immediate use of emergency

backup power generators to alleviate stress on the power grid by providing access to additional energy capacity. (Meeks). However, these backup generators have drawbacks, such as environmental impacts. Most are involved combustion technologies that are fueled by gasoline or diesel fuel. ((EPA)).

Aging systems, water resource constraints, and increased demand add to the challenges of retrofitting cybersecurity solutions into the power generation, capacity, and consumption of the power sector. These systems were not built with cyber connectivity in mind. The aging electric grid is being pushed to function in ways unimagined 75 years ago. The complex network of systems of systems that make up the electric grid also includes the transmission lines to transport energy and distribution systems to deliver electricity to the consumer. These systems are designed to be fault-tolerant but not necessarily with cybersecurity in mind, leading to unintended vulnerability.

Guidance is available that identifies how to address specific cybersecurity threats and vulnerabilities such as the National Institute of Standards and Technology (NIST) "Special Publication 800-82 Revision 2 (SP 800-82 Rev. 2) Guide to ICS Security." SP 800-82 Rev. 2 guides how to secure Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations such as Programmable Logic Controllers (PLC) found in critical infrastructures such as power and water. (Stouffer et al.). However, widely available, low-cost IP devices are replacing older components. Low-cost IP devices increase the vulnerability footprint of these assets to cyber-induced events, and cyber-induced events can come from many sources such as by accident or human error, disgruntled employees, malicious or hostile state actors. Any disruption along the energy infrastructure can create significant impacts. Impacts of not addressing cybersecurity include physical, economic,

social, and mission has implications of multi-concern assurance need:

- Physical Impacts. The potential effects include personal injury, loss of life, and loss of assets—possible environmental damage.
- Economic Impacts. Unavailability of critical infrastructure (i.e., power, fuel, water) can have an economic impact far beyond the systems sustaining direct and physical damage.
- Social Impacts. Another second-order effect is the loss of national or public confidence in an organization.
- Mission Impacts. Unavailability of critical infrastructure could cause loss of command and control and prohibit mission continuity.

Cyber connectivity, as well as motivation, can be a double-edged sword. Any type of malicious actor can be motivated to cause any unexpected impacts for financial or other types of gain. Untrained employees or unhappy employees can contribute to cyber-attack activities. (Akwetey Henry Matey). However, national interest can also cause conflict and a motivation to disrupt critical infrastructure delivery of function. For example, when construction of the mega-dam Grand Ethiopian Renaissance Dam (GERD) project in Ethiopia across the Blue Nile started in 2011, a destabilizing regional dispute among Egypt, Sudan, and Ethiopia ignited. GERD, formerly known as the Renaissance dam project, is based on an original survey of the Blue Nile made by the United States Bureau of Reclamation in the late 1950's/early 1960s. (Technology). The reservoir and dam impact water use from the Nile River by Ethiopia, Egypt, and Sudan, potentially affecting more than 140 million people in Egypt and Sudan. They depend on the annual flow of the Nile River for agriculture, industry, and drinking water. (Kandeel). Egypt relies on the Nile for more than 90 percent of the nations' water needs and perceives GERD as an "existential threat" tapping into its water rights and resources. (Piliero).

Additional background research about what is known about cybersecurity vulnerability and unexpected impacts is shown by the political disputes GERD caused among neighboring countries. GERD can retain up to 88 percent of the Nile River's annual flow, which caused Egypt and Sudan to seek formal intervention by the United Nations Security Council (UNSC) to resolve the growing freshwater dispute, which has been ongoing since construction started. GERD is a 6,450 MW project owned and operated by the Ethiopian Electric Power company. ((IHA)). China backs GERD. (Zelalem).

Chinese involvement is seen as part of a broader political strategy in Africa. (Piliero). An essential design of GERD is to enhance Ethiopian economic and food security by access to electricity and enhancement of farmland management. The dam could provide electricity to 65 million people in Ethiopia, whereas less than half of citizens have access to power. (Alvarez). According to the World Bank, 48.3 percent of Ethiopia's population has access to electricity compared to 100 percent in Egypt and 53.8 percent in Sudan. (Bank). The UNSC advocates for diplomacy to prevent future water-related conflict related to how Ethiopia will regulate the Blue Nile's water flow, particularly during a drought. (Alvarez). In 2020, hackers targeted regional police force training centers with threatening messages of a "Pharaonic curse" upon Ethiopians. They left similar messages on other Ethiopian government websites that included the message: "If the river's level drops, let all the Pharaoh's soldiers hurry and return only after the liberation of the Nile, restricting its flow" (Zelalem).

2. Chapter Two – Literature Review

Research about what is known about the subject of disagreement among professionals in the cybersecurity community by literature review is presented in this chapter. The issue of cybersecurity vulnerability of control systems induced by misalignment is not widely studied, precisely uncertainty of agreement among professionals about remediation of control system vulnerability due to discrepancies in engineering practice, paradigms, processes, and culture. There is research in the field of cybersecurity as well as in the field of control system cybersecurity. Still, attributes of cybersecurity and control systems by quantifying agreement among professionals are sparse. From the literature perspective, very little is known about cyber vulnerabilities in the power utility sector and user behavior. (Akwetey Henry Matey).

Publications reviewed consist of a range of current research that includes survey data published in scientific journals in the following categories:

1) Security of CPS.
2) CPS cybersecurity models, standards, and methods.
3) Workforce readiness skills.
4) Policy and governmental initiatives.

2.1. Surveys on the Security of Cyber-physical Systems (CPS)

Wolfgang Schwab and Mathieu Poujol provided a survey of the state of industrial cybersecurity in 2018. Schwab and Poujol's findings were that most companies surveyed stated cybersecurity for OT/ICS is a significant priority. While most thought the company would be a

target of a cybersecurity attack in the OT/ICS space as likely, only 23 percent were compliant with minimal mandatory industry standards or government guidelines and regulations. (Schwab and Poujol). While half the participants stated the company did not experience a cyber incident in the previous 12 months, Schwab and Poujol observed that participants may not have recognized if they had as most could not detect an event or track them. The data showed that 8 percent revealed they do not know, and 10 percent do not measure cybersecurity incidents with control systems. Most companies surveyed had started the digital transformation, thus increasing the cyberattack surface. Only 30 percent of the participants responded that their organization must report industrial security breaches and incidents to a regulatory body. Schwab and Poujol cited the low maturity of cybersecurity for OT/ICS further limited by a skill gap and lack of collaboration among IT and OT professionals. A finding is that IT and OT professionals possess varying goals, processes, tools, and even language. (Schwab and Poujol). Further, 58 percent of the companies surveyed responded that the issue of hiring ICS cybersecurity personnel with the right skills is global.

Hakan Kayan et al. reviewed cybersecurity of industrial CPS in 2021. Kayan et al. provide a chronological summary from 2009 to 2020 of previous studies in a table categorized by industrial, Control Systems (CS), CPS, IoT, Wireless Sensor Networks, and cybersecurity. (Kayan et al.). Of the 22 previous surveys, only two were classified covering both CS and cybersecurity, Manuel Cheminod et al. in 2013 and William Knowles et al. in 2015. Kayen et al. concluded that despite the benefits of IoT integration, cybersecurity is becoming a primary concern due to the increased attack surface and unique OT system characteristics. (Kayan et al.). Their literature review concluded, "no paper proposes a framework that explains the relationship with complementary industrial systems" (Kayan et al.). Evaluated studies propose security mechanisms but lack how to integrate adaptive security mechanisms and governance policies to address

weaknesses such as lack of security policy enforcement. While there is literature about the vulnerabilities, few surveys bring together the mechanics to evaluate cybersecurity for control systems to help overcome the uncertainty of agreement among professionals. Kayen et al. found confusion as new terms emerge to describe new technologies and capabilities without clearly distinguishing the relationships of terms (e.g., IIoT, SCADA, ICS). (Kayan et al.). The concept of defense-in-depth to provide a secure environment was identified as critical to all assets to defend against sophisticated cyber-attacks with the following characteristics: robustness, resilience, and redundancy. (Kayan et al.). Kayan et al. describe available attack taxonomies and observe that most current taxonomies focus on IT.

Taxonomies that address OT primarily consider a particular characteristic (e.g., application) which makes them non-usable for various OT systems. They evaluate 15 known significant industrial cyber-physical incidents starting in 2000 with a water services sewage spill caused by a former employee hacking the system with a laptop and radio transmitter to ransomware attacks in 2019. Six incidents of the 22 evaluated had a cyber-physical scope. The Fukushima Daiichi Nuclear Disaster was included. However, the cause of the disaster was an earthquake. The event did lead to a re-examination of safety at similar facilities. (Kayan et al.).

Bhamare et al. surveyed cybersecurity for ICS, particularly about migrating industrial processes to cloud environments, in 2019. Bhamare et al. provide a summary of cybersecurity approaches for ICS and SCADA. Cloud-based environments offer cost-benefit, increased throughput, and enhanced functionality to ICS and SCADA and enable remote access to systems. Simulation experiments are a means of assessing security for ICS; However, simulation environments have extensibility limitations. (Bhamare et al.). Machine Learning (ML) techniques are a trend identified for anomaly detection for ICS security. However, Bhamare et al. found that

obtaining real-time, unbiased datasets is a significant obstacle. Bhamare et al. highlight the need for an ICS security testbed to model real ICS and threat impacts. “The testbed would provide an innovative environment where researchers can explore cyber-attacks and defense mechanisms while evaluating their impact on control systems.” (Bhamare et al.). A testbed would help explore the applicability of ML and new intrusion detection methods for control systems.

Iosif Progoulakis et al. carried out a survey between February and July 2020 on cybersecurity for Offshore Oil and Gas assets. (Iosif Progoulakis). A total of 66 anonymous responses were gathered from 350 professionals contacted (i.e., 18.8 percent response rate). Sixty-four percent responded that oil and gas sector employees receive cyber security training regarding cybersecurity. Constraints in cybersecurity implementation were cited as 48 percent of participants stated a lack of understanding of cyber security threats and consequences, followed by operational and capital budget constraints (41%) and organizational cyber-security culture (35%). The most significant cybersecurity vulnerabilities were cited as portable Universal Serial Bus (USB) devices (67%), low employee awareness (59%), outdated control and monitoring systems, and architecture (53%). A dedicated department or entity within the organization was confirmed by 86 percent for cyber security responsibilities and duties. Cybersecurity initiatives identified the following: firewalls (95%), policies (e.g., procedures, passwords) (94%), antivirus software (91%), while cybersecurity initiatives such as the use of dual authentication for Virtual Private Network (VPN) (2%), allow listing (3%), and other Security Information and Event Management (SIEM) (3%). Threat scenarios showed the probable source as email hacks (67%), ransomware (56%), phishing (55%), malicious insider threats (45%), remote control of systems (44%). Industry standards for cybersecurity risk assessment and management in the Offshore Oil and Gas sector cited by survey participants showed International Organization for Standardization (ISO) 27001 (47%),

International Ship and Port Facility (ISPS) Code (39%), API STD 780 (39%), NIST SP 800-30 (21%), NIST SP 800-37 (14%), ISO/IC 18045: 2008 (17%), ISO/International Electrotechnical Commission (IEC) 15408-1: 2009 (15%), followed by others. Progoulakis et al. concluded there is no direct correlation between survey responses and literature review and no association between the survey results and technical issues raised in the literature review. The authors further concluded there are two spectrums evident: the human and corporate organization. The human element relates to the perception of mitigation. "The lack of understanding of cyber security principles and its effect in the operations or organization in the case of an incident also pose a very credible threat in the proactive and reactive mitigation of breach incidents" (Iosif Progoulakis). Progoulakis et al. cited other surveys that cybersecurity is not fully understood and lacks awareness as a significant threat. The corporate organization for the Offshore Oil and Gas vertical showed that cybersecurity is adopted through training, use of mitigation tools, understanding of industry standards, and incorporation into operational management. Collaboration was established with government entities through joint exercises. The survey showed that cybersecurity is a conflicting subject in understanding operations and personnel. While the corporate entity adapted cybersecurity tools and countermeasures, lack of knowledge of cyber security principles among personnel hindered the mitigation, including through "negligence and lack of awareness from field personnel on the subject." (Iosif Progoulakis).

2.2. Surveys on CPS Cybersecurity Models, Standards, and Methods

Simon Yusuf Enoch et al. surveyed model-based cybersecurity models in 2021 and discussed the development of a Hierarchical Attack Representation Model (HARM) for domains such as IoT. Enoch et al. conclude that security modeling can help identify vulnerabilities and help

develop and execute effective defense strategies. "Model-based security evaluation provides a systematic way to capture possible attack scenarios and analyze security based on system vulnerabilities" (Enoch et al.). Enoch et al. described security metrics to measure security effectiveness for attack scenarios and the potential impact of the attackers' objective. For example, metrics include measuring system vulnerability, attack scenarios and impact, the effectiveness of defenses, economic value and impact, dynamic networks, and threats. Enoch et al. classified various security metrics and highlighted challenges based on security models and applications. Challenges identified include the frequency of change of modern network components, which causes frequent change to security posture and countermeasure effectiveness, the scalability of security evaluation extended to every node as a possible entry point (e.g., IoT), and the lack of empirical data for cyber-physical systems and emerging IoT. (Enoch et al.).

Costas Boletsis et al. surveyed modeling and socio-technical cybersecurity risk assessment to visually map cybersecurity and raise awareness and improve communication among professionals. In Boletsis et al.'s 2021 research, the risk message challenges professionals to understand the presented data and its relevance. Boletsis et al. survey proposed cybersecurity evaluation tools such as online surveys to measure maturity levels, gamification approaches for raising security awareness levels, and automated counseling dialogues for self-assessment and training. (Costas Boletsis). Boletsis et al. introduce visualizations to improve cybersecurity awareness, improve understanding among professionals, and encourage proactive engagement and desired cybersecurity behaviors.

A conceptual validation of a System Security Modeler (SSM) asset-based risk-analysis modeling approach is also presented. This approach brings a presentation of risk and threat together to enhance understanding and drive behavioral change related to cybersecurity in a

context-specific and relevant model. "The System Security Modeler (SSM) is an asset-based risk-analysis tool for socio-technical systems, providing an information-security perspective on the interactions between assets across the whole system. Assets may be people, technology, or environments." (Costas Boletsis). The SSM automates risk assessment to model the system, identify primary assets and business impact failure would cause, specify security controls (e.g., firewalls), and examine potential high-threat risks to the system. (Costas Boletsis).

Georgios Kavallieratos et al. surveyed cybersecurity and safety co-engineering methods for cyber-physical systems in 2020. Kavallieratos et al. identified three types of dependences of cybersecurity and safety: conditional for safe operations (i.e., modification of sensor data that interferes with safety system functions); reinforcement of complementary safety and cybersecurity measures (i.e., activity logging for attack detection and accident anticipation); and conflict where safety and cybersecurity requirements are conflicting. (Kavallieratos, Katsikas and Gkioulos). According to the selection criteria explicitly related to cybersecurity and safety co-engineering methodology, sixty-eight methods were reviewed. The period of methods reviewed spanned 20 years, with most proposed since 2013. Kavallieratos et al. attributed the timeliness to the increased proliferation of cyber-physical systems. Kavallieratos et al. used the following attributes to categorize the methods reviewed: type of joint analysis (e.g., type), model type the analysis is based on, standards (e.g., safety, security standards), application domain, approach (e.g., quantitative, qualitative), the goal of the analysis (e.g., security, safety, both), system lifecycle in which the method is applied (e.g., requirements, risk analysis, generic phase), and stakeholders involved (e.g., safety experts, security experts, developers, designers, users or system experts). Kavallieratos et al. further reviewed the methods by characteristics such as process (e.g., systematic, structured), scalability, creativity (i.e., are mechanisms guidewords, or checklists),

communication among stakeholders, conflict resolution, and software tools to support the application of the method. (Kavallieratos, Katsikas and Gkioulos). Kavallieratos et al. concluded that model-based methods prevail, less than half reviewed are informed by safety and security standards, and most were used to analyze general CPS architectures. Most of the methods followed a qualitative approach, with only two fully quantitative methods. "Attempting to analyze security, particularly security risk, has been shown quantitatively to be either infeasible or inadvisable in most real-world situations." (Kavallieratos, Katsikas and Gkioulos). Most methods' goal was to ensure safety and security, with only six methods solely focused on providing protection. Only fifteen methods surveyed are frameworks that apply to any lifecycle phase. The other models are used for the system lifecycle's requirements and risk analysis phases. Scalability is discussed as a challenge for most methods surveyed are mechanisms to stimulate creativity, particularly when the method calls for multi-disciplinary, multi-stakeholder involvement. All methods reviewed by Kavallieratos et al. are process-based, and most do not address conflict resolution. Finally, most of the reviewed methods are not supported by any software or toolkit. (Kavallieratos, Katsikas and Gkioulos). Kavallieratos et al. concluded the need to develop a holistic, integrated, model-based, safety and security co-engineering approach.

Martin “Trae” Span et al. surveyed cybersecurity architecture analysis approaches in 2018. Span et al. identified the definition of the term “cybersecurity” as one of the least understood within the DoD.[2] “Despite being often cited; this definition tends to cause confusion because it is packed with domain-specific IT jargon: availability ensures the system is used as anticipated; integrity is the protection from unauthorized modification; confidentiality is keeping data private; authentication is a validation of the claimed identity; and, nonrepudiation is the ability to prove that an action has taken place.” (Span, Mailloux and Grimaila). Span et al. observe that the DoD

definition is hindered by legacy terminology rather than a more straightforward definition to protect critical systems from cyber threats. Span et al. surveyed architectural approaches for applicability to complex system cybersecurity based on literature focused on weapon systems. Most predecessor surveys focus exclusively on computer network and IT system security controls (e.g., compliance-based Information Assurance (IA)). (Span, Mailloux and Grimaila). The predecessor surveys are considered inadequate for the complexity of control system cybersecurity. Span et al. surveyed applicable approaches to cybersecurity architectural analysis: DoD Architecture Framework (DoDAF), Unified Architecture Framework (UAF), commercial custom architectural analysis approaches and DoDAF extensions, the DoD Risk Management Framework (RMF) for Cybersecurity, the Air Force Research Laboratory (AFRL) and Air Force Institute of Technology's (AFIT) Center for Cyberspace Research developed Avionics Cyberspace Vulnerability Assessment and Mitigation (ACVAM) Workshop, Attack Path Analysis, Massachusetts Institute of Technology (MIT)'s System Theory Process Analysis (STPA) approach security-related extension, known as STPA-Sec, DOD has adopted Functional Mission Analysis for Cyber (FMA-C). (Span, Mailloux and Grimaila). Span et al. found that threat modeling and analysis should not solely focus on identifying problems (e.g., assessments and document-based engineering). Dynamic adversary tactics necessitate dynamic tools and countermeasures that integrate modeling approaches such as MBSE. MBSE can help provide traceability mapped to the component level and fit-for-purpose views to enable more effective decision-making. (Span, Mailloux and Grimaila). Span et al. concluded that professionals do not understand an architectural cybersecurity analysis well. "Moreover, given cybersecurity's widespread interest, it was surprising to find a general lack of understanding or consistency regarding what it means to conduct architectural analysis for cybersecurity." (Span, Mailloux and Grimaila).

2.3. Surveys on Workforce Readiness Skills

Deloris McBride surveyed cybersecurity curriculum designs, workforce readiness skills, and applied effectiveness for undergraduate students at Historically Black Colleges and Universities (HBCU) in 2021. McBride concluded that cybersecurity programs lack experimental learning, are more theory-based, and lag in preparing skilled cybersecurity personnel for the workforce. McBride found that cybersecurity education's limited effective instructional design and a deficit in developing qualified potential cybersecurity employment candidates contribute to the talent shortage. Minorities struggle to gain a foothold in the cybersecurity field, representing 3 percent of hired personnel. (McBride). Workforce readiness skills include IT fundamentals such as web applications and system administration, coding skills (C, C++, Java, PHP, Perl, Ruby, Python), architecture understanding of administration and operating systems, and certifications. (McBride). Demands for cybersecurity skills coupled with hands-on experience and critical thinking ability will continue in both the private and public sectors. Inadequate cybersecurity skills are attributed to 95 percent of cyber threats to organizations. Therefore, academia needs to ensure graduating students are prepared with the right readiness skills. (McBride). NSA/CSS and DHS jointly sponsor a program to improve the quality of cybersecurity education at the university level. Universities designated as National Centers of Academic Excellence in Cyber Defense Education (CAE-CDE) must map courses to select knowledge units. (McBride). CAE-CDE complements IT coursework and pervasively integrates cybersecurity into a university program.

Information Systems Audit and Control Association (ISACA) "State of Cybersecurity 2020, Part 1: Workforce Efforts and Resources" results identified the need for trained and experienced cybersecurity professionals. Respondents were asked questions about hiring and retention practices such as what cybersecurity KSAs are in the highest demand, what companies

can do to staff positions more quickly, types of cyber-attacks, and questions about gender-balance diversity on cybersecurity teams. Respondents confirmed an industry-wide cybersecurity skills gap (i.e., corporate cybersecurity teams are understaffed, and cybersecurity positions unfilled). ((ISACA)).

Nonprofit membership association $(ICS)^2$ focuses on cybersecurity professions. $(ICS)^2$ collects data from cybersecurity professionals annually to measure the cybersecurity profession estimate size of the available pool of cybersecurity professionals worldwide and the cybersecurity workforce gap of additional cybersecurity professionals needed to defend critical assets adequately. ((ISC)2 *(Isc)2 Cybersecurity Workforce Study, 2021*). However, the surveys are not specifically about control systems.

$(ICS)^2$ collected data about the cybersecurity workforce from 3,790 security professionals in a study from April to June 2020 ($(ICS)^2$ 2020). The $(ICS)^2$ "Cybersecurity Workforce Study, 2020" focused on defining cybersecurity skills shortage and estimating the workforce's size and constitution, such as job satisfaction, salary benchmarks, and perceived value of certifications. Key takeaways are a shortage of dedicated cybersecurity staff at all levels of organizations, a distribution of the greater percentage of workers are in IT services, and a high value placed on cybersecurity certifications of both vendor-specific and vendor-neutral cybersecurity certifications. Top cybersecurity skills needed identified cloud computing security as the greatest area of focus. The survey did not ask specific questions about control systems. The segments $(ICS)^2$ measured and percentage respondents: cloud computing security (40%); risk assessment, analysis, and management (28%); security analysis (28%); governance, risk management and compliance (GRC) (26%); threat intelligence analysis (26%); application security (25%); security engineering (24%); security administration (23%); data management protection (22%); and

penetration testing (22%). ((ISC)2 *(Isc)2 Cybersecurity Workforce Study, 2021*).

$(ICS)^2$ collected data about the cybersecurity workforce again in 2021 from 4,753 cybersecurity professionals. ((ISC)2 *(Isc)2 Cybersecurity Workforce Study, 2021*). The findings show a global cybersecurity workforce estimate of 4.19 million professionals. The data shows changing pathways to cybersecurity jobs, with more than half of the participants starting outside the IT field. Although IT is still the most common entry route (47%). Industry distribution data was collected by IT services (24%), financial services (10%), government (10%), manufacturing (8%), consulting (5%), healthcare (4%), retail (4%), and telecommunications (4%). ((ISC)2 *(Isc)2 Cybersecurity Workforce Study, 2021*) The data showed there is continued high value placed on cybersecurity certifications. The study data shows that among the survey participants, the cybersecurity field is predominately male (76%) and Caucasian (72%). Meaningful diversity, equity, and inclusion (DEI) initiatives might tap into a broader resource pool. Key takeaways from the study are that more than 700,000 cybersecurity professionals will join the workforce in 2021. Hiring practices need to change to meet the cybersecurity gap. The lack of cybersecurity professionals on teams is a significant concern, particularly for talent to support security provision, analyze, and protect and defend roles. Remote work is seen as an opportunity to remove geographical hiring barriers. ((ISC)2 *(Isc)2 Cybersecurity Workforce Study, 2021*).

2.4. Surveys on Policy and Governmental Initiatives

The global COVID-19 pandemic increased the speed of the digitalization trend that was already taking place and brought an increasing trend of cyber-attacks. Many workers quickly moved to online work environments without cybersecurity training, processes, plans, or tools to ensure that fundamental cybersecurity rules followed the remote work transition. (Tasheva). Iva Tasheva presented the case for policymakers' action to adopt European Commission's Network and Information Systems (EU NIS2) Directive and the Cyber Resilience Act3 without delay. Further, to develop democracy, diversity, and inclusion standards for cybersecurity tools and services and make cyber awareness training materials easier to share among nations and engage with significant government and private-sector entities. (Tasheva).

"A Report to the President of the United States on Strengthening the Nation's Cybersecurity Workforce for Cyber-Physical Systems & Control Systems," Secretaries of the Department of Defense (DOD), Department of Homeland Security (DHS), Department of Energy (DOE), and Department of Transportation (DOT) highlighted the need to address CPS/CS cybersecurity competency gaps as a significant competency gap in the workforce. (Esper). The report was prepared by the Office of the Principal Cyber Advisor and coordinated with the DOD CIO. The report states that the sophistication of the adversarial "workforce" threatens to outpace that nation and creates a global threat. "Our nation's private and public sector cybersecurity practitioners and educators serve an indispensable role in our national security. [The importance of this role] is especially true for critical infrastructure, for which CPS/CS presents a unique challenge for adequate cyber workforce training. Our adversaries, including nation-state adversaries, are increasingly targeting this sector, specifically the supporting CPS/CS, to cause physical damage, outages, or injury. The sophistication of the skills, tools, and methods of this adversarial

'workforce' threatens to outpace our defenders, as evidenced in recent attacks carried out across the globe. The comparative weakness of our CPS/CS workforce comes at a risk of high consequences in an increasingly complex and connected environment." (Esper). The report to the President of the United States emphasizes the convergence of traditional IT systems with OT that can cause physical damages, outages, destruction, or injury. It provides recommended actions with suspense dates in Fiscal Year (FY) 2020 and FY21, as shown in Table 2.

Table 2 Report on Strengthening the CPS/CS Workforce Key Findings (Esper 2020)

KEY FINDINGS	RECOMMENDED ACTIONS	OWNER – SUSPENSE
CPS/CS cybersecurity and workforce policy and guidance lacking	Develop Roadmap	Federal Government Q4 FY20
	Represent CPS/CS in Cyber Workforce Initiatives	Department of Commerce (DOC) Q4 FY20
	Improve Recruitment and Hiring Process	Office of Personnel Management (OPM) Q4 FY20
	Establish/improve Governance	Federal Government Q4 FY20
Lack of prioritization of cybersecurity on CPS/CS	Publish CPS/CS training opportunities online	Department of Homeland Security (DHS) October 2020
	Update and maintain online cybersecurity content; focus on Tier 2	NIST with the DOD Chief Information Officer (CIO) FY21
Need for better inclusion of CPS/CS in acquisition processes	Establish workforce, acquisition, and contract requirements	DOD, Department of Homeland Security (DHS), Department of Energy (DOE), Department of Transportation (DOT) October 2020
	Require security configuration curricula and guidance	DOD October 2020

KEY FINDINGS	RECOMMENDED ACTIONS	OWNER – SUSPENSE
	Facilities and programs for cyber evaluation and training on CPS/CS	DOD, DOE October 2020
	Verify implementation of cybersecurity by Government Contractors	DOD FY21
A desire for additional and enhanced on-the-job training (OJT)	Develop OJT programs with Industry partners	All Government Q4 FY20
	Provide sustainable funding for new workforce programs	
Little cross-training and collaboration among operators and IT	Programming for dual workforce development	Federal Government FY21
	Strategy to ensure dedicated positions for protecting CPS/CS	OPM October 2020

Of note is the breadth of governmental departments included in the report (i.e., Federal Government, Department of Commerce (DOC), Office of Personnel Management (OPM), Department of Homeland Security (DHS), DOD CIO, Department of Energy (DOE), Department of Transportation (DOT)), and non-federal partners such as NIST. The ownership of suspense actions to address critical findings is found across the government.

In May 2021, the White House issued an Executive Order (EO) about national cybersecurity. (JR.)). Subsequently, the White House issued a statement outlining collaboration with NIST and other industry partners to develop a security framework. The critical cyber incident reporting policy for the federal government is Presidential Policy Directive (PPD)/PPD-41, United States Cyber Incident Coordination, which defines the roles of federal agencies during a cyber event and identifies DHS as the lead agency for asset response to significant cyber events (Obama).

Earlier key governmental policy publications about cybersecurity include: “Enabling Distributed Security in Cyberspace – Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action,” (Reitinge), Memorandum of Agreement between the Department of Homeland Security and the Department of Defense Regarding Cybersecurity,” (Janet Napolitano).

The DOD CIO published a cybersecurity reference and resource guide in 2020. The reference provides an overview of relations across the U.S. government and partners regarding policies and standards. (Department of Defense). The U.S. National Security Strategy (NSS) is a statutory document signed in 2017. This statute is supported by the Committee for National Security Systems Policy (CNSSP) No. 15, Use of Public Standards for Secure Information Sharing, October 2016. Key DOD directives, instructions, and documents include the National Defense Strategy (NDS), National Cyber Strategy, DOD Cyber Strategy, the DOD Digital Modernization Strategy, DOD Instructions (DoDI) 8500.01 Cybersecurity, DoDI 8510.01 RMF for DOD Information. NSS is also supported by non-DOD standards published by NIST, the Federal Information Processing Standards (FIPS), ISO, and others. Key non-DOD documents include NIST SP 800-137, Information Security Continuous Monitoring (ICSM) for Federal Information Systems and Organizations, and NIST SP 800-82, Guide to Industrial Control Systems (ICS) Security. DOD frameworks that support the DOD control system cybersecurity include the Presidential Executive Order (EO) 13800; Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, May 2019; the Defense Industrial Base (DIB) Guide to Implementing the Cybersecurity Framework, October 2019; The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT); and NIST’s Framework for Improving Critical Infrastructure Cybersecurity, April 2018. (Department of Defense). Industry resources that operate research and development centers sponsored by the U.S. federal government include not-for-profit MITRE.

In August 2020, NIST released NIST SP 800-207, Zero Trust Architecture. (Kerman et al.). The DOD followed with the Joint Defense Information Systems Agency (DISA) and NSA engineering team preparing and releasing the DOD Zero Trust Reference Architecture in February 2021. ((DISA) and (NSA)). Zero Trust is a security design principle that recognizes vulnerability threats in all system elements, internally and externally. It requires continuous verification of near real-time data from multiple threat information sources. ((DISA) and (NSA)). Zero Trust principles assume a system has been compromised or a security breach is inevitable. (Marsh). "Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned)." (Kerman et al.).

3. Chapter Three – Cybersecurity Awareness

This chapter shares principles of cybersecurity awareness, showing how disagreement and misalignment can lead to vulnerability greater than the innate system design vulnerability. Other research establishes uncertainty among professions through literature research described in the previous chapter and other studies using similar survey tools. The statistical modeling helps interpret data that quantify real-world responses about their understanding of cybersecurity for control systems. Thus, the regression analysis is valuable to gaining insights about the workforce, leading to recommendations to address the vulnerability of disagreement and misalignment among professions. Cybersecurity industry associations work to share expert advice, guidance, services, cyber-threat sharing about specific threat information, and support to overcome cybersecurity awareness challenges.

3.1. Workforce Cybersecurity Awareness

Correlation with other studies shows cybersecurity awareness among people is a weak link leading to a cybersecurity vulnerability. For example, Tzipora Halevi et al. studied the ongoing challenge cybersecurity presents to security professionals based on cultural, personality, and demographic variables (Tzipora Halevi). Tzipora Halevi et al. examined behavior across various cultures to gain insight into cyber security behavior, self-efficacy (i.e., user confidence in the ability to mitigate cyber-security risk), privacy attitudes, sharing of personal information, and trust, including other factors such as gender and computer expertise. A survey was used to measure risk perception and cybersecurity. The study found that cybersecurity behavior and self-efficacy show only a moderate correlation. For example, a person's culture was a significant predictor of privacy

attitudes but was not a predictor of self-efficacy. Significant predictors of behavior included personality traits such as conscientiousness. People with greater risk perception showed higher confidence in mitigating risks, and gender and cybersecurity majors were also strong predictors of self-efficacy. (Tzipora Halevi). Tzipora Halevi et al. found that particular security behavior and perception trends supported a global approach to security-related systems geared to specific personality characteristics and user demographics. (Tzipora Halevi).

3.2. Cybersecurity Awareness Practice

Is it possible to go further by measuring disagreement in segments of the cybersecurity profession to identify different vulnerability types? IT focuses on data management (i.e., processing and information, and information processes). Control systems (e.g., OT) focus on physical system control and biological processes (i.e., devices and sensors and software that controls physical processes). When brought together, IT and OT can have powerful value creation. Closer cooperation between IT and OT results in more significant optimization and benefits. For example, automation of security controls can protect both data and the physical control processes. The principles are the same for IT and OT protecting data and remote access to networks, monitoring user and entity behavior, dealing with social engineering, and other cybersecurity awareness best practices. The difference is that IT is traditionally managed by the IT department to collect data and information flow. IT functions at the higher levels of Enterprise Resource Planning (ERP) and Business to Business (B2B) in architecture and has a lifecycle of less than two to three years, as shown in Figure 3. While control systems (e.g., OT) are traditionally managed by the Industrial/Control System Department to control physical world processes and manage near real-time operations with a lifecycle spanning more than 75 years, as shown in Figure 3.

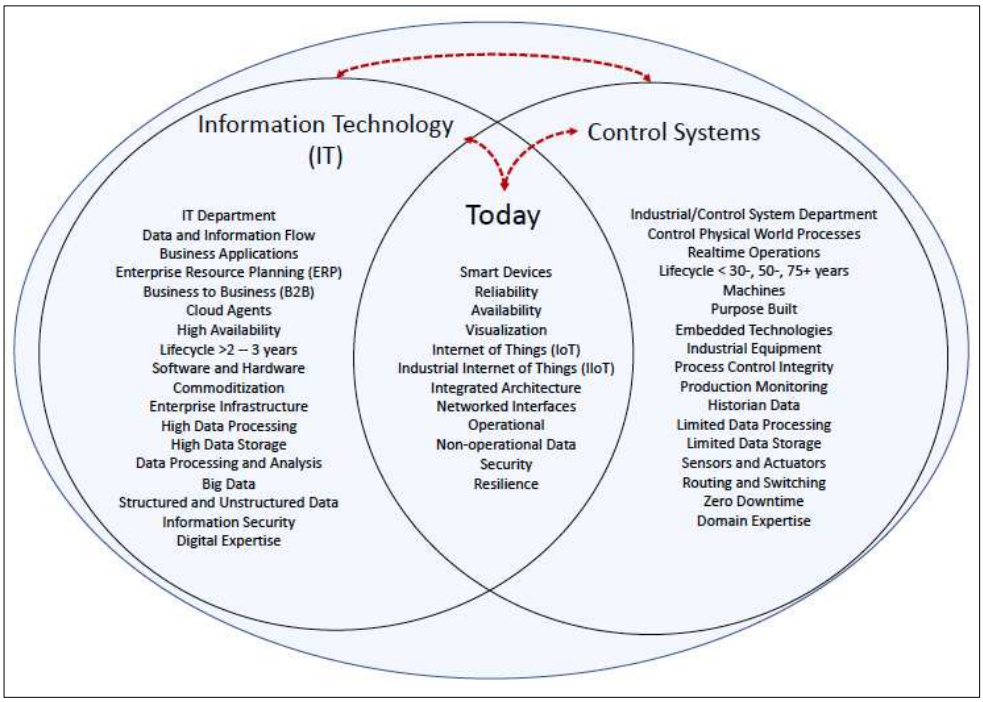

Figure 3 IT and Control Systems Today

For example, an organization can implement data loss prevention through technical security controls with regular security policy enforcement for all accounts (i.e., frequent password changes and high password strength) and continuous education via security awareness training. (A. Scalco and S. Simske "Cybersecurity Awareness for Systems Engineers Graduate Coursework"). Two examples for data loss prevention are:

1) Keep data safe by regular protected backups, and
2) Protect the network by protecting remote access (e.g., VPN), protecting wireless access points, and using strong passwords. (A. Scalco and S. Simske "Cybersecurity Awareness for Systems Engineers Graduate Coursework").

The same two examples used for data loss prevention may be applied to protect physical

control processes:

1) Keep data safe by regular protected backups to ensure continuity of operations in case of system failure; and
2) Protect the network by protecting remote access (e.g., VPN), protecting wireless access points, and using strong passwords to protect against unauthorized access to the physical system.

Monitoring user and entity behavior using analytics for all system administrator activity is a best practice that simplifies the discovery process to detect vulnerabilities and assess safeguards, continually learning new threat vectors for business and physical control systems. Evaluating network traffic enables organizations to generate security alerts and identify potential intrusions. The analytics help stakeholders make security decisions and provide network situational awareness to improve security. Research shows that professionals may have a negativity bias in processing information and pay greater attention to negative information than positive information. (Irwin P. Levin). The impact of negative information may be more substantial than positive information, which has been used to demonstrate why people are reluctant to trade an option they have for another different option. (Irwin P. Levin). Search analytics allow "review reports and identify any known or reported exceptions from the network and antivirus security tools" (Diogenes and Ozkaya). A second way to simplify the discovery process is by using machine analytics to scan large amounts of data to support analysis (Diogenes and Ozkaya), (Scalco "Cyber-Physical System (Cps) and Control System (Cs) Architecture for Cyber Defensive Capability — Mosaics").

Social engineering (e.g., phishing, pharming, spoofing, stolen accounts, blackmail) is an

attack surface that can be used against a system or product that can quickly spread the attack surface beyond the initial compromise. (Terry Merz). Data and information may be exploited via overzealous social internet activity to obtain sensitive information or use the information to escalate password privileges. "Users are known to use weak passwords due to laziness or lack of awareness about the threats" (Diogenes and Ozkaya). Sensitive information about a user can provide an attacker with information to access other organizational accounts using similar information, or by >clicking< or opening attachments sent via social media, malware is unleashed in the computer and into systems. (A. Scalco and S. Simske "Cybersecurity Awareness for Systems Engineers Graduate Coursework").

"The single greatest vulnerability is people (untrained, unmotivated, or malicious insiders)" (Simske). Network administrators tend to use weak password settings and fail to install patches in time, creating system security vulnerabilities. Training security staffers may address these lack of security tendencies, which is different from the threat surface of an underpaid security staffer. The potential in the latter is that the perceived underpayment might lead to the security staffer being "unmotivated" or becoming an active insider threat (i.e., purposely sharing information with unauthorized individuals or intentionally causing other damages). Both lack security tendencies and insider threats present exploitable weaknesses that need to be addressed in the overall risk management plan to safeguard assets. Most breaches involve weak, stolen, or infrequently changed passwords, and most involve "insider" actions, so bringing the "underpaid" and "undertrained" resources in alignment with the business is critical. (A. Scalco and S. Simske "Cybersecurity Awareness for Systems Engineers Graduate Coursework").

Concepts understood by IT professionals need to be better understood by the other

professions. Disagreement and misalignment will otherwise result in vulnerability greater than innate system design vulnerability. For example, how cyber-attack TTP can reach the exfiltration stage needs to be understood. Structured Query Language (SQL) is a standard language used for communicating with relational database (DB) management systems. SQL-based tools are used to retrieve or manipulate SQL DB system data. For example, an organization can link a SQL DB to a website to generate access to the data, such as water distribution network data to manage wastewater and stormwater data. (Campbell). A SQL injection is a type of vulnerability found in web applications. The best way to prevent SQL injection is to ensure data is verified and sanitized before being entered into the database. SQL can be prevented by using known coding techniques, code reviews, and testing to "sanitize" user inputs (Simske, 2020). "[A]lways look at the [Open Web Application Security Project] OWASP Top 10 for latest update in the list of most critical web applications" (Diogenes and Ozkaya). Installation of security plugins, regularly updating websites, and using a SQL injection scanner may also prevent SQL attacks. (A. Scalco and S. Simske "Cybersecurity Awareness for Systems Engineers Graduate Coursework").

Once an attack has reached the exfiltration stage, it is "considered successful" (Diogenes and Ozkaya). However, success may be at the reconnaissance stage during which system vulnerabilities are discovered. Finally, once there is a delivery, the system is compromised. (A. Scalco and S. Simske "Cybersecurity Awareness for Systems Engineers Graduate Coursework").

Logging provides visibility of what goes on in a network on a per-user or per-application basis (Diogenes and Ozkaya). There are two concepts regarding logging to consider. The first is for forensics, and the second is for monitoring and actively using logs for trend analysis. Maintaining extensive log records (and backup of logging) for security controls is essential to understanding security incidents during a forensic investigation. Comprehensive logs are also

helpful in establishing baselines, showing the system's value, and showing the operational trends of users and administrators during audits and forensic analysis. Another key concept of extensive logging (and backup of logging) is actively using these logos to monitor security-related activities. Again, maintaining logs is essential for post-incident forensic investigation. So is near real-time monitoring and analyzing so that organizations can detect attacks and deploy appropriate countermeasures. (A. Scalco and S. Simske "Cybersecurity Awareness for Systems Engineers Graduate Coursework").

Two examples of how security training can be made more effective are:

1) Continuous staff training and security awareness to make cyber security awareness habitual for everyone in an organization; and
2) Training key concepts repeatedly to reinforce learning and retention using suitable materials and changing these frequently to avoid monotonous repetition (Simske, 2020).

Software threat modeling is a critical process that helps improve the software by identifying potential threats and vulnerabilities to be fixed. System asset access and exit points are potential attack surfaces. For example, there could be an open port, protocol, or authentication mechanism to be protected from misuse—characterizing the correlation and data flows represent where and how data is stored or in transit. Identifying system entry and exit points as part of the system baseline under Configuration Management (CM) are used to understand the system better and address potential threats. The system entry and exit points identify how attackers can exploit the software application or the system. In addition, entry and exit points serve as interfaces with other internal system components. Identifying potential vulnerabilities and threats can help to inform security design decisions. For example, actively review logs and security alerts to detect anomalous activity for all system components.

A Use Case is an abstract scenario of the interaction between an application and the actors. It helps the design development team deliver code and applications that meet a requested capability need statement. Use Cases are essential, the "path of least resistance" to show what the client wants the application to do. An Abuse Case is a type of interaction where the interaction results are harmful to the system, actors, or stakeholder mission. The Abuse Case is an approach of thinking like a hacker to check each function to see how an unethical user or hacker could break the system functions. The Abuse Case describes the minimal abuse of privilege necessary to cause harm. Essentially, it explains how not to use the system. The importance of both Use and Abuse case scenarios in defining Security Operations (SecOps) is to model and understand forms of defense and forms of abuse that we want to prevent. The attack and defend standpoints are two main approaches used in writing cyber strategies. "When written from the attack perspective, cyber strategies focus on the security testing techniques used to find and fix security vulnerabilities" (Diogenes and Ozkaya). For example, the threat actor may do a test run exfiltration to buy time to perform another attack even more harmful than the first exfiltration run. Thereby moving past a data and software attack to the hardware and lower-level processes of a system. (Diogenes and Ozkaya).

Viruses, worms, and trojans are all types of malware. A computer virus attaches itself to a computer program or a file that enables it to spread from one computer to another via an executable file. A "virus is malware that when executed tries to replicate itself into the other executable code (CRISPR Code 9); when it succeeds, the code is infected. When the infected code executes, so does the viral code" (Simske). A virus cannot infect the asset without the malicious program executing, which traditionally required human action to spread. Given today's automated environment, an automated course of action (COA) could potentially take the place of a human in

launching the executable file. A virus attaches to an executable file and (typically) requires a human action to spread.

A worm has the potential of laterally moving from computer to computer without human assistance. It is like a virus, but it can travel using information transport features on a system without human action. In addition, a worm can replicate itself on a system. A "worm is a program that runs independently and propagates a complete working version of itself onto other hosts on a network" (Simske). For example, a worm could send a copy of itself to everyone listed in an Email address book, and then everyone listed in the receiver's address book further manifesting itself. Worms can spread and replicate themselves on a system without human interaction.

A Trojan horse is a malicious software code that may appear helpful, but that is a type of malware designed to damage by deleting files and destroying information on a system. A "Trojan horse is a 'useful' program that has a hidden and possibly malicious function that evades surveillance ... [It] often uses legitimate actions to launch the hidden attack code" (Simske). Trojans are also used to create backdoors on computers that give unauthorized system access. Trojans require human action but do not self-replicate. (A. Scalco and S. Simske "Cybersecurity Awareness for Systems Engineers Graduate Coursework").

Exploit kits are automated toolkits or frameworks designed to find and exploit vulnerabilities to deliver malicious payload onto a machine. Exploit kits are sold or are made available on invitation-only forums to avoid discovery by law enforcement. (A. Scalco and S. Simske "Cybersecurity Awareness for Systems Engineers Graduate Coursework").

A zero-trust security solution approach is meant to minimize the attack surface, help to limit lateral movement across the network, and restrict unauthorized, unauthenticated access to

networks, applications, and data. The zero-trust model assumes that potential attackers are present internally and externally to an organizational network. Organizations using the zero-trust model approach to security use multifactor authentication, least-privilege access, near real-time monitoring, and various endpoint monitoring, detection, and response capabilities as part of the defense strategies. (A. Scalco and S. Simske "Cybersecurity Awareness for Systems Engineers Graduate Coursework").

Two design methods for system hardening are Multifactor Authentication (MFA) and one that accelerates authentication upon suspicious behavior that would require re-authentication. (A. Scalco and S. Simske "Cybersecurity Awareness for Systems Engineers Graduate Coursework"). An MFA uses two inputs, a two-factor authentication (2FA) for the hash (e.g., Public Key Infrastructure (PKI) public key) and the Mandatory Access Control (MAC) address of the device, particularly when combined with a trusted timestamp approach. Both system hardening approaches reduce the risk of unauthorized access to protected information. MFA requires more than one credential to verify a user's identity. MFA immediately neutralizes risks associated with compromised passwords by adding a layer of security to protect personal information. ((CMU)). When MFA is combined with a trusted timestamp approach, communication is part of the data transmission (i.e., party A sends the email to party B at this time, rather than simply it is party A's data). While re-authentication is an essential method of reducing the risk of unauthorized access, it comes with some usability issues by burdening the user who needs to re-authenticate if there is the detection of incongruent behavior in a contextual case. (A. Scalco and S. Simske "Cybersecurity Awareness for Systems Engineers Graduate Coursework").

3.3. Cybersecurity Industry Associations and Governmental Organizations

Many significant cybersecurity industry associations have emerged to promote and advocate cybersecurity. These include the Information Sharing and Analysis Centers (ISAC). The ISAC associations provide stakeholders a forum for sharing threat information and mitigation strategies such as the WaterISAC, Electricity ISAC (EISAC), the Oil & Natural Gas ISAC (ONG-ISAC), National Defense ISAC (ND-ISAC), and other sector-based ISACs. (WaterISAC). The National Council of ISACs (NCI) advocates ISACs to collaborate and comprises 25 member organizations. Regional alliances also share cybersecurity threat information and advance cybersecurity among citizens, such as the CyberWyoming Alliance, CyberOregon, and CyberTexas Foundation. These industry associations serve an essential role in promoting education, workforce development, and preparedness among practitioners, industries, law enforcement, and local governments.

InfraGard is a partnership between the Federal Bureau of Investigation (FBI) and the private sector of key critical infrastructure sectors. Its mission is to promote communication between members and the FBI related to cyber threats to critical infrastructure. InfraGard provides education, networking, and workshops about emerging technologies and threats to various professions to promote access to vulnerable critical infrastructure as targets for cyber-attacks. (InfraGard).

DHS CISA is an essential federal entity that provides advisories and reports about threats to critical infrastructure networks and provides advisories and reports about protecting industrial control systems. It has been suggested that estimating how often organizations face attacks is difficult due to underreporting to law enforcement. (Keeney et al.). The partnerships with DHS CISA, InfraGard with the FBI, and industry associations provide essential services in sharing information, reporting incidents, and promoting, developing, and establishing mutual aid and

assistance agreements. (Hemme). The National Institute of Standards and Technology (NIST) is an essential non-regulatory governmental organization that promotes the development of technology and standards, including cybersecurity. The NIST Cybersecurity Framework makes information available to help organizations improve their cybersecurity. (White and Sjelin). The International Organization for Standardization (ISO) standards are reviewed every five years, and perspectives for conducting security audits are published. (Sabillon).

4. Chapter Four – Section I Summary

The previous section provided background research about cybersecurity and control systems. Questions are formed about observations about cybersecurity concepts needed to plan for the remediation of critical infrastructure vulnerability. The need for better understanding leads to science and research scientific discovery methodology (i.e., the development of an uncertainty model experiment, development of survey questions, creation of experiment method, protocol authorization, and approval authority for monitoring the research). However, little is known during science and analysis about the alignment of cybersecurity standards, readiness, inspection, training, performance, products, and usage, nor logistics and sustainment in the DOTMLPF-P process. There is no agreement about a standard for certification. There is no defined Concept of Operation (CONOP), no understanding of governance and requirements, few (if any) legal authorities, nor performance standards during scientific discovery. Cybersecurity industry organizations provide insights, training, and exchange of information to help professionals and organizations be more successful in improving and maintaining overall cybersecurity. The goal is to gain quantitative data about the disagreement and misalignment that leads to system vulnerability. The information from the quantitative data can be used to transition from disagreement found in a chaotic domain (e.g., act, sense, respond) to misalignment in a complex environment (e.g., probe, sense, respond). A report is used to advance emergent practice by good practice and eventually demonstrate expertise transferable to C2 operational context best practice.

SECTION II – HYPOTHESIS, METHODOLOGY, AND TEST RESULTS introduce the uncertainty model.

SECTION II – HYPOTHESIS, METHODOLOGY, AND TEST RESULTS

5. Chapter Five – Hypothesis and Assessment Methodology

A hypothesis and resulting predictions to be measured based on background research are presented in this chapter. In 2020, a global pandemic focused attention on essential critical infrastructure workers as key infrastructure sectors underwent a global transformation. (C. I. S. A. (CISA) "Infrastructure Security Month 2020"). Dramatic changes to how critical infrastructure systems are controlled took hold driven by mass telework factors, instant access to information, and desire for greater efficiencies increased motivation to open more critical infrastructure to cyber control. While a digital transformation of engineering was already well underway, public and private sector organizations relied more heavily on internet-enabled functions and connectivity to critical infrastructure sectors during the global pandemic. The reliance reveals vulnerabilities to expanded threats, potential unintentional faults, insider threats by trusted current or former employees, vendors, or external adversarial attacks. Synchronizing organizational ability to recognize and respond to these threats was questioned by notable, publicly visible breaches. Adversaries target critical infrastructure systems such as power, fuel, water, and FRCS by automated cyber-attack. Control Systems control physical equipment that can cause significant physical, environmental, and socio-economic harm given adverse conditions. Attributes such as safety, availability, and cybersecurity need to be managed simultaneously to achieve mission assurance. The amount of time to drive change in a physical system can be months rather than the minutes required in an IP-based system. As physical systems become IP-connected, so does the potential to revolutionize the responsiveness of C2 from months to minutes. These systems interact over broad geographical areas. Emerging and increasingly complex functions require connectivity secure from cyber-attack without compromising the system attributes. Sources of adverse

conditions may be environmental, typical lifecycle-associated failure, or human-induced (either accidental or malicious) system degradation. (Rick Hefner). While cybersecurity is widely understood in the enterprise business IT context, it is less understood in the control system context. For example, the malicious actor group that launched the ransomware attack on the Colonial Pipeline business system claimed the goal was monetary rather than creating problems in the physical systems. (Menn and Satter). Malicious actors deployed DarkSide ransomware against the company's IT network, but there was no indication that the attack directly affected the OT. (T. C. a. I. S. A. (CISA)). In a ransomware attack, the attacker gains access to data repositories, encrypts them, and demands payment to provide the key to decrypt the file. The principle of least privilege, limiting a user account or system functions, reduces the potential of successful ransomware attacks. The user or the operating system will not have permission to install malware infections such as ransomware. Unauthorized access to general operations data can disrupt critical infrastructure (e.g., telecommunications, networks, water, Heating, Ventilation, and Air Conditioning (HVAC)), disrupting operations, shared facilities, equipment, and resources necessary to deliver functions. The potential outcome could have had a far greater consequence if the ransomware group intended to cause harm and physical damage rather than monetary gain. Instead, it was a costly wake-up call, which presents the multi-concern assurance challenge presented by digital transformation addressed in this paper.

The IIoT presents cyber access to non-IP system assets that communicate in the physical control system environment previously not widely connected to the Internet. (Munirathinam). Examples of non-IP systems domains include fire protection, material handling, building control, utility control, security, and other devices such as drones. In the United States DOD, there are an estimated 500,000 installations, 4,600 sites, 276,000 buildings, 185,00 structures, 145,000 linear

structures, and an unknown number of control system devices. (Haegley). The vulnerability threat surface is enormous, and little is understood about the workforce and job roles that manage these systems and devices.

The control system context is different from that of an IT system. In addition to operating within a diverse environment, OT operators respond to operational anomalies differently than IT users. (A. Scalco and S. Simske "Engineering and Development of a Critical Infrastructure Cyber Defense Capability for Highly Context-Sensitive Dynamic Classes — Part 1, Engineering"). OT personnel come into their field through backgrounds and education in engineering disciplines such as electrical engineering, mechanical engineering, industrial engineering, and on-the-job training (OJT). IT personnel come into their field predominantly through computer sciences, vendor-specific or non-vendor-specific training and certifications, and OJT. Skills found in OT occupations generally require more extraordinary experience with older technologies than those found in IT enterprises. (Harp and Gregory-Brown).

Retrofitting IT onto OT is a considerable risk because the OT systems were designed without knowledge about the future of IT. Retrofitting security is problematic. A better approach is an early collaboration between IT security and operations teams, or SecOps, to enhance security by integrating tools, processes, and technology from the ground up into the system. Standards are still emerging and are voluntarily implemented. Unlike bulk power systems, distribution utilities are generally not subject to mandatory Federal Energy Regulatory Commission (FERC) cybersecurity standards that exclude local electricity distribution. ((GAO)).

Maintaining C2 at near real-time or operational-relevant real-time is critical to the military forces' effectiveness. C2 is how the DOD exercises authority and direction by command channels and subordinate forces to assign tasks and objectives to accomplish the mission. C2 is comprised

of information management, decision management, and execution management. C2 includes a complex system of people, processes, procedures, technology, and doctrine, coordinated to realize the mission. The entire system, including its role at the time of operation and the environment in which it will operate, can be impacted by any change to any system elements. Analysis of agreement is essential in concept evaluation, identifying risks, and examining mechanisms and ways to effectively solve capability gaps in support of the DOTMLPF-P framework used by the United States military to examine future solutions and force readiness. (Defense "Jcids Process").

5.1. Hypothesis

An observation is that if the degree of agreement among professionals about how to defend these systems varies, then the capacity to accomplish the assigned control system mission may also vary, affecting C2 over the cyber-physical control system domain. This research attempts to discover where the uncertainty of agreement by professionals exists. The research method uses a Likert Score and sensitivity analysis using R-squared (r^2) values to measure overall agreement or uncertainty of agreement about cybersecurity for control systems that can be debilitating for an organization's effectiveness and uses semantic differential scales to reduce measurement error. (Munshi).

The model is a repeatable, novel approach to better understand how to achieve multi-concern assurance given the C2 of control system complexity. The research hypothesis for this study is that there is a likely and measurable disagreement among professionals on how to achieve cybersecurity for control systems. A questionnaire was the test of that hypothesis.

5.2. Assessment Methodology

The experiment methodology was to obtain empirical, quantitative research data using a questionnaire to gather the research data. The data collection method was a web-accessible questionnaire consisting of 203 multiple-choice questions. The timeline for data collection occurred from August 2020 to February 2021. Participation was entirely voluntary. No incentives or other reward was offered in exchange for completing the questionnaire. An essential part of the research was obtaining Institutional Review Board (IRB) protocol approval from Colorado State University, issued on July 8, 2020 (Protocol Number 20-10209H, July 8, 2020). (A. Scalco and S. J. Simske). A total of 187 people responded, with 100 participants completing all 203 questions. The mean for all responses of the post questionnaire instrument is 126. Calculating the mean removing those who did not go beyond the consent question gives a mean of 145 – further removing those participants who stopped taking the questionnaire after responding to the initial profile questions results in a mean of 170 for NNN users.

5.3. Mathematical Model

A Likert Scale questionnaire makes complex opinions simpler to understand. C2 of cybersecurity for control systems is highly complex and may complicate responses. There is no single question that makes someone sure about the cyber domain. Therefore, instead of asking one question, the researchers measure the degree to which professionals agree with various statements about cybersecurity with a rating scale. A Likert scale usually offers one or more questions, a series of answers, and a neutral midpoint. For example, participants were asked whether critical assets related to control systems in their organization had been identified. Response options included "Yes," "No," and a neutral option, "I do not know." The researchers provided clear definitions and

illustrations to reduce the potential for bias, such as an image of the Purdue Enterprise Reference Architecture (PERA) model that participants could refer to when responding. (Hong Li).

The resulting questionnaire developed consisted of nine sections of questions about aspects of multi-concern assurance:

1) Participant data was collected (e.g., occupational field, role, employment sector, education, age, gender).
2) Network systems data was collected about participant knowledge of network systems in the organization.
3) Infrastructure data was collected about participant knowledge of facilities and infrastructure used in operations.
4) Incident response data was collected about how the participant's organization handles a data breach or cyberattack, including the way consequences of the attack or breach (the "incident") are managed.
5) Resource data was collected about participant knowledge of processes by which materials, energy, services, staff, knowledge, or other assets are made available.
6) Training data was collected about representative control system training and certification courses that the participant has taken.
7) Knowledge, Skill, and Abilities (KSA) data was collected about attributes representing a body of information applied directly to the performance of a function.
8) Red Team data was collected about the participants' ability to evaluate Computer Network Defense Service Providers (CNDSPs) detection and response capabilities before live play on networks.
9) Security Consideration data was collected about the participant's cybersecurity practices,

such as penetration testing and encryption.

A numerical value was assigned to each item. For example, if the Likert scale includes the response options: "Yes," "No," or "I do not know." Responses are coded to have "yes" = 1, "no" = 2, and "I do not know" = 3 so that a higher score reflects a higher level of uncertainty of each item. After entering the individual scores, the mean was calculated or the mean score for the whole group for each question. Data in each category was given both a Likert Entropy (LE) score (Eq. 1) and a Likert Coefficient of Variation (COV) rank (Eq. 2), given as follows:

$$LE = -\sum_{i=1}^{n_{bins}} p(i) \cdot \log_2(p(i)) \quad (1)$$

$$\text{COV(LE)} = \sigma(\text{LE})/\mu(\text{LE}) \quad (2)$$

where p(i) = percent of Likert responses in bin I, n_{bins} = the number of possible Likert responses, μ(LE) = the mean Likert value for a question, and σ(LE) = the standard deviation of the Likert value for a question. Calculating the COV as the measure of dispersion is helpful when comparing scores with different units of analysis or means, which allows us to understand the disbursement of scores from participant to participant. The percentage COV generated is a dimensionless ratio of the Standard Deviation divided by the mean (Eq. 2). The ranking is by questions and overall comparison of ranks. Entropy and COV are ranked and summed for a total overall rank of uncertainty illustrated in a scatter chart. The measures of dispersion of a dataset of response relative to the mean are first calculated as the square root of variance by determining each data point deviation to the mean to generate the charts from the survey results. In other words, the measure of the dispersion of individual participant responses to the questions is calculated by all participant responses to questions placed in a bin based on the nine sections of questions described earlier

about aspects of multi-concern assurance. For example, a set of questions might be a block of questions about network systems, infrastructure, incident response, or training and certifications. Responses to the set of questions are analyzed by x- and y-variables such as occupation (i.e., engineers, computer scientists, technicians), by employment sector x- and y-variables (i.e., federal, non-federal, commercial sector), or by critical infrastructure sector x- and y-variables (i.e., transportation, communications, IT).

The mean Likert value for a question and the standard deviation of the Likert value is then calculated. For example, the Standard Deviation of the response count from all engineers to questions about network systems is calculated for each question. The mean and COV are calculated for each question by all responses by each employment sector, such as engineers. The same calculation is performed for each sector (i.e., computer scientists, technicians, safety personnel). Finally, the value of the function y is plotted against x to see if one variable response is fully explained by the other. The test was run viewing variables such as engineering as the y-variable and computer scientists as the x-variable and flipped around as engineering as the x-variable and computer scientists as the y-variable to observe the relationship. Entropy and COV were each ranked in the bin for each question. The ranking of scores is from 1 to N, the maximum domain and range of the chart is 2N assigned to the data. A total rank-sum of entropy and COV was calculated and plotted in a scatter graph for the set.

A scatter plot is used as a tool for analysis to examine the responses by two variables such as engineers and computer scientists, engineers, and safety occupations and show how much the two occupational variables correlate by giving a visual sense of the data. The strength of the relationship is established by how close the data points are plotted on a straight line. Data points on a straight line from the origin to high x- and y-values show a positive correlation. Entropy

measures the amount of uncertainty, or unknown, in the data with a visual perception of correlation explained by measuring data related to x- and y- variable pairings by the amount of space taken on the scatter plot. The experimental points are plotted and later reviewed to see if there is an agreement in the relative ranks using linear regression. The experimental points plotted are: {(rank_Entropy(x)+rank_ COV(x)), (rank_Entropy(y)+rank_COV(y))}, which is the graphical representation of the relative values of X=(rank_Entropy(x)+rank_COV(x)) and Y=(rank_Entropy(y)+rank_COV(y)). The researchers later look to see if there is an agreement in the relative ranks using linear regression.

As participant certainty or knowledge of the state of the whole cybersecurity of control systems increases, the entropy goes down. As uncertainty increases, the entropy goes up. The entropy is measured by pairings between variables such as by profession (i.e., engineers and computer scientists, engineers, and safety professionals) or critical infrastructure sector (i.e., communications and energy, or communications and IT). For example, participants were asked 23 questions about network systems such as: "User accounts and credentials are managed in our organization by the following authentication approach," graphically represented as the point of origination (10, 11) in Figure 4 engineer (y-coordinate 11) agreement with computer scientists (x-coordinate 10) about network systems. X-coordinate 10 is the total rank sum of the rank entropy and rank COV of the computer scientists' response to the question, x=(rank_Entropy(x)+rank_COV(x)). Y-coordinate 11 is the rank sum of the rank Entropy and rank COV of engineers' responses to the question, y=(rank_Entropy(y)+ rank_COV(y)).

Similarly, the total rank-sum of rank Entropy and rank COV is plotted for the other questions in the bin as {(rank_Entropy(x)+rank_ COV(x)), (rank_Entropy(y)+rank_COV(y))}. The scatter chart shows the total overall rank of uncertainty about an aspect of multi-concern

assurance. It is illustrated in a scatter chart along with the rank sum of entropy and COV response points to other questions such as: "I have decision authority for which risks are accepted as related to cyber-physical systems (CPS)," shown as point (28, 29). X-coordinate 28 is the total rank sum of the rank entropy and COV of the computer scientists' response to the question. Y-coordinate 29 is the rank sum of the rank entropy and rank COV of engineers' responses to the question. The correlation of agreement between engineers and computer scientists is plotted as point (28, 29), as shown in Figure 4, Correlation between Engineers and Computer Scientists for Network Systems Questions.

Another example is the response to the network systems question: "Our organization uses threat detection capabilities," demonstrated as point (37, 23) for the y-coordinate sum of rank entropy and rank COV for engineers (23) and the x-coordinate sum of rank entropy and rank COV for computer scientists (37). Higher entropy shows perceived information entropy, or level of uncertainty, between the two variables, graphed, in this case, the correlation between the variables of engineers and computer scientists. The graphical representation is effective for the complexity of cybersecurity for control systems.

5.4. R-Square (r^2) Pattern

The correlation coefficients indicate the strength and direction of the predicted values of the pattern by the observed value of the linear relationship between movements of two variables and quantify the strength of the relationship. A value of 1 implies that the equation perfectly describes the relationship between two variables. The correlation coefficient is denoted by r. R-square (r^2) is the proportion of explained variance or the pattern's strength. The r^2 is the statistical measure of the proportion of variance for the dependent variable explainable by the independent

variable in the mathematical model. Data were assessed by occupation, employment sector, and critical infrastructure sector. The questionnaire's occupational field options included engineering, computer science, industrial management, mathematics, physical sciences, safety, and technicians. Employment sector field options included federal, non-federal, Federally Funded Research and Development Centers (FFRDC), University Affiliated Research Centers (UARC), commercial industry, academia, student, and military service.

6. Chapter Six – Test Results

The method of conducting an experimental test of the hypothesis to determine if the data supports the hypothesis or not and the results of the experiments performed are presented in this chapter.

6.1. Participant General Profile

Participants were asked to identify the best option that described their work role as supporting IT, OT, or both the IT and OT technology community. Responses were 31.10% support IT, 11.59% OT, and 57.32% support IT and OT, as shown in Table 3. In response to questions about cyber awareness training, 95.56% said they have the training, and 4.44% said they did not have cyber awareness training. When asked if cyber awareness training is required for their position, 88.15% said, "yes;" 8.15% said, "no," and 3.70% said, "I do not know." Responses to the question if cyber awareness training is fully funded and available for their position 82.96% said, "yes;" 11.11% said, "no;" and 5.93% said, "I do not know." The response data shows that most respondents, regardless of IT, OT, or both, have some cyber awareness training, as shown in Table 4.

Table 3 Questionnaire Participant Work Roles

Response Option	Option
Support to Information Technology (IT)	31.10%
Support to Operational Technology (OT)	11.59%
Support to both IT and OT	57.32%

Table 4 Questionnaire Participant Cyber Awareness Training Data

Response Option	Yes	No	I do not know
"I have cyber awareness training."	95.56%	4.44 %	0%
"Cyber awareness training is required for my position."	88.15%	8.15%	3.70%
"Cyber awareness training is fully funded and available for my position."	82.96%	11.11%	5.93%

When responding to familiarity with the PERA reference, 58.21% said they were familiar, and 41.79% said they were unfamiliar, as shown in Table III.

Table 5 Questionnaire Participant Familiarity with PERA Architecture Reference

Response Option	Responses
Familiar with PERA Reference	58.21%
Unfamiliar with PERA Reference	41.79%

6.2. R-Square (r^2) Pattern by Occupation

Occupational field options in the questionnaire provided example occupational descriptors such as for engineering (e.g., aerospace, civil, electrical, mechanical, systems engineering); computer science (e.g., computer science, IT, management); industrial management (e.g., telecommunications, contracting, Quality Assurance (QA), transportation, marine cargo); mathematics (e.g., mathematics, mathematical statistics); physical sciences (e.g., general physical science, geophysics, chemistry); safety (e.g., safety and occupational health management, emergency management); technician (e.g., operations, maintenance).

6.2.1. Network systems (r^2) pattern by occupation

In the question section about network systems, an image of the PERA model is used to reference a control system network to understand multi-concern workforce assurance agreement in the risk management process. Risk reduction is the activity of applying security controls, or safeguards, to eliminate or reduce the threat or vulnerability. Figure 4 shows engineers' agreement with computer scientists about network systems has an r^2 value of 0.7529, which quantifies the strength of the correlation. An r^2 of 0.7529 means that a 76% variation of one variable is entirely explained by the other. However, the agreement of engineers with safety personnel about network systems shows no statistically relevant correlation, with an r^2 of 0.0003, as shown in Figure 5. The same questions participants were asked about network systems when examined by engineers and safety occupations show: "I have decision authority for which risks are accepted as related to cyber-physical systems (CPS)," as point (15, 28) in Figure 4; and "Our organization uses threat detection capabilities," as point (15, 23) in Figure 5. Plot (46, 46) in Figure 4 shows responses engineer (y-coordinate 46) with computer scientists (x-coordinate 46) to the question: "I have cyber awareness training," which for engineers (y-coordinate 46) and safety personnel (x-coordinate) is plotted as (15, 46). X-coordinate 15 is the total rank sum of the rank entropy and rank COV of the safety personnel response to the question. Y-coordinate 46 is the rank sum of the rank Entropy and rank COV of engineers' responses to the question. The correlation of agreement between engineers and safety personnel is plotted as point (15, 46). Recall that the points plotted are: {(rank_Entropy(x)+ rank_ COV(x)), (rank_Entropy(y)+rank _COV(y))}, which is the graphical representation of the relative values of X= (rank_Entropy(x)+rank_COV(x)) and Y=(rank_Entropy(y)+rank_COV(y)).

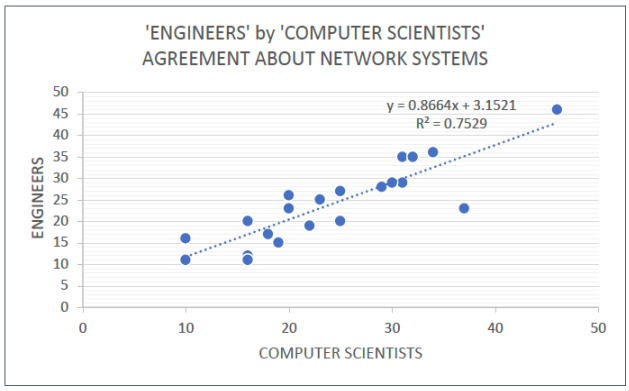

Figure 4 Correlation between Engineers and Computer Scientists for Network Systems Questions

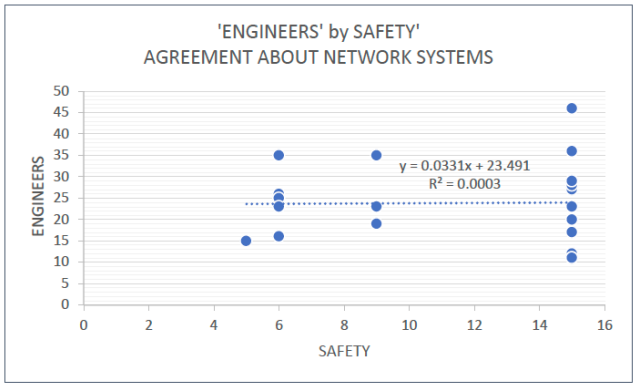

Figure 5 Correlation between Engineers and Safety Personnel for Network Systems Questions

6.2.2. Infrastructure (r^2) pattern by occupation

Figure 6 compares engineers (y-coordinate) and computer scientists (x-coordinate) in a like manner about infrastructure and has an r^2 value of 0.7495. Thus, an r^2 of 0.7495 for engineers and computer scientists is relatively high for the data set. However, engineers' (y-coordinate) agreement with technicians (x-coordinate) about infrastructure has an r^2 of 0.0361, as shown in Figure 7. Participants were asked 20 questions about infrastructure, such as: "I have access to the physical network topology," demonstrated as engineers (y-coordinate) and computer scientists (x-coordinate) point (17, 14) in Figure 6, and as engineers (y-coordinate) and technicians (x-coordinate) point (8, 14) in Fig. 4. Furthermore, "I know the single points of failure" is shown as

point (29, 32) in and as point (8, 32) in Figure 7. The origination points in Figure 6 in response to the question: "In our organization, a timestamp is used to reference persistent time-based trends" as point (13, 11). Timestamp data is an essential element for practical cybersecurity. Trusted digital timestamping is used to prove specific data before a particular point in time. The feature tracks the creation and modification of an artifact. Once created, the timestamp data should not be changeable (not even by the originator) to ensure the timestamp integrity cannot be compromised. It is helpful in cybersecurity practice to identify external party access to an operational system making application changes without the possibility that the originator can make changes to the timestamp. However, responses to the same question visualized by engineers (y-coordinate) and technicians (x-coordinate) are seen as points (8, 11), as shown in Figure 7.

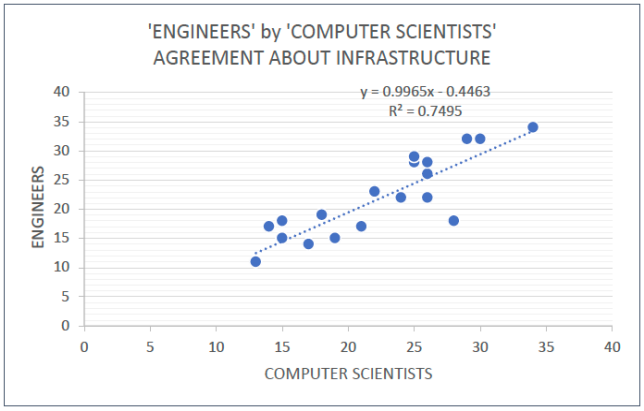

Figure 6 Correlation between Engineers and Computer Scientists for Infrastructure Questions

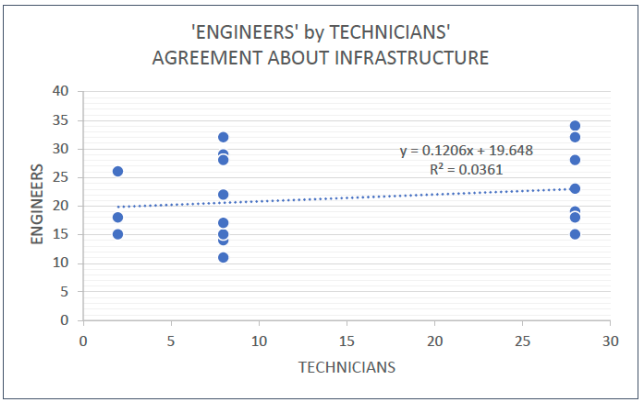

Figure 7 Correlation between Engineers and Technicians for Infrastructure Questions

6.2.3. Incident Response (r^2) pattern by occupation

Participants were asked eight questions about the incident response in their organization, such as: "Cyber incident response policies, procedures, and logistics are well documented in our organization;" and "Our incident response plan includes a cybersecurity element." Figure 8 shows the dependent variable is by engineers, and the independent variable is the computer scientist occupations agreement about incident response. Engineer agreement with computer scientists about incident response has a moderate r^2 value of 0.5096. An r^2 of 0.5096 means there is a modest correlation. Figure 9 shows the agreement of engineers with industrial management about incident response has an r^2 of 0.3313. When examined on the scatter chart, the point of origination is the point response to the question: "Upstream and downstream Points of Contact (POC) are known," as point (5, 5) in Figure 8.

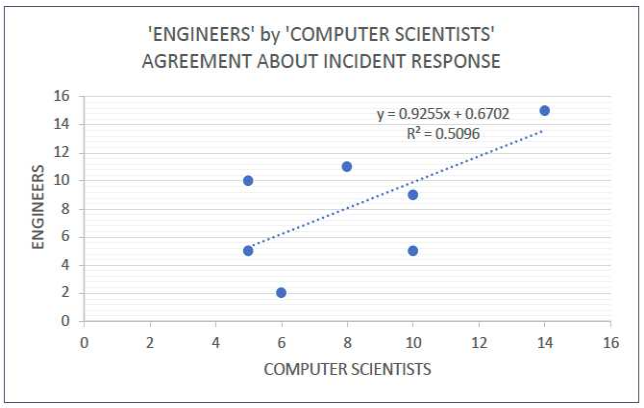

Figure 8 Correlation between Engineers and Computer Scientists for Incident Response Questions

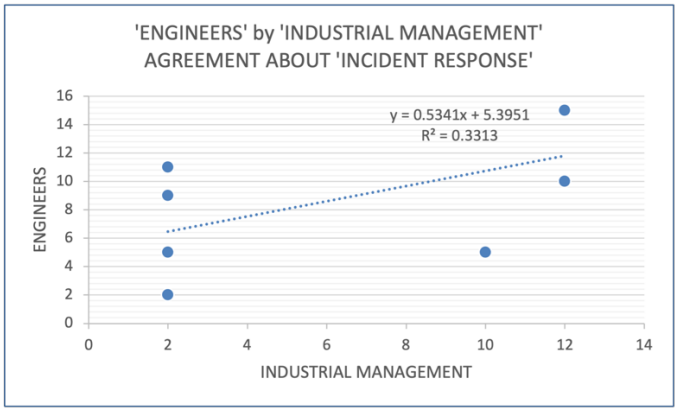

Figure 9 Correlation between Engineers and Industrial Management for Incident Response Questions

6.2.4. Resource (r^2) pattern by occupation

Participants were asked 12 questions about resources, or the processes by which materials, energy, services, staff, knowledge, or other assets are made available to the organization, such as: "Our organization has contracted vendor-supplied technical support," shown as point (11, 9) in Figure 10 and point (14, 9) in Figure 11; and "Our vendor-supplied support contract includes an incident response element," as shown as point (11, 11) in Figure 10 and point (14, 11) in Figure 11. Figure 10 shows that engineer agreement with computer scientists about resources is weak in an r^2 value of 0.3739. This r^2 means that the variation of one variable cannot be explained by the

other. Figure 11 shows the agreement of engineers with technicians about resources has an r^2 value of 0.0544. Point (23, 15) in Figure 10 shows the response to the question "Our organizations know about US Government incident response support and resources." Furthermore, point (16, 22) in Figure 11 shows the response when asked, "Our organization has cleared employees authorized to access classified information." The same two questions in Figure 11 are shown as points (14, 15) and (14, 22).

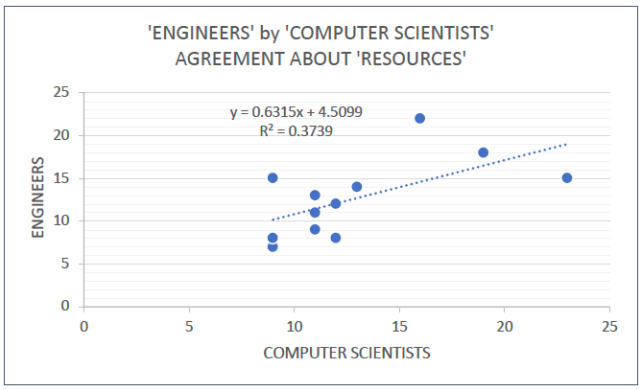

Figure 10 Correlation between Engineers and Computer Scientists for Resource Questions

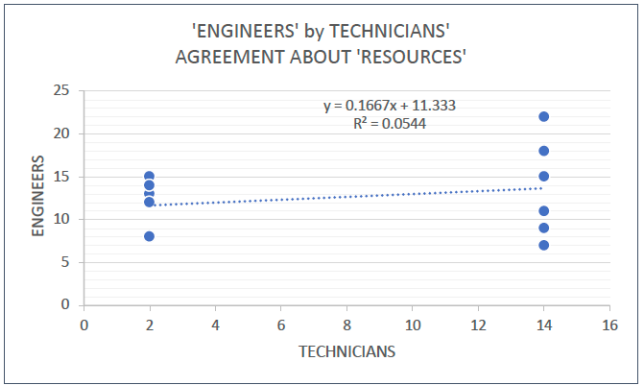

Figure 11 Correlation between Engineers and Technicians for Resource Questions

6.2.5. Training (r^2) pattern by occupation

A series of questions were asked regarding training and certifications. The sections identified representative available training and certification courses. Participants were asked

questions about having taken available training such as the Naval Post Graduate School's (NPS): "Cyber Security Incident Response and Recovery," shown as the point of origination (17, 18) in Figure 12 engineer agreement with computer scientists about training. Agreement of engineers with computer scientists about training has an r^2 value of 0.1646.

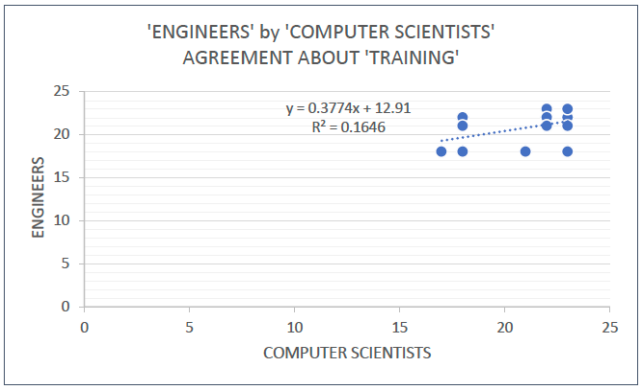

Figure 12 Correlation between Engineers and Computer Scientists for Training Questions

6.2.6. Knowledge, Skills, and Abilities (KSA) (r^2) pattern by occupation

Participants were asked about KSA applied directly to the performance of a function. Participants were asked 56 questions about KSA, such as: "I maintain awareness of vulnerabilities to legacy or older systems (due to age)," shown as point (45, 44) in Figure 13; and "I maintain awareness and active, valued communication between workforce groups about ongoing vulnerabilities and newly discovered threats," shown as point (48, 57). Figure 13 shows the correlation of agreement between engineers and computer scientist occupations about KSA. For example, engineering with computer scientists about KSA has an r^2 value of 0.222. This r^2 means that the variation of one variable cannot be explained by the other.

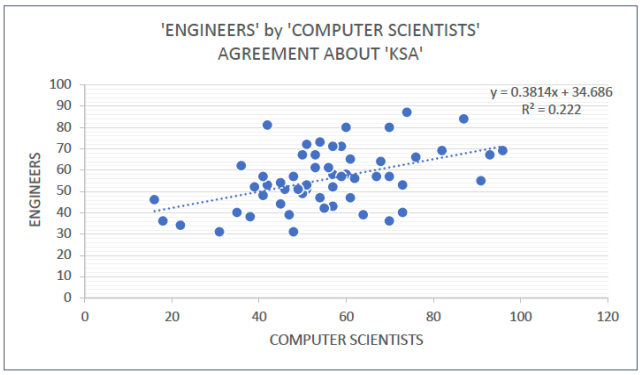

Figure 13 Correlation between Engineers and Computer Scientists for Knowledge, Skills, and Abilities (KSA) Questions

6.2.7. Red team (r^2) pattern by occupation

A Red Team assesses security for vulnerability from an opposing view, and the blue team looks at how to identify, evaluate, and respond to intrusions. The questionnaire posed 14 questions in the Red Team section is about the use of security feedback and the ability to assess CNDSP to live "play" on the DOD network. A Red Team tests a systems' networks, applications, technologies, human vulnerabilities, processes, and physical components to expose potential vulnerabilities and risks. Participants were asked questions about Red Team activities such as: "Red Team recommendations are tracked to resolution (e.g., patch or remediation) as part of the risk management process," as shown as point (14, 14) in Figure 14; and "Red Teams meet current mission requests made by our organization," as shown as point (11, 12) in Figure 14. Figure 14 shows the correlation of agreement between engineers and computer scientist occupations about Red Team. Engineer agreement with computer scientists about Red Teams has an r^2 value of 0.6067. An r^2 of 0.6067 for engineers and computer scientists is moderate for the data set.

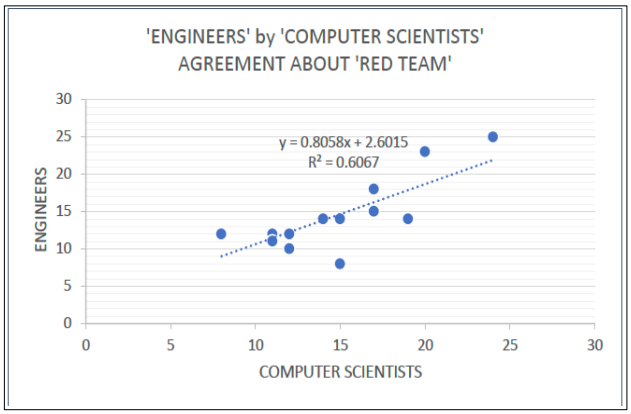

Figure 14 Correlation between Engineers and Computer Scientists for Red Team Questions

6.2.8. Security considerations (r^2) pattern by occupation

Questionnaire participants were given statements to describe the organizational knowledge of cybersecurity quality attributes such as baselining the system, including details concerning system interfaces and maintenance of configurations; timestamp data classification, encryption, and backup controls; Incident Response Plans (IRP) to recover from an attack; patch management to reduce risks from zero-day attacks; perimeter defense policies such as the use of VPN; and employee training. For example, participants were asked to respond to statements about security considerations such as: "In our organization time services are managed and provisioned separately for IT and OT systems management process," shown as point (23, 22) in Figure 15; "Intrusion Prevention Systems (IPS) deployed on control systems to actively block suspect traffic are tested to ensure that a given signature will not block a legitimate control command," as shown as point (25, 23) in Figure 15; and "Traditional statistical forecasting strategies (e.g., dynamic regression) are used in our organization as a baseline for prediction of network performance," is shown as point (23, 23) in Figure 15. Dynamic regression allows for including information in a forecasting model that may be relevant predictor variables to network performance. Figure 15 shows that the correlation between engineers and computer scientists about security considerations is weak, with an r^2 value of 0.325.

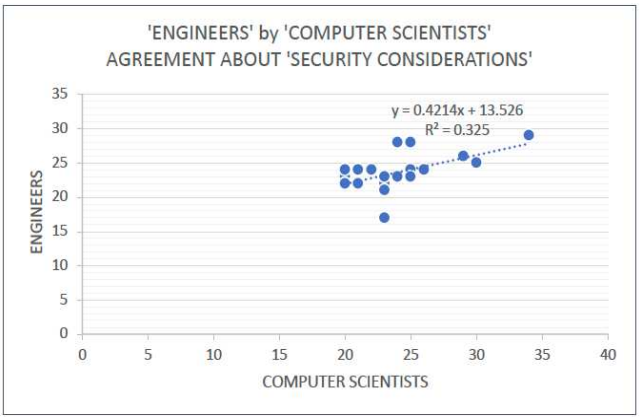

Figure 15 Correlation between Engineers and Computer Scientists for Security Consideration Questions

6.3. R-Square (r^2) Pattern by Employment Sector

Employment field options in the questionnaire provided example employment sector descriptors such as for federal (e.g., non-elected and non-military public sector employees); non-federal (e.g., state, municipality, local, tribal); FFRDC; UARC; commercial industry; academia (e.g., professor, academic researcher); student; military service (e.g., Army, Navy, Air Force, Marines, Coast Guard, military reserves).

6.3.1. Network systems (r2) pattern by employment sector

In the question section about network systems, the data is analyzed by the employment sector, like the pattern by occupation. An image of the PERA model is used to reference a control system network to understand multi-concern workforce assurance agreements in the risk management process. Figure 16 shows federal employees' agreement with commercial industry employees about network systems has an r^2 value of 0.4296, which quantifies the strength of the correlation. An r^2 of 0.4296 means that a 43% variation of one variable is entirely explained by the other. The federal employees' agreement with military services personnel about network systems has an r^2 of 0.559, as shown in Figure 17. The same questions participants were asked

about network systems when examined by federal and commercial industry occupations show: "I have decision authority for which risks are accepted as related to cyber-physical systems (CPS)," as point (24, 28) in Figure 17; and "Our organization uses threat detection capabilities," as point (25, 27) in Figure 17. Plot (46, 46) in Figure 16 shows responses federal (y-coordinate 46) with commercial industry (x-coordinate 46) to the question: "I have cyber awareness training," which for federal sector occupations (y-coordinate 46) and commercial sector (x-coordinate) is plotted as (46, 46). X-coordinate 46 is the total rank sum of the rank entropy and rank COV of the commercial industry professionals who responded to the question. Y-coordinate 46 is the rank sum of the rank Entropy and rank COV of engineers' responses to the question. The correlation of agreement between engineers and the commercial industry is plotted as point (46, 46). Recall that the points plotted are: {(rank_Entropy(x)+rank_ COV(x)), (rank_Entropy(y)+rank _COV(y))}, which is the graphical representation of the relative values of X= (rank_Entropy(x)+rank_COV(x)) and Y=(rank_Entropy(y)+rank_COV(y)).

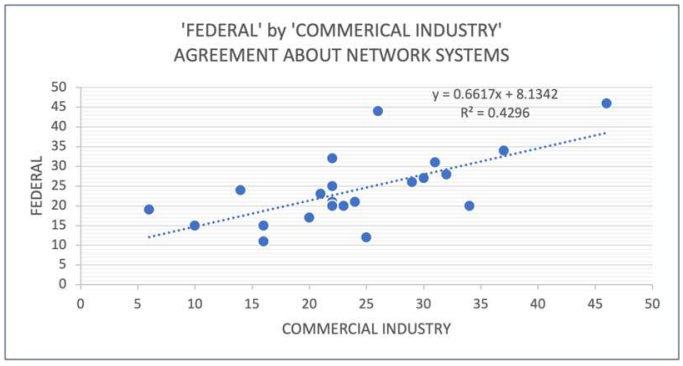

Figure 16 Correlation between Federal and Commercial Industry for Network Systems Questions

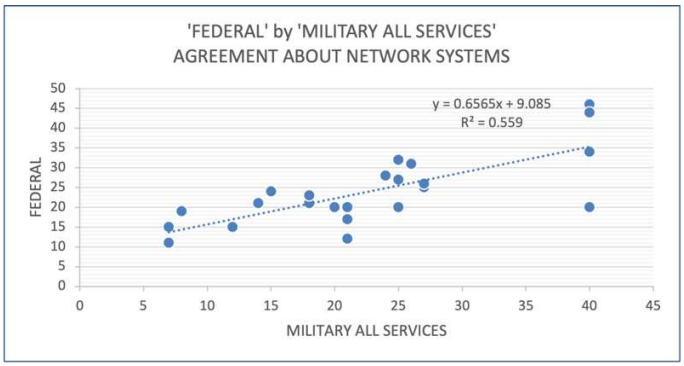

Figure 17 Correlation between Federal and Military for Network Systems Questions

6.3.2. Infrastructure (r2) pattern by employment sector

Figure 18 compares federal (y-coordinate) and commercial industry (x-coordinate) in a like manner as by occupation about infrastructure and has an r^2 value of 0.4196. Thus, an r^2 of 0.4196 for federal and commercial industry professionals is moderate for the data set. However, federal (y-coordinate) agreement with military services (x-coordinate) about infrastructure has an r^2 of 0.6477, as shown in Figure 19. Participants were asked 20 questions about infrastructure, such as: "I have access to the physical network topology," demonstrated as federal (y-coordinate) and commercial industry (x-coordinate) point (17, 17) in Figure 18, and as federal (y-coordinate) and military services (x-coordinate) point (12, 17) in Figure 19. Furthermore, "I know the single points of failure" is shown as point (27, 32) in and as point (29, 32) in Figure 19. The origination point (12, 13) in Figure 18 in response to the question: "In our organization, a timestamp is used to reference persistent time-based trends." Timestamp data is an essential element for practical cybersecurity. Responses to the same question visualized by federal (y-coordinate) and military services (x-coordinate) are seen as points (12, 13), as shown in Figure 19.

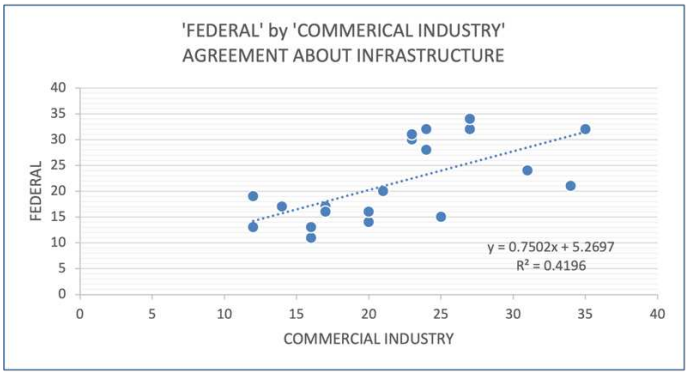

Figure 18 Correlation between Federal and Commercial Industry for Infrastructure Questions

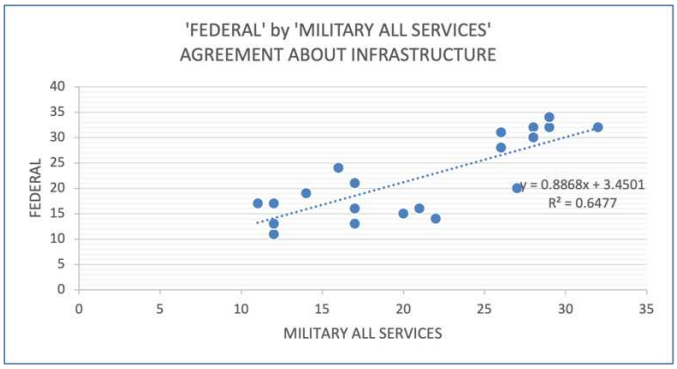

Figure 19 Correlation between Federal and Military for Infrastructure Questions

6.3.3. Incident Response (r2) pattern by employment sector

Participants were asked eight questions about incident response in their organization, such as: "Cyber incident response policies, procedures, and logistics are well documented in our organization;" and "Our incident response plan includes a cybersecurity element." Figure 20 shows that the dependent variable is federal, and the independent variable is the commercial industry agreement about incident response. Federal agreement with the commercial industry about incident response has a weak r^2 value of 0.0792. An r^2 of 0.0792 means there is a weak correlation. Figure 21 shows that the federal agreement with military services about incident response has a weak r^2 of 0.0442. When examined on the scatter chart, the point of origination is the point

response to the question: "Upstream and downstream Points of Contact (POC) are known," as point (3, 8) in Figure 20, and as point (9,8) in Figure 21.

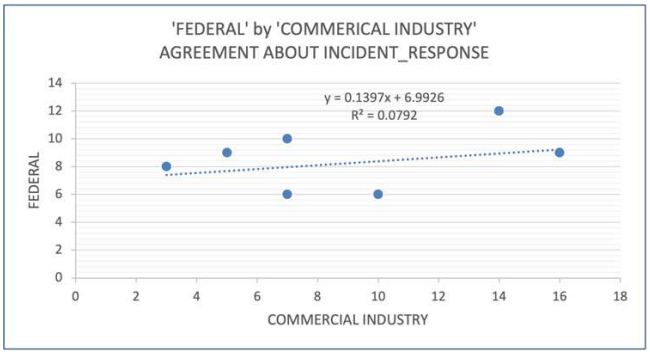

Figure 20 Correlation between Federal and Commercial Industry for Incident Response Questions

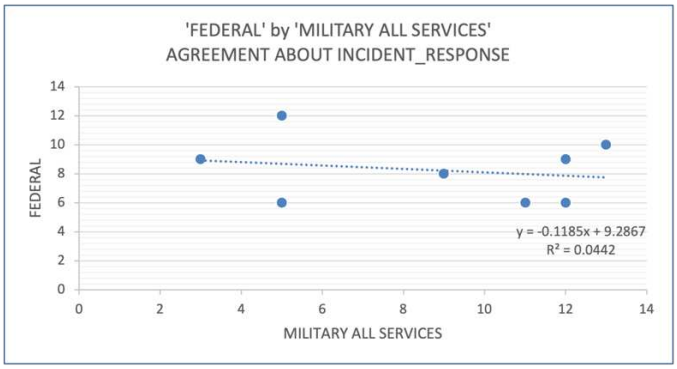

Figure 21 Correlation between Federal and Military for Incident Response Questions

6.3.4. Resource (r2) pattern by employment sector

Participants were asked 12 questions about resources, or the processes by which materials, energy, services, staff, knowledge, or other assets are made available to the organization, such as: "Our organization has contracted vendor-supplied technical support," shown as point (14, 10) in Figure 22 and point (8, 10) in Figure 23; and "Our vendor-supplied support contract includes an incident response element," as shown as point (9, 11) in Figure 22 and point (9, 11) in Figure 23. Figure 22 federal agreement with commercial industry about resources shows no statistically

relevant correlation, with an r^2 value of 0.0693. This r^2 means that the variation of one variable cannot be explained by the other. However, Figure 23 shows that federal agreement with military services about resources has an r^2 value of 0.7034. An r^2 of 0.7034 means that a 70% variation of one variable is entirely explained by the other. Point (9, 9) in Figure 22 shows the response to the question, "Our organization is aware of the Department of Energy (DOE) Cybersecurity Risk Information Sharing Program (CRISP)." Furthermore, point (7, 11) in Figure 22 shows the response when asked, " Our organization has used the available DHS support services." The same two questions in Figure 23 are shown as points (7, 9) and (10, 11), respectively.

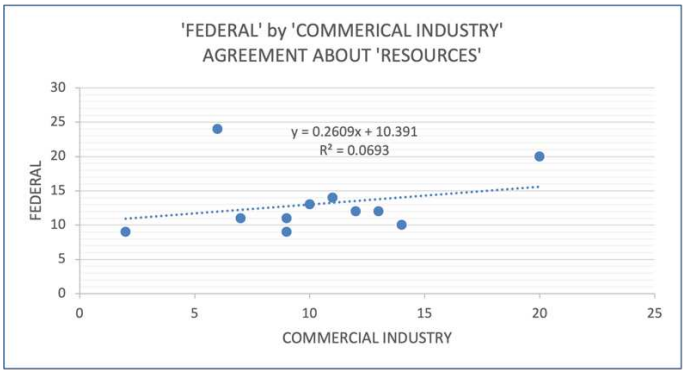

Figure 22 Correlation between Federal and Commercial Industry for Resources Questions

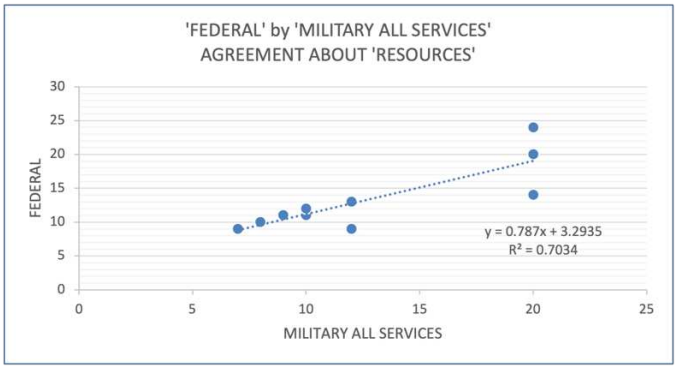

Figure 23 Correlation between Federal and Military for Resources Questions

6.3.5. Training (r2) pattern by employment sector

A series of questions were asked regarding training and certifications. Participants were asked questions about having taken available training such as the ISA.org: "Cyber Security of Automation, Control, and SCADA Systems," shown as the origination point (23, 16) in Figure 24 federal with commercial industry about training. The same questions are shown as points (21, 16) in Fig. 26 and (22, 16) in Figure 26. Agreement of federal with commercial industry about training has an r^2 value of 0.1152. Figure 25 shows that the federal agreement with military services about training has an r^2 value of 0.3866. Figure 26 shows the federal agreement with FFRDC about training has an r^2 value of 0.1606.

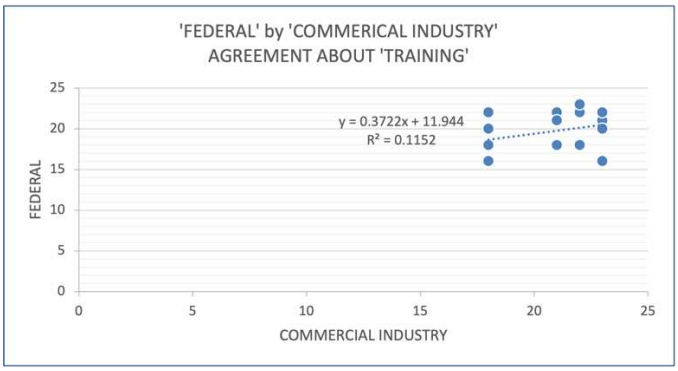

Figure 24 Correlation between Federal and Military for Training Questions

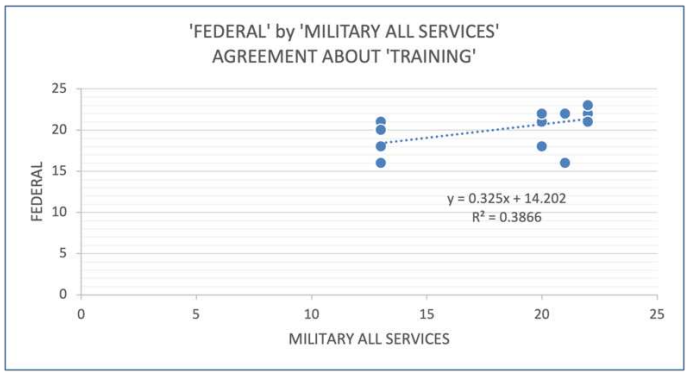

Figure 25 Correlation between Federal and Military for Training Questions

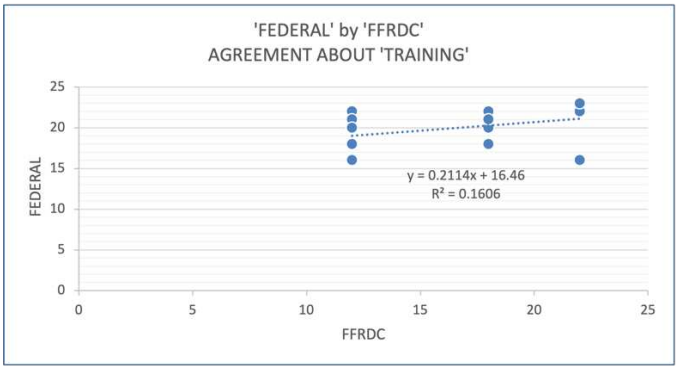

Figure 26 Correlation between Federal and FFRDC for Training Questions

6.3.6. KSA (r2) pattern by employment sector

Participants were asked about KSA applied directly to the performance of a function. Participants were asked 56 questions about KSA, such as: "I maintain awareness of vulnerabilities to legacy or older systems (due to age)," shown as point (53, 19) in Figure 27; and "I am able to provide updates on vulnerabilities and identify changes in vulnerabilities," demonstrated as point (21, 59).

Figure 28 shows the correlation of agreement between federal and military services about KSA. The same questions are shown as points (56, 19) and (10, 59) in Figure 28. The federal and commercial industry agreement about KSA has an r^2 value of 0.0804. Agreement of federal and military services about KSA has an r^2 value of 0.1488. The r^2 values mean that the variation of one variable cannot be explained by the other.

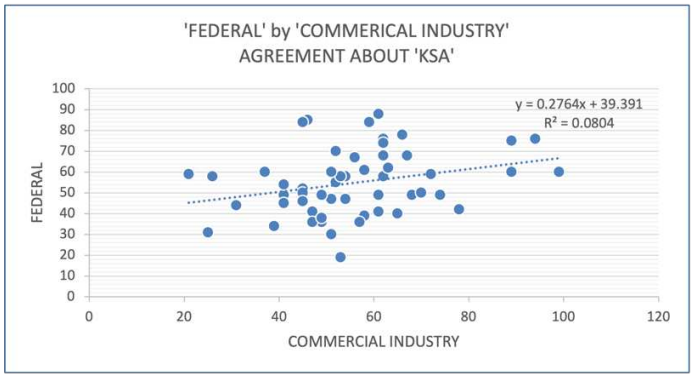

Figure 27 Correlation between Federal and Commercial Industry for KSA Questions

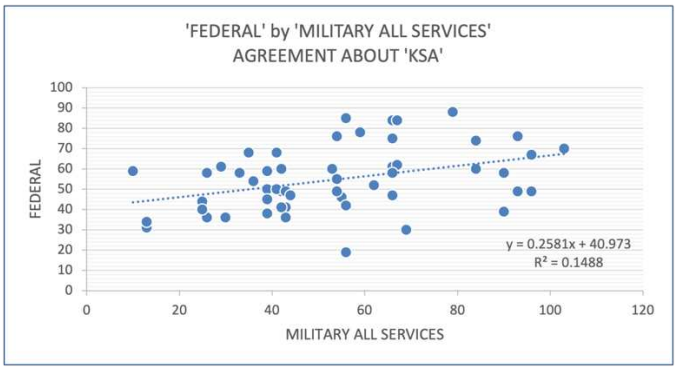

Figure 28 Correlation between Federal and Military for KSA Questions

6.3.7. Red Team (r2) pattern by employment sector

A Red Team assesses security for vulnerability from an opposing view, and the blue team looks at how to identify, evaluate, and respond to intrusions. The questionnaire posed 14 questions in the Red Team section is about the use of security feedback and the ability to assess CNDSP to live "play" on the DOD network. Employment sector responses were evaluated. Participants were asked questions about Red Team activities such as: "Red Team recommendations are tracked to resolution (e.g., patch or remediation) as part of the risk management process," as shown as point (14, 8) in Figure 29; and "Red Teams meet current mission requests made by our organization," as shown as point (14, 7) in Figure 29. Figure 29 shows the correlation of agreement between the

federal and the commercial industry employment sector about Red Team. Federal agreement with the commercial industry about Red Teams has an r^2 value of 0.4048. An r^2 of 0.4048 is moderate for the data set. The same questions are shown as points (14, 8) and (13, 7) in Figure 30. Federal agreement with military services about Red Teams has an r^2 value of 0.5115. An r^2 of 0.5115 is moderate for the data set.

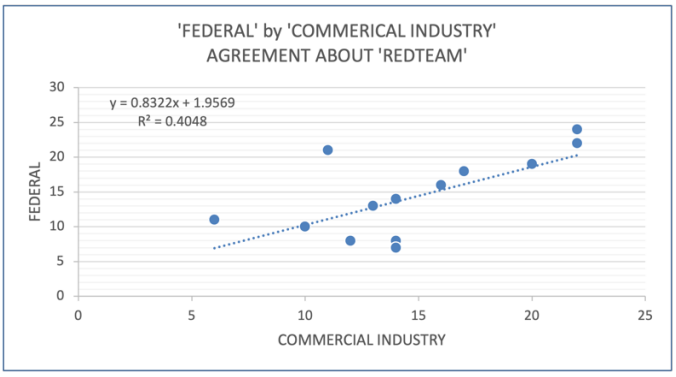

Figure 29 Correlation between Federal and Commercial Industry for Red Team Questions

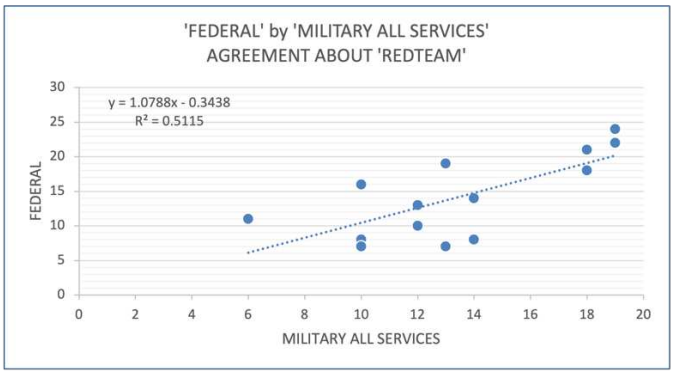

Figure 30 Correlation between Federal and Military for Red Team Questions

6.3.8. Security Considerations (r2) pattern by employment sector

Questionnaire participants were given statements to describe the organizational knowledge of cybersecurity quality attributes. For example, participants were asked to respond to comments about security considerations such as: "In my current job function, timestamp data is used to

reference persistent time-based trends for IT systems (e.g., enterprise network systems)," shown as point (32, 14) in Figure 31; "In my current job function, timestamp data is used to reference persistent time-based trends for OT systems (e.g., cyber-physical systems and control systems)," as shown as point (31, 13) in Figure 31; and "Network traffic is externally encrypted using a network-based encryption appliance on our organization's network systems," is shown as point (17, 22) in Figure 31. Network traffic encryption guarantees privacy and authentication. Fig. 11 indicates that the federal and commercial industry correlation with security considerations is weak, with an r^2 value of 0.2483. The same questions are shown as points (25, 14), (24, 13), and (23, 17), respectively, in Figure 32 for federal and military services. Figure 33 shows that the correlation between federal and UARC about security considerations is weak, with an r^2 value of 0.0008. Federal and UARC responses to the questions are shown as points (21, 14), (31, 13), and (22, 17), respectively.

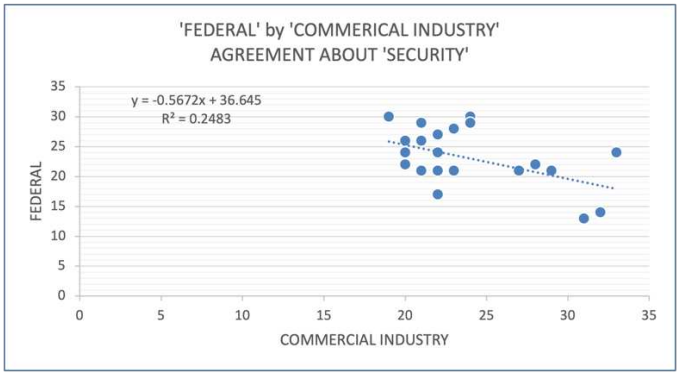

Figure 31 Correlation between Federal and Commercial Industry for Security Questions

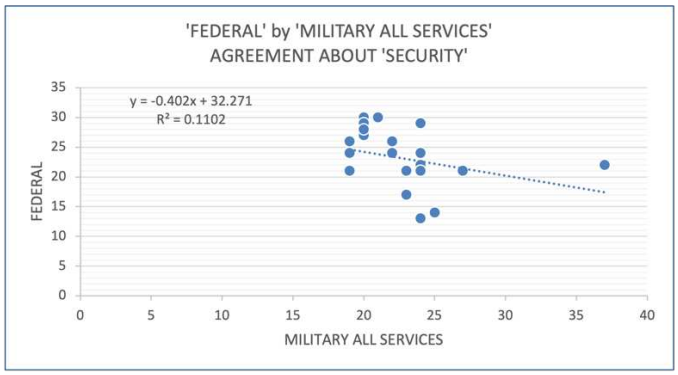

Figure 32 Correlation between Federal and Military for Security Questions

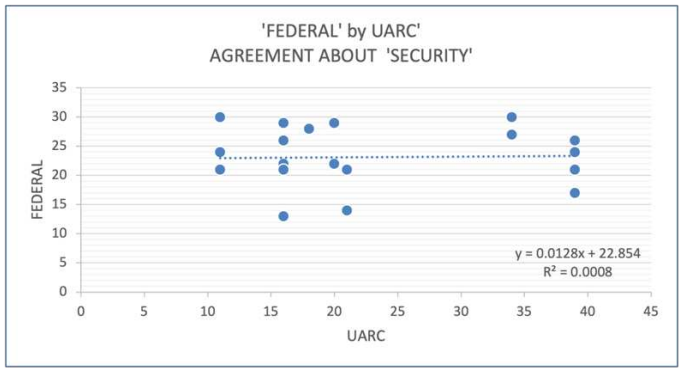

Figure 33 Correlation between Federal and UARC for Security Questions

6.4. R-Square (r^2) Pattern by Critical Infrastructure Sector

Critical infrastructure sector options in the questionnaire provided example vital infrastructure sector descriptors such as for chemical; commercial facilities; communications; critical manufacturing; dams; Defense Industrial Base (DIB); emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials, and waste; transportation systems; water and wastewater systems.

6.4.1. Network systems (r2) pattern by the critical infrastructure sector

Again, in the question section about network systems, an image of the PERA model is used to reference a control system network to understand multi-concern workforce assurance agreement in the risk management process. Figure 34 shows that all sectors' agreement with government facilities about network systems has an r^2 value of 0.3203, which quantifies the strength of the correlation. An r^2 of 0.3203 shows no statistically relevant correlation, as shown in Figure 34. The same questions participants were asked about network systems when examined by all sectors and government facilities show: "User accounts and credentials are managed in our organization by the following authentication approach," as point (4, 14) in Figure 34; and "Our organization uses threat detection capabilities," as point (28, 12) in Figure 34. Figure 34 shows responses all sectors (y-coordinate 20) with government facilities (x-coordinate 16) to the question: "Another outside organization has access to the Industrial Control System (ICS)/ Supervisory control and data acquisition (SCADA) capabilities of our organization," which for all sectors (y-coordinate 20) and government facilities (x-coordinate 16) is plotted as (20, 16). X-coordinate 16 is the total rank sum of the rank entropy and rank COV of the government facilities' personnel response to the question. Y-coordinate 20 is the rank sum of the rank Entropy and rank COV of all sectors' responses to the question. The agreement correlation between all sectors and government facilities personnel is plotted as point (20, 16). Recall that the points plotted are: {(rank_Entropy(x)+rank_ COV(x)), (rank_Entropy(y)+rank _COV(y))}, which is the graphical representation of the relative values of X=(rank_Entropy(x)+rank_COV(x)) and Y=(rank_Entropy(y)+rank_COV(y)). The same questions are shown in Figure 35 for all sectors and transportation systems as points (4, 5), (28, 16), and (20, 23), respectively. Figure 35 shows that the correlation between all sectors and transportation about security considerations is weak, with an r^2 value of 0.0218. Figure 36 shows

all sectors, and Healthcare and Public Health responses to the questions are shown as points (4, 7), (28, 31), and (20, 14), respectively. Figure 36 shows the correlation between all sectors and Healthcare and Public Health about security considerations is weak with an r^2 value of 0.1426.

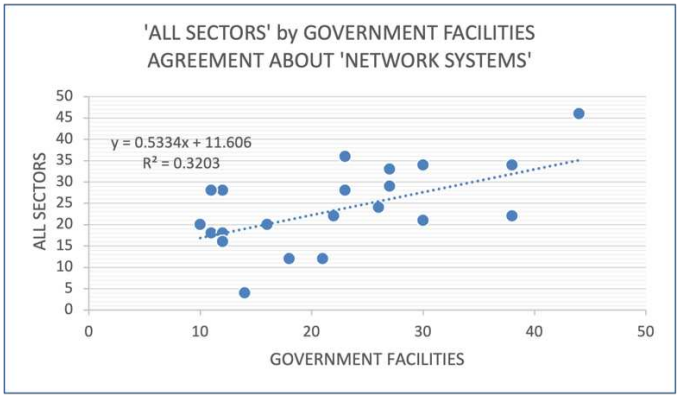

Figure 34 Correlation between All Sectors and Government Facilities for Network Questions

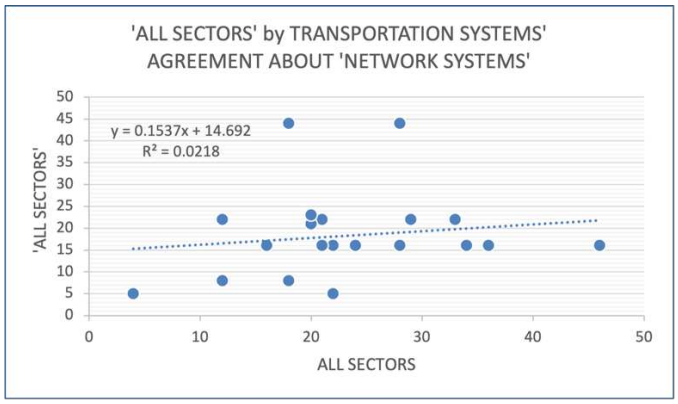

Figure 35 Correlation between All Sectors and Transportation for Network Questions

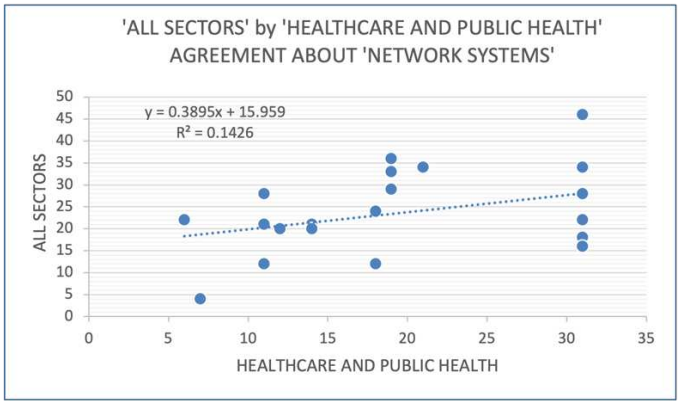

Figure 36 Correlation between All Sectors and Healthcare and Public Health for Network Questions

6.4.2. Infrastructure (r2) pattern by the critical infrastructure sector

Figure 37 compares government facilities (y-coordinate) and financial services (x-coordinate) regarding infrastructure and has an r^2 value of 0.0417. Government facilities (y-coordinate) agreement with the energy sector (x-coordinate) about infrastructure has an r^2 of 0.0847, as shown in Figure 38. IT sector (y-coordinate) agreement with the healthcare and public health sector (x-coordinate) about infrastructure has an r^2 of 0.0013, as shown in Figure 39. Participants were asked 20 questions about infrastructure, such as: "I have access to the physical network topology," demonstrated as government facilities (y-coordinate) and financial services (x-coordinate) point (11, 23) in Figure 37, as government facilities (y-coordinate) and energy sector (x-coordinate) point (10, 23) in Figure 38, and as IT (y-coordinate) and healthcare and public health (x-coordinate) point (21, 18) in Figure 39. Furthermore, "Defensive countermeasures are in place to protect operations," shown as point (33, 14) in Figure 37, as point (25, 14) in Figure 38, and as point (13, 26) in Figure 39. The origination point in Figure 37 in response to the question: "Standard operations and activities are characterized" as point (33, 19). Responses to the same question visualized by government facilities (y-coordinate) and the energy sector (x-coordinate) are seen as points (25, 19), as shown in Figure 38. However, responses to the same question

visualized by IT (y-coordinate) and the healthcare and public health sector (x-coordinate) are seen as points (13, 22), as shown in Figure 39.

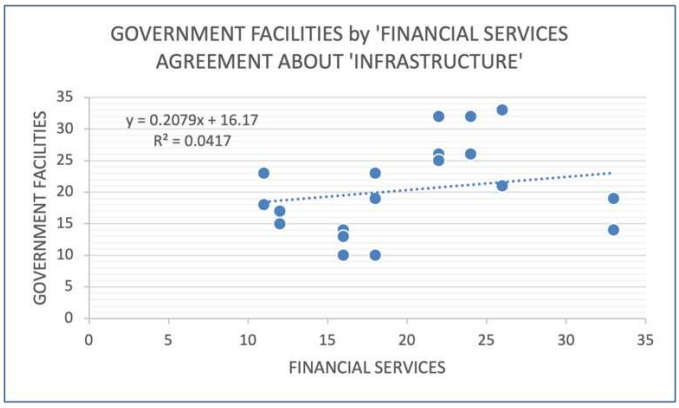

Figure 37 Correlation between Government Facilities and Financial Services for Infrastructure Questions

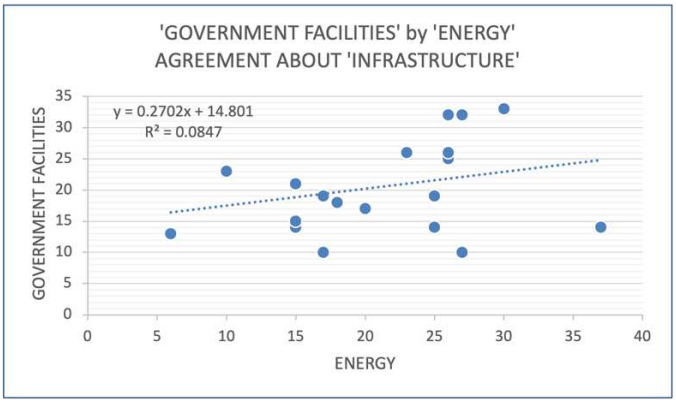

Figure 38 Correlation between Government Facilities and Energy for Infrastructure Questions

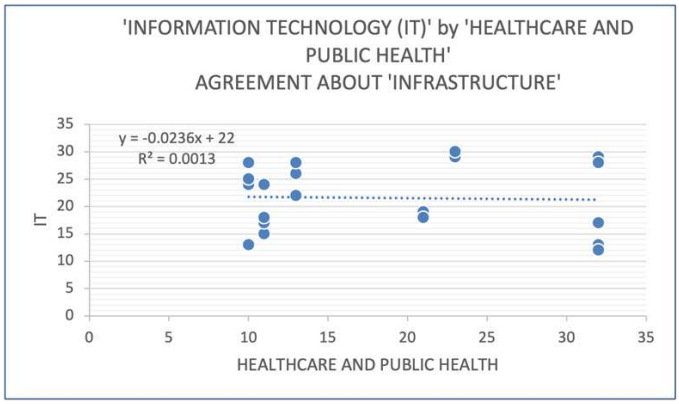

Figure 39 Correlation between Information Technology (IT) and Healthcare and Public Health for Infrastructure Questions

6.4.3. Incident Response (r2) pattern by the critical infrastructure sector

Participants were asked eight questions about incident response in their organization. Figure 40 shows that the dependent variable is by all sectors, and the independent variable is the DIB agreement about incident response. All sector agreement with the DIB about incident response has an r^2 value of 0.0103. An r^2 of 0.0103 means there is no correlation. Figure 41 shows the agreement of all sectors with the energy sector about incident response has an r^2 of 0.0021. Figure 42 shows the agreement of all sectors with the financial services sector about incident response has an r^2 of 0.0004. Figure 42 shows the agreement of all sectors with the healthcare and public health sector about incident response has an r^2 of 0.0032. When examined on the scatter chart, the point of origination is the point response to the question: "Upstream and downstream Points of Contact (POC) are known," as point (8, 2) in Figure 40, as point (14, 2) in Figure 41, as point (6, 2) in Figure 42, and as point (3, 2) in Figure 43. When examined on the scatter chart, the point of origination is the point response to the question: "Incident response procedures impact operations.," as point (7, 11) in Figure 40, as point (12, 11) in Figure 41, as point (5, 11) in Figure 42, and as point (3, 11) in Figure 43.

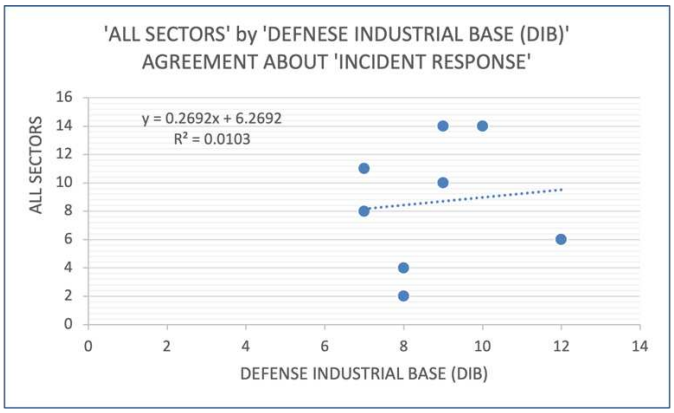

Figure 40 Correlation between All Sectors and Defense Industrial Base (DIB) for Incident Response Questions

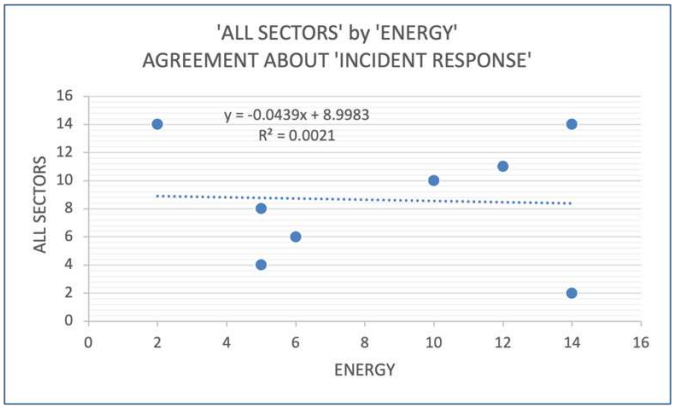

Figure 41 Correlation between All Sectors and Energy for Incident Response Questions

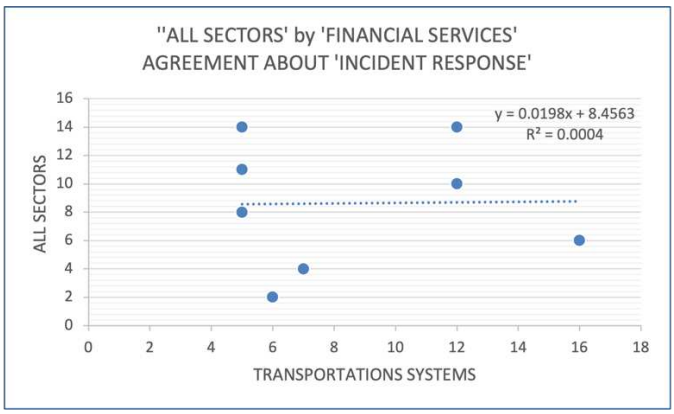

Figure 42 Correlation between All Sectors and Financial Services for Incident Response Questions

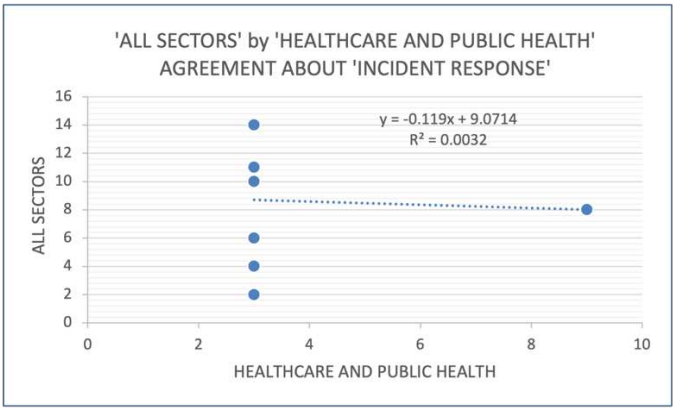

Figure 43 Correlation between All Sectors and Healthcare and Public Health for Incident Response Questions

6.4.4. Resource (r2) pattern by the critical infrastructure sector

Participants were asked 12 questions about resources, or the processes by which materials, energy, services, staff, knowledge, or other assets are made available to the organization, such as: "Our organization has contracted vendor-supplied technical support," shown as point (13, 6) in Figure 44, as point 12, 6) in Figure 44, and point (17, 6) in Figure 46; and "Our vendor-supplied support contract includes an incident response element," as shown as point (13, 8) in Figure 44, point (13, 8) in Figure 44, and point (17, 8) in Figure 46. Figure 44 shows that all sector personnel agreement with government facilities about resources is an r^2 value of 0.1351 weak. This r^2 means that the variation of one variable cannot be explained by the other. Figure 44 shows the agreement of all sectors with the DIB sector about resources has an r^2 value of 0.1879. Figure 46 shows the agreement of all sectors with the financial services sector has an r^2 value of 0.0196 weak.

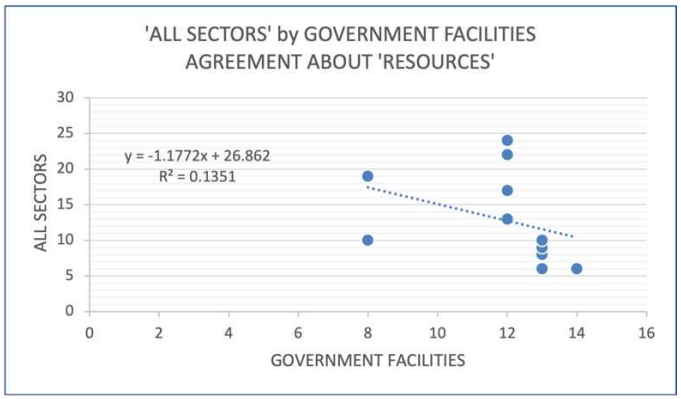

Figure 44 Correlation between All Sectors and Government Facilities for Resource Questions

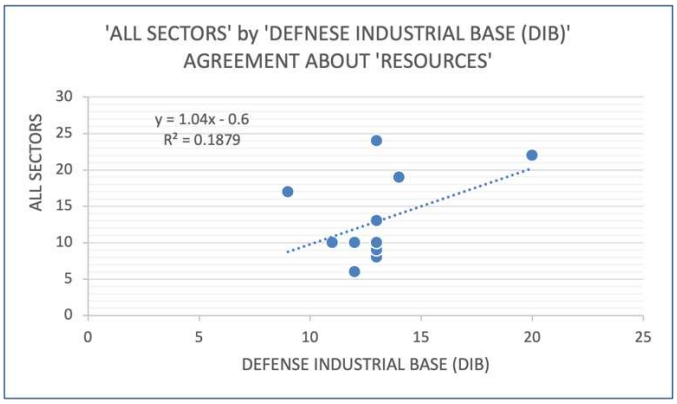

Figure 45 Correlation between All Sectors and Defense Industrial Base (DIB) for Resource Questions

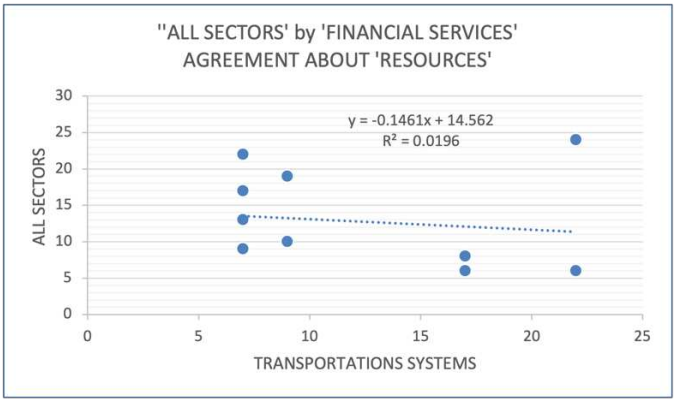

Figure 46 Correlation between All Sectors and Financial Services for Resource Questions

6.4.5. Training (r2) pattern by the critical infrastructure sector

A series of questions were asked regarding training and certifications. The sections identified representative available training and certification courses. Participants were asked questions about taking available training such as the SANS: "Incident Response Team Management," shown as the origination point (11, 23) in Figure 47. Agreement of all sectors with DIB sector professionals about training has an r^2 value of 0.0088. Response of all sectors with energy sector professionals to the same question is shown as point (23, 23) in Figure 48, and all sectors with government facilities personnel as point (10, 23) in Figure 49. Figure 44 shows all sectors with energy sector professionals about resources is an r^2 value of 0.5793 moderate. Figure 49 shows that all sector personnel agreement with government facilities about resources has an r^2 value of 0.1435.

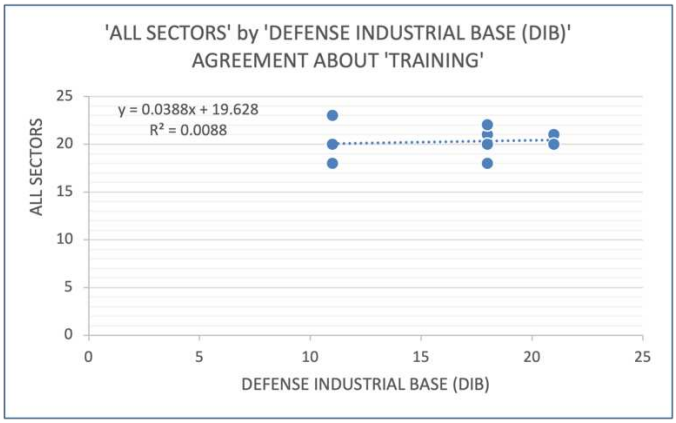

Figure 47 Correlation between All Sectors and Defense Industrial Base (DIB) for Training Questions

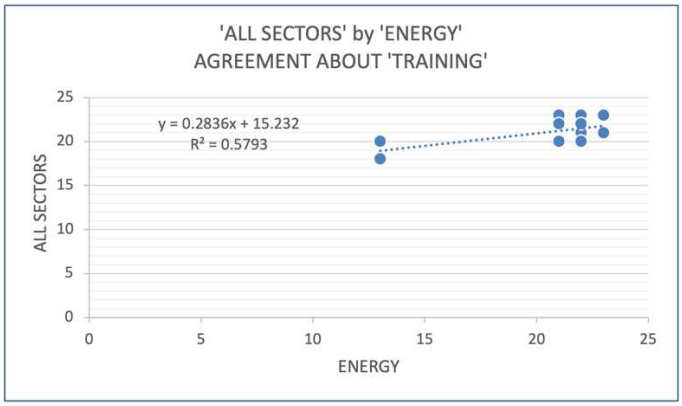

Figure 48 Correlation between All Sectors and Energy for Training Questions

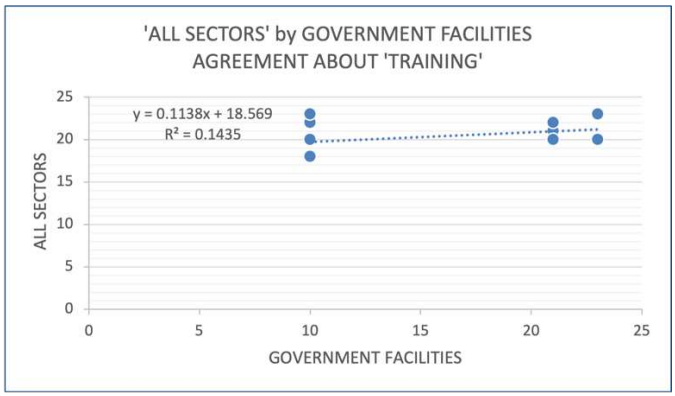

Figure 49 Correlation between All Sectors and Government Facilities for Training Questions

6.4.6. KSA (r2) pattern by the critical infrastructure sector

Participants were asked about KSA applied directly to the performance of a function. Participants were asked 56 questions about KSA, such as: " I have knowledge of countermeasures design for identified security risks," shown as point (7, 110) in Figure 50; and "I provide coordination of information from cyber systems.," demonstrated as point (7, 27). Figure 50 shows the correlation of agreement between financial services and the communications sector about KSA. For example, the financial services and the communications sector about KSA has an r^2 value of 0.0471. This r^2 means that the variation of one variable cannot be explained by the other. Figure 50 shows the correlation of agreement between financial services and the communications sector about

KSA has an r^2 value of 0.0028. Figure 52 shows the correlation of agreement between financial services and the communications sector about KSA has an r^2 value of 0.0034. Responses to the same two questions show as point (15, 110) in Fig. and point (11, 110).

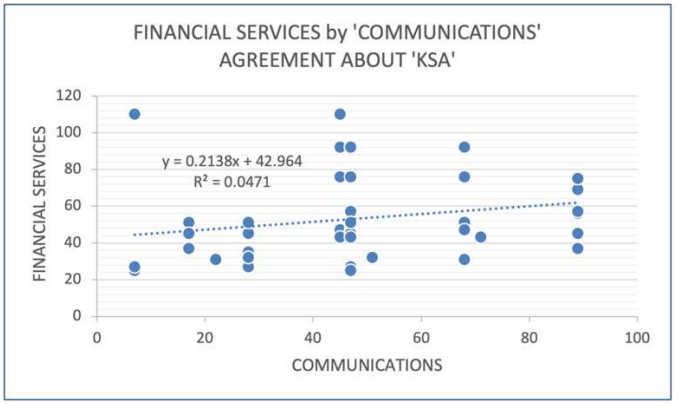

Figure 50 Correlation between Financial Services and Communications for KSA Questions

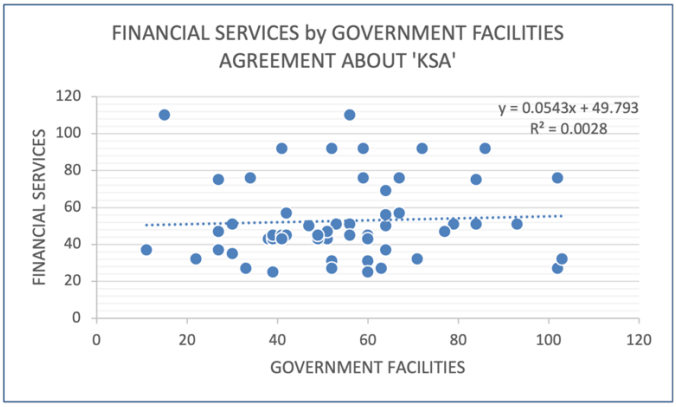

Figure 51 Correlation between Financial Services and Government Facilities for KSA Questions

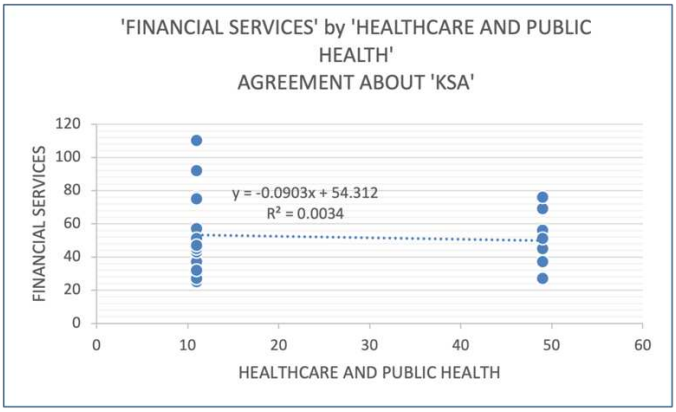

Figure 52 Correlation between Financial Services and Healthcare and Public Health for KSA Questions

6.4.7. Red Team (r2) pattern by the critical infrastructure sector

Participants were asked questions about Red Team activities such as: "Red Team recommendations are tracked to resolution (e.g., patch or remediation) as part of the risk management process," as shown as point (14, 5) in Figure 53; and "Red Teams meet current mission requests made by our organization," as shown as point (14, 11) in Figure 53. Figure 53 shows the correlation of agreement between energy and financial services about Red Team. Engineer energy with financial services about Red Teams has an r^2 value of 0.0809 weak. Figure 54 shows the correlation of agreement between energy and government facilities about Red Team has an r^2 value of 0.6853. An r^2 of 0.6853 for energy and government facilities is moderate for the data set. However, responses to the same two questions, "Red Team recommendations are tracked to resolution (e.g., patch or remediation) as part of the risk management process," are as shown as point (3, 5) in Figure 54; and "Red Teams meet current mission requests made by our organization," as shown as point (3, 11) in Figure 54.

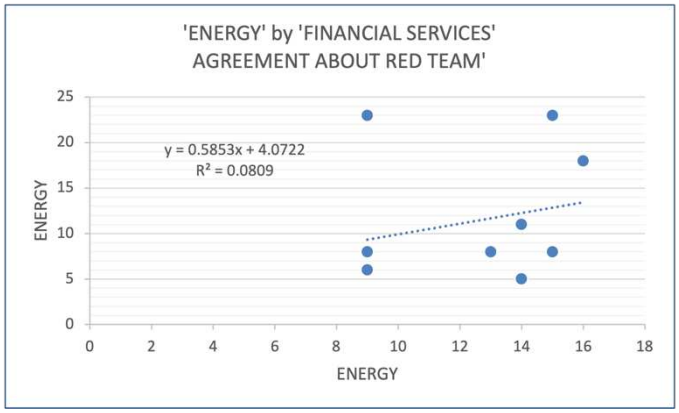

Figure 53 Correlation between Energy and Financial Services for Red Team Questions

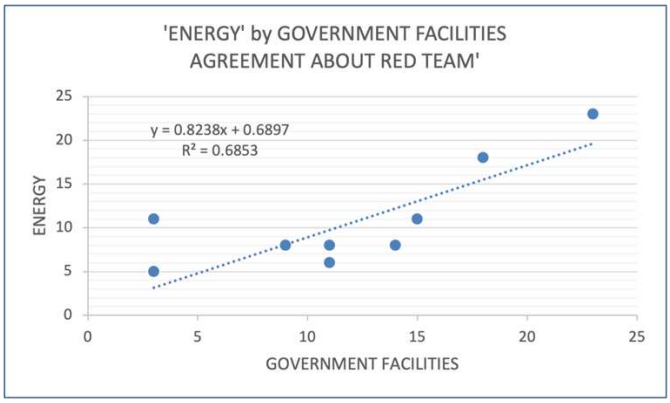

Figure 54 Correlation between Energy and Government Facilities for Red Team Questions

6.4.8. Security Considerations (r2) pattern by the critical infrastructure sector

Questionnaire participants were given statements to describe the organizational knowledge of cybersecurity quality attributes. For example, participants were asked to respond to comments about security considerations such as "Software-Defined Networking (SDN) solutions are in evaluation for use in our organization," shown as point (20, 17) in Figure 55; "Intrusion Prevention Systems (IPS) deployed on control systems to actively block suspect traffic are tested to ensure that a given signature will not block a legitimate control command," as shown as point (36, 23) in Figure 55; and "Traditional statistical forecasting strategies (e.g., dynamic regression) are used in our organization as a baseline for prediction of network performance," is shown as point (25, 25)

in Figure 55. Figure 55 shows the correlation between all sectors and energy about security considerations is moderate with an r^2 value of 0.5979. However, responses to the same questions by all sectors and government facilities are shown as point (24, 17), point (24, 23), and as point (25, 21) in Figure 56. Figure 56 shows that the correlation between all sectors and energy about security considerations is weak, with an r^2 value of 0.3765.

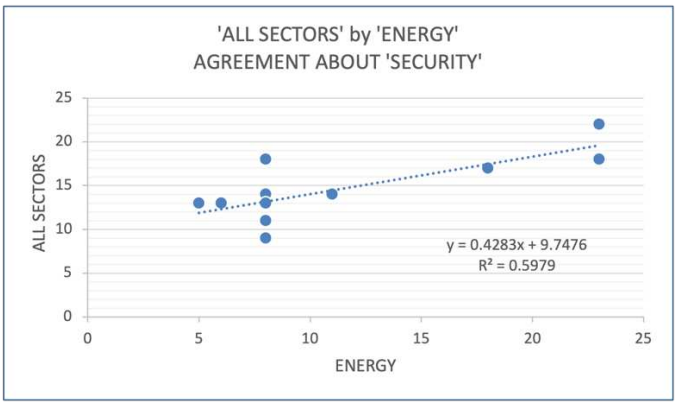

Figure 55 Correlation between All Sectors and Energy for Security Questions

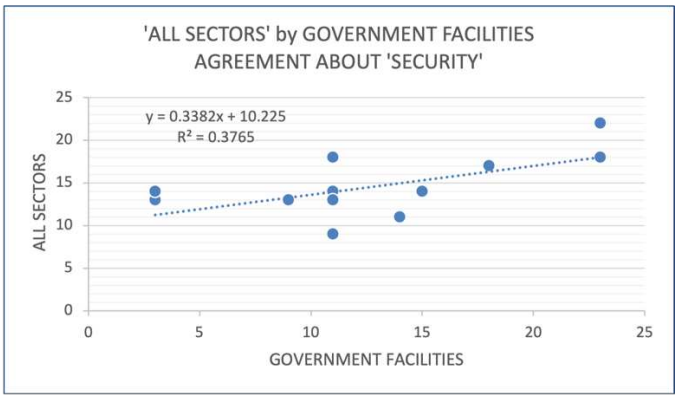

Figure 56 Correlation between All Sectors and Government Facilities for Security Questions

7. Chapter Seven – Test Result Findings

This chapter presents the experiment test findings. The primary purpose of the questionnaire test tool was to provide fundamental data points to test the hypothesis that there is an uncertainty of agreement among professionals. (Scalco "Cyber-Physical System/Control System Workforce Survey"). The online questionnaire from August 2020 to February 2021 collected responses from 187 professionals to 203 questions about control systems.

7.1. Findings Summary

Our analysis of the response data identifies key points about attitudes toward cybersecurity and control systems. We found:

- Critical infrastructure sectors have moderate to a strong agreement when asked about Red Teams. However, a knowledge gap and training opportunity exist to leverage Red Team interaction with stakeholders at all organizational levels to improve the certainty of the agreement by professional occupations about risk assessments and effectiveness of system security against current real-world attack techniques.
- Fundamental cyber awareness training is prevalent among questionnaire respondents. Almost 96% of respondents said they have cyber awareness training. In addition, most said cyber awareness training is required for their position, 88.2%, and most said the training is fully funded and available for their job, 83.0%. Thus, a knowledge gap and training opportunity exist to require and support cyber awareness training for all positions and provide a path for advanced and specialized training beyond essential cyber awareness.
- Knowledge about the Perdue Model is limited. When asked, 41.8% said they were not

familiar with the Perdue Model as a reference. The Purdue Model, also known as the PERA model, subdivides enterprises into logical segments of system functions and is used to model protection of the OT network from unwanted traffic and exploits. Thus, a knowledge gap and training opportunity exist to ensure the hierarchical functions of operations from primary devices that control the physical world and IT systems that manage data are well-understood by all.

- By profession, engineers and computer scientists agree about network systems, infrastructure, and moderate agreement about incident response and Red Teams. However, there is more significant uncertainty of understanding among other professionals. There is a knowledge gap and training opportunity for cross-training between OT professions and engineers and computer scientists. Collaboration and cross-training on cyber hygiene and control system operations can develop new skills sets. Cross-training professionals would improve the overall ability to achieve and maintain C2 and is key to addressing multi-concern assurance (i.e., safety and technicians' understanding of cybersecurity, and engineers and computer scientists' understanding of control system safety). In addition, identifying similarities and differences between traditional enterprise systems and control systems will help ensure the domain workforce is knowledgeable in both traditional IT and control systems (i.e., adopting IT cybersecurity practices to corporate connectivity and remote access capabilities for control systems).
- There is a lack of understanding about required skills. Certainty of agreement about KSA requirements for work roles was lacking by all occupations. Engineers' and technicians' responses, when asked about KSA, had zero correlation. There is a moderate agreement by the employment sector about infrastructure. However, the certainty of agreement when

asked questions about other aspects of multi-concern assurance is weak. There is a knowledge gap and training opportunity to define the KSAs required to manage cyber operations in control system environments for potential new roles, redesign work roles, training and certification needed, and upskilling. (Dik).

- The federal employment sector agrees with the military services about resources and moderate agreement about network systems and infrastructure. UARC and FFRDC are also in moderate agreement about resources. A knowledge gap and training opportunity exist to establish measures and metrics for the DOTLMPF-P assessment (i.e., promoting institutional knowledge of control systems) and improve awareness of existing best practices and benchmarks used in other sectors such as IT. The measure of an organization's agreement about cyber capability can help identify where uncertainty can impede mission.
- There is a shortage of agreement among professionals at all levels of organizations and across sectors. Particularly disagreeable parings were engineers and computer scientists with technicians, industrial management, and safety professionals. Professionals found little to no agreement about KSAs, resources, and incident response. A knowledge-gap and training opportunity exists to leverage the knowledge from the matured sectors and associations and raise awareness and understanding of existing guidance such as the Advanced Cyber Industrial Control System (ACI) Tactics, Techniques, and Procedures (TTP). ((USCYBERCOM)). Ramifications for policy, Governance, and operations are almost inevitable given the shift to mass permanent telework environments and increased desire for mobile access.
- Threats to assets can arise from a broad spectrum of threat agents. The single greatest organizational vulnerability is people, whether untrained, unmotivated, or malicious

insiders. (Simske). Network administrators tend to use weak password settings and fail to install patches in time, creating system security vulnerabilities. Training security staffers may address these lack of security tendencies, which is different from the threat surface of an underpaid security staffer. The potential in the latter is that the perceived underpayment might lead to the security staffer being "unmotivated" or becoming an active insider threat (i.e., purposely sharing information with unauthorized individuals or deliberately causing other damages). These exploitable weaknesses need to be addressed as part of the overall risk management plan to safeguard assets. Most breaches involve weak, stolen, or infrequently changed passwords, and most involve "insider" actions, so bringing the "underpaid" and "undertrained" resources in alignment with the business is critical.

- Specific and verifiable requirements for cybersecurity will look different in day-to-day operations than previously. Ramifications might imply actions to help prevent an attacker from gaining access by the security policy of Mandatory Access Control (MAC), active user account management, principle of least privilege restricting access to all administrator-level accounts and administrative tools, configuration files, and settings of the least level of privilege to make it more difficult for users to escalate their privileges. Cybersecurity governance strategy is not a "one and done," nor only the responsibility of the IT department. Ramifications for governance functions to 'direct, monitor, evaluate, and communicate' implies administrative functions will need to capture the disagreeable pairings by ensuring cybersecurity governance is part of and entirely consistent with broader organizational Governance; secure processes are applied across all roles, especially when non-employees have access to sensitive resources; and regular cybersecurity status reporting and issue escalation to higher management is performed. Technical Governance

activities include configuration audits and verification that all installed components are authorized and correct; enforcement of approved standards, guidelines, and procedures; and performing logging and auditing at critical points in a Defense-in-Depth (DID) architecture. (Simske). Improved defense strategy uses DiD, network segmentation, Zero Trust (ZT), and security automation. (D. F. a. S. S. Aleksandra Scalco).

- The energy sector and financial services sector has moderate agreement about red teams, and the energy sector and government facilities also have a moderate agreement about red reams. There is a knowledge gap and opportunity to use red team strategies and actual data in other sectors to validate vulnerability findings and verify successful mitigation. A vulnerability assessment only provides subjective evidence of a vulnerability possibility.
- There is a shortage of agreement among professionals across all sectors about incident response. A knowledge gap and opportunity exist to improve understanding of managing security incidents supported by a framework that includes all relevant stakeholders, tools, identification, response, recovery, and review processes. An opportunity exists to model the process to include all actions related to detecting, containing, and recovering from an incident.

7.2. Value of Null Findings

The value of null findings in the uncertainty model is equally important in informing policy and practice and in helping to interpret positive results obtained by the survey. For example, the results can significantly improve the probability of finding evidence that if the degree of agreement among professionals about how to defend these systems varies, then so can the capacity to accomplish the assigned control system mission vary, affecting C2 over the cyber-physical control

system domain, see Chapter 3.1 Hypothesis. Unfortunately, acknowledging null findings means that sound, and often critical input, is kept away from the collective knowledge and the potential to save lives. On the other hand, null findings benefit the broader community by increased transparency of where there may be system vulnerabilities. More significantly, the null findings of the research study challenge claim that cyber security-specific training alone improves cyber fluency in control system operations. Two examples of weak voices departure from a concurrence of agreement that proved deadly correct are the Apollo 1 launchpad capsule flash fire and the Challenger space shuttle explosion.

7.2.1. Apollo 1 Launchpad Capsule Flash Fire

In January 1967, three astronauts died in a flash fire inside their Apollo 1 command module during what was supposed to have been a routine simulated launch test at Cape Canaveral, Florida. Astronauts Virgil "Gus" Grissom, Ed White, and Roger Chaffee voiced concerns about the command module to the Apollo Spacecraft Program Office Manager Joseph F. Shea earlier, citing the number of flammable materials used in the model. Despite the astronauts' concerns, the combined nylon and Velcro materials were used to hold the module's tools and equipment in place. The material was never removed. Grissom expressed frustration with spacecraft design changes and rework and inability to update the training simulator by hanging a lemon he brought from his home on the simulator. (Howell).

The astronauts proved to be correct. A spark that may have been caused by faulty electrical wiring ignited a fire—in a few seconds, creating a deadly inferno of flammable material, fed by high pressure, pure oxygen in the cabin. All three astronauts died in the blaze. (Klein). National Aeronautics and Space Administration (NASA) Flight Director Gene Kranze later said[4], "We were too 'gung-ho' about the schedule, and we blocked out all of the problems we saw each day in our

work. Every element of the program was in trouble, and so were we." (Klein).

7.2.2. Challenger Shuttle Explosion

Evidence of the cause for the Challenger Space Shuttle explosion that killed its seven astronauts on January 28, 1986, shows that a rubber O-ring seal failed to seal correctly at launch due to below-freezing temperatures that impacted the integrity of the O-ring material. In addition, a second wind shear condition further damaged the seal 37 seconds into the flight. At this point, the result was catastrophic. (Atkinson). Like concerns voiced before the test event about the Apollo 1 command module, five contractors working on the Challenger Space Shuttle booster rocket expressed safety concerns about the forecast temperatures on the planned launch day.

Similarly, the program schedule advanced despite the uncertainty of agreement. The cold temperature at launch affected the rubber seals that were supposed to prevent rocket fuel from leaking to fail. Before liftoff, contractor engineers tried unsuccessfully to convince stakeholders to postpone liftoff. As a result, the Challenger Space Shuttle disintegrated on January 28, 1986 – 73 seconds after launch. (Berkes). Real-world problems in the physical world have little room for unintentional outcomes and consequences. As with any risk, the uncertainty of agreement must be understood and managed. MBSE and MBSAP models ensure traceability to the lowest level system component. Adding uncertainty measures to the model can demonstrate where there may be issues. "In all systems, uncertainty is a key issue" (Blockley and Godfrey).

8. Chapter Eight – Section II Summary

This section is intended to explain the methodology (i.e., background research, the development of an experiment, development of survey questions, creation of experiment method, protocol authorization, and approval authority for monitoring the research) for the remediation of critical infrastructure vulnerability. The uncertainty model leads to report findings to understand the workforce better. However, little is known about integrating uncertainty of agreement findings into the DOTMLPF-P process from emergent practice into an applied approach to meet the operational context for advisory to plan for mitigation. In the JCIDS process, this may be accomplished by capability demonstration using research, Commercial-off-the-shelf (COTS), Government off-the-shelf (GOTS), or modified GOTS in a pilot. The pilot is demonstrated on a network only by an Initial Authority to Operate (IATO) or Authority to Operate (ATO) certification. An initial CONOP is integrated into a technology transition plan to meet requirements. In the DOD, USC Title 50 is the legal authority to produce a technology demonstration; performance standards are variable based on the JCTD Integrated Management Team's (IMT) discretion with the Office of the Undersecretary of Defense (OUSD) oversight.

The goal is to demonstrate and field the capability into operations successfully. The information obtained from the MUA can be used to transition innovation from a complicated domain (e.g., sense, analyze, respond) to a complex environment (e.g., probe, sense, respond). The demonstration is used to advance good practice into a reusable template and standards for best practice in an exacting C2 domain (e.g., sense, categorize, respond). SECTION III USE THE MODEL TO MEASURE DISAGREEMENT AS A MEANS OF IDENTIFYING VULNERABILITY – introduces the application to a power utility and water facility use case.

SECTION III – USE OF THE MODEL TO MEASURE DISAGREEMENT AS A MEANS OF IDENTIFYING VULNERABILITY

9. Chapter Nine – Power System Use Case

The experiment to test the hypothesis was presented in previous chapters, and the data analysis was presented. This chapter presents conclusions drawn from the experiment data and elucidates how the experiment's output can be applied to a power system. In response to cybersecurity vulnerabilities to control systems for critical infrastructure, the DOD kicked off the Joint Capability Technology Demonstration (JCTD) in 2019, known as MOSAICS, for "More Situational Awareness for Industrial Control Systems." MOSAICS was the initial demonstration of a cyber defensive operating capability for control systems. Navy system operators successfully demonstrated the MOSAICS capability in a Military Utility Assessment (MUA) for a power utility site in August 2021. The model for a better understanding of the uncertainty of agreement among professionals presented in this paper can be applied to the capability and other critical infrastructure verticals such as water, transportation, healthcare, public health, or dams.

For example, the next phase of MOSAICS moves the capability from a fielded prototype into an acquisition program, which presents many alignment challenges. Stakeholder alignment and agreement are needed to deploy, test, and validate the effective cybersecurity leave-behind capability for critical power infrastructure and extensibility deployment to a second mission-critical infrastructure vertical, water, as well as for additional cybersecurity quality attributes such as Operational Technology Software Defined Networking (OT-SDN) and Zero Trust principles.

Recall that the questionnaire participants were given statements to describe the organizational knowledge of cybersecurity quality attributes. For example, participants were asked to respond to comments about security considerations such as "Software-Defined Networking

(SDN) solutions are in evaluation for use in our organization," shown as point (20, 17) in Figure 55. Stakeholder alignment is needed to support the transition from S&T research to a fielded operational capability and a formal acquisition program.

Once new technology and capability solutions are demonstrated, a second next phase is to operationalize the capability. The operationalization requires greater understanding and agreement among broader sets of professions and resource and policy alignment, which takes years to develop. The MOSAICS concept of automation integration Operational View 1 (OV-1) was presented in the last quarter of the Fiscal Year 2018 (FY18). An Implementation Directive (ID) and JCTD Management Plan were subsequently signed in FY19, followed by a signed Transition Technology Agreement (TTA) with the Navy in FY20. A CONOPS was also developed in FY20. An objective of the JCTD was to provide leave-behind capabilities tested in a testbed environment and during the MUA at a power site.

(Kilcoyne). The Naval Facilities Engineering Systems Command (NAVFAC) plans to deploy the capability at NAVFAC Facilities Engineering command (FEC) Southwest (SW) and FEC Hawaii (HI) in FY23 and FEC Mid-Atlantic (MIDLANT) and FEC Southeast (SE) in FY24. NAVFAC included the MOSAICS in its Navy Program Objective Memorandum (POM)/Budget Estimate Submission (BES) to the Office of the Secretary of Defense for 2024 (POM24) for production and deployment, and operations and sustainment of the capability. (Kilcoyne). The POM/BES involves allocating resources in a five-year planning cycle as part of the Future Year Defense Program (FYDP) process. Stakeholders make trade-off decisions about where resources will be directed for future years.

The uncertainty model presented in this research can be used in the FYDP process for resource planning and prototyping strategy effectiveness, particularly to prepare for a capability

transition. The center of the process begins with understanding the organizational objectives and the operational site needs. A better understanding of the uncertainty of agreement among professionals is helpful in the critical decision support process. It supports the effectiveness and speed of mitigation deployment in new sites. The uncertainty model supports the planning, programming, budgeting, and execution phases of portfolio management for operations. Figure 57 shows the r^2 value of engineers' agreement throughout the control system lifecycle with other professionals for the capability.

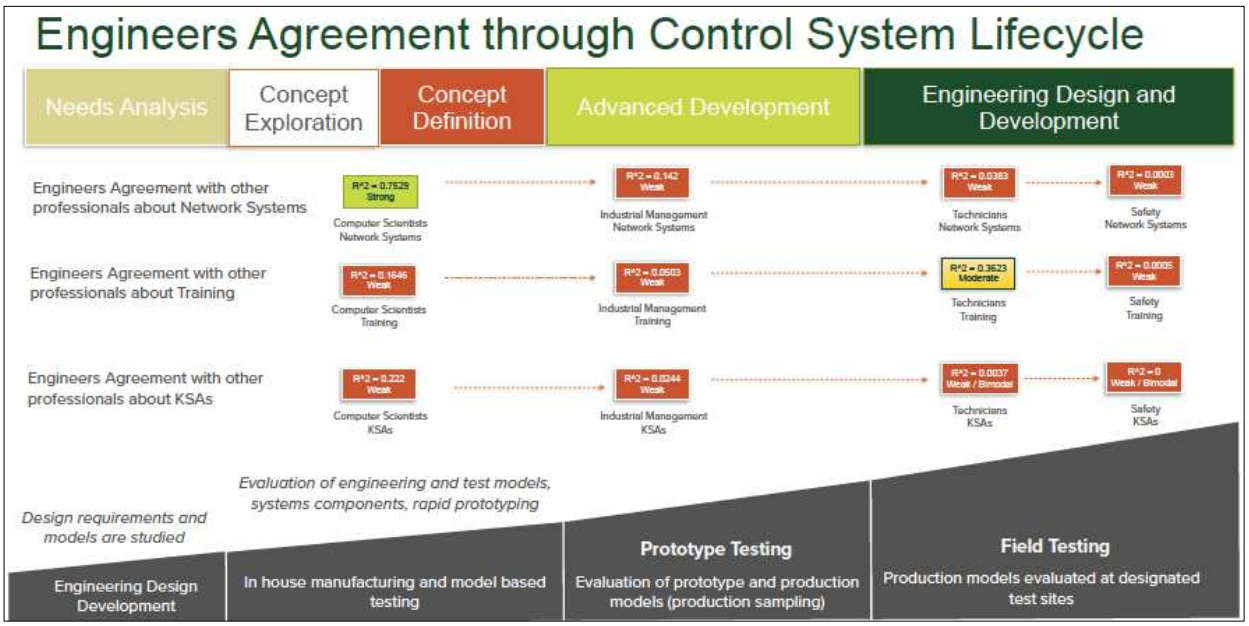

Figure 57 Engineers Agreement through the Control System Lifecycle

Engineers' agreement with other professionals about network systems becomes weaker through the development lifecycle of a cybersecurity control system solution. In the early needs analysis, concept development, and concept definition phases, engineers work with computer scientists to design requirements and evaluate and test engineering models. As seen in Figure 57, engineers' agreement with computer scientists is strong r^2 of 0.7529. The uncertainty model can guide the transition strategy from in-house manufacturing and model-based testing to final field

testing when the production model is evaluated at the designated test site. Every organizational asset throughout the lifecycle should support the strategy in the DOTMLPF-P (e.g., people, processes) and ensure that the design can meet the expected performance requirements (e.g., training, resources).

9.1. Requirements

The initial control system prototype started with an initial set of 206 functional requirements. Of those, 104 applicable requirements were allocated to the MOSAICS prototype (Spirals 0 – 5). As the development of the prototype began in 2019, technical requirements were written to meet the functional needs, and 23 operational requirements were developed and allocated to MOSAICS. By Fall 2020, more than 600 technical requirements were written. (Vermilye). Of the initial technical requirements, 334 were assigned to the MOSAICS prototype.

The initial focus was on the high-level operational needs to address the desired capabilities for a control system: identity, protect, monitor, detect, analyze, visualize, decide, mitigate, recover, and share information. (Rich Scalco). Gaps identified at the MUA demonstration included 51 functional requirements deemed out of scope from the original set of 206 applicable requirements. (Vermilye). The functions not implemented in the initial prototype will be addressed in subsequent development, including component identification and baselining, management of access permissions authorized users, monitoring of system anomalies, additional mitigation responses, and recovery. (Vermilye). Of the more than 600 technical requirements, 267 were mapped to functional requirements but not allocated in the initial MUA demonstration. These technical requirements include additional system protection, visualization, event and incident response, and information sharing capability.

The starting point for the architecture is a requirements baseline derived from the participant DOD COCOM. The CONOPS is a description in advance of a specification. "A CONOPS expresses the needs and assumptions of the operational end-user; describes processes, missions, and constraints; and provides context for trade studies and design decisions. It includes all the functions, behaviors, and characteristics a system must exhibit to be satisfactory in its intended usage" (Borky, 2019). The performance specifications provide design guidance and may define the minimum acceptable thresholds and levels of desired performance objectives. Performance specifications effectively establish the design trade space "within which performance, cost, schedule, risk, reliability, and other variables can be analyzed to optimize the solution" (Borky, 2019).

The solution is found in the enterprise security layer of the architecture. Four broad categories of architecture drivers may be considered: high-level requirements, business constraints, technical constraints, and quality attributes. "Performance requirements are verified by measuring the appropriate parameters and comparing them to required values;" and "NFRs may be verified through inspection of the system and its documentation, analysis of compiled data on things like failure and repair rates, feedback from operational users, design audits against applicable standards, and many other sources," (Borky, 2019)

9.2. Prototyping Strategy

A prototyping strategy is developing and testing a prototype to demonstrate that the design can meet each domain's performance requirements. As seen in Figure 57, engineers' agreement with computer scientists is strong early in the concept exploration. However, as the prototype

moves into later stages of development, there is disagreement and uncertainty among professions, leading to vulnerability. System performance expectations are based on the prototype testing and demonstration conducted at the system element level and establish an initial baseline. The prototype can provide tangible evidence of a stable System of Systems (SoS) architecture design. Distributed Interactive Simulation (DIS) and High-Level Architecture (HLA) standards are valuable tools for engineering an SoS architecture. (Scalco "Cyber-Physical System (Cps) and Control System (Cs) Architecture for Cyber Defensive Capability — Mosaics"). The research showed little to no agreement among professionals about KSAs, resources, and incident response. A knowledge gap and training opportunity exist to leverage the knowledge from the matured sectors and associations and raise awareness and understanding of existing guidance such as the ACI TTP. ((USCYBERCOM)). A system-level prototype and the model and methodology presented can test and demonstrate critical aspects of the system before field testing. Agreement alignment among professionals about cybersecurity should improve as concerns are addressed and capability demonstrated.

9.2.1. Comprehensive Verification & Validation (V&V) Approach

The primary motivation for prototyping as part of a system development effort is to verify problem fixes, verify trade studies and support ongoing engineering activities in smaller developmental increments. If professions disagree, this also presents a problem that needs to be fixed to support ongoing engineering activities. This approach provides experiments from smaller builds with few system elements "up to the full system" (J.M. Borky and T.H. Bradley). These development builds are small in scope and less expensive to execute. The uncertainty model can measure the uncertainty of agreement among stakeholders throughout development builds. An incremental approach was used in the development of the MOSAICS capability. The development

team tested small increments in prototype development phases before completing the final test increment. This approach allowed corrections to the system and verification of test data that informed ongoing engineering development efforts using the Perdue Model. However, recall that a research finding was that knowledge about the Perdue Model is limited. When asked, 41.8% said they were not familiar with the Perdue Model as a reference. The Purdue Model, also known as the PERA model, subdivides enterprises into logical segments of system functions and is used to model protection of the OT network from unwanted traffic and exploits. Thus, a knowledge gap and training opportunity exist to ensure the hierarchical functions of operations from primary devices that control the physical world and IT systems that manage data are well-understood.

A comprehensive approach to Verification and Validation (V&V) was used to build test cases against the requirements in a simulation environment using virtual prototyping. "[T]he uses of virtual prototyping involves its use to develop, analyze, refine, and communicate the [architecture]" (J.M. Borky and T.H. Bradley). The methods to use a spiral approach to successively integrate new capabilities to meet requirements in each prototype test against the requirements in a virtual environment and then in a physical environment with hardware and software in the loop. Differences in relative responses by different groups are expected during this phase. They can help pinpoint disagreement because of the complexity of the power utility system and the cyber defensive requirements. This approach allows incremental V&V to be implemented and provides productive feedback to the engineering team to correct problems.

Additionally, a well-formed model of the target system developed in a simulation environment allows software testing to manage risk reduction. Trade studies are used to augment the various levels of abstraction to quantify component performance in the system. Finally, the system is tested with the operator human-in-the-loop in the final MUA demonstration. The

prototype is determined to have utility for integrating network system production operations.

All stakeholders require collaboration to ensure risk reduction and successful fielding (e.g., facility management, engineer designers, In-service Engineering Agents (ISEA), technicians, and safety personnel), as shown in Figure 58. Risk reduction is the activity of applying security controls, or safeguards, to eliminate or reduce the threat or vulnerability. However, research findings show that engineer agreement with computer scientists about network systems shows engineers' understanding with computer systems has an r^2 value of 0.7529, which quantifies the strength of the correlation, correlation among technicians, industrial management, and safety personnel is weak. An r^2 of 0.7529 means that a 76% variation of one variable is entirely explained by the other. However, the agreement of engineers with industrial management, technicians, and safety personnel about network systems shows no statistically relevant correlation. Engineers' agreement with industrial management about network systems has an r^2 value of 0.141. Engineers' agreement with technicians about network systems has an r^2 value of 0.0383. Engineers' agreement with safety personnel about network Of the questionnaire participants, 96 percent responded 'yes' to "I have cyber awareness training," as shown in Multi-concern assurance flows between each of the eight domains of a DOTMLPF-P analysis, as shown in Figure 2, and impacts the high-level operational concept as shown in Figure 58. Stakeholders must understand the system operations from the highest business level function in the architecture to the lowest level PLC. The data show the uncertainty of agreement may not be due to a lack of cyber awareness training but rather something else about cybersecurity for control systems. Uncertainty and lack of understanding among professionals about introducing cyber capability into operations create interest.

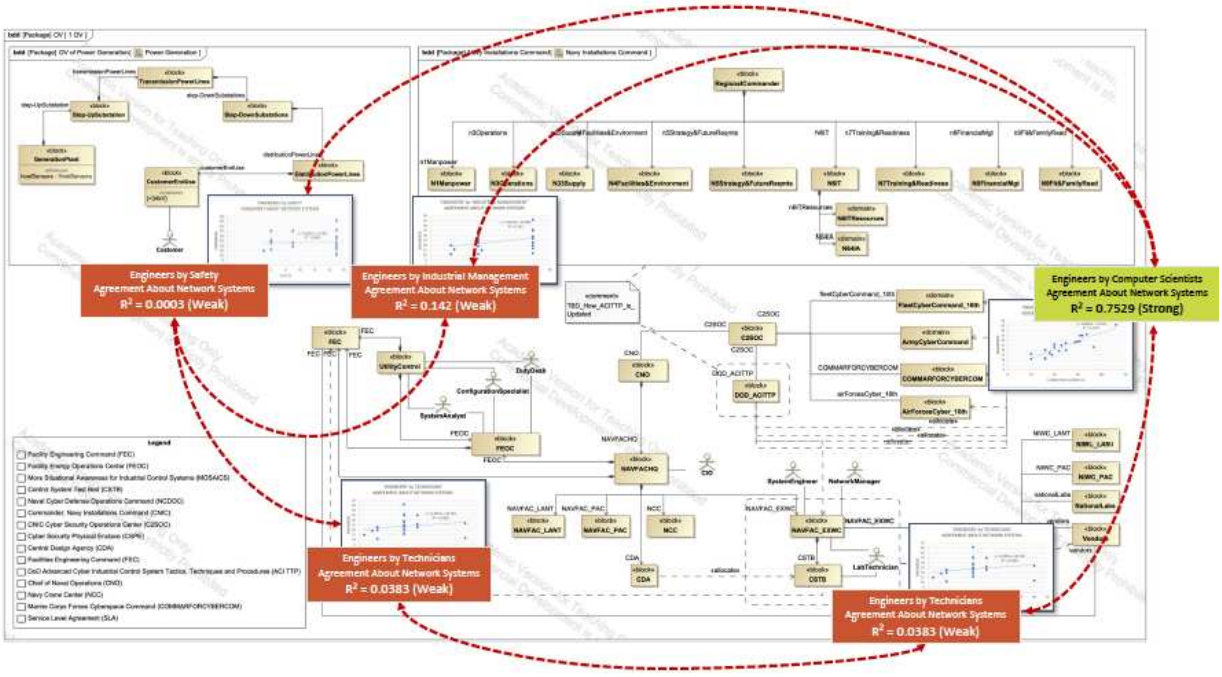

Figure 58 BDD MOSAICS OV-1 High-Level Operational Concept Showing r^2 About Network Systems

The MOSAICS prototype system performance expectations are demonstrated at the system element level (e.g., PLC) and establish an initial baseline in a model. Thus, the model becomes an essential tool for shared information and understanding from the baseline architecture's highest to lowest level non-IP components. In addition, the model offers vital information about the complexity of content and processes central to managing changing technologies. A system model's uncertainty of agreement data can help identify pain points.

9.2.2. Shared Information and Understanding

Shared Information and shared understanding levels of interoperability for MOSAICS mean that the training, operating procedures, and CONOPs are consistent across power utility sites and operators to facilitate consistent rules for emergencies and mission conditions. For example, shared situational awareness of mission conditions enables consistent safety precautions. Common visualization allows for shared data and interpretation of alerts by operators about changes to the

network. Shared data and standard message formats allow for the identification of alerts and common prioritization of operations based on the experience and rating of operators. Standard data links and channels ensure interoperability of communications to networks and channels. "Information Sharing – creates higher-quality information from all available sources and uses it to create common awareness of the operational situation among all participants; this is the Shared Information level of interoperability," and "[s]hared Situational Awareness – enables collaborative decisions, self-organization and synchronization of activities, mutual support and sustainability, and speed and correctness of decision-making; this relies on the Shared Understanding level of interoperability," (J.M. Borky and T.H. Bradley).

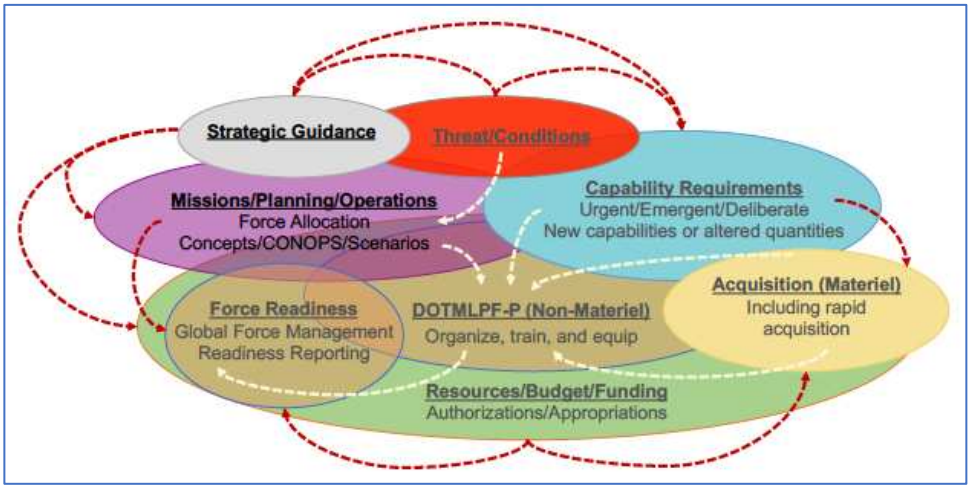

Figure 59 DOTMLFP-P Activity Flow

9.2.3. Commonly Encountered Challenges

Some commonly encountered SoS challenges that would be likely to arise includes (Scalco "Cyber-Physical System (Cps) and Control System (Cs) Architecture for Cyber Defensive Capability — Mosaics").

- Heterogeneity – The Primary and Smart Microgrid systems may be built on varying

technology baselines and respond to different priorities.

- Complexity – The functions, interfaces, constraints, and technologies may exceed the capabilities of any individual system, particularly as new functionality and capability are added to the Smart Microgrid A system over time, such as Security Orchestration, Automation, and Response (SOAR).
- Extending System Engineering Models – There is a need for a generally accepted SoS Engineering (SoSE) strategy and methodology. For example, a DOD Power Utility system may have an ATO based on Cyber Security Physical Enclave (CSPE) security. However, Smart Microgrid systems may not have the inherited protection of the CSPE, and therefore there needs to be a strategy on how to obtain an ATO for those systems.
- Requirements Definition and Validation – There may be competing priorities and needs for the Primary Grid and the Smart Microgrid A system. For example, what services have priority when an unscheduled power outage or intentional brownouts for load reduction in an emergency. Typically, the Primary Grid requirements will prioritize medical and emergency services.
- Interface Definition and Management – The Primary and Smart Microgrid A system may have technical and functional differences. For example, the Primary Grid may use SDN capability with different interfaces within the SoS than traditional routing and cabling.
- Enterprise Evolvability – Changes to an Enterprise such as introducing 5G at a Smart Microgrid A system-level (e.g., SmartBase/SmartCity) might not be used to manage Primary Grid at Level 6, 5, 4 of the Pera Model for safety and security. Open architectures and loose coupling are critical to ensure that the SoS can evolve with these

changes. The concept of a SmartBase is discussed in Section 12.5.2.

- Governance – The service strategy and operations design become increasingly complicated when adding systems that utilize separate Change Control Boards (CCB) and Governance models.

9.3. Capability Demonstration

Throughout the JCTD, the team evaluated available COTS technologies and addressed gaps with the reuse of GOTS technologies. Using a model to measure the correlation of agreement among sets of professions can pinpoint where there is uncertainty about the technologies. Future experimentation might measure uncertainty among occupations as a means of identifying vulnerability. Open communication with industry was maintained via technology exchanges, meetings, and demonstrations. The JCTD hosted three industry information exchange days to share lessons learned. The commercial sector has the most significant potential to offer commercial capabilities to productize the JCTD's demonstrated capability further, replace the GOTS, and advance the solution shown by the MOSAICS MUA. Additionally, the commercial sector may offer the holistic capability back to the DOD and commercial entities as a service. However, to do so, stakeholders must be in alignment.

The technical management approach for the MOSAICS JCTD used a strategy and framework to adopt an extensible, adaptive COTS approach. Notably, using the spiral model for the software development process. The spiral development approach is a systems development lifecycle method used to manage the risk that starts with a small set of requirements and incrementally introduces new requirements through each phase. The capability was incrementally introduced to the MOSAICS system with each demonstration and integration event. Integration

events leading to the demonstration test were used to validate the functionality and the operations before the final MUA. MOSAICS malicious process attack scenarios were demonstrated for facility engineers during early spirals, including crash override threat, cyber anomaly detection, automated TTP execution of integrity checks, and mitigation response options. The operation of the MOSAICS system during the integration events was performed by the design development team, with operational personnel involved as part of system training. The objective was to get the complete end-to-end system integrated and operating, including all the components.

Further events were provided for the final development and integration efforts to complete the visualization development, remaining alerting implementation, integrity checks, integration of certificate-based authentication, and data sharing. Additionally, the design development team assessed the build test in harness and executed all test procedures. Recall that a finding is a lack of understanding about required skills. Certainty of agreement about KSA requirements for work roles was lacking by all occupations. Engineers' and technicians' responses, when asked about KSA, had zero correlation. Participation during integration events enabled for planning future skill requirements. The uncertainty model can provide a standardized view of the professional skills needed in a logical structure that can be adapted to the operator's needs and help define the KSAs required for potential new roles, redesign work roles, training, certification, and needed upskilling. (Dik).

9.3.1. Developmental and Operational Independent Test

The overall purpose of the MOSAICS MUA test was to assess the MOSAICS capability for enhancing cybersecurity awareness on the pilot control system. The MOSAICS capability was evaluated by the Air Force 47th Cyber Test Squadron and the 346th Test Squadron. (Squadron and Squadron). In addition, an independent evaluation of the capability was conducted throughout the

JCTD by Air Force cyber Developmental Test and Evaluation (DT&E) by hands-on technical requirements evaluation and Air Force cyber Operational Test and Evaluation (OT&E) experts who observed and assessed operators conducting mission scenarios. (Squadron and Squadron). The focus areas were the baselining and threat detection capability and the operator training. A sample of the cybersecurity survey questions used to measure the uncertainty of agreement among professionals about cybersecurity for control systems and response options mapped to operational requirements and MOSAICS capability is shown in Table 6.

Table 6 Sample Cybersecurity Survey Questions Mapped to Operational Requirements and MOSAICS Capability

Requirement Number	Operational Requirement Text	Capability	Sample Cybersecurity Survey Question(s) (Response Options)
O1.1	Inventory IT and OT system devices and system components in the targeted environment.	Identify	Q48. I have access to the physical network topology. (Yes; No; I do not, but I know who does have the physical network topology.)
O1.2	Identify internal and external data flows and connections relative to the target environment.	Identify	Q191. Sensitive network connections between traffic sources and points of encryption are monitored on our organization's network systems. (Yes; No; I do not know.)
O1.3	Enable prioritization of components and system devices.	Identify	Q111. I maintain configuration management of a Control System(s). (Yes; No; Not currently, but I have previously performed this function; Not currently, I would need training to perform this function.)
O2.1	Enable and support access control mechanisms within the environment.	Protect	Q47. User accounts and credentials are managed in our organization by the following authentication approach. (Modern Authentication; Cloud Identity Authentication; Federated Authentication; I do not know.)
O2.2	Authenticate authorized devices, users, and	Protect	Q120. I [can] to identify if an individual device is being tampered with within a

Requirement Number	Operational Requirement Text	Capability	Sample Cybersecurity Survey Question(s) (Response Options)
	processes.		complex system. (Yes; No; Not currently, but I have previously performed this function; Not currently, I would need training to perform this function.)
O2.3	Implement controls to limit access to physical and logical assets.	Protect	Q136. I [can] identify cyber connections to critical physical systems. (Yes; No; Not currently, but I have previously performed this function; Not currently, I would need training to perform this function.)
O2.4	Protect data in transit and data at rest.	Protect	Q58. In our organization, timestamp data is used to reference persistent time-based trends. (Yes; No; I do not know.)
O2.5	Manage maintenance activities for system components.	Protect	Q130. I ensure that maintenance procedures or workarounds do not void anomaly detection in control systems. (Yes; No; Not currently, but I have previously performed this function; Not currently, I would need training to perform this function.)
O2.6	Create and manage audit logs.	Protect	Q140. In my current job function, I use data collected from a variety of cyber defense tools (e.g., Intrusion Detection System (IDS) alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats. (Yes; No; Not currently, but I have previously performed this function; Not currently, I would need training to perform this function.)
O2.7	Enable facility operations to maintain a mission capable state.	Protect	Q. 186. Traditional statistical forecasting strategies (e.g., dynamic regression) are used in our organization as a baseline for prediction of network performance. (Yes; No; I do not know.)
O3.1	Continuously monitor system components to detect indications of the	Monitor	Q194. Physical separation using a data diode or unidirectional gateway is used for monitoring across the critical zone

Requirement Number	Operational Requirement Text	Capability	Sample Cybersecurity Survey Question(s) (Response Options)
	presence of threat actor/anomaly.		boundaries to assure that all log transmissions occur in one direction of our organization's network systems. (Yes; No; I do not know.)
O4.1	Evaluate the severity and type of detected threats.	Analyze	Q116. I provide for the identification of new vulnerabilities. (Yes; No; Not currently, but I have previously performed this function; Not currently, I would need training to perform this function.)
O4.2	Provide analytics and decision support based on mission priorities.	Analyze	Q166. I coordinate with partner target activities and intelligence organizations and present candidate targets for vetting and validation. (Yes; No; Not currently, but I have previously performed this function; Not currently, I would need training to perform this function.)
O4.3	Provide situational awareness of system operations and relevant events.	Analyze/ Visualize	Q127. I maintain awareness and active, valued communication between workforce groups about on-going vulnerabilities and newly discovered threats. (Yes; No; Not currently, but I have previously performed this function; Not currently, I would need training to perform this function.)
O5.1	Provide alert management.	Visualize	Q195. Security analytics such as Security Information and Event Management Systems (SIEMS) are used for anomaly detection of our organization's network systems. (Yes; No; I do not know.)
O6.1	Evaluate events and where necessary present courses of action to execute.	Decide	Q. 69 Cyber incident response policies, procedures, and logistics are well documented in our organization. (Yes; No; I do not know.)
O6.2	Prioritize response to support mission assurance.	Decide	Q134. I [can] identify anomalies in usage and trace to cyber activity. (Yes; No; Not currently, but I have previously performed this function; Not currently, I would need

Requirement Number	Operational Requirement Text	Capability	Sample Cybersecurity Survey Question(s) (Response Options)
			training to perform this function.)
O7.1	Present cyber threat mitigation techniques.	Mitigate	Q139. I have knowledge of countermeasures design for identified security risks. (Yes; No; Not currently, but I have previously performed this function; Not currently, I would need training to perform this function.)
O7.2	Implement the ACI TTP and other relevant cyber defense best practices, as appropriate.	Mitigate	Q118. I establish procedures to minimize the exploitation of vulnerabilities. (Yes; No; Not currently, but I have previously performed this function; Not currently, I would need training to perform this function.)
O8.1	Support recovery actions to maintain a mission capable state.	Recover	Q36. We maintain system backups. (Yes; No; I do not know.)
O8.2	Collect and archive incident data and evidence data to support future analysis and sharing.	Recover/ Share	Q69. Cyber incident response policies, procedures, and logistics are well documented in our organization. (Yes; No; I do not know.)
O9.1	Enable sharing of threat and incident information.	Share	Q74. A list of useful incident response services is available. (Yes; No; I do not know.)
O9.2	Share data about MOSAICS.	Share	Q122. I provide coordination of information from cyber systems. (Yes; No; Not currently, but I have previously performed this function; Not currently, I would need training to perform this function.)

DT&E conducted five test events against the MOSAICS technical requirements: Quarterly Test in December 2019 (147 technical requirements tested); Field Test #1 in August 2020 (236

technical requirements tested); Field Test #2 Part 1 in March 2021 (62 technical requirements tested), and Field Test #2 Part 2 in May 2021 (63 technical requirements tested); and Final Technical Demonstration in July 2021 (63 technical requirements tested). The test method was to initiate cyber-attacks against the control system protected by MOSAICS and verify that the solution correctly assesses and alerts the operator. Testers observed that the engineering design and integration progress increase the MOSAICS capability with each development spiral. OT&E assessed the operational requirements to determine the suitability and effectiveness in an operating environment. (Squadron and Squadron). The team evaluated 74 measures to address the Critical Operational Issue (COIs) covered during the MUA. The. The MUA results showed that MOSAICS identified 14 of 16 devices in the asset list with 87.5 percent accuracy. Of the 22 attack scenarios executed, MOSAICS detected 20 out of 22 with a 90.5 percent success rate with less than 5 percent false positive. The operators' rated the overall training as 7 using a survey tool based on a Likert scale from 1 (low) – to 10 (high). (Squadron and Squadron).

Table 7 Critical Operational Issues (COI)

CRITICAL OPERATIONAL ISSUE (COI)	QUESTION COVERED
COI 1	Will MOSAICS allow operators to detect cyber threats on the ICS network?
COI 2	Will MOSAICS allow operators to defend and mitigate cyber threats on ICS networks?
COI 3	Will MOSAICS enable ICS networks to continue to operate in a cyber-contested environment?
COI 4	Can MOSAICS be sustained in its operational environment?

The research findings identified a knowledge gap and training opportunity for cross-training between OT professions and engineers and computer scientists. Collaboration and cross-

training on cyber hygiene and control system operations can develop new skills sets. Cross-training professionals would improve the overall ability to achieve and maintain C2 and is key to addressing multi-concern assurance (i.e., safety and technicians' understanding of cybersecurity, and engineers and computer scientists' understanding of control system safety). Addressing this knowledge gap would be helpful in the risk decision management process to reduce vulnerability.

9.3.2. Uncertainty of Risk Decision Authority

Risk decision authority defines who may approve risk decisions at each level of an organization and who is responsible for the risk decision (i.e., a system ATO approval). Research participants were asked about decision authority. Participants were asked the following two questions: "I have decision authority for which risks are accepted as related to cyber-physical systems (CPS)"; and "I have decision authority for which risk mitigations are implemented as related to cyber-physical systems and control systems." Most participants who supported either OT or IT responded that they do not have decision authority. However, those participants who support both IT and OT in their job function did have some risk decision authority, as shown in

Table 8. The key to the responses is the first row is the count of responses, the second row is the percent of the total, the third row is the row percentage, and the fourth row is the column percentage.

The same questions participants were asked about network systems when examined by engineers and safety occupations show: "I have decision authority for which risks are accepted as related to cyber-physical systems (CPS)," as point (15, 28) in Figure 4. Risk decision authority is key to testing and fielding mitigation capability, further discussed.

Table 8 Cybersecurity Survey Participants Risk Decision Authority Responses

		Q44				Q45			
		I have decision authority for which risks are accepted as related to cyber-physical systems (CPS).				I have decision authority for which risk mitigations are implemented as related to cyber-physical systems and control systems (CPS/CS).			
		Yes	No	I do not know.	Total	Yes	No	I do not know.	Total
Q5 Please select the option that best describes your role.	Information Technology (IT)	7	35	0	42	8	34	0	42
		5.22% (*)	26.12% (*)	0%		5.97% (*)	25.37% (*)	0%	
		16.67% (*)	83.33% (*)	0%		19.05% (*)	80.95% (*)	0%	
		18.92% (*)	36.84% (*)	0%		17.78% (*)	39.08% (*)	0%	
	Operational Technology (OT)	2	12	1	15	5	9	1	15
		1.49%	8.96%	0.75%		3.73%	6.72%	0.75%	
		13.33%	80%	6.67%		33.33%	60%	6.67%	
		5.41%	12.63%	50%		11.11%	10.34%	50%	
	In my job function I support BOTH the IT and OT technology community.	28	48	1	77	32	44	1	77
		20.9% (*)	35.82% (*)	0.75%		23.88% (*)	32.84% (*)	0.75%	
		36.36% (*)	62.34% (*)	1.3%		41.56% (*)	57.14% (*)	1.3%	
		75.68% (*)	50.53% (*)	50%		71.11% (*)	50.57% (*)	50%	

9.3.2.1. Interim Authority to Test (IATT) Delays

MOSAICS was demonstrated during an MUA in August of 2021. The MOSAICS JCTD Operations Manager (OM) shared that during MOSAICS Industry Day #3, there were delays in obtaining the required Interim Authority to Test (IATT) until the days before the test event. (Roley). The DOD requires new technology tested on a live system, has cybersecurity assessment, and obtains an IATT. Getting an IATT involves understanding cybersecurity principles and the system on which the solution is tested. Arriving at an IATT for MOSAICS required a complicated series of communications between the Authorizing Official (AO), Information System Owner (ISO), Information System Security Manager (ISSM), Information System Security Officer (ISSO), and the JCTD technical team about the cybersecurity controls implemented. An IATT is required for all testing of new technology in a DOD test environment. It is not an ongoing ATO. Instead, an IATT is timebound. However, the final ATO system may be different from the initial IATT.

While an expert engineering team with cybersecurity knowledge led the technical design and stakeholders' total commitment to support the cybersecurity process, it was challenging to bring professionals into agreement about integrating new technology into the systems. The technical design team included engineers, computer scientists, federal, UARC, and FFRDC team members. Recall Figure 15 shows the correlation between engineers and computer scientists about security considerations is weak with an r^2 value of 0.325. Fig. 11 indicates that the federal and commercial industry correlation with security considerations is weak, with an r^2 value of 0.2483. Figure 33 shows that the correlation between federal and UARC about security considerations is weak, with an r^2 value of 0.0008. Risk decision authority discussions are needed throughout the lifecycle development process. Stakeholder understanding of security considerations is required. However, UARC and FFRDC responses to security considerations show less uncertainty than federal. For example, UARC's response to the question "Network traffic is externally encrypted using a network-based encryption appliance on our organization's network systems" is shown as point (39, 17) in Figure 33. One of the research findings was that measuring an organization's agreement about cyber capability can help identify where uncertainty can impede mission. The federal employment sector can benefit by using UARC and FFRDC best practices. A knowledge gap and training opportunity exist to establish measures and metrics for the DOTLMPF-P assessment (i.e., promoting institutional knowledge of control systems) and improve awareness of existing best practices and benchmarks used in other sectors (e.g., IT, UARC, FFRDC).

9.3.2.2. Vendor Support Connections During Test

Additionally, the MOSAICS JCTD OM shared that during MOSAICS Industry Day #3, a significant spike in alerts occurred during the demonstration. (Roley). An objective of the MOSAICS capability is to prioritize security alerts, narrowing the number from hundreds of

notifications to curated notifications, thereby minimizing the manual effort by operators. The appearance of many alerts led the MUA team to identify the cause of alerts of changes to the system baseline. Investigation showed a third-party vendor connecting to the operating system (OS) to perform patch updates.

Many organizations use third-party vendors for cybersecurity services such as security software patches. However, "service providers are potential security vulnerabilities, and thus might well be intermediate targets in an offensive operation directed at the true (ultimate) target," (David Clark). Three questions in the survey asked participants about vendors' support and connectivity to the network: Q62 – Vendors remotely support the network; Q63 – Vendors directly connect their equipment to the network; Q64 – Vendors can directly update their software over the network. During the MUA, a third-party vendor remotely connected to the network, directly connecting their equipment to the network, and updating their software over the web. The operators were unaware that this was coinciding with the demonstration. Recall that in the questionnaire, participants were asked 12 questions about resources, or the processes by which materials, energy, services, staff, knowledge, or other assets are made available to the organization, such as: "Our organization has contracted vendor-supplied technical support," shown as point (14, 10) in Figure 22 and point (8, 10) in Figure 23; and "Our vendor-supplied support contract includes an incident response element," as shown as point (9, 11) in Figure 22 and point (9, 11) in Figure 23. Figure 22 federal agreement with commercial industry about resources shows no statistically relevant correlation, with an r2 value of 0.0693. This r2 means that the variation of one variable cannot be explained by the other. Uncertainties about realities about the system can yield suboptimal outcomes because professionals do not fully understand the situation. (David Clark). Further, "[u]nder conditions of high uncertainty, crisis decision-making processes are often flawed." (David Clark).

10. Chapter Ten – Water Facility Use Case

In 2021, someone tried to poison the water supply of Oldsmar, Florida. There are approximately 15,000 residents in Oldsmar. The plant's remote access system vulnerability allowed hackers to access the water treatment system. The hacker then attempted to increase the amount of sodium hydroxide, or "lye," by a factor of 100 into the water supply. While Lye is not harmful in small quantities, it can be toxic in larger volumes. Thankfully, the intrusion was caught, the hack averted, and the unauthorized changes were reverted immediately.

A facility supervisor saw the hacker's pointer move across the screen to make unauthorized changes to settings. Serendipity is not security. The intruder was reportedly active for less than 5 minutes. This breach highlights the far more severe impacts that hackers can have on control systems. According to reports, the hacker first appeared in the morning on February 5, 2021. A plant operator noticed remote access to the monitoring and control computer system used for water chemical levels. Initially, the plant operator did not take any action. Logging into the system was easy to do. The city had replaced the software six months earlier, but the software was never uninstalled. According to FBI findings, a single shared password was used for all the facility computers, no two-factor verification was required, and no firewalls protected the controls from the internet. Further, all the computers were still running on a decade-old, discontinued operating system (Microsoft Windows 7) that had stopped issuing regular software updates to plug its security vulnerabilities. The hacker reappeared in the afternoon, visibly taking over the computer and opening the plant's control system software.

The intruder departed after increasing the water's sodium hydroxide level from 100 parts

per million to 1,100 parts per million. There is little formal visibility into the number of attacks on water utilities. Many go undetected or unreported, as no federal law requires regulators or law enforcement disclosure. There was legislation in 2018, but Congress never appropriated the necessary funds. Water Utilities perform "self-assessments." However, if there is disagreement or uncertainty among professions, self-assessment may not resolve the cybersecurity problems. "Uncertainties may relate to the actual balance of power (e.g., difficulties of cyber threat assessment), the intentions of the various actors (e.g., defensive actions by A are seen as provocative by B, inadvertent actions by A are seen as deliberate by B), the bureaucratic interests pushing decision-makers in certain directions (e.g., cyber warriors pushing for operational use of cyber tools), and the significance of an actor's violation of generally accepted norms." (David Clark). Most children are taught to recognize dangerous or suspicious situations. However, there is no comparable education for cybersecurity basics for laypeople to take cybersecurity seriously. (David Clark). Cybersecurity is perceived to be too difficult for users, administrators, and operators to understand, and technology features are often disabled or bypassed by users for ease of access. (David Clark).

There are more than 148,000 public water systems in the United States. Virtually all rely on remote access to monitor and administer facilities. Most operations are unattended and operate 24/7. Most have not separated IT from control system functions such as the safety systems. U.S. water infrastructure lacks centralization. Therefore, a widespread water hack would be challenging as each facility runs independently. (Collier). Rural areas often get their water from small plants, often run by a handful of employees rather than dedicated cybersecurity experts. Some that serve large populations are more extensive operations with dedicated. (Collier). The WaterISAC is a non-profit formed in 2002 in coordination with the EPA to serve as an organization to be the all-

threats security information source for the water sector. (WaterISAC).

In most cases, it is up to individual water plants to protect themselves, even if they are aware they have been hacked. More than 80 percent of surveyed facilities' significant vulnerabilities were software flaws discovered before 2017, indicating a rampant problem of employees not updating their software. (Collier). The Oldsmar, Florida, water treatment facility is an example of the vulnerabilities of outdated security mechanisms. Attackers mainly target companies that lack security personnel with industrial security expertise via phishing e-mails. (Kayan et al.).

10.1. Remote Access

A best practice is to protect the network by protecting remote access (e.g., Virtual Private Network (VPN)), protecting wireless access points, and using strong passwords to protect against unauthorized access to the physical system, as shown in Additionally, temporary or emergency accounts may also access critical assets that an access control policy must regulate. (Kayan et al.).

Table 9. Additionally, temporary or emergency accounts may also access critical assets that an access control policy must regulate. (Kayan et al.). Control system cybersecurity operational requirements can help to overcome that uncertainty. Cyber operations consist of many functions (e.g., management, sense-making, decision-making, response actions). Integration and automation of services that can be executed to respond in cyber-relevant time can help defend systems from adversaries. (Herring and Willett). The Genesis of the operational requirements for control system cybersecurity is from the DOD Advanced Cyber Industrial Control System Tactics, Techniques, and Procedures (ACI TTP) and the MOSAICS Joint Capability Technology Demonstration (JCTD). Questions formulated for the test tool on the right show how the questions

map to operational requirements. The first row reflects access control and user accounts and credentials. Security-responsible behavior elements include strong passwords, keeping operating systems up to date, and updating virus protection software. Still, research shows users often forgo security features because the feature may be seen as an obstacle to convenience. (David Clark). Authentication management is an essential principle of cybersecurity. However, often devices such as PLCs have vendor-assigned default passwords. Additionally, temporary or emergency accounts may also access critical assets that an access control policy must regulate. (Kayan et al.).

Table 9 Strategy Recommendations, Initiatives, Action Plans, and Example Metrics

REQUIREMENT NUMBER	OPERATIONAL REQUIREMENT TEXT	CAPABILITY	SAMPLE CYBERSECURITY SURVEY QUESTION(S) (RESPONSE OPTIONS)
O2.1	Enable and support access control mechanisms within the environment.	Protect	Q47. User accounts and credentials are managed in our organization by the following authentication approach. (Modern Authentication; Cloud Identity Authentication; Federated Authentication; I do not know.)

The general conditions for the Use Case Protect are developing and implementing appropriate safeguards to ensure the delivery of mission-critical services. The two (2) technical use cases for a water treatment facility are: Monitoring makes any data processed on the edge device available. The data monitoring helps the user understand the use case and provides insights into operations. The Remote-Control module inside the IoT agent enables access to the edge device through a client installed on the user's PC. Once connected, the user can access the whole device. In addition, the remote-control module allows the user to react to the data gathered in the monitoring process. MQTT is a machine-to-machine (M2M) connectivity protocol used for the Internet of Things (IoT), as shown in Figure 60. MQTT is a lightweight publish-subscribe

messaging protocol which probably makes it the most suitable for various IoT devices. The Internet of Things Network uses MQTT to publish device activations and messages that enable publishing a specific device response. The primary application use cases are remote operations, remote assistance, and remote alarming. A commonality of cybersecurity intrusion on water utility facilities has been remote access, compromised Passwords, and the use of outdated, end-of-life Operating Systems (OS).

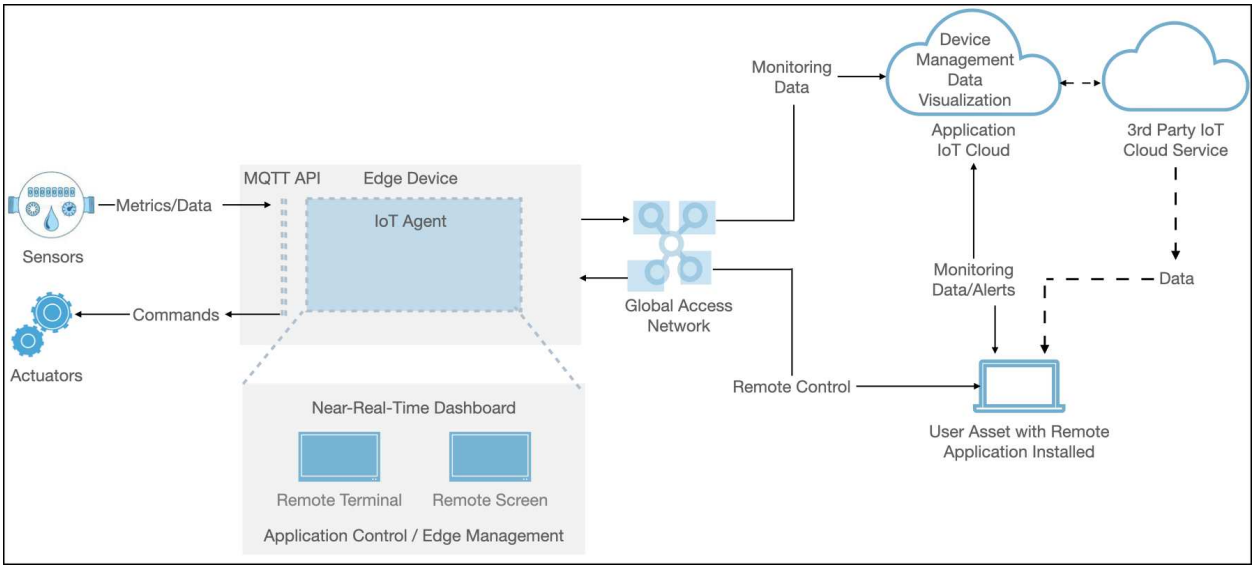

Figure 60 Remote Operations Network Architecture for Water Utility

A strategy is to use the uncertainty of agreement analytic framework to identify vulnerability in the water treatment system by measuring disagreement in segments of the cybersecurity profession to identify vulnerabilities. An example of moving through the model starting with disagreement is the use of administrative passwords on multiple systems, resulting in a misalignment of VPN accounts allowing remote access and threat actors obtaining credentials, which would result in a vulnerability of compromised credentials that enable unauthorized access. Similarly, it is possible to move backward through the model, starting with software flaws as a known vulnerability and moving through the model to alignment, which might involve the

purchase of an updated OS and updated software and agreement to perform regular software updates and implement credential management.

10.2. Misalignment R^2

Recall that the r^2 statistical significance score that indicates that there is a pattern: An r^2 value is < 0.3, is considered as non or very weak effect size; an r^2 value is $0.3 < r < 0.5$, is considered as moderate effect size; and an r^2 value of $r < 0.7$, is considered as strong effect size. Figure 71 compares engineers (y-coordinate) and computer scientists (x-coordinate) in a like manner about infrastructure and has an r^2 value of 0.7495. Thus, an r^2 of 0.7495 for engineers and computer scientists is relatively high for the data set. However, engineers' (y-coordinate) agreement with technicians (x-coordinate) about infrastructure has an r^2 of 0.0361, as shown in Figure 72. Participants were asked 20 questions about infrastructure, such as: "I have access to the physical network topology," demonstrated as engineers (y-coordinate) and computer scientists (x-coordinate) point (17, 14) in Figure 71, and as engineers (y-coordinate) and technicians (x-coordinate) point (8, 14) in Figure 72. Furthermore, "I know the single points of failure" is shown as point (29, 32) in Figure 71 and as point (8, 32) in Figure 72. The origination points in Figure 71 in response to the question: "In our organization, a timestamp is used to reference persistent time-based trends" as point (13, 11). Timestamp data is an essential element for practical cybersecurity. Trusted digital timestamping is used to prove specific data before a particular point in time. The feature tracks the creation and modification of an artifact. Once created, the timestamp data should not be changeable (not even by the originator) to ensure the timestamp integrity cannot be compromised. It is helpful in cybersecurity practice to identify external party access to an operational system making application changes without the possibility that the originator can make

changes to the timestamp. However, responses to the same question visualized by engineers (y-coordinate) and technicians (x-coordinate) are seen as points (8, 11), as shown in Figure 72.

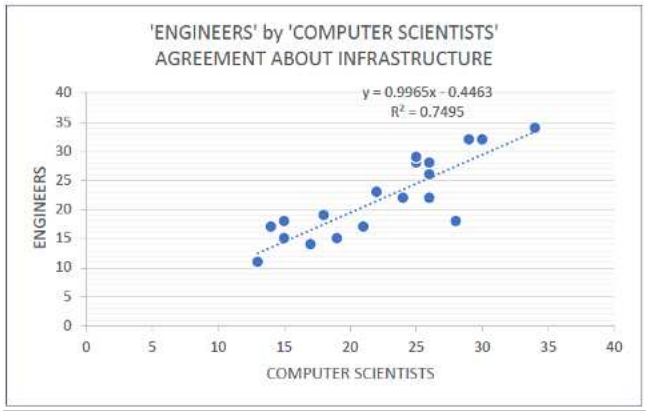

Figure 61 Correlation between Engineers and Computer Scientists about Infrastructure Questions

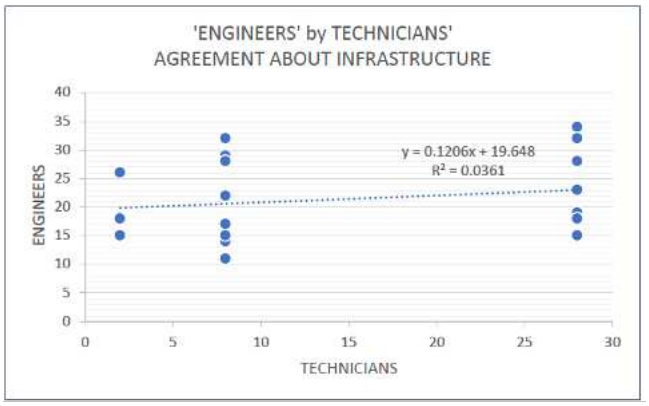

Figure 62 Correlation between Engineers and Technicians about Infrastructure Questions

Stakeholders responsible for the cybersecurity of the water treatment system are surveyed to measure the correlation of agreement about aspects of cybersecurity and the control system. A consensus among professionals needs to be present to ensure the alignment of resources and component security. Components of the remote operations, assistance, and alarms include:

- Sensors and actuators — Any device connected to the edge device that sends or receives data can serve as a sensor or actuator.

- Application Control — This provides the ability to create a custom user interface for the device or system the IoT agent is installed.
- Edge Management allows the operator to view the data processed on the device in real-time and create rules reacting to the data processed directly on the edge.
- Remote Terminal — Provides complete access to the operating system.
- Remote Screen — This allows the user to access a screen attached to the edge device.
- System monitoring — This provides data about the internal system conditions of the device, such as CPU load or used disk space, and many others.
- Cloud Dashboard — This allows access to the IoT solution.

Following the uncertainty of agreement methodology, there is measurable disagreement among professionals about administrative passwords used on multiple systems, which leads to misalignment of practice such as VPN account used to allow remote access that enabled threat actors to obtain credentials, which leads to the vulnerability of compromised credentials enabling access to the water treatment system. That same example can be walked back through the model as vulnerability such as software flaws move to alignment by purchasing updated operating system (OS) and updated software, and ultimately agreement which performs regular software updates and credential management. If two agents disagree entirely on where the system is most vulnerable or uncertain, there is an overall vulnerability. Where the correlation is very poor, these professionals will be at competing ends, which is worse than not fixing the infrastructure. Groups of the people fixing the infrastructure will be competing against each other. The result will be a system vulnerability that allowed hackers to access the water treatment system in Oldsmar, Florida.

11. Chapter Eleven – Section III Summary

The effectiveness of the regression approach was shown in the previous chapter as a method to analyze data about the correlation of agreement by sets of professions. This section is intended to explain how the model is used to achieve alignment in technology demonstrations to address the vulnerability. A technology demonstration is used to determine if the capability meets the requirements. However, at this point, the solution is used for analysis, guidance, plans, and budgets. The training available is primarily the demonstration user manual and vendor training. In the DOD, USC Title 10 is the legal authority for fielded systems. Performance standards are deterministic with high certainty and budgeted Program of Record (POR) oversight. The methodology uses DOD 5000 and COTS with limited GOTS. The objective is functional, operational, and interoperable capability for C2. Governance and requirements are derived from the JCIDS process, lead command, Capability Development Document (CDD), and Capability Production Document (CPD). The CONOPS is formalized in law, doctrine, policy, instruction, and TTP. A readiness inspection is required. The solution usage is explicit by orders and directives. Logistics and sustainment are managed by license and a depot by Army Service, or the Navy's In-Service Engineering Agent (ISEA).

Military standards apply using near-real-time operational mission data. Training is matured from user manuals and vendor training to the formalized schoolhouse and hands-on training. The complexity of practice is tested and improved into a reusable template and standards for best practice in an exacting C2 domain (e.g., sense, categorize, respond). The goal is to use a model to observe anomalies. SECTION IV – RECOMMENDATIONS FOR FUTURE WORK AND CONCLUSION introduces how the model is applied to other verticals to achieve alignment.

SECTION IV – RECOMMENDATIONS FOR FUTURE WORK AND CONCLUSION

12. Chapter Twelve – Strategy Recommendations

Using a relatively traditional type of survey, and correlations with other studies, to gain analytic insights. We found measurable disagreement among professionals about defending control systems in the cyber domain. An observation is that if the degree of agreement among professionals about protecting these systems varies, then the capacity to accomplish the assigned control system mission may also vary, resulting in vulnerability greater than the innate system design vulnerability. The model is a repeatable, novel approach to understand better how to achieve multi-concern assurance given control system complexity leading to strategy recommendations. A questionnaire was the launch point to test the hypothesis that professionals have a likely and measurable disagreement on achieving cybersecurity for control systems. The results allow us to target where the field is vulnerable and foundational to recommendations to develop strategies to overcome why people view threats differently.

The following are five strategy recommendations that are keys to overcoming uncertainty of agreement among professionals to help make critical infrastructure safe from cyber vulnerability for people, processes, technology, and simulation and test environment. For example, use the uncertainty model and analytic methodology as a cornerstone mechanism for informing KSA development, creating a digital engineering organization, creating a schoolhouse, creating a DOTMLFP-P model of an installation "SmartBase" site to identify potential mitigation pain points. This site could serve as the initial schoolhouse, usher new science and technology discoveries into research pilots, test and demonstrate new capability, and transition matured technology into fielded solutions. In addition, the strategy recommendations provide a model and mechanism for integrating contextual information from context-sensitive critical infrastructure control system

dynamic classes into an analytic model. Strategy recommendations, initiatives, action plans, and example metrics are shown in Table 10 Strategy Recommendations, Initiatives, Action Plans, and Example Metric.

Table 10 Strategy Recommendations, Initiatives, Action Plans, and Example Metric

STRATEGY	INITIATIVE	ACTION PLAN(S)	EXAMPLE METRIC(S)
Means of Identifying Vulnerability	Analytic Model	Use analytic model and methodology to measure disagreement in segments of the cybersecurity profession as a means of identifying vulnerabilities	r^2 statistical significance score that indicates that there is a pattern r^2 value is < 0.3, is considered as non or very weak effect size r^2 value is 0.3 < r < 0.5, is considered as moderate effect size r^2 value r < 0.7, is considered as strong effect size
People	Hiring Practices	Create diversity, equity, and inclusion (DEI) initiatives to tap into a broader resource pool	Percentage change in workforce demographics (i.e., percentage of professionals from monitored groups compared with industry benchmarks)
		Make cybersecurity jobs more inclusive, affordable, and accessible for everyone	Percentage change in workforce demographics (i.e., percentage of professionals from monitored groups completing training and certification compared with industry benchmarks) Survey engagement scores (i.e., compare professional engagement scores from monitored groups, including IT and OT professionals)

STRATEGY	INITIATIVE	ACTION PLAN(S)	EXAMPLE METRIC(S)
		Gain shareable, transparent insights into the hiring process, pay equality, and promotion opportunities	Percentage change of applications from members of monitored groups compared to non-members of the monitored group Percentage change in lateral moves (i.e., percentage of lateral movements, appointments, training, and development participation from monitored groups compared with industry benchmarks) Equal pay and rewards across rank and function (i.e., earnings from the monitored group on average compared with the non-monitored group in the organization and compared with industry benchmarks)
	Work Roles	Define KSA	Number of control system cybersecurity roles clearly defined Number of Key Performance Indicators (KPI) tied to specific job description tasks Number of functional performance tasks Number of tasks matched to job roles

STRATEGY	INITIATIVE	ACTION PLAN(S)	EXAMPLE METRIC(S)
		Designate key Lead Systems Engineer (LSE) roles in the organization for Mission-Critical Control Systems (MCCS) to establish, coordinate, and direct technology strategy for MCCS (e.g., FRCS SCADA), Process Control Systems (e.g., DCS) to ensure the organization evolves in advance of emergent critical infrastructure capabilities (including providing the workforce access to digital tools)	Measures of Effectiveness (MOE) trend curves (i.e., product operational safety, suitability and effectiveness, Return on Investment (ROI), schedule) Measures of Performance (MOP) trend curves (i.e., systems engineering fundamentals such as requirements analysis, functional definition, systems analysis and control, product Verification and Validation (V&V))
	Training	Integrate Red Team interaction with stakeholders at all organizational levels	Measures of Effectiveness (MOE) trend curves (i.e., risk assessment effectiveness) Measures of Performance (MOP) trend curves (i.e., system security against actual world attack techniques effectiveness) Number of stakeholder interactions
		Train workforce on use of digital tools	Number of professionals completing hands-on training (i.e., architecture modeling tools)

STRATEGY	INITIATIVE	ACTION PLAN(S)	EXAMPLE METRIC(S)
		Cross-train IT and OT professionals	Cross-training rate (i.e., number of the workforce monitored receiving training outside original work role) Measures of Effectiveness (MOE) trend curves (i.e., risk assessment effectiveness) Measures of Performance (MOP) trend curves (i.e., system security against actual world attack techniques effectiveness) Workforce retention numbers Increase in MOP Increase in number of certifications outside of original work role Percentage change in IT workforce ability to perform tasks outside of original role, and OT workforce ability to perform tasks outside of the original role
Process	Digital Engineering	Digital Transformation (Dx)	Count number of work activities using digital processes (i.e., technology used) Count use of digital tools to guide action (i.e., architecture modeling tools) Count number of workforce reskilled from original job role Use digital design to discover and resolve pain points

STRATEGY	INITIATIVE	ACTION PLAN(S)	EXAMPLE METRIC(S)
	Governance	Develop cybersecurity governance-driven principles for control systems (i.e., for Service Level Agreements (SLAs), contract language)	Key Performance Indicators (KPI) for control system cybersecurity (i.e., system baseline, documented processes, implemented best practices) Count number of SLA Count SLA compliance Percentage of incidents resolved within SLA Number of cybersecurity incidents Digital awareness score (i.e., cybersecurity for control systems in contract language)
	Taxonomy	Balance taxonomy in cybersecurity control system category	Workforce testing (i.e., successful category selection, successful correlation, average navigation time) Count item use per category (i.e., ICS, CS, CPS) Workforce knowledge testing of hierarchical functions of operations (i.e., primary devices that control the physical world and IT systems that manage data are well understood)

STRATEGY	INITIATIVE	ACTION PLAN(S)	EXAMPLE METRIC(S)
Technology	Tools	Use tools to enhance system design	Count Use Cases, classes, diagrams, all items Count model-based systems, subsystems, and operations (i.e., domain-specific views of hardware, software, and operations) Count system architecture models (i.e., number of system architecture models used as integration framework, distributed model repositories, distributed simulation workflows) Measures of Effectiveness (MOE) trend curves (i.e., reproducibility, reliability, integration of processes and models across disciplines and system lifecycle, percentage of engineering hours reduced) Measures of Performance (MOP) trend curves (i.e., system security against real-world attack techniques effectiveness evaluated using modeling and simulation)
	Open API	Use publicly available open Application Programming Interface (API) requirements	API performance measures (i.e., ease of integration between applications, uptime, usage, performance) Measure of scalability

STRATEGY	INITIATIVE	ACTION PLAN(S)	EXAMPLE METRIC(S)
	Automation	Deploy automated Courses of Action (COA)	Degree of automation Operation and Maintenance (O&M) cost Count number of COA (i.e., playbooks) Operational availability (i.e., uptime vs. downtime) Number of cyber-attacks detected Number of cyberattacks mitigated Staffing requirements (i.e., number of Full Time Employees (FTE), education and skill level of operators, labor categories)
Environment	Schoolhouse	Charter National Cybersecurity Schoolhouse	Number of the workforce completing training Knowledge assessments Performance data Training cost per professional (i.e., training cost per professional = cost of training/number of professionals trained) Benchmark (i.e., system security against real world attack techniques effectiveness of schoolhouse trained monitored groups compared with industry benchmarks) Operational metrics (i.e., cyber incidents, time to recover)

STRATEGY	INITIATIVE	ACTION PLAN(S)	EXAMPLE METRIC(S)
		Create a threat-informed curriculum that includes both theoretical and hands-on training	Count number of training modules Count number of threat-informed Courses of Action (i.e., playbooks) Mean Time to Detect (MTTD) Mean Time to Resolve (MTTR) Mean Time to Contain (MTTC) Survey uncertainty of agreement model scores (i.e., scores in a SysML model)
		Create a sharable curriculum for schools and universities that includes both theoretical and hands-on training	Number of schools and universities offering the curriculum Number of students enrolled in curriculum Number of graduates hired into work roles
	Testbed	Establish a control system cybersecurity testbed that allows for simulation and testing solutions throughout the entire DOTMLPF-P environment across all sectors, government, and commercially owned	Mean Time to Detect (MTTD) Mean Time to Resolve (MTTR) Mean Time to Contain (MTTC) Solution lifecycle cost
	Digital Twin	Create, test and build cybersecurity solution for control system cybersecurity in a virtual environment to demonstrate capability	Mean Time to Detect (MTTD) Mean Time to Resolve (MTTR) Mean Time to Contain (MTTC) Solution total lifecycle cost impact Near, real-time monitoring of performance and in-service engineering

12.1. Analytic Model – Means of Measuring Vulnerability for Other Verticals

Communicating outcomes and how the experiment method works are presented in the following chapter. The keys to overcoming uncertainty of agreement among professionals for achieving cyber security require a model and a mechanism for integrating contextual information from context-sensitive critical infrastructure control system dynamic classes into a model for the intended vertical. Recall that there are 16 highly complex, dynamic essential sectors of infrastructure identified by the Department of Homeland Security (DHS) (C. a. I. S. A. (CISA) "Securing Industrial Control Systems: A Unified Initiative Fy 2019—2023"; D. o. H. S. D. C. I. S. A. (CISA)). This research about overcoming uncertainty of agreement for achieving cyber security using a model and mechanism for integrating contextual information from context-sensitive critical infrastructure control system dynamic classes into a model applies to any of these 16 sectors (e.g., chemical, dams, energy, transportation systems). The uncertainty model and methodology offer valuable insight for fact-based management for other critical infrastructure vertical(s) for integrating cybersecurity into control systems and areas of future work. The approach uses a RA and SA and uncertainty of agreement measures and metrics to achieve C2 for DOD federally owned and commercially owned assets across both. While each sector may have independent governance and oversight, the path to performing analysis and planning for the remediation of the critical infrastructure cyber vulnerability is the same for any mitigation.

12.2. People – Hiring Practices, Work Roles, and Training

We found there is a lack of understanding about required skills. Certainty of agreement about KSA requirements for work roles was lacking by all occupations. The lack of knowledge about required KSA is despite most having cyber awareness training. Our findings show that cyber awareness training is prevalent among questionnaire respondents. Almost 96% of respondents said they have cyber awareness training. In addition, most said cyber awareness training is required for their position, 88.2%, and most said the training is fully funded and available for their job, 83.0%. The response data shows that most respondents, regardless of IT, OT, or both, have some cyber awareness training, as shown in Table 4.

Yet, engineers' and technicians' responses, when asked about KSA, had zero correlation. There is a moderate agreement by the employment sector about infrastructure. However, the certainty of agreement when asked questions about other aspects of multi-concern assurance is weak. There is a knowledge gap and training opportunity to define the KSAs required to manage cyber operations in control system environments for potential new roles, redesign work roles, training and certification needed, and upskilling. (Dik).

The uncertainty model can analyze an organization's readiness before integrating a mitigation solution to help identify the uncertainty of agreement related to mitigation. Currently, there are no matured KSAs for professional development. The uncertainty model can improve professional understanding over time, identify desirable KSAs, and equally essential show anomalies.

Introducing new capability to a legacy operational process introduces many issues such as change process and cultural and technical challenges. Steps to help prepare an organization's

personnel are to ensure the affected professionals understand the goals and benefits of the new capability. Uncertainty of agreement data can establish organizational improvement metrics among professionals. The metrics track progress over time while the rules identify specific operational processes to achieve objectives. The regulations and metrics interact in a governance process to provide measurable values to show how effectively operational goals are achieved and track progress. Specifically, providing "top-down support, empowered decision-making with involvement of all stakeholders, continuing focus on alignment with policy and strategic objectives, and clear direction to the organizations responsible for implementing such projects are universal" (J.M. Borky and T.H. Bradley).

Cybersecurity professionals are predominately male. This research data showed that professionals are predominately men (79.75%). The ICS^2 Cybersecurity Workforce Study data showed that in 2021 among the survey participants, the cybersecurity field is predominately male (76%) and Caucasian (72%). Meaningful diversity, equity, and inclusion (DEI) initiatives might tap into a broader resource pool. ((ISC)2 *(Isc)2 Cybersecurity Workforce Study, 2021*) Women tend to view the field of cybersecurity as dominated by men. ((ISC)2 *(Isc)2 Cybersecurity Perception Study*). Gender balance and diversity on cybersecurity teams may meet the industry-wide cybersecurity skills gap (i.e., understaffed corporate cybersecurity teams and unfilled positions). ((ISACA)). The organization should make cybersecurity jobs more inclusive, affordable, and accessible for everyone with no discriminatory biases. (Tasheva). Future research about the barriers to career entry into the cybersecurity field may help find qualified professionals. We believe more shareable, transparent insights into managing the hiring process and understanding job requirements may help address the existing cybersecurity talent gap described with correlated studies.

12.3. Process – Digital Engineering, Governance, and Taxonomy

The convergence of IT and OT, or the IIoT, is happening at an accelerated, broader scale. System design and architecture need to be understood from the bottom to the top of the stack (i.e., component to enterprise level), governed with cybersecurity principles in mind, and tapped into the total resource pool of talent wealth by Diversity, Equity, and Inclusion (DEI) initiatives. Organizations look for what works now, potentially missing better answers. A digital engineering organization begins with involving system stakeholders supported by knowledgeable personnel. In addition to DEI, cybersecurity governance-driven principles should be central to the digital engineering organization. These governance-driven principles can be used for Service Level Agreements (SLA) and contract language. For example, increased monitoring of cyber security performance indicators and the abolition of devices such as USB from the available toolkits. (Iosif Progoulakis). As another example, capital and operational expenditure for cyber security measures need to be allocated for cyber security dictated by industry technical standards adopted in the digital engineering organization that is dynamically evaluated and implemented using models to keep up with advancements. (Iosif Progoulakis). A digital engineering organization will also want to avoid "vendor lock," which causes the organization to be tied to a single vendor solution that may prevent future integration of new solutions. Openness is the "characteristic that promote[s] competitive acquisition and upgrading, long-term operational stability, design reuse, interoperability, and other benefits" (J.M. Borky and T.H. Bradley). For example, in the MOSAICS JCTD, the components were selected based on an open Application Programming Interface (API) requirement. This approach is a publicly available API that governs access to proprietary software applications for integration and is tested in a model before the field test. Testing in a model is a crucial system attribute so that the cost-effectiveness gained by software

licensing does not limit future new integrations.

A Mission-Critical Control Systems (MCCS) Lead Systems Engineer (LSE) is needed to establish, coordinate. Direct technology strategy for MCCS (e.g., FRCS SCADA) and Process Control Systems (e.g., DCS) to ensure the organization evolves in advance of emergent critical infrastructure capabilities, including providing the workforce access to digital engineering tools. MCCS is information systems monitoring and controlling physical infrastructures essential to the direct mission fulfillment. The LSE-MCCS coordinates and advises other stakeholders (e.g., NAVFAC); DOD (e.g., DOD CIO); Department of Energy (DOE); DHS (e.g., CISA); NSA; and UARC and FFRDC to ensure alignment of requirements and standards for data sharing, threat intelligence fusion, and operational technologies and applied MCCS mitigations, and supports vital experimentation and technology analyses as pathfinders for MCCS. The LSE-MCCS independently executes significant portions of projects addressing the security of control systems (i.e., OT systems consisting of ICS, SCADA, PLC, Discrete Process Control (DPC) systems). The LSE-MCCS supports the digital engineering organization in executing various initiatives for threat-informed mitigation in coordination with other agency MCCS mitigation, secure architecture design (e.g., Zero Trust), and transition of new technology and capability into operations support site owners in the development and application of mitigations.

12.3.1. Digital Engineering

Digital engineering ensures systems engineering is used for rigorous traceability through all elements of a solution and can help address the uncertainty of agreement. In addition, the architecture can support system engineering activities used in the process flow. This approach includes linkage of the evolving architecture to both physical and virtual (simulation) prototype; rigorous traceability through the flow of architecture development from customer requirements to

the elements of a delivered solution; support for the implementation of SOA; complemented by a good architecture model that facilitates understanding and communication by and among its users. (John M. Borky and Thomas H. Bradley). In a digital organization, a model formalizes aspects of systems engineering. Using the regression approach to measuring disagreement in segments of the cybersecurity profession to identify vulnerabilities in the model would be valuable information to pinpoint where there may be misalignment in the model that leads to the vulnerability. The model helps to motivate stakeholders through a shared vision and recognize the properties of subsystems and components. (Blockley and Godfrey). For example, such as the OV, which is the conceptual data model (i.e., data discovery), the Logical View (LV), which is the logical data model (i.e., data management), and Physical View (PV), which is the physical data model (i.e., data management).

Participants in the research questionnaire may be actors in a model. Modeling quantitative response data from the questionnaire provides insight into how uncertainty may influence system model behavior. An Actor is "anything outside the boundary of a system but with which the system interacts or that in some way influences system behavior is modeled as an Actor. Actors are most commonly associated with Use Cases, which are part of the behavioral aspect of an architecture [sic]. They have an important role in structure because they are used to explicitly declare relationships between a system and external entities." (John M. Borky and Thomas H. Bradley). For example, the operator SCADA workstation and engineering SCADA workstation in a Block Definition Diagram (BDD) of the SCADA context are in Figure 63. The SCADA display and manager/supervisor are also demonstrated in Figure 63. The PLC controllers and field devices are shown at the lower levels (e.g., flow and pressure meters, motors and pumps, switchgear, communication gateway, and generator).

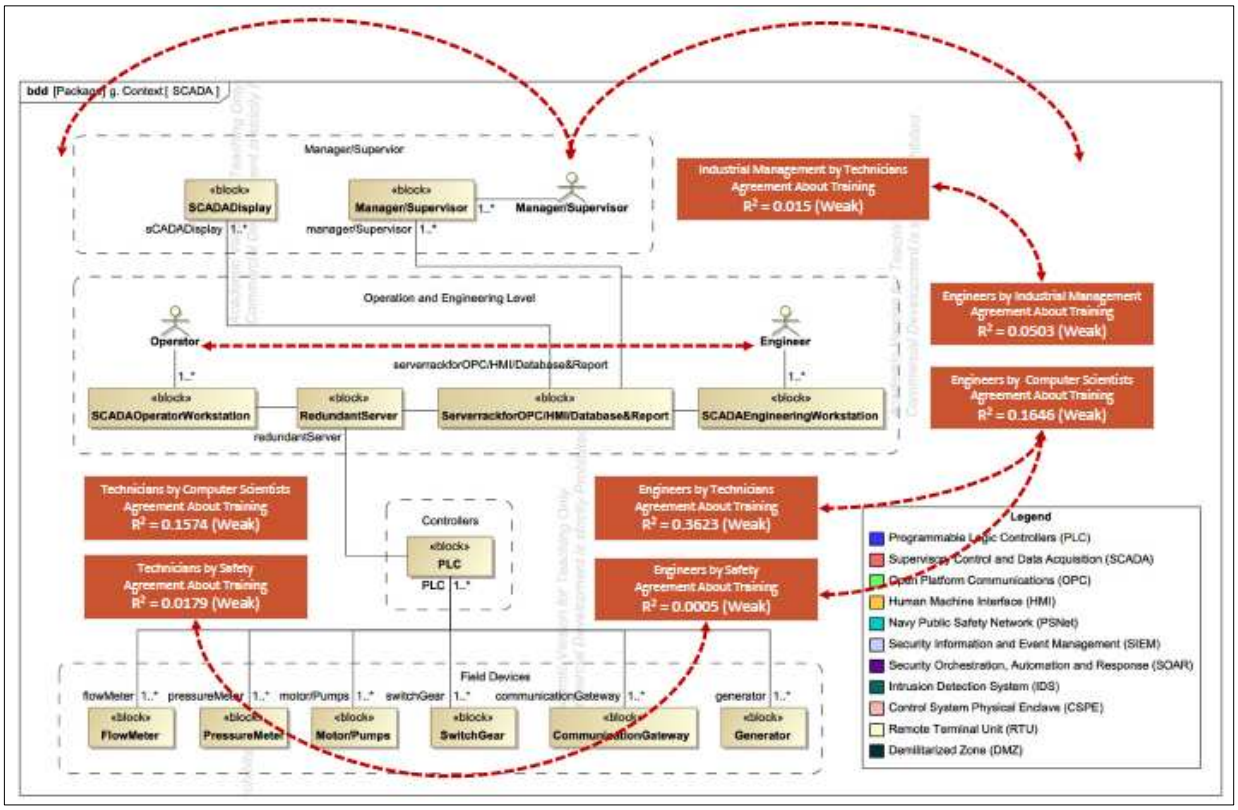

Figure 63 SCADA System Personnel and Controllers

Recall that when a series of questions were asked regarding training and certifications, participants responded about having taken available training such as the ISA.org: "Cyber Security of Automation, Control, and SCADA Systems" and Infosec Institute: "SCADA Security Online." Figure 64 shows the agreement of engineers with safety about training has an r^2 value of 0.0005. ISA.org: "Cyber Security of Automation, Control, and SCADA Systems," demonstrated as engineers (y-coordinate) and safety (x-coordinate) point (3, 22) and Infosec Institute: "SCADA Security Online," as point (3, 22) in Figure 64. Figure 65 shows the agreement of technicians with safety about training has an r^2 value of 0.0179.

Participant response to the same questions ISA.org: "Cyber Security of Automation, Control, and SCADA Systems," demonstrated as technicians (y-coordinate) and safety (x-

coordinate) point (3, 8) and Infosec Institute: "SCADA Security Online," as point (3, 8) in Figure 64. Figure 66 shows the agreement of the engineers with industrial management about training has an r^2 value of 0.0503.

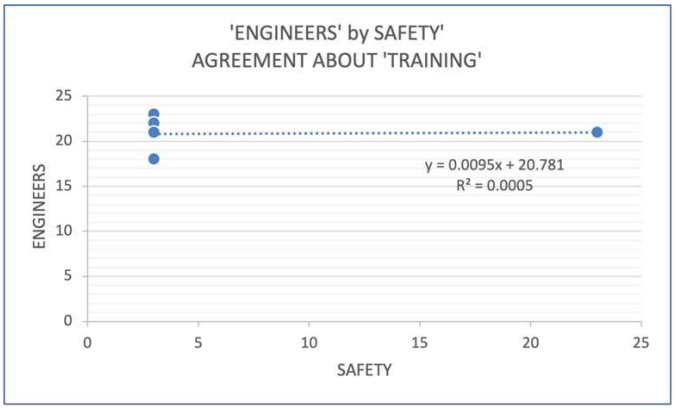

Figure 64 Correlation between Engineers and Safety for Training Questions

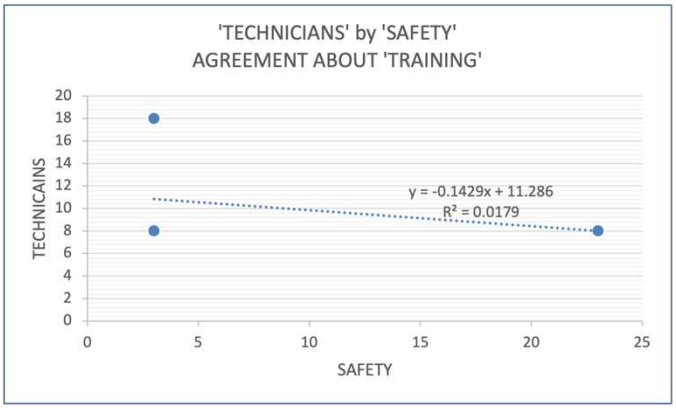

Figure 65 Correlation between Technicians and Safety for Training Questions

Response to the same questions is revealed as points (13, 22) and (13, 22) in Figure 66. Cross-training is an essential element for practical cybersecurity. Understanding and managing different stakeholder perspectives and managing the uncertainty of agreement among professionals helps leaders champion and communicate changes and improvements to the system and the balance of handling and accepting risk. The uncertainty model can give insight into the status of

potential uncertainty of agreement, lack of maturity and integration of systems and tools, and other shortcomings that can result in mitigation failure. An organization can use the data to identify where automated COA tools governance (e.g., processes and procedures) can improve mitigation.

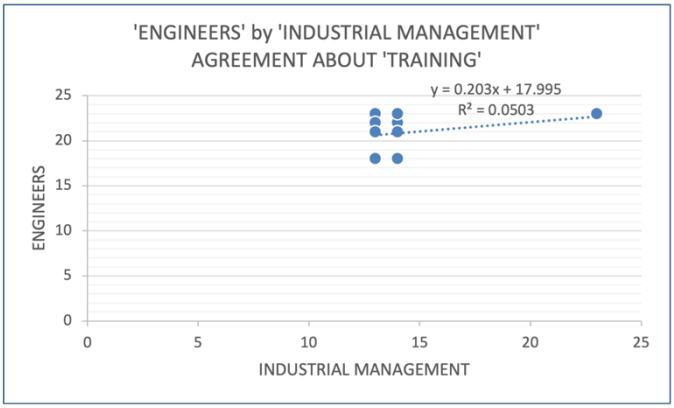

Figure 66 Correlation between Engineers and Industrial Management for Training Question

12.3.2. Reference Architecture (RA)

A control system prototype output is a reusable, extendable RA that includes system configuration requirements defining basic system behavior. However, there is no output to show where there is disagreement among professionals, or misalignment, to pinpoint where there may be a vulnerability. Efforts to protect control systems have focused on safeguarding central processes leaving the network and field devices vulnerable to attack. (Graham, Hieb and Naber). The means to measure uncertainty can be used as part of a formal verification process to assure that the specialized properties of the systems and cybersecurity solutions are well understood.

The operational, functional, and technical requirements derived from the ACI TTP are reusable across other critical infrastructure sectors. ((USCYBERCOM)). The content of a reference model that could be used as a starting point to improve the quality and consistency of the RA includes the Quality of Service (QoS) management function used to guarantee performance

(i.e., bandwidth, delay). The content from the LV QoS network function provides capabilities to prioritize data from appliances and substations to enable information delivery across the grid. For example, other content sources are Smart Meter Standards (i.e., ISO/IEC), Standards for Substation Automation Systems, Interface for meter reading and control, Communication systems for meters and remote meter reading, provider interface information, National Information Exchange Model (NIEM) for Distribution Information Exchange Models, Common information model, ISO Industrial automation systems and integration, IEEE Substation automation information), and other communication protocols applicable to Smart Grid. Engineers need access to control systems for troubleshooting, mainly when the systems are geographically dispersed. (Graham, Hieb and Naber). Measuring agreement and alignment among professions with remote access can help identify if these access points are secured sufficiently. RA is an abstraction of design patterns that can be tailed to new situations "while retaining the proven underlying principles" (Borky, 2019). On a large scale, this idea is the basis for reuse creating savings in system development in effort and cost, facilitating interoperability, interfaces, functions, and standard design approaches in implementation. Further, the RA and correlation scores can identify where vendors may have remote system access and measure the alignment of maintenance benefits against access to the control system.

Sources of information in creating the RA are Use Cases and business process mission threads aligned with actual mission equipment, subsystems, or systems. "If existing systems being used as inputs to an RA have specialized Use Cases for activities like strategy development, operational planning, operational oversight and assessment, process control, and process measurement and reporting, they can be copied in the RA. The RA team will typically have to analyze these raw materials to discover and describe universal behaviors such as strategy,

planning, process execution, communications, system monitoring, and reporting that become the top-level Use Cases of the RA. These Use Cases can then be fleshed out with content such as pre- and postconditions, associated User Roles and data objects, and scenarios" (Borky, 2019). Consistent architecture and functional design, and standard interface definitions can reduce time and cost, facilitate high-quality systems engineering process and methodology to ensure consistent quality, and prove policy compliance that reduces risk and effort in the design and satellite build. (Borky, 2019). A specific set of capabilities is met by activities from the most general to the most particular requirements in a reference model to a realized, typical system architecture, as shown in Table 11.

Table 11 Capabilities of a Typical Architecture

Overarching Rules and Policies	Structure, Behavior, and Rules for a Specific System Type
Common Vocabulary	Requirements Template and Allocations
Governance Principles	Detailed Services Catalog
Application Guidance	Operational & Logical Views
Requirements Template and Allocations	Services Taxonomy and Allocations
Tailorable Use Cases, Domains, Threads, Data Model	May include artifacts from multiple RAs
Design Patterns and Timing Model (Operational & Logical Views)	Tailorable Use Cases, Domains, Threads, Data Model, Design Patterns, and Timing Model
Generic Services Taxonomy and Allocations	Supplementary Data and Documentation
Generic Focused Views (e.g., Network, Security, Infrastructure)	Focused Views (e.g., Network, Security, Infrastructure) Operational, Logical and Physical Views

12.4. Technology – Tools, Open API, and Automation

Our findings show the need to use tools, Open API, and automation to allow the digital footprint of any cybersecurity control system solution to permeate from design inception throughout the engineering development lifecycle and operational fielding. Cybersecurity challenges for control systems are developing accurate models that precisely reflect the physical system properties. Capability such as digital twin technology provides a virtual representation of the physical components of a system. Since near real-time monitoring of the system is desired for cybersecurity, technology-enabled capabilities such as tools, Open API, and automation enable modeling based on any changes to a system's configuration. These technology approaches would allow organizations to understand design change impacts, communicate design intent, and analyze and predict product design before acquiring, building, and fielding a solution into operations. System architecture models developed across multiple domains such as program management, product support, verification, software, and mechanical and electrical components can help bring alignment among professions. Advancements such as remote access, cloud environments, and the internet of things enabled by sensors with connectivity and bandwidth factors and cyber communication) are making the virtualization technologies significant.

Virtual integrated model-based representation of physical components allows the simulation of the product in a real-world setting dynamically and demonstrates closed loops between the virtual and physical space. Open API design ensures multiple vendors can collaborate consistently and effectively. Open API is machine-readable, tested against system specifications, and kept to standards. Humans simply do not work at the speed of automation. Adversaries are using automated attack TTP. Organizations need to respond in near real-time based on operational mission requirements. Architecture can contribute to successful system development by providing

a consistent approach to dealing with a complex entity, maintaining traceability from requirements to physical components, and ensuring all system behaviors are captured and mapped to solution elements. (D. F. a. S. S. Aleksandra Scalco).

12.5. Environment – Schoolhouse, Testbed, and Digital Twin

12.5.1. Create a Schoolhouse and Extendable Schoolhouse Model

Our findings show a knowledge gap and training opportunities exist for cross-training between OT and IT professions. Collaboration and cross-training on cyber hygiene and control system operations can develop new skills sets. Cross-training professionals would improve the overall ability to achieve and maintain C2 and is key to addressing multi-concern assurance (i.e., safety and technicians' understanding of cybersecurity, and engineers and computer scientists' understanding of control system safety). A formal schoolhouse can offer to cross-train and prepare leaders to understand better and manage complex, multi-technology, and information-intensive control system assets that control critical infrastructure to achieve cybersecurity assurance. Self-study cybersecurity training and certification cannot singularly help professionals manage the complexity of systems-of-systems that control the physical world. Integration of new capabilities based on advanced technology requires a formal schoolhouse program, or professionals will undoubtedly continue to have an uncertainty of agreement or simply be overwhelmed (e.g., chaos).

When asked about Red Teams, we found moderate to strong agreement by critical infrastructure sectors. However, a knowledge gap and training opportunity exist to leverage Red Team interaction with stakeholders at all organizational levels to improve the certainty of the agreement by professional occupations about risk assessments and effectiveness of system security against current real-world attack techniques. A formal schoolhouse to develop national-level

experts would enhance the body of knowledge of mitigation of critical infrastructure vulnerability.

C2 governance and requirements are guided by the JCIDS process and led by a lead military command under USC Title 10 legal authorities. The lead command oversees a budgeted Program of Record (POR) governed by DOD 5000 acquisition policies. Performance standards are deterministic to meet military utility requirements. The C2 is embodied in law, doctrine, policy, instructions, and TTP. A "schoolhouse" provides theoretical and practical knowledge needed for professionals given duties of increased complexity. Schoolhouse programs are augmented by self-study certification training (e.g., ISA.org "Cyber Security of Automation, Control, and SCADA Systems") and on-the-job learning to prepare professionals for job responsibilities. (Caine).

For example, during World War II, the loss ratio of enemy aircraft to US aircraft was 14:1. During the first years of aerial combat in Vietnam, that ratio fell to 2.5:1, surprising considering the United States employed sophisticated, high-performance, missile-armed fighters. There were many complicating factors, but that ratio indicated problems. (Baranek). For example, there was a lack of professional agreement on whether a pilot needed capability for close aerial combat. The high value of the F-4 Phantoms was the ability to destroy enemy planes from 10 miles beyond visual range. Beyond visible scope is how the Navy trained F-4 Phantom pilots to fight. Most did not know how to fight any other way. However, doctrine prohibited a pilot from firing beyond visual range. A fighter pilot had first to confirm the target visually, potentially attributed to the opinion that the enemy would be confronted from a distance using missiles. (Pedersen).

As a result of the failing ratio, the Navy Fighter Weapons School, known as Top Gun, was created. After Top Gun and other measures, the Navy's ratio was back to a ratio of 13-to-1. (Baranek). Similarly, doctrine today about remediation of critical infrastructure vulnerability is not in alignment with the reality of near real-time cyber domain intersection with the physical domain.

Authorities are dispersed among departments from the DOD, DOE, DHS, Department of Transportation (DOT), and other entities. Government assets have a high symbiotic relationship with commercial assets. However, there is a lack of understanding about deploying innovation and new capability into live system operations.

Navy system operators successfully demonstrated the MOSAICS initial cyber defensive operating capability for control systems in an MUA for a power utility site in August 2021. The USCYBERCOM ACI TTP manual mitigation was the genesis of the MOSAICS requirements. An initial high-level RA was created for reuse to deliver the urgently needed mitigation capability. National-level experts from the services and national laboratories (e.g., UARC, FFRDC) contributed to the initial science, research, and advisory to demonstrate the capability. The MOSAICS body of knowledge is foundational for the formation of a schoolhouse. What was learned by the MOSAICS demonstration in the mission approach should be used in the schoolhouse to formalize and improve the CONOP, recommend law and policy, doctrine, instructions, and provide the valuable feedback loop to the USCYBERCOM ACI TTP.

12.5.2. Create a Testbed That Extends Throughout the DOTLMPF-P

Our findings show a knowledge gap and training opportunity exist to establish measures and metrics for the DOTLMPF-P assessment (i.e., promoting institutional knowledge of control systems) and improve awareness of existing best practices and benchmarks used in other sectors such as IT. The measure of an organization's agreement about cyber capability can help identify where uncertainty can impede mission. Design and planning of future military installations include using advanced digital and intelligent technologies to manage mission operations in physical and cyber domains. Elements include fire protection, utility control systems, material handling, building control systems, petroleum and oil, physical security, Electronic Security Systems (ESS),

mobile ranges, and drones. The analytic model supports DOTMPLF-P analysis of new capabilities. The DOTMLPF-P study is a first step in the Functional Solutions Analysis (FSA) part of the DOD JCIDS acquisition process. MOSAICS addresses the control system protection of critical infrastructure for non-kinetic attacks on systems that support joint warfighting operations. The technical approach develops COTS solutions for contractor-delivered ICS and SCADA systems. Three components serve as critical elements in an Independent Assessment Plan (IAP) to ensure MOSAICS meets the COCOM needs: the CONOPS, the ACI TTP for DOD ICS, and the DOTMLPF-P analysis. DOTMLFP-P provides the roadmap for the successful delivery of the capability. A measure of uncertainty of agreement offers insights into where there may be misalignment in the DOTMLFP-P that leads to vulnerability.

The U.S. Navy acquisition priorities in FY22 include the Navy Shipyard Infrastructure Optimization Program to repair, modernize and upgrade the efficiency of four public naval repair yards. (Eckstein). A recommendation is to create a DOTMLFP-P model of an installation "SmartBase" site using the uncertainty of agreement model and methodology to identify where there may be mitigation pain points. A "SmartBase" testbed for DOD bases and installations for IoT and cyber technologies. (Atherton). The sharable DOTMLFP-P model of an installation "SmartBase" site will enable services to share system elements to accomplish systems engineering with the power of a formal architecture methodology, as shown in Figure 67. The shared model ensures rigor, repeatability, and production; promotes design quality and correctness; reduces risk; and enhances communication and synchronization throughout the JCIDS DOTMLFP-P assessment, as shown in Figure 1. Stakeholder communication and agreement should be in alignment and agreement throughout to address known vulnerability and prepare for emerging exposure in any part of the system services, as shown in Figure 69.

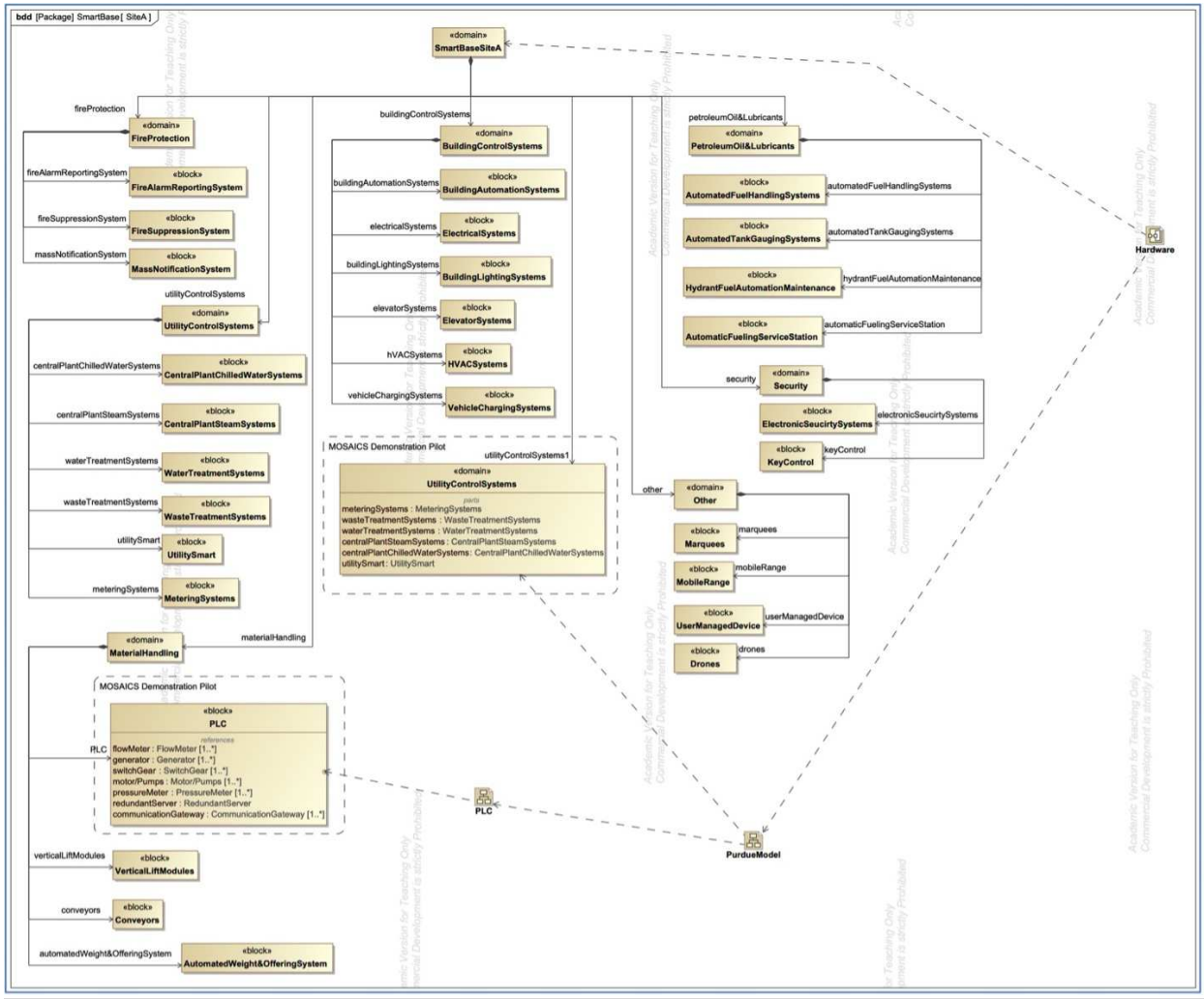

Figure 67 SmartBase "Site A" Overview

The Navy creates digital twins to test new technology and capabilities and address environmental issues. It is possible to shut down IT systems when an anomaly is detected. However, this is not the case for OT systems. OT systems need to be operating through an intrusion. (Kayan et al.). The digital twin is a transformative approach to installation management and is an opportune time to introduce cybersecurity capability for control system critical infrastructure. For example, a challenge is testing operating system and application patches against control system configurations customized for each site. Operators often do not have the training required to test patches, nor the time to apply these on a consistent schedule. (Graham, Hieb and

Naber).

The contract awarded $1.3 billion and $63 million to improve installation facilities at Portsmouth Naval Shipyard in Maine. An additional $500 million was awarded to support Pearl Harbor Naval Shipyard and Intermediate Maintenance Facility in Hawaii (HI), Puget Sound Naval Shipyard, and the Intermediate Maintenance Facility in Washington. (Eckstein). Similarly, the Army Installations Strategy and Air Force Installation of the Future (IoTF) lean on IoT technologies and pilot programs to test installation effectiveness. (Eckstein).

JCIDS is the authoritative process to support the development of a DOD materiel solution. The DOD must unambiguously align the entire ecosystem from strategic guidance to the DOTMLPF-P strategy to achieve objective mission success. (Scalco "Preliminary Exam"). Any time something game-changing is introduced, it affects the DOTMLPF-P process and can create uncertainty. Multi-concern assurance flows between each of the eight domains of a DOTMLPF-P analysis, as shown in Figure 2. Therefore, a significant emphasis of DOTMLPF-P is to support the development of a materiel solution. The output of the JCIDS analysis defines needed capabilities, guides materiel development, and directs the production of capabilities in coordination with the Joint Staff. Introducing any solutions follows this process. A DOTMLPF-P model will help address the uncertainty of agreement about mitigations as it encompasses all real-world factors.

13. Chapter Thirteen – Conclusions

Disagreement among professionals about how to treat cybersecurity leads to misalignment and ultimately vulnerability greater than innate system design vulnerability. Back to the tranquility of the TVA reservoir dam system and the city of Oldsmar – like many small towns and cities throughout the United States – the extension of connectivity in the digital transformation of engineering to critical infrastructure introduces new capabilities to control systems and multi-concern assurance uncertainty. Ramifications for policy, governance, and operations are almost unavoidable given the shift to mass permanent telework environments and increased desire for mobile access. Agreement among professionals is a countable measure of understanding to follow a specific COA, such as using the ACI TTP to defend control systems from cyber-attacks. ((USCYBERCOM)). Increasing certainty of agreement across all sectors about cybersecurity for control systems is vital to a DiD strategy.

This is what Top Gun did. The Navy established Top Gun to prepare better personnel to face an enemy. Industry and government worked together to improve technology advances. A core of specialists was based on training fighter crews in innovative ways and replicated the capabilities of likely enemy fighters. A schoolhouse needs to be established like Top Gun for cybersecurity for control systems, so innovation can safely fail, fail fast, improve, and rapidly deploy mitigation into control systems. A digital engineering organization needs to be created to demonstrate and test the capability before deployment and enable stakeholders to understand all aspects of the remediation and budget. This schoolhouse requires government and commercial collaboration. (Baranek).

Unfortunately, the transformation of control systems through IP-connectivity in the cyber

domain introduces new complexities that some systems were initially designed to address. Cyber vulnerabilities were unimaginable when some of the critical infrastructures were built. Retrofitting cybersecurity into legacy systems is a tremendous challenge – so is developing cybersecurity into new designs. All aspects of multi-concern assurance need to be well-understood by all stakeholders, such as knowledge of network systems in the organization, knowledge of facilities and infrastructure used in operations; how the participant's organization handles a data breach or cyberattack, including the way consequences of the attack or breach (the "incident") are managed; the processes by which materials, energy, services, staff, knowledge, or other assets are made available; what representative training and certification courses related to control systems stakeholders have taken; what KSAs apply directly to the performance of a function; how to evaluate detection and response capabilities before live play on networks; and cybersecurity practices, such as penetration testing and encryption. Innovation by automation will help, as will cybersecurity training. However, there is much urgency to resolve tremendous complexity. DEI initiatives benefit organizations by tapping into a broader talent pool with greater creativity to help understand and resolve complexity, offer differing perspectives, and add a variety of qualities to the needed capacity-building to fill the cybersecurity gaps.

A new capability must often traverse the formidable "valley of death" before innovation meets milestone realization between domains. Additionally, the uncertainty of agreement among professionals exists throughout about early prototyping, experimental concepts, operational use, and competition for resources. Cybersecurity training alone will not resolve the uncertainty of agreement. The complexity and sometimes chaos of the problem space requires a better understanding of the uncertainty lurking. Rigorous systems engineering is necessary. Threats to assets can arise from a broad spectrum of threat agents, and today's requirements for cybersecurity

will look different in day-to-day operations than previously.

Sun Tzu wrote, "To win one hundred victories in one hundred battles is not the acme of skill. To subdue the enemy is the acme of skill." (Sun-Tzu). Quantification of agreement among control system professionals increases visibility into areas where divergence arises. System defense is challenging if neither the adversary nor the professionals designing, operating, and managing the system are well understood or known. A model and methodology for measuring multi-concern assurance through the statistical uncertainty analysis of Likert and semantic differential scales help to guide and define the acme of skill. The approach provides a needed compass for "Context-sensitive Critical Infrastructure Dynamic Classes" characterized in a meaningful way while best practices, guidance, standards, and policy "catch up." Well understood cybersecurity for control systems by everyone in the system DOTMLPF-P lifecycle is an approach to subdue the adversary.

While all risks are uncertain and might affect system security if they happen, uncertainty does not only include the potential of bad things or threats. (Yanjuan). Possible good things are also "uncertainties that matter." That is why measuring uncertainty and measuring multi-concern assurance is worth understanding. Any "uncertainty" needs to be identified, assessed, and managed to ensure the best possibility of cyber defender teams into a source of competitive advantage for maintaining C2 at "near real-time" over critical infrastructure control systems. This research contributes to the body of knowledge to achieve, by measurable statistical difference, using a novel mathematical model for the uncertainty of agreement and methodology to maintain C2 over the cyber and control system domains — with greater certainty across the many "valleys of death" in the acquisition lifecycle from disagreement found in chaos to the confidence of agreement to address the vulnerability.

Avoiding cyberspace conflict can be accomplished by defending control systems from cyber-attack. A model and mechanism for integrating contextual information from context-sensitive critical infrastructure control systems are the keys to overcoming uncertainty of agreement for achieving cyber security. "Invincibility lies in the defense; the possibility of victory in the attack." (Sun-Tzu).

Extension of connectivity in the digital transformation of engineering to critical infrastructure introduces new system engineering challenges. Implementing policy or adding new capabilities to defend control systems will not work if there is disagreement among professionals. While governments are trying to bring critical components together, a genuine concern is that throwing money at this problem is not resolving vulnerabilities until stakeholders agree on the resources. Despite all the valiant effort, there will continue to be increased exposure if disagreement and misalignment on what constitutes a cybersecurity vulnerability are not addressed. It is worrisome when there are competing views between professionals. When the data shows no correlation between two professional groups, that is a vulnerability. When that vulnerability is identified, future research can lead to resources allocated given known disparities between how professionals think a control system's cybersecurity is functioning. The professionals will be competing against one another and, worse, undermine the work that has been done to secure the system. Shared understanding is needed, or we will not build a design from the ground up to address cybersecurity. Let alone retrofit security into a system. The professionals will be working from different assumptions and not come together. The process presented is a new means of addressing the uncertainty using measurable data that otherwise ends up in vulnerability.

The result of the research will contribute to the Systems Engineering Body of knowledge to achieve, by measurable statistical difference, and maintain Command and Control (C2) over the

Cyber-Physical System/Control System domain — Helping to resolve disagreement among professionals, which leads to misalignment, which results in vulnerability. The approach is a new, innovative model and a novel methodology. The output from this model leads us to identify specific areas of vulnerability that can then be resolved. The research shows that the relative ranking and the relative concern that people have with things differently and the order they differ in can be rolled into the cyber r^2 value, which shows that they have different priorities. If they have other orders, they have different priorities. If professionals have different priorities, they have different things that they think are the genuine concern. That is disagreement which is a misalignment in terms of what they will try to fix, which is a vulnerability. There are all kinds of vulnerabilities, but they will be easier to address and more cost-sensitive if professionals agree with what they are trying to do. We know that there is vulnerability. This model and methodology measure disagreement in segments of the cybersecurity profession to identify vulnerabilities.

Citations

,,,,,,,,,,,("TVA"), Tennessee Valley Authority. "A Guide to Information About the Tennessee Valley Authority." Tennessee Valley Authority ("TVA") 2021. Web. July 8, 2021 2021.

---. "Tva Fun." Tennessee Valley Authority ("TVA") 2021. Web. July 8, 2021 2021.

(CISA), Cybersecurity & Infrastructure Security Agency. "Alert (Aa21-042a) Compromise of U.S. Water Treatment Facility." Ed. (DHS), Department of Homeland Security: Cybersecurity & Infrastructure Security Agency (CISA), 2021. Print.

---. "Infrastructure Security Month 2020." Ed. (CISA), Cybersecurity & Infrastructure Security Agency: Department of Homeland Security (DHS), 2020. 16. Print.

(CISA), Cybersecurity and Infrastructure Security Agency. "Alert (Aa21-131a), Darkside Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks." Ed. (DHS), Department of Homeland Security: Cybersecurity and Infrastructure Security Agency (CISA). 1. Print.

---. "Securing Industrial Control Systems: A Unified Initiative Fy 2019—2023." Ed. (DHS), Department of Homeland Security: Cybersecurity and Infrastructure Security Agency (CISA), 2019. 15. Print.

(CISA), Department of Homeland Security (DHS) Cybersecurity & Infratructure Security Agency. "Critical Infrastructure Sectors." Department of Homeland Security (DHS) 2019. Web. December 6 2019.

(CISA), The Cybersecurity and Infrastructure Security Agency. "Alert (Aa21-131a), Darkside Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks." Ed. (DHS), Department of Homeland Security: The Cybersecurity and Infrastructure Security Agency (CISA). 1. Print.

(CMU), Carnegie Mellon University. "Multi-Factor Authentication: What It Is and Why You Need It." Computing Services. Carnegie Mellon University (CMU) 2019. Web2020.

(CPNI), Centre for the Protection of National Infrastructure. "Critical Infrastructure Sectors." Ed. Government, United Kingdom. Online: United Kingdom Government, 2021. Print.

(DHS), Department of Homeland Security. "Worldwide Attacks against Dams — a Historical Threat Resource for Owners and Operators." Ed. (DHS), Department of Homeland Security. Washington, DC: Department of Homeland Security (DHS), 2012. Print.

(DISA), Defense Information Systems Agency, and National Security Agency (NSA). "Department of Defense (Dod) Zero Trust Reference Architecture." Ed. Defense, Department of: Department of Defense, 2021. 170. Print.

(EIA), U.S. Energy Information Administration. "Electricity Explained: Electricity Generation, Capacity, and Sales in the United States." U.S. Energy Information Administration (EIA). Web. July 21, 2021 2021.

(EPA), United States Environmental Protection Agency. "Distributed Generation of Electricity and Its Environmental Impacts." About Distributed Generation. www.epa.gov: United States Environmental Protection Agency (EPA), 2021. Print.

(GAO), United States Government Accountability Office. "Electricity Grid Cybersecurity: Doe Needs to Ensure Its Plans Fully Address Risks to Distribution Systems." Washington, DC, USA: United States Government Accountability Office (GAO), 2021. Print.

(IHA), The International Hydropower Association. Ethiopia - Grand Ethiopian Renaissance

Dam (Gerd). www.hydropower.org: The International Hydropower Association (IHA), 2001. Print.

(ISACA), Information Systems Audit and Control Association. State of Cybersecurity 2020, Part 1: Workforce Efforts and Resources2020. Print.

(ISC)2. (Isc)2 Cybersecurity Perception Study: (ISC)2, 2020. Print.

---. (Isc)2 Cybersecurity Workforce Study, 2021. On-line2021. Print.

(USCYBERCOM), United States Cyber Command. "Advanced Cyber Industrial Control System Tactics, Techniques, and Procedures (Aci Ttp) for Department of Defense (Dod) Industrial Control Systems (Ics)." Ed. (DOD), Department of Defense: United States Cyber Command, 2016. 162. Vol. 1. Print.

---. "Advanced Cyber Industrial Control System Tactics, Techniques, and Procedures (Aci Ttp) for Department of Defense (Dod) Industrial Control Systems (Ics)." Ed. Defense, Department of2018. 209. Vol. 2. Print.

Akwetey Henry Matey, Paul Danquah, Godfred Yaw Koi-Akrofi. "Predicting Cyber-Attack Using Cyber Situational Awareness: The Case of Independent Power Producers (Ipps)." International Journal of Advanced Computer Science and Applications (IJACSA) 13 (2022). Print.

Aleksandra Scalco, David Flanigan and Steven Simske. "Control Systems Cyber Security Reference Architecture (Ra) for Critical Infrastructure: Healthcare and Hospital Vertical Example." Journal of Critical Infrastructure Policy 2.2 (2021): 125 -43. Print.

Aleksandra Scalco, Erika Palmer. "Social Systems Engineering for Achieving Cyber Physical-Social System Multi-Concern Assurance." 19th International Conference on Systems Engineering (CSER 2022). Norwegian University of Science and Technology, 2022. Print.

Aleksandra Scalco, Manan Jayswal, Steve Simske. "More Situational Awareness for Industrial Control Systems (Mosaics) Joint Capability Technology Demonstration (Jctd): A Concept Development for the Defense of Mission Critical Infrastructure." Homeland Defense & Security Information Analysis Center (2019). Print.

Aleksandra Scalco, Steve Simske. "Championing Cultural Change and Control Systems Cyber Security." AIAA-INCOSE Wasatch Aerospace and Systems Engineering Mini-Conference. AIAA Utah Section, 2021. Print.

Alvarez, Alejandro. Egypt Pleads for Un Security Council Intervention over the Grand Ethiopian Renaissance Dam. www.theowp.org: The Organization for World Peace, 2021. Print.

Atherton, Kelsey. "Army Seeks Security for 'Smart' Base Networks." Breaking Defense (2022). Print.

Atkinson, Joe. "Engineer Who Opposed Challenger Launch Offers Personal Look at Tragedy." NASA October 5, 2012 2012. Web. November 18, 2021 2021.

Bank, The World. "Access to Electricity (% of Population)." Access to Electricity (% of population). The World Bank 2021. Web. July 21, 2021 2021.

Baranek, Dave. "Origins of Topgun." HistoryNet. Print.

Berkes, Howard. "Challenger: Reporting a Disaster's Cold, Hard Facts." National Public Radio (NPR) (2006). Print.

Bhamare, Deval, et al. "Cybersecurity for Industrial Control Systems: A Survey." Computers & Security (2018): 12. Print.

Biden, President Joseph. "Executive Order on Improving the Nation's Cybersecurity." Ed. Office, Executive. Washington, D.C.: Executive Office, 2022 of Executive Order. Print.

---. "National Security Memorandum to Improve the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems." Ed. Office, Executive. Washington, D.C.: Executive Office, 2022 of National Security Memorandum. Print.
Blockley, David, and Patrick Godfrey. Doing It Differently. ICE Publishing, 2017. Print.
Borky, J.M., and T.H. Bradley. Effective Model-Based Systems Engineering. Springer International Publishing, 2019. Print.
Borky, John M., and Thomas H. Bradley. "Protecting Information with Cybersecurity." Effective Model-Based Systems Engineering. Cham: Springer International Publishing, 2019. 345-404. Print.
Braue, David. "Global Ransomware Damage Costs Predicted to Exceed $265 Billion by 2031." Cybercrime Magazine (2021). Print.
Caine, Bruce T. "Military Professional Education System." Education Encyclopedia. Education Encyclopedia 2021. Web. November 27, 2021 2021.
Campbell, Christa. "The Utility Network: Resources for Water Utilities." ArcGIS Blog 2021. Web.
Collier, Kevin. "50,000 Security Disasters Waiting to Happen: The Problem of America's Water Supplies." NBC News: NBC News, 2021. Print.
Congress, 117th. "National Defense Authorization Act (Ndaa) for the Fiscal Year 2022." Ed. Congress, 117th. Washington, D.C.2021. Print.
Cybersecurity for Smes: Introducing the Human Element into Socio-Technical Cybersecurity Risk Assessment. Proceedings of the 16th International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications (VISIGRAPP 2021). 2021. Print.
David Clark, Thomas Berson, Herbert S. Lin. At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues. Washington, D.C.: The National Academies Press, 2014. Print.
David E. Whitehead, Kevin Owens, Dennis Gammel, Jess Smith. "Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies." 70th Annual Conference for Protective Relay Engineers (CPRE). Print.
Defense, Department of. "Jcids Process." Acquisition Notes. Defense Aquisition University (DAU) 2021. Web. March 2021 2021.
---. "National Defense Strategy of the United States of America." Ed. Defense, Department of: Department of Defense, 2018. Print.
Department of Defense, Chief Information Officer. "Cybersecurity Reference and Resource Guide." Ed. Department of Defense, Chief Information Officer2020. 53. Print.
Dik, Bryan J. Redeeming Work: A Guide to Discovering God's Calling for Your Career. West Conshohocken, PA: Templeton Press, 2020. Print.
Diogenes, Yuri, and Erdal Ozkaya. Cybersecurity — Attack and Defense Strategies. Ed. Packt>. Vol. 2nd Edition. Birmingham, UK: Packt Publishing Ltd., 2019. Print.
Dubova, Maria. "Cybersecurity and Defense of Critical Energy Infrastructure in Ukraine: Frame Analysis of the Discourse." Masaryk University, 2019. Print.
Eckstein, Megan. "Us Navy Acquisition Chief Outlines Fy22 Priorities." Defense News (2021). Print.
Elmhorst, Rick. "Oldsmar Water Hack: What Happened and Why It Could Happen Again." To The Point Already. Ed. Elmhorst, Rick. Spectrum Bay News 9: Spectrum Bay News 9, 2021. Print.

Model-Based Cybersecurity Analysis: Past Work and Future Directions. 67th Annual Reliability and Maintainability Symposium (RAMS). May 18, 2021 2021. IEEE. Print.
EPA. "Epa Cybersecurity Best Practices for the Water Sector." EPA 2022. Web2022.
Esper, M., Wolf, C., Brouillette, D., Chao, E. . A Report to the President of the United States on Strengthening the Nation's Cybersecurity Workforce for Cyber-Physical Systems & Control Systems. Washington, D.C.2020. Print.
Esposito, Frank. "Westchester Village Finds Clever Solution to Thwart Hacking of Critical Infrastructure." Rockland/Westchester Journal News (2020). Print.
Fruhlinger, Josh. "What Is Stuxnet, Who Created It and How Does It Work?" CSO Online (2017). Print.
Government, Canadian. "National Strategy for Critical Infrastructure." Canada: Canadian Government, 2009. Print.
Graham, James, Jeffrey Hieb, and John Naber. "Improving Cybersecurity for Industrial Control Systems." 2016 IEEE 25th International Symposium on Industrial Electronics (ISIE). IEEE, 2016. Print.
Group, World Bank. Global Economic Prospects. Washington, DC: World Bank Group, 2021. Print.
Haegley, Daryl. "Dod Cyber Strategy Implementation." MOSAICS Industry Day. MOSAICS Industry Day: OUSD, 2020. Print.
Dod Advanced Control Systems Tactics, Techniques and Procedures. September 14, 2016 2016. The PMC Group LLC. Print.
Hahn, Adam, and Manimaran Govindarasu. "An Evaluation of Cybersecurity Assessment Tools on a Scada Environment." IEEE Power and Energy Society General Meeting. IEEE, 2011. Print.
Hans de Bruijn, Marijn Janssen. "Building Cybersecurity Awareness: The Need for Evidence-Based Framing Strategies." Government Information Quarterly 34 (2017): 1-7. Print.
Harp, Derek R., and Bengt Gregory-Brown. "Bridging the Divide." NexDefense2014. Print.
Hemme, Kris. "Critical Infrastructure Protection: Maintenance Is National Security." Journal of Strategic Security 8 (2015): 25-39. Print.
Herring, Michael, and Keith Willett. "Active Cyber Defense: A Vision for Real-Time Cyber Defense." Journal of Information Warfare (JIW) 13 (2014): 46-55. Print.
Hong Li, Theodore J. Williams. "Some Extensions to the Purdue Enterprise Reference Architecture (Pera): I. Explaining the Purdue Architecture and the Purdue Methodology Using the Axioms of Engineering Design." Computers in Industry 34.3 (1997): 247-59. Print.
House, U.S. "House Resolution 1833 (H.R. 1833) "Dhs Industrial Control Systems Capabilities Enhancement Act of 2021"." Ed. House, U.S. Washington, D.C.: U.S. House, 2021. Print.
Howell, Elizabeth. "Apollo 1: A Fatal Fire." 2017. Web. November 14, 2021 2021.
InfraGard. "Infragard." https://www.infragard.org/Application/Account/Login: https://www.infragard.org/Application/Account/Login, 2022. Print.
Iosif Progoulakis, Nikitas Nikitakos, Paul Rohmeyer, Barry Bunin, Dimitrios Dalaklis and Stavros Karamperidis. "Perspectives on Cyber Security for Offshore Oil and Gas Assets." Journal of Marine Science and Engineering 9 (2021): 27. Print.
Irwin P. Levin, Sandra L.Schneider, Gary J.Gaeth. "All Frames Are Not Created Equal: A Typology and Critical Analysis of Framing Effects." Organizational Behavior and Human Decision Processes 76.2 (1998): 149-88. Print.

Irwin P.Levin, Sandra L.Schneider, Gary J.Gaeth. "All Frames Are Not Created Equal: A Typology and Critical Analysis of Framing Effects." Organizational Behavior and Human Decision Processes 76.2 (1998): 149-88. Print.

Jaganmohan, Madhumitha. "Hydropower and Renewable Energy Capacity 2008-2020." Existing renewable energy capacity worldwide. Staistica 2021. Web. July 21, 2021 2021.

---. "Largest Hydroelectric Power Generating Countries Worldwide in 2019 (in Terawatt Hours)." Largest hydropower producing countries 2019. Statistica 2021. Web. July 21, 2021 2021.

Janet Napolitano, Robert Gates. "Memorandum of Agreement between the Department of Homeland Security and the Department of Defense Regarding Cybersecurity." Ed. CYBERSECURITY, DEPARTMENT OF HOMELAND SECURITY AND THE DEPARTMENT OF DEFENSE REGARDING: DEPARTMENT OF HOMELAND SECURITY AND THE DEPARTMENT OF DEFENSE REGARDING CYBERSECURITY, 2010. 5. Print.

JR.), White House (JOSEPH R. BIDEN. "National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems." Ed. House, White. WH.GOV: White House, 2021. 1. Print.

Kandeel, Amal. "Nile Basin's Gerd Dispute Creates Risks for Egypt, Sudan, and Beyond." Atlantic Council (2020): 1. Print.

Kavallieratos, Georgios, Sokratis Katsikas, and Vasileios Gkioulos. "Cybersecurity and Safety Co-Engineering of Cyberphysical Systems—a Comprehensive Survey." Future Internet (2020): 17. Print.

Kayan, Hakan, et al. "Cybersecurity of Industrial Cyber-Physical Systems: A Review." arXiv:2101.03564 (2021): 32. Print.

---. "Cybersecurity of Industrial Cyber-Physical Systems: A Review." Association for Computing Machinery (ACM) Computing (2022). Print.

Keeney, Michelle, et al. Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors2005. Print.

Kerman, Alper, et al. "Implementing a Zero Trust Architecture." Ed. (NCCoE), National Cybersecurity Center of Excellence: National Cybersecurity Center of Excellence National Institute of Standards and Technology, 2020. Print.

Mosaics Transition Strategy. MOSAICS Industry Day #3/TechConnect. 2021. MOSAICS JCTD, 2021. Print.

Klein, Christopher. "Remembering the Apollo 1 Tragedy." History August 22, 2018 2017. Web. November 14, 2021.

Lewis, James A. Cybersecurity and Critical Infrastructure Protection: Center for Strategic and International Studies, 2006. Print.

Madnick, Stuart. "What Executives Get Wrong About Cybersecurity." Sloan Management Review.Winter 2017 (2017): 22-24. Print.

Marsh, Stephen P. "Formalizing Trust as a Computational Concept." Ontario Tech University, 1999. Print.

McBride, Deloris Y. "An Analysis of Cybersecurity Curriculum Designs, Workforce Readiness Skills, and Applied Learning Effectiveness." Doctoral. Capitol Technology University, 2021. Print.

Meeks, Alexandra. "A California Reservoir Is Expected to Fall So Low That a Hydro-Power Plant Will Shut Down for First Time." Ed. Meeks, Alexandra. www.cnn.com: CNN, 2021.

Print.
Menn, Joseph, and Raphael Satter. "Pipeline Hackers Say Their Aim Is Cash, Not Chaos." Reuters (2021). Print.
Moon, We Hack the. "Hack the Moon." https://wehackthemoon.com/bios/gene-kranz. Web. November 17, 2021 2021.
Munirathinam, Sathyan. "Chapter Six - Industry 4.0: Industrial Internet of Things (Iiot)." Advances in Computers 117.1 (2020): 129-64. Print.
Munshi, Jamal. "“a Method for Constructing Likert Scales”." SSRN Electronic Journal (2014): 13. Print.
Navy, U.S. Department of. "Plank Owners, Plank Owner Certificates, and Planking." Naval History and Heritage Command. U.S. Department of Navy April 23, 2019 2007. Web. September 25, 2021 2021.
Networks, Nozomi. What You Need to Know to Fight Ransomware and Iot Vulnerabilities Including Recommendations for Enhancing Cyber Resilience. nozominetworks.com: Nozomi Networks, Inc., 2021. Print.
Obama, Executive Office of President Barack. "Presidential Policy Directive/Ppd-41, United States Cyber Incident Coordination." Ed. House, The White. Washington, DC: Executive Office of the President of the United States, 2016. Print.
Officials, Association of State Dam Safety. "Dams 101." Association of State Dam Safety Officials 2021. Web. July 21, 2021 2021.
Pedersen, Dan. Topgun an American Story. New York: Hachette Books, 2019. Print.
Piliero, Raphael J. "Ethiopia’s Grand Renaissance Dam: Assessing China’s Role." U.S.-China Perception Monitor 2021. Web.
Pultarova, Tereza. "Cyber Security - Ukraine Grid Hack Is Wake-up Call for Network Operators [News Briefing]." Engineering & Technology 11 (2016): 12-13. Print.
Reitinge, Philip. "Enabling Distributed Security in Cyberspace —Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action." Ed. Deputy Under Secretary for the National Protection and Programs Directorate (NPPD), U.S. Department of Homeland Security: U.S. Department of Homeland Security, 2011. 29. Print.
Ribeiro, Anna. "Hackers See Big Bucks in Ot Infrastructure, Cloud Adoption Picks Up." Industrial Cyber (2021). Print.
---. "Hackers See Big Bucks in Ot Infrastructure, Cloud Adoption Picks Up." Industrial Cyber (2021). Print.
Rich Scalco, Dr. Bill Waugaman, Jorge Lacoste, John Andrews, Bill Beary, Ross Roley, . "More Situational Awareness for Industrial Control Systems (Mosaics) Joint Capability Technology Demonstration (Jctd)." Johns Hopkins University Applied Physics Laboratory (JHU APL) 2018. Web. October 2019 2019.
Rick Hefner, Ph.D. "“Resiliency in Systems Engineering”." Prepared for C-NO INCOSE Chapter –18 August 2020: California Institute of Technology Center for Technology and Management Education, 2020. 17. Print.
Mosaics Jctd Operations Manager. MOSAICS JCTD Industry Day #3. 2021. Print.
Sabillon, Regner. "Audits in Cybersecurity." Research Anthology on Business Aspects of Cybersecurity: IGI Global, 2022. 1-18. Print.
Scalco, Aleksandra. "Cyber-Physical System (Cps) and Control System (Cs) Architecture for Cyber Defensive Capability — Mosaics." Using Model-Based Systems Engineering

(MBSE) and Model-Based System Architecture Process (MBSAP) Methodology. Colorado State University Systems Engineering Architecture, SYSE 567: Colorado State University, 2020. Print.

---. "Cyber-Physical System/Control System Workforce Survey." GradShow 2020: Colorado State University (CSU), 2020. Print.

---. "Months to Minutes - Command and Control (C2) of Control Systems." Ed. Simske, Steve. INCOSE Chesapeake Chapter: INCOSE, 2022. Print.

---. "Months to Minutes: Command and Control (C2) of Cyber Physical Systems (Cps)/Control Systems (Cs)." Colorado State University, 2021. Print.

The Case for Control Systems Cybersecurity Capability. MOSAICS Industry Day #3/TechConnect. October 19, 2021 2021. MOSAICS JCTD. Print.

Scalco, Aleksandra, and Steve Simske. "Cybersecurity Awareness for Systems Engineers Graduate Coursework." Cybersecurity Awareness for Systems Engineers: Colorado State University, 2020. Print.

---. "Digital Transformation of Cyber-Physical Systems and Control Systems." Journal of the Homeland Defense & Security Information Analysis Center (HDIAC) Vol. I and II (2021). Print.

---. "Engineering and Development of a Critical Infrastructure Cyber Defense Capability for Highly Context-Sensitive Dynamic Classes — Part 1, Engineering." Journal of the Homeland Defense & Security Information Analysis Center (HDIAC) (2020). Print.

---. "Engineering and Development of a Critical Infrastructure Cyber Defense Capability for Highly Context-Sensitive Dynamic Classes — Part 2, Development." Journal of the Homeland Defense & Security Information Analysis Center (HDIAC) (2020). Print.

---. "Model for Multi-Concern Assurance in the Digital Transformation of Engineering of Critical Infrastructure Control Systems." (2021). Print.

Scalco, Aleksandra, and Steven J. Simske. "Cyber-Physical Systems/Control System (Cps/Cs) Workforce Questionnaire." Protocol Number 20-102009H. Colorado State University (CSU) Institutional Review Board (IRB)2019. Print.

Schwab, Wolfgang, and Mathieu Poujol. "The State of Industrial Cybersecurity 2018." Ed. Lab, Kaspersky. Munich, Germany: CXP Group, 2018. 33. Print.

Simske, Steven J. "Cybersecurity Lectures." SYSE 569 Course. Fort Collins, Colorado, USA: Colorado State University, 2020. Print.

Snowden, David J., and Mary E. Boone. "A Leader's Framework for Decision Making." Harvard Business Review 1999. Web. November 20, 2021 2021.

Span, Martin "Trae", Logan O. Mailloux, and Michael R. Grimaila. "Cybersecurity Architectural Analysis for Complex Cyber-Physical Systems." The Cyber Defense Review 3.2 (2018). Print.

Developmental and Operational Independent Testing. MOSAICS Industry Day #3/TechConnect. October 19, 2021 2021. MOSAICS JCTD, 2021. Print.

Statistica. "Revenue of the Electric Power Industry in the United States from 1970 to 2019." Revenue of the electric power industry in the United States. Statistica 2021. Web. July 21, 2021 2021.

Stouffer, Keith, et al. "Nist Special Publication 800-82 Revision 2: Guide to Industrial Control Systems (Ics) Security." Ed. Commerce, Department of. Gaithersburg, MD 20899-8930: National Institute of Standards and Technology (NIST), 2015. Print.

Sun-Tzu, and Samuel B. Griffith. The Art of War. Oxford: Clarendon Press, 1964. Print.

Tasheva, Iva. "Cybersecurity Post-Covid-19: Lessons Learned and Policy Recommendations." European View (2021). Print.

Technology, Water. "Grand Ethiopian Renaissance Dam Project, Benishangul-Gumuz." Water Technology. 2021. Web. July 21, 2021 2021.

Terry Merz, Corey Fallon, Aleksandra Scalco. "A Context-Centred Research Approach to Phishing and Operational Technology in Industrial Control Systems." The Journal of Information Warfare (2019). Print.

Turton, William, and Kartikay Mehrotra. "Hackers Breached Colonial Pipeline Using Compromised Password." Bloomberg (2021). Print.

Tzipora Halevi, Nasir Memon, James Lewis, Ponnurangam Kumaraguru, Sumit Arora, Nikita Dagar, Fadi Aloul, Jay Chen. "Cultural and Psychological Factors in Cyber-Security." iiWAS '16: Proceedings of the 18th International Conference on Information Integration and Web-based Applications and Services (2106): 318-24. Print.

A Cybersecurity Culture Research Philosophy and Approach to Develop a Valid and Reliable Measuring Instrument. SAI Computing Conference. July 13-15, 2016 2016. Print.

More Situational Awareness for Industrial Control Systems (Mosaics) Requirements. MOSAICS Inudstry Day #3/TechConnect. October 19, 2021 2021. MOSAICS JCTD. Print.

WaterISAC. "Waterisac." https://www.waterisac.org/about-us: WaterISAC, 2022. Print.

Weiss, Joseph, Rob Stephens, and Nadine Miller. "Control System Cyber Incidents Are Real—and Current Prevention and Mitigation Strategies Are Not Working." Computer 55 (2022): 128-37. Print.

White, Gregory B., and Natalie Sjelin. "The Nist Cybersecurity Framework." Research Anthology on Business Aspects of Cybersecurity: IGI Global, 2022. Print.

WOLFF, ERIC. "Energy: Hoover Dam Could Stop Generating Electricity as Soon as 2013, Officials Fear." The San Diego Union-Tribune: The San Diego Union-Tribune, 2010. Print.

Yanjuan, Y. "Risk Is Uncertainty That Matters Interview with Dr. David Hillson." PM World Journal VIII.IX (2019). Print.

Zelalem, Zecharias. "An Egyptian Cyber Attack on Ethiopia by Hackers Is the Latest Strike over the Grand Dam." Quartz Africa (2020). Print.

Endnotes

[1] Any questions regarding Protocol Title "Cybersecurity Workforce Cyber-Physical Systems (CPS) Questionnaire," Protocol Number 20-10209H may be directed to the Research Director Steve Simske, steve.simske@colostate.edu or the Colorado State University IRB Office, RICRO_IRB@mail.Colostate.edu. The initial exempt determination was granted on July 8, 2020, to recruit adults with the approved recruitment and consent procedures. The research activity has been reviewed and determined to be minimal risk and meet exempt review by the Institutional Review Board under exempt category 2(i) of the 2018 Requirements. This study is not funded.

[2] The DoD defines the term "cybersecurity" as "The prevention of damage to, protection of, and restoration of electronic systems to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation," Department of Defense, "DoDI 8500.01 Cybersecurity," 2014.

[3] EU NIS2 is revised as the Directive on measures for a high standard level of cybersecurity across the Union, COM(2020) 823, https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union

[4] Gene Kranze was known for "The Kranz Dictum" after the Apollo 1 fire, which is that NASA Flight Control engineers are accountable and cannot take anything for granted. (Moon).