Championing Cultural Change and Control Systems Cyber Security

Aleksandra Scalco[1] and Steve Simske[2]
Colorado State University (CSU), Fort Collins, Colorado, 80523-1301, United States

Aspects of this work are being used in fulfillment of the requirements for a Systems Engineering Ph.D. at Colorado State University.

I. Abstract

The recent water infrastructure event in Florida is an example of how Information Technology (IT) and Operational Technology (OT) perspectives overlap in the cyber domain (Ref. [1]). IT and OT workforces approach challenges differently. IT manages data at rest or traversing networks. OT manages equipment and operations that control the physical world. Specific competency engineers may find early indicators helpful for design decisions or needed process changes. Cross-functional team connections make systems engineers sensitive to adverse conditions and valuable for forecasting indicators and championing such change. An example of a control system cyber domain capability on the horizon that blends approaches is the Department of Defense (DOD) More Situational Awareness for Industrial Control Systems (MOSIACS). This paper examines the significant cultural adjustment needed to operationalize MOSAICS and the systems engineering role in championing change.

II. Introduction

On February 5, 2021, someone tried to poison the water supply of the city of Oldsmar, Florida, by a cyberattack (Ref. [2]). By chance, a facility supervisor saw the pointer of the hacker's movements across the screen in an attempt to make unauthorized changes to settings. The supervisor then prevented an unwarranted and illicit increase in the amount of sodium hydroxide ("lye") used in the water treatment process that would have made 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 took action. However, serendipity is not security.

Further examination is needed to assess others' preparedness given a similar situation, but in this case, it appears serendipity was indeed in play. This event highlights the value of facility workforce training to ensure physical systems' safety and mission assurance. Between Tampa and Clearwater is the city of Oldsmar. Oldsmar is similar to many small towns and cities throughout the United States. The city has a population of slightly more than 15,000 residents (Ref. [3]). 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 as a way of thinking 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 disinfectant such as lye – that may have been used to kill disease-causing agents – before piping to consumers. Making water safe to drink is generally similar in U.S. municipalities, and drinking 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 in the cyber domain to affect operations. 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 "C.I.A."). The Oldsmar cyber-attack on February 5 demonstrated the varying perspectives of

[1] Engineer, Department of Navy (DON); Systems Engineering Ph.D. Student, Systems Engineering Department. In partial fulfillment of the requirements for a Systems Engineering Ph.D. at Colorado State University (CSU).
[2] Faculty, Systems Engineering Department.

the IT and OT personnel. The facility supervisor's observations and actions, fortunately, averted the attack. 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.

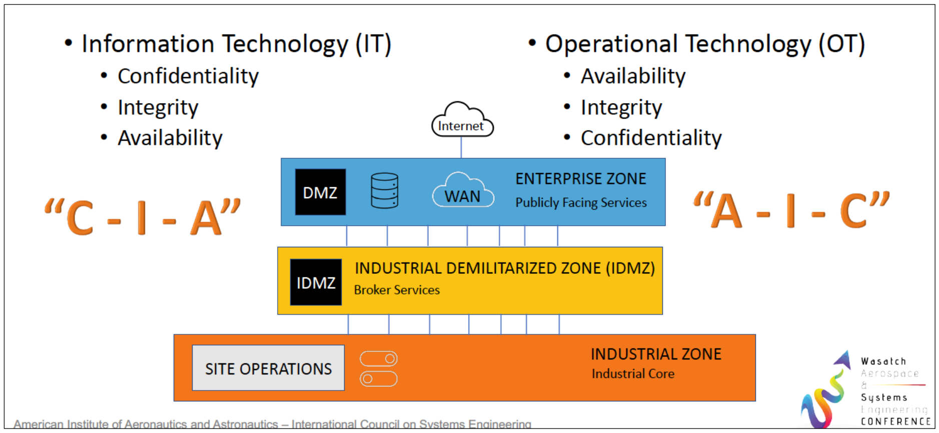
The integration of IT capabilities into traditional OT environments in recent years has yielded extraordinary new direct monitoring and control capabilities of physical devices and processes at the smallest component level. Component equipment levels such as Programmable Logic Controllers (PLC) are used to interface air traffic controllers with maintenance operation computers and automated monitoring and control of airfield lighting equipment. Control systems are designed to control physical world processes. Control systems are purpose-built for planned lifecycles of thirty years or more with minimum to zero downtime and a high degree of safety and near-real-time operational control. In recent decades, physical control systems were kept discretely separate from digital systems. The IT domain is traditionally the computer sciences domain, which focuses on software and software interfaces with hardware considered part of the cyber domain. Training is needed to make the IT more knowledgeable about the physical systems connected in the IT environment. Let us take, for example, computation and computer system-level programming. The field of computer engineering integrates computer science and electrical engineering. In computer system and hardware development, components such as circuit boards and software for an embedded system. Information systems engineering applies IT to solve enterprise problems; for example, an airport ticketing system.

Engineering solves technical problems using physics and mathematics principles for systems in the physical domain. Cybersecurity involves every aspect of integrating IT capabilities into these OT environments, including the spectrum of applications used, information accessed, networks used, operational processes practiced, encryption of data, access control, end-user training, and disaster recovery. Advanced capabilities such as programmable event and alarm filters to air traffic controllers and maintenance personnel interfaces IT with OT physical systems, allowing engineers and personnel to monitor and make desirable system changes from remote locations. The design of aerospace solutions also has different contextual considerations varied by the type of physical control systems. As demonstrated in Oldsmar, cyber vulnerabilities introduced by IT capabilities can impact equipment and operations that control the physical world. Engineers have new, evolving threats to consider in system requirements to meet safety expectations that require cultural change.

III. Professional Cultural Change

It is challenging to measure the prevention of attacks, as many are unreported. Training is demonstrated to reduce the cost of an incident and speed of recovery from a breach. Accenture asserts the value of improved cybersecurity performance of a non-leader worker to that of a leader could reduce an incident's cost by as much as 72 percent (Ref. [4]). "The speed with which organizations find security breaches is faster for those who provide higher levels of training. The best at training found 52 percent of security breaches in less than 24 hours, compared with only 32 percent for the rest" (Ref. [5]). The workforce approach challenges differ based on the field, sector, education, and experience of the personnel involved. Professionals will judge what is considered good or bad in systems design just as internalized evaluations are made about work based on work orientations (Ref. [6]). Professional cultural differentiation can create uncertainty in design decisions or process changes in areas outside traditional competencies. For example, an aerospace engineering team may be highly sensitive to aircraft or spacecraft products' safety requirements, and a computer science team may be highly sensitive to operating system requirements. The intersections between these fields are narrowing. Traditional IT personnel focus on confidentiality, integrity, and data availability, known as the principle of "C.I.A." Traditional OT personnel focus on availability first, as well as integrity and confidentiality.

The emphasis on availability first is reversed from the IT perspective, as shown in Fig. 1 Information Technology (IT) and Operational Technology (OT) perspectives). The IT perspective traditionally is centered around the higher levels in an architectural stack known as the "Enterprise Zone." The Enterprise Zone is where the business processes enabled by IT take place. This zone is where the internet broadly connects public-facing services. Broker services reside in the Industrial Demilitarized Zone (IDMZ). This zone is where IT provides tools that enable the workforce to transform products and services from multiple sources. Examples of devices found in this zone are solution integrations that support an airport operational database, such as baggage processing information using International Air Transport Association (IATA) Passenger and Airport Data Interchange Standards (PADIS) and Aviation Information Data Exchange (IDX) (Ref. [7]).



- Information Technology (IT)
  - Confidentiality
  - Integrity
  - Availability
- Operational Technology (OT)
  - Availability
  - Integrity
  - Confidentiality

American Institute of Aeronautics and Astronautics – International Council on Systems Engineering

Fig. 1 Information Technology (IT) and Operational Technology (OT) Perspectives.

The systems engineer may be a valuable champion for the cultural change needed. The systems engineering role differs from the IT and functional engineering role because of the numerous interdisciplinary connections made as part of a major system development project. The systems engineer deals with systems problems addressed by the amalgamated knowledge of engineers and specialists' technical expertise from varying disciplines and cross-functional teams that include physical and cyber domain Subject Matter Experts (SMEs). Systems engineering can help tie the technologies and training to the business cost. As a point of reference, the global average cost of a data breach in 2020 is $3.86 million (Ref. [8]). The cost varies by sector, with the average data breach cost in the transportation sector of $2.9 million (Ref. [9]). Each data breach represents an opportunity and investment loss for the entity attacked. The systems engineering interdisciplinary connection to the computer science and engineering competencies and business enterprise goals and objectives suits the systems engineering usefulness for forecasting indicators and championing change.

IV. Adverse Cyber Security Conditions

The Oldsmar water treatment facility event is an example of adverse cybersecurity conditions in physical systems and control systems. A facility supervisor knowing the physical system and possessing cybersecurity awareness averted disaster. A subsequent Joint Cybersecurity Advisory about the Oldsmar water treatment compromise, co-authored by the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA), the Department of Justice (DOJ) Federal Bureau of Investigation (FBI), the Environmental Protection Agency (EPA) and multi-state Information Sharing and Analysis Center (ISACs), reported the cyber actors likely exploited fundamental cybersecurity weaknesses in the water treatment facility. Water treatment facilities have systems with long lifecycles of thirty years or more, much longer than the lifecycle of IT components and systems. Therefore, it is not surprising that the computer networks hosting Windows 7 Operating Systems (OS) with end-of-life status were exploited to gain access. Outdated OS versions such as Windows 7 are susceptible to exploitation as security updates for the end-of-life OS are no longer supported to defend against emerging vulnerabilities. A question an organization might ask is whether outdated operating systems are used in their operations.

Physical security measures such as installing independent cyber-physical safety systems with limited cybersecurity capability add safety protection to limit the damage. Limiting who can release caustic chemicals and limiting the amounts that somebody can be released is a safety control—another important cyber hygiene mitigation security of remote access control to the system. Remote party access is routinely used as a tool for legitimate remote control of computer systems. The remote capability can also allow unauthorized entities to gain access to control systems. General mitigation recommendations published in the water treatment facility advisory shown in Table 1 Mitigation Recommendations would apply to any cyber-physical system to mitigate those risks (Ref. [10]). In this case, dual-factor authentication would have prevented the attack, as well.

DHS CISA Cyber Hygiene Mitigation Recommendations
Use multiple-factor authentication.
Use strong passwords to protect Remote Desktop Protocol (RDP) credentials.
Ensure anti-virus, spam filters, and firewalls are up to date, properly configured, and secure.
Audit network configurations and isolate computer systems that cannot be updated.
Audit networks for systems using RDP, close unused RDP ports, apply multiple-factor authentication, log RDP attempts.
Audit logs for all remote connection protocols.
Train users to identify and report attempts at social engineering.
Identify and suspend access of users exhibiting unusual activity.

Table 1 Cyber Hygiene Mitigation Recommendations (Ref. [11]).

Threat actors may be either internal or external threat sources using either physical or electronic pathways. Three potential threat actors to the physical system are an internal, disgruntled employee, a third-party external contractor, or even potentially a nation-state threat actor with the security cost increasingly high. A disgruntled employee, depending on the organizational role, may know sensitive details about the facility. Their motivation may be malicious damage or brief attention. Violent radicals may have the skills and capabilities to shut down operations. They may use assistance from facility employees to gain insider information to penetrate a sabotage attack. High on the threat list for critical infrastructure is a terrorist. Terrorists may have detailed knowledge of how to launch a cyber-attack on a control system and may be motivated and willing to cause equipment damage and even loss of life. Identifying potential vulnerabilities if threats are not mitigated is an activity for the systems engineer. Possible attack access points exist throughout a facility that requires mitigation. Potential vulnerabilities include remote access to external endpoints (e.g., laptops) using unsecured data links or unauthorized access to physical assets such as a computer workstation in a sensitive area that an attacker can compromise.

Authentication confirms the user's identity is ("Are you whom you claim to be?"). Authorization is the administration of permissions, meaning that the user has permission to access the system and what actions the user has permissions to perform. For example, a user's Authentication may confirm the user's identity attempting to access a logical area. However, the user may or may not have permission or authorization to access the logical area or may or may not have permission to perform certain functions in the system. User authentication requires strong passwords, the expectation of password protection (i.e., not posted on a device), re-authentication for sensitive systems, and role separation for system access (i.e., facility worker designated by role rather than individual access authorization based on person). Certificate management is a method to ensure unauthorized actors are denied access to facility networks by cyber access. Digital certificates are used to identify and control who can access and operate a facility network to achieve safety and mission assurance. People and devices connecting to a network are identified and authenticated using a private key, identity, and a public key. A certificate signed request is made to a certificate authority, and a digital certificate is issued verifying the person and the device. This method is used for Wireless Access Points (WAP), restricting access to external devices and who can access a facility's devices. In the example of Oldsmar, the WAP would have been restricted by certificate management. An unauthorized person would not be given access to any network devices, thereby protecting the system from unauthorized attempts to change settings. Network security of a physical system is about restricting access to logical areas of the system using enclave security zone, applying firewall rules, access control lists, and using Intrusion Detection Systems (IDS) to segment or micro-segment sensitive information and process zones that require monitoring and protection from less secure zones (Ref. [12]).

Insider threats also pose a significant threat. The weakest link in the system continues to be people charged with operating a system. Insiders include employees, third-party vendors, visitors, and trusted third parties. Security awareness is an essential component of mitigating the risk of insider threat. From an internal perspective, threat sources can be either accidental or intentional and may be perpetrated by employees or third-party contractors. A former internal threat source may become an external threat source capable of targeting the organization with specific system knowledge. "The single greatest vulnerability is people (untrained, unmotivated, or malicious insiders)" (Ref. [13]). Network administrators tend to use weak password settings and fail to install patches in time, creating system security vulnerabilities. This lack of security tendencies may be addressed by training security staffers, which is different from an underpaid security staffer's threat surface. The potential that the perceived underpayment might lead to the security staffer being "unmotivated" or becoming an active insider threat (i.e., purposely share information with unauthorized individuals or intentionally cause other damages). Either of these presents exploitable weaknesses that need to be addressed as part of the overall risk management plan to safeguard assets. Insider threat mitigation foremost requires a threat-aware culture. Expectations regarding security need to be established and well-understood by employees. A risk-informed, insider threat program should include consistent security awareness training, current threat-based vulnerability risk assessments, and risk scoring and prioritization. Such a program requires senior leadership acknowledgment of the importance of detecting and preventing insider threats. Technical solutions and processes should also be employed to detect unauthorized activities (Ref. [14]).

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. People are vulnerable to the use of social Internet activity. 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. Data and information may be exploited via overzealous social internet activity to obtain information that can be used in passwords or as answers to secret questions used to reset some accounts or use the information to escalate password privileges. User information and details can give sensitive information about a user that provides an attacker with access to other organizational accounts using similar data. By opening attachments sent via social media, malware is unleashed in the computer and into systems. Employees can also make accidents and inadvertent errors. It can be challenging to distinguish accidental cyber errors from an authentic, external attack, and unintentional mistakes can be equally destructive. Regular insider threat awareness training and realistic Table-Top Exercise (TTX) help raise awareness of technical and behavioral indicators. Frequent training is needed to familiarize employees with security policies and procedures and emergency response. Clear guidelines need to be established for reporting suspicious behavior to supervisors and security personnel. Finally, there needs to be an expectation, open communication culture for communicating observable indicators without negative reflection on the person reporting. An organization may also employ dual-factor authentication, which combines different identification factors (i.e., something known, such as a password, and something in possession, such as a token, mobile phone, a key fob). The advantages are unique identification, copy prevention, and tamper evidence. The use of dual-factor or Multi-factor Authentication can track user logs to gain analysis data that notifies anomalous behaviors or when an unknown or risky device is used. The overall organizational policy and objectives are to protect sensitive information and processes. Formally documented management expectations are written as the policy used to direct decisions and ensure consistent activities.

The Governance Board must be knowledgeable of cybersecurity risk, asset valuation in quantitative (e.g., cost) and qualitative (i.e., relative importance) values to assess the consequence of loss of operation or disruption to function due to a cyber event. A Governance strategy is to implement a high-level risk management approach to cybersecurity integrated with the organizational strategy supported by the highest level of senior engagement and thought the organization. The plan is to promote a cybersecurity culture among all employees, identify and protect sensitive data and processes by the implementation of appropriate security safeguards, develop and implement strategies by use of detection technologies to identify malicious or unintentional events impacting operations and respond and recover by encouraging the timely and effective action to mitigate incidents and execute plans for resilience. Cybersecurity governance encompasses all information systems Governance includes cybersecurity policies and strategies that are reviewed, at minimum, on an annual basis. On a bi-annual basis, the Governance Board performs a strategic deep dive of a current IT enterprise assessment, business requirements, and technology outlook. The strategy includes perimeter defense to protect against the introduction of malicious and unauthorized access using technology and perimeter management. Critical information is protected regardless of location using encryption and access control methods. Governance capabilities to detect and respond are shaped by business and mission processes accompanied by a resilient architecture to limit potential exfiltration of data, restrict unauthorized access, operate through degraded mode, and recover from interruption of operations (e.g., attack). This Governance strategy is maintained continuously, shaping all aspects of organizational technology, operations, and personnel resources. The assessment outcome is the roadmaps and finance/budget, and review of Governance and decision-making of policies and investments. The Chief Security Officer conducts regular weekly, monthly reviews (SCO) and Chief Information Officer (CIO), including program managers, system designers, and others as required (Ref. [15]).

Governance functions direct, monitor, evaluate, and communicate. Organizational roles and responsibilities include the Chief Information Officer (CIO), responsible for establishing and maintaining the security program, creating plans and requirements, and managing the security implementation and assessment. IT strategy, information system, risk management and oversight responsibilities (e.g., IT strategy, computer network, 3rd party systems) also typically falls under the CIO; the Chief Executive Officer (CEO) who is responsible for the entire operation, and organizational support; the Chief Security Officer (CSO) who is responsible for physical security; the Chief Information Security Officer (CISO) who is responsible for digital security; additionally, the cybersecurity governance strategy is to identify roles, responsibilities and access authority for anyone with information system access part of effective cybersecurity enterprise planning, including program managers, system designers and developers, information security engineers, system integrators; mission/business owners, information system owners, typical control providers, information owners/stewards, system administrators, system security officers who have information security implementation and operational responsibilities; and auditors, system evaluators, assessors, independent verifiers/ validators, analysts, information system owners who have information security and assessment and monitoring responsibilities. Cybersecurity governance strategy is not a one and done, nor only the responsibility of the IT department. The governance strategy includes all staff levels in accountability down to the account-level managers responsible for specifying authorized users of the information system, group and role membership, and access authorizations. Administrative governance activities include: 1) Ensure cybersecurity governance is part of and entirely consistent with broader organizational Governance — establish and control user access privileges 2) Apply secure processes for procurement and contracting, especially when non-employees have access to sensitive resources 3) Implement personnel practices, including hiring, discipline, training, and monitoring to minimize insider threat risks 4) Develop and periodically review security plans and procedures — perform regular cybersecurity status reporting and issue escalation to higher management (Ref. [16]).

Protecting global aviation systems from a growing cybersecurity threat to safety and aviation security was identified in a 2013 AIAA Decision Paper, "The Connectivity Challenge: Protecting Critical Assets in a Networked World: A Framework for Aviation Cybersecurity," and a framework was proposed to address cybersecurity for aviation. The framework included recommendations for the aviation community that are valid and relevant today (Ref. [17]). Still, relevant today is the need to establish common cyber standards for aviation systems. The need to develop a cybersecurity culture among aviation workforce personnel. The need to understand the threat and risk vectors, including identifying the elements that need protection in an aviation system. Other recommendations made were the need for shared situational awareness to communicate threats and incident response capability. Engineering recommendations included the desire for cybersecurity design principles that consider evolving cyber domain threats and research and development focused on secure and resilient system architectures. The operational tenets' recommendations focused on strong cyberculture for systems deployed in the field, operational standards and best practices that mitigate threats, and a unified government and industry cyber partnership (Ref. [18]). The American Institute of Aeronautics and Astronautics (AIAA) continues to develop content and events to drive cybersecurity integration into aerospace practice on par with safety and mission assurance (Ref. [19]). The breadth of new direct monitoring and control capabilities of the physical world requires professional cultural change by the workforce as outlined in the AIAA 2013 decision paper. Aircraft manufacturing, air traffic control, and airport infrastructure modernization offer opportunities to integrate new direct monitoring and control capabilities into physical systems and processes at the smallest component level. The modernizing of infrastructure also offers the opportunity to invest and improve cybersecurity with technologies that bring new capabilities. However, significant cultural adjustment is needed to ensure that these new capabilities are protected from exploiting added safety and mission assurance vulnerabilities. An example of a control system cyber domain capability on the horizon that blends approaches is the Department of Defense (DOD) Joint Capability Technology Demonstration (JCTD) More Situational Awareness for Industrial Control Systems (MOSIACS).

V. Forecasting Indicators

Security technologies such as Security, Orchestration, Automation and Response (SOAR), Artificial Intelligence (AI), Next-generation Firewalls can have a significant impact on the ability to detect and defend against an attack (Ref. [20]). MOSAICS is an example of a control system domain capability that connects IT and OT perspectives to achieve cybersecurity that incorporates SOAR technology. The objective of the MOSAICS JCTD is to automate detection, mitigation, and recovery procedures to defend mission-critical infrastructures such as power, water, or Heating, Ventilation, and Air Conditioning (HVAC) from cyber threats and attacks (Ref. [21]). MOSAICS presents a significant capability as the World Economic Forum 2020 report states that cyberattacks on critical national infrastructure are ranked as the fifth top risk by experts across sectors, including transportation (Ref. [22]). Additionally, the MOSAICS capability introduces analytics, visualization, decision support, and information sharing commercial technologies. The ability to detect changes to a control system requires a system to demonstrate the capability to baseline a physical system to the lowest level of products and services below basic digital components using Internet Protocol (IP) in the network architecture. The baseline includes the PLCs and Remote Terminal Units (RTUs) and field devices such as switches, valves, and actuators. A goal of the JCTD is to transition the capability to the commercial sector for further development and commercialization. The commercial demand signal indicates that MOSAICS capabilities would be incredibly beneficial to component and solution providers in the supply chain for all critical infrastructure sectors (e.g., water, power utility, aeronautics, and aerospace). The operational need for the capability to defend physical systems from cyber-introduced vulnerability echoed by the North American Electric Reliability Organization (NERC) 's GridEx Exercises, the Army Cyber Institute (ACI) 's Jack Voltaic Table-Top Exercises (TTX), DOD initiatives led by the Under Secretary of Defense for Acquisition and Sustainment, U.S. Strategic Command, and the services (i.e., U.S. Navy Task Force Cyber Awakening, U.S. Air Force Task Force Cyber Secure), and National Defense Authorization Acts (NDAA). Understanding how commercial and national-level efforts and cyber research projects, and NDAA relationships may influence cybersecurity decisions in respective project areas can be overwhelming to professionals working in specific functional areas trying to make sense of the many change influencers. NDAAs exemplify government expectations and commitments through U.S. Policies. The consensus is that the integration of the IT and OT workforce is transformational.

Another forecast indicator of change is in the emerging policy. HR 1833 "DHS Industrial Control Systems Capabilities Enhancement Act of 2021 introduced to the 117th Congress in February 2021 would give greater authority to CISA to defend critical systems against cyber-attack (Ref. [23]). If passed, the CISA director will be responsible for maintaining capabilities to identify and address threats and vulnerabilities related to the automated control of critical infrastructure processes, including cybersecurity threats to Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition Systems (SCADA). ICS and SCADA are also found in aircraft manufacturing, air traffic control, and airport infrastructure. If passed, the capability to coordinate across industry sectors, manufacturers, and other stakeholders will significantly impact the industry and workforce and be a significant cultural change driver.

VI. Workforce Enhancement

As adversaries target critical infrastructure (such as power, fuel, water, and facilities) using automated, cyber-attack methods, organizations will look for advanced technology defense capabilities to help cyber defenders and control system engineers identify, respond to, and recover from asymmetric attacks in mission-relevant time on critical infrastructure (Ref. [24]). These technology-based solutions will change and challenge organizations and personnel to maintain safety and mission assurance requirements while developing and maturing new knowledge, skills, and abilities (KSAs). Lack of understanding of these new work roles to support workforce enhancement. The Colorado State University (CSU) Department of Systems Engineering (SYSE) is leading research to understand the workforce better. A questionnaire was used to collect data from 181 participants about Cyber-physical Systems (CPS)/Control Systems (CS) from August 2020 – February 2021. Participants responded to 203 questions about network systems, infrastructure, incident response, Red Teams, resources, training and certifications, cybersecurity principles, and their KSAs on control systems. The authors will submit the analysis to the INCOSE for consideration of publication for the 32nd Annual INCOSE International Symposium (IS).

In earlier research, AIAA surveyed members and published a Cyber Security Market Study report in 2020. The study results reported a strong demand to increase cybersecurity awareness, the need for cybersecurity inclusion in supply chain management, development, engineering, production, and a cybersecurity curriculum needed for students and professionals. The AIAA report closely aligns with recommendations by CISA and those found by the authors in their research.

Credentialing of workforce professionals is a way that organizations can bridge the OT and IT workforce capabilities. Credentialing of Industrial Control System (ICS) security professionals includes certifications offered by Global Information Assurance Certification (GIAC), Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), Industrial Control System Information Sharing and Analysis Center (ICS-ISAC), the International Society of Automation (ISA), the National Institute of Standard and Technology (NIST), SANS Institute and others. OT workforce may be interested in similar credentialing as the IT workforce. The following are some certifications to consider: International Information Systems Security Certification Consortium, Inc. (ICS)^2 Certified Information Systems Security Professional (CISSP), Information Systems Security Engineering Professional (CISSP-ISSEP) and Information Systems Security Architecture Professional (CISSP-ISSAP); International Council of Electronic Commerce Consultants (EC-Council) Certified Chief Information Security Officer (CCISO); ISACA Certified Information Security Manager (CISM); and the Computing Technology Industry Association (CompTIA) Advanced Security Practitioner (CASP+). The Cybersecurity and Infrastructures Security Agency (CISA) offers virtual learning free of cost as well as regional instructor-led training courses at no cost to organizations or attendees about cybersecurity for Industrial Control Systems (ICS) (Ref. [25]). The average course runs about two hours. Courses include ICS for managers and determining critical risk in ICS. The link to the CISA training is https://ics-training.inl.gov/learn (Ref. [26]).

VII. Conclusion

The Oldsmar averted cyber event demonstrates the need for organizational and workforce cultural change as physical systems become more integrated with the cyber domain to recognize and prevent malicious intrusion and effect. Government and industry partnership is advancing policy and practices for shared situational awareness and raised collective defense. Efforts by organizations such as AIAA and INCOSE are major drivers leading the cultural change. Efforts to better understand the workforce, such as the Colorado State research, will inform organizations and agencies on where there may be uncertainty or risk exposure.

The key points are:

- Systems engineers are helpful for forecasting indicators and championing cultural change.
- Safe and secure cyber systems require regular updates and improvements.
- Technology-based solutions alone will not "fix" challenges.
- Cyber threats and cybersecurity solutions will change and challenge organizations.
- Workforce cultural changes are required:
    - Credentialing CISA free training is available at https://ics-training.inl.gov/learn (Ref. [27])
    - Designing and engineering systems
    - Handling or processing information, using networks, or interacting with cyber-connected systems by personnel
    - Changing degree, experience, and work-based learning requirements
    - Looking for a new generation of systems and cybersecurity thinkers.

Appendix

Authors thank the American Institute of Aeronautics and Astronautics (AIAA) for developing content and events to drive the integration of cybersecurity into aerospace practice and for leading cybersecurity market studies to measure the knowledge and interest about cybersecurity in the community.

References

[1] Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency (CISA), "Joint Cybersecurity Advisory: Compromise of U.S. Water Treatment Facility," 2021. URL: https://us-cert.cisa.gov/ncas/alerts/aa21-042a [retrieved March 2021].

[2] Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency (CISA), "Joint Cybersecurity Advisory: Compromise of U.S. Water Treatment Facility," 2021. URL: https://us-cert.cisa.gov/ncas/alerts/aa21-042a [retrieved March 2021].

[3] U.S. Census Bureau, 2021. URL: https://www.census.gov [retrieved March 2021].

[4] Accenture, "Innovate for Cyber Resilience: Lessons from Leaders to Master Cybersecurity Execution," Third Annual State of Cyber Resilience, 2020, pp. 34. URL: https://www.accenture.com/_acnmedia/PDF-116/Accenture-Cybersecurity-Report-2020.pdf [retrieved March 2021].

[5] Accenture, "Innovate for Cyber Resilience: Lessons from Leaders to Master Cybersecurity Execution," Third Annual State of Cyber Resilience, 20`20, pp. 34. URL: https://www.accenture.com/_acnmedia/PDF-116/Accenture-Cybersecurity-Report-2020.pdf [retrieved March 2021].

[6] Dik, Bryan J, Zinta S. Byrne, and Michael F. Steger. *Purpose and Meaning in the Workplace*, American Psychological Association, Washington, DC, 2013, pp. 175–177.

[7] International Air Transport Association (IATA), "Passenger and Airport Data Interchange Standards," 2015. URL: https://www.iata.org/contentassets/18a5fdb2dc144d619a8c10dc1472ae80/pnrgov20edifact20implementation20guide2015_1.pdf [retrieved March 2021].

[8] IBM, "2020 Cost of a Data Breach Report," 2020. URL: https://www.ibm.com/security/data-breach [retrieved March 2021].

[9] IBM, "2020 Cost of a Data Breach Report," 2020. URL: https://www.ibm.com/security/data-breach [retrieved March 2021].

[10] Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency (CISA), "Joint Cybersecurity Advisory: Compromise of U.S. Water Treatment Facility," 2021. URL: https://us-cert.cisa.gov/ncas/alerts/aa21-042a [retrieved March 2021].

[11] Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency (CISA), "Joint Cybersecurity Advisory: Compromise of U.S. Water Treatment Facility," 2021. URL: https://us-cert.cisa.gov/ncas/alerts/aa21-042a [retrieved March 2021].

[12] Scalco, A. "Cybersecurity Considerations for Systems Engineers of a Power Utility Information-enabled Enterprise Electrical Substation Automated System (SAS)," Paper, Colorado State University, July 2021.

[13] Simske, S. "Cybersecurity for Systems Engineers," Lectures, Colorado State University, 2020.

[14] Scalco, A. "Cybersecurity Considerations for Systems Engineers of a Power Utility Information-enabled Enterprise Electrical Substation Automated System (SAS)," Paper, Colorado State University, July 2021.

[15] Scalco, A. "Cybersecurity Considerations for Systems Engineers of a Power Utility Information-enabled Enterprise Electrical Substation Automated System (SAS)," Paper, Colorado State University, July 2021.

[16] Simske, S. "Cybersecurity for Systems Engineers," Lectures, Colorado State University, 2020.

[17] American Institute of Aeronautics and Astronautics (AIAA), "The Connectivity Challenge: Protecting Critical Assets in a Networked World: A Framework for Aviation Cybersecurity," AIAA, Decision Paper, August 2013. URL: https://www.aiaa.org/docs/default-source/uploadedfiles/issues-and-advocacy/aiaa-cyber-framework-final.pdf?sfvrsn=7bd09ec9_0 [retrieved March 2021].

[18] American Institute of Aeronautics and Astronautics (AIAA), "The Connectivity Challenge: Protecting Critical Assets in a Networked World: A Framework for Aviation Cybersecurity," AIAA, Decision Paper, August 2013. URL: https://www.aiaa.org/docs/default-source/uploadedfiles/issues-and-advocacy/aiaa-cyber-framework-final.pdf?sfvrsn=7bd09ec9_0 [retrieved March 2021].

[19] American Institute of Aeronautics and Astronautics (AIAA), "The Connectivity Challenge: Protecting Critical Assets in a Networked World: A Framework for Aviation Cybersecurity," AIAA, Decision Paper, August 2013. URL: https://www.aiaa.org/docs/default-source/uploadedfiles/issues-and-advocacy/aiaa-cyber-framework-final.pdf?sfvrsn=7bd09ec9_0 [retrieved March 2021].

[20] Accenture, "Innovate for Cyber Resilience: Lessons from Leaders to Master Cybersecurity Execution," Third Annual State of Cyber Resilience, 2020, pp. 34. URL: https://www.accenture.com/_acnmedia/PDF-116/Accenture-Cybersecurity-Report-2020.pdf [retrieved March 2021].

[21] Scalco, A., and Simske, S., "More Situational Awareness for Industrial Control Systems (MOSAICS): 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*, Vol. 7, No. 1, 2020, pp. 36–44. URL: https://www.hdiac.org/journal-article/more-situational-awareness-for-industrial-control-systems-mosaics-engineering-and-development-of-a-critical-infrastructure-cyber-defense-capability-for-highly-context-sensitive-dynamic-classes-par-2/ [retrieved March 2021].

[22] World Economic Forum, "The Global Risks Report 2020," 2020. URL: https://reports.weforum.org/global-risks-report-2020/ [retrieved March 2021].

[23] U.S. House, House Resolution 1833 (H.R. 1833) "DHS Industrial Control Systems Capabilities Enhancement Act of 2021," 2021. URL: https://www.congress.gov/bill/115th-congress/house-bill/5733 [retrieved March 2021].

[24] Scalco, A., Jayswal, M., and Simske, S., "More Situational Awareness for Industrial Control Systems (MOSAICS): A Concept Development for the Defense of Mission Critical Infrastructure," *Journal of the Homeland Defense & Security Information Analysis Center*, Volume 6, Number 4, February 14, 2020. URL: https://www.hdiac.org/journal-article/more-situational-awareness-for-industrial-control-systems-mosaics-joint-capability-technology-demonstration-jctd-a-concept-development-for-the-defense-of-mission-critical-infrastructure/ [retrieved March 2021].

[25] Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency (CISA), "Joint Cybersecurity Advisory: Compromise of U.S. Water Treatment Facility," 2021. URL: https://us-cert.cisa.gov/ncas/alerts/aa21-042a [retrieved March 2021].

[26] Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency (CISA), "Joint Cybersecurity Advisory: Compromise of U.S. Water Treatment Facility," 2021. URL: https://us-cert.cisa.gov/ncas/alerts/aa21-042a [retrieved March 2021].

[27] Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency (CISA), "Joint Cybersecurity Advisory: Compromise of U.S. Water Treatment Facility," 2021. URL: https://us-cert.cisa.gov/ncas/alerts/aa21-042a [retrieved March 2021].