AIR WAR COLLEGE

AIR UNIVERSITY

BREAKING STOVEPIPES:

BRIDGING GAPS IN AIR FORCE INDUSTRIAL CONTROL SYSTEMS MANAGEMENT TO ENABLE MULTI-DOMAIN MISSION ASSURANCE

by

Patrick J. Obruba, Lt Col, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: William E. Young, Col, USAF

16 February 2016

DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government, the Department of Defense, or Air University. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Biography

Lieutenant Colonel Patrick J. Obruba is assigned to the Air War College, Air University, Maxwell AFB, AL. Prior to attending Air War College, Colonel Obruba was assigned as Acting, and later Deputy, Director of Operations, Air Force Civil Engineer Center, Tyndall AFB, FL where he oversaw the certification and accreditation of all 1,900 real property industrial control systems in the Air Force inventory. Among other assignments, he commanded the 92d Civil Engineer Squadron at Fairchild AFB, WA and served as an Air Force legislative fellow in Washington, DC.

Colonel Obruba was awarded a Master of Science degree in Engineering and Environmental Management from the Air Force Institute of Technology in 2001, a Bachelor of Science degree in Civil Engineering from the United States Air Force Academy in 1996, and a Certificate of Legislative Affairs from the Government Affairs Institute at Georgetown University in 2009.

Abstract

Air Force doctrine inadequately addresses Industrial Control Systems (ICS) security and as a result, the service is improperly organized and trained to secure missions across the domains of air, space, and cyberspace. In response, the Air Force must consider significant changes at the strategic, operational, and tactical levels to provide mission assurance to commanders.

An important question that the Chief of Staff's Task Force Cyber Secure (TFCS) asks is: How do we organize, train, and equip Air Force forces to support the five core missions, in and through cyber? By their nature, air, space, and cyber dominance are tied to physical platforms from which the Air Force projects power. Increasingly, the line between physical and cyber has blurred as ICS become a key factor in enabling mission assurance through the basing system. Functional "stovepipes," specifically those of civil engineer and cyber surety, have resulted in ICS vulnerabilities, threating mission assurance at every one of the service's installations.

While changes can be made to the way units analyze systems or task organize under a wing, none of that will be effective until Air Force doctrine, both civil engineer and cyber surety adequately recognizes the differences between cyberspace and the traditional physical domains of air and space. The TFCS infrastructure work group should prioritize revising both sets of doctrine to enable the force to view cyberspace for what it is, a digital battlefield that comes under fire every day, whether at home station or forward deployed. Without this revision, the limited mindset of Airmen in the field employing ICS enabled installations and the mission commanders they serve will never change.

Introduction

Sirens wail through the hot, tropical air as Airmen and machines roar from their camouflaged dispersal locations toward the expeditionary landing strip in the dark of night. The piercing screech is soon replaced by a cacophony of sounds: the loud boom of exploding sub-munitions, the metallic thud of jackhammers on concrete, and the decisive shouts of engineers calling out for repair materiel. A collective sense of urgency permeates the airfield. Suddenly, radios go silent, generators sputter, and lights flicker and fail. An in-bound F-35, returning from its first strike mission for a quick-turn, has to divert as the runway is not ready in time. One missed strike would not stall the operation; however, this same phenomenon has happened at every dispersed recovery field. It will be days before the AFFOR recognizes that it has been the victim of a targeted cyber-attack against its networked, Industrial Control Systems (ICS) for which it was not prepared.

An important question that the Chief of Staff's Task Force Cyber Secure (TFCS) asks is: How do we organize, train, and equip Air Force forces to support the five core missions, in and through cyber?[1] By their nature, air, space, and cyber dominance are tied to physical platforms from which the Air Force projects power. Increasingly, the line between physical and cyber has blurred as ICS become a key factor in enabling mission assurance through the basing system.[2] Functional "stovepipes," specifically those of civil engineer and cyber surety, have resulted in ICS vulnerabilities, threating mission assurance at every one of the service's installations.[3]

Thesis

Air Force doctrine inadequately addresses ICS security and as a result, the service is improperly organized and trained to secure missions across the domains of air, space, and cyberspace. In response, the Air Force must consider significant changes at the strategic (doctrine), operational (organization), and tactical (training) levels to provide mission assurance to commanders.

The purpose of this paper is to influence the Air Force Deputy Chief of Staff for Logistics, Engineering, and Force Protection and the Chief, Information Dominance and Chief Information Officer to direct doctrinal changes that will drive modifications to the organization

and training of civil engineer and cyber surety Airmen to better provide multi-domain mission assurance through securing ICS. First, the paper will suggest that the civil engineer and cyber surety views of ICS originate from fundamentally *divergent perspectives*, which in-turn, have led to the service unknowingly taking on infrastructure induced risk to mission accomplishment such as that illustrated by the opening vignette. The argument presented will offer that the root of this disconnect lies in doctrine. After framing the problem, the paper will recommend *convergent solutions* to align and alter the organization and training of civil engineer and cyber surety Airmen with the goal of closing the gap and subsequently, enhancing mission assurance. While the vignette offered provides a deployed example, the lessons are equally valid for home station or deployed-in-place missions.

Divergent Perspectives

For the purpose of this paper, ICS represent the intersection of two types of technology: one that controls operations in the physical realm and a second that controls the transfer of information. The National Institute of Standards and Technology (NIST) defines a security control as:

> A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.[4]

Disconnects between champions of Operational Technology (OT) and Information Technology (IT) resulting in insufficient mission assurance at the operational level are not unique to the Air Force. The following paragraphs will first define the two categories then suggest that the Air Force perspectives on each are rooted in the manner by which ICS and the Air Force Network (AFNET) independently developed. This independent development leads to competing priorities when the physical demands of ICS interact with the information-centric focus of cyberspace.

For the Air Force, ICS represents the intersection between the theoretical domain of cyberspace and the physical domains of air and space.

Technology: Operational versus Information

Generally speaking, OT controls are standardized actions, automation, or states of being designed to keep desired functions happening. IT controls originate from the opposite perspective—keeping undesired actions from happening. The Garnet IT Glossary and the National Information Assurance Glossary, respectively, provide solid working definitions to frame the discussion:

> Operational Technology: hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise[5]
>
> Information Technology: any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency.[6]

Note that OT focusses on control, "…of physical devices, processes and events…" while IT is primarily concerned with control, "…of data or information…" Michael Sing, in his blog post, "The Fusion of Two Cultures…Information and Operational Technology Convergence," describes the difference between OT and IT views of ICS, albeit in the context of the mining industry. Sing notes that, "The OT perspective concentrates on the plant, processes and equipment required to perform the actual mining and processing operations,"[7] in his words a "bottom-up" view. In contrast, he describes the IT perspective as a "top-down" approach that, "…focuses on the business, operations and enterprise information systems required to operate and support a mining business." While the systems theory approach that the paper will later

offer is not limited in direction, the bottom-up versus top-down perspective tendencies speak to the cultural disconnect in the Air Force ICS enterprise.

OT and IT, as independent systems, are built and contextualized from diametrically opposed directions. While both systems rely on the implementation of controls to bring order, the divergent perspectives of the builders result in controls that often end up with competing outcomes. These disjoint results offer a trade space where leaders must make risk avoidance decisions by satisfying one perspective at the expense of the other.

It is from these opposing perspectives that the controls applied by OT and IT professionals often fail to completely overlap in both form and function. Figure 1 is a graphical representation of the challenges the two perspectives impart on managing ICS. Section 1 represents the convergence of IT and OT controls. An example of compatible IT and OT controls would be a physical lock on the door of a server room (section 1) that would result in an overlapping functionality (section 2). From an OT perspective, a locked server room would prevent an unauthorized individual from altering the settings on an ICS control. From an IT perspective, the same lock would prevent someone from gaining unauthorized access to the network at large. Section 3 represents a case where an OT control creates degraded IT functionality. An example would be where an ICS continues to adequately operate with proprietary software in a computer language that is no longer supported, but that software has known IT vulnerabilities. Section 4 represents a case where an IT control creates a degraded OT functionality. An example would be where a downward mandated patch closes a port that connects the server to an HVAC system rendering it inoperable.

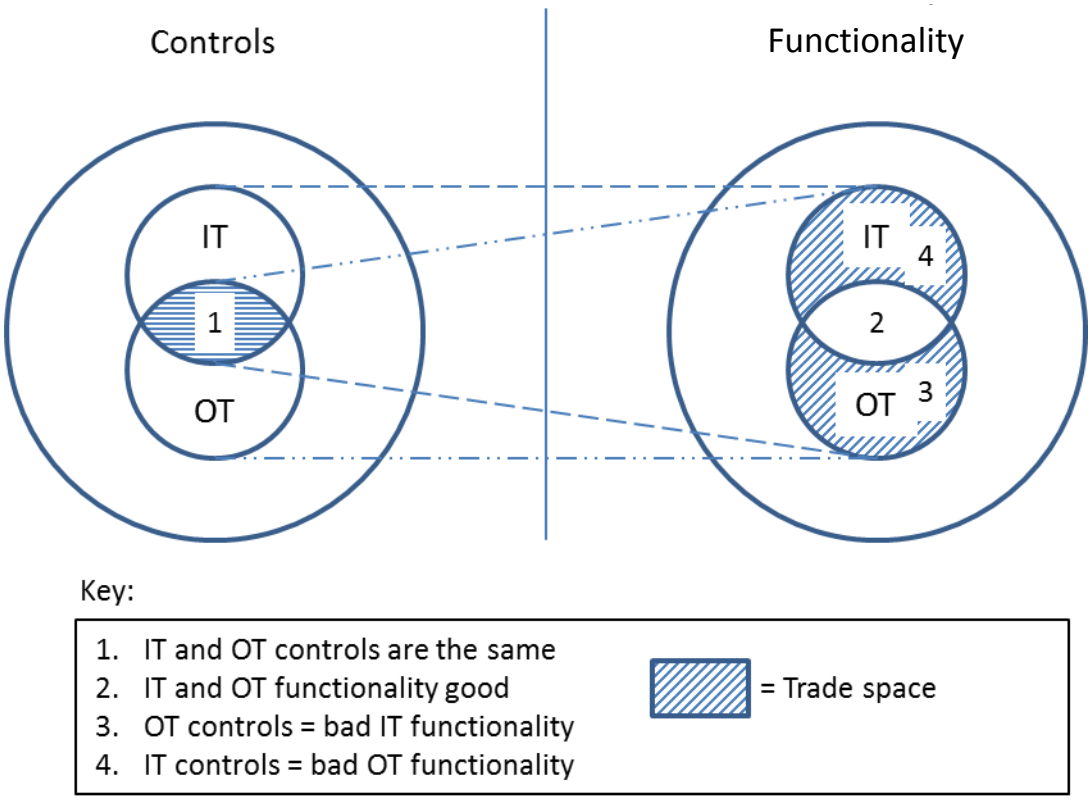

Figure 1. Interrelationship between Information Technology (IT) and Operational Technology (OT) controls and desired functionality

Civil Engineer Perspective

Air Force civil engineers, following an OT-focused view, have constructed and maintained ICS on a decentralized, process-based model (Figure 2). The result for the Service is an installation-by-installation, customized ICS limited only by the number of manufacturers of sub-systems and components and the ingenuity of local personnel. The following paragraphs will contextualize ICS from the perspective of Air Force civil engineers.

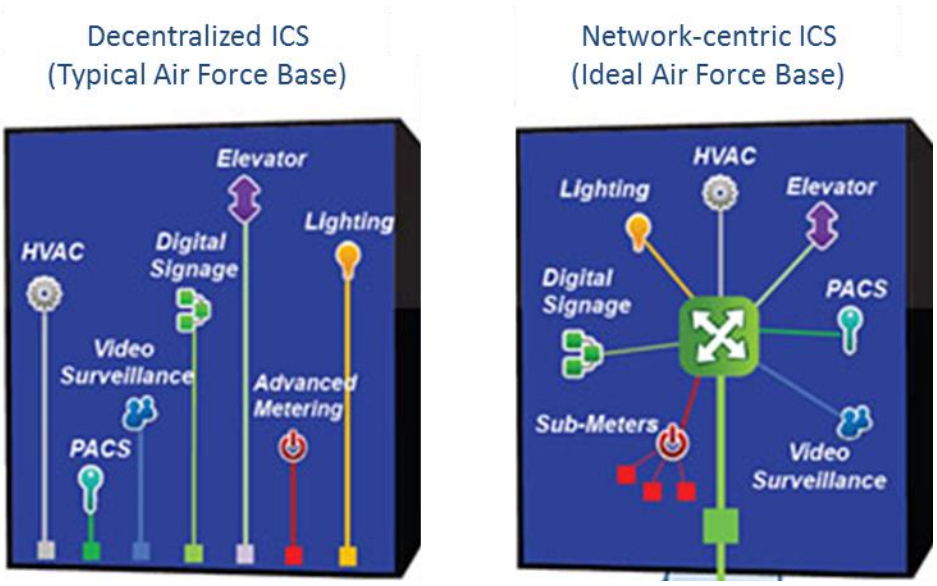

Figure 2. Notional Industrial Control System (ICS) Configuration[8]

Both Joseph Weiss, in his book, *Protecting Industrial Control Systems from Electronic Threats*, and the National Institute of Standards and Technology (NIST) categorize ICS by the function they serve:

- Supervisory control and data acquisition (SCADA) systems
- Distributed Control Systems (DCS)
- Programmable Logic Controllers (PLC)[9]
- Remote terminal units, field controllers, sensors, drives, emission controls, building controls, and meters[10]

Air Force civil engineers have operationalized this definition by organizing real property ICS in the following eight categories (Table 1)[11]:

Table 1. Air Force Civil Engineer Real Property Industrial Control Systems, *Engineering Technical Letter 11-1*

1. Supervisory Control And Data Acquisition (SCADA)	Fuel Distribution Systems
	Protective Relays
	Cathodic Protection systems
	Power generation systems
	Natural gas distribution systems
2. Energy Management and Controls Systems (EMCS)	
3. Automated Meter Reading Systems (AMRS)	
4. Fire alarm/fire suppression/mass notification systems	
5. Utility Monitoring and Control (UMAC) systems	Electrical distribution
	Generator monitoring
	Water system controls
	Natural gas distribution systems
6. Airfield control systems	Lighting systems
	Aircraft Arresting System (AAS) controls
7. Traffic signal controls and barriers	
8. Civil engineer maintained Intrusion Detection Systems (IDS)	

Air Force ICS categories such as airfield control, fuel and power distribution as well as electrical distribution systems at face value provide a link between a possible degradation or failure and an impact to a mission in air, space, or cyberspace. While the Air Force is postured well to assure the mission for routine system failure (back-up power, redundant systems, on-call maintenance personnel…etc.), ICS and its cyber vulnerabilities could render current provisions ineffective. As the opening vignette portrays, it is easy to explain the effect of a failed ICS to a commander when it impacts his mission. It is immensely more difficult to explain the risks entailed in unevenly applying limited resources of money and manpower to securing the same before an impact occurs. This difficulty begs the question, how did the Air Force end up with a disconnect between ICS and mission? One must look to history for the answer.

Air Force civil engineers have connected facility and infrastructure controls together as early as the early 1960s in the analog precursors to modern ICS. The Air Force Civil Engineer magazine first mentions interconnections of facility controls when covering the buildup of

facilities in the early 1906s to bed down the nuclear missile force.[12] These "networked" systems evolved over the ensuing decades to include digital components in step with industry practice.[13] This slow crawl toward digitally-dependent systems masked the implications of tying OT to the network that IT provided. The 2011 publishing of Engineering Technical Letter (ETL) 11-1, "*Civil Engineer Industrial Control System Information Assurance Compliance,"* was the first formal recognition by Air Force engineers of the importance of IT security.[14]

Civil engineer units are intended to be organized, trained, and equipped to maintain Real Property and Real Property Installed Equipment (RPIE) at their assigned installations for in their doctrinal role to provide Agile Combat Support (ACS) to the warfighting commander. The Air Force defines RPIE as follows:

> An item of equipment that is affixed and built into a facility as an integral part of that facility. To qualify as RPIE, the equipment must be necessary to make the facility complete, and if removed, would destroy or severely reduce the designed usefulness and operation of the facility…. RPIE includes such items as *control systems*, heating, cooling, electrical, emergency lighting …etc. [italics added for emphasis][15]

This engineer-centric definition fails to recognize the role of IT and security with respect to ICS (Figure 3). The result is that the lines of responsibility for securing ICS at every Air Force installation are disjoint and consequent gaps in the form of vulnerabilities threaten missions Service wide.

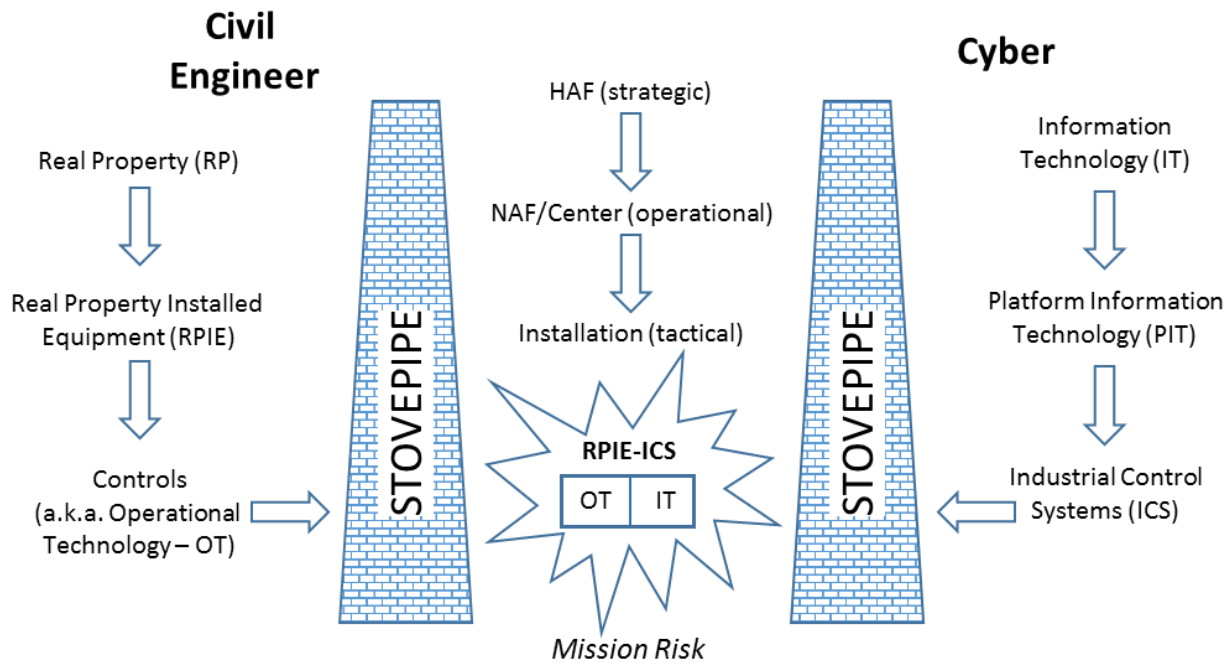

Figure 3. Illustration of Air Force functional stovepipes hindering security of Real Property Installed Equipment-Industrial Control Systems (RPIE-ICS)

ETL 11-1 formalized roles and responsibilities for securing ICS from the installation level to the Air Staff. It was at the time, a major breakthrough for civil engineers and the securing of ICS from cyber threat. The major flaw of the document is that it is written entirely from the civil engineer perspective. The letter mandates training and experience that falls outside of the core expertise of engineers and fits squarely in that of a cyber surety professional. The resulting ground truth is that few if any civil engineer squadrons trained or even appointed personnel per the ETL[16]. A second, emergent flaw places important responsibility on MAJCOM-level engineers whose positions were eliminated in the 2015 stand-up of the Air Force Installation and Mission Support Center.[17] A third, and perhaps more fundamental problem, is the omission of a link between ICS and the mission it supports. Without that link the Air Force risks wasting resources securing systems that have limited, or worse off, no impact to mission assurance.

Cyber Surety Perspective

In contrast to civil engineers, cyber surety professionals, following an IT-focused view, have constructed a network on a centrally controlled, standardized model (Figure 2). The result is a relatively well ordered network that expects standardization from connected sub-systems and components. Cyber surety professionals define IT, Platform IT (PIT), and ICS as nested system subsets (Figure 3).

Until recently the Air Force cyber surety community viewed ICS security (and all PIT security for that matter) as the responsibility of the function that owned the system. Thus in effect, both the civil engineer and cyber functional stovepipes viewed security of ICS as, "someone else's problem."[18] Of note, recent partnerships between the Air Force Civil Engineer Center (AFCEC) and Air Force Cyber Command (24th Air Force or AFCYBER) are reversing this trend. Additionally the cyber surety professionals suffer from the same flaw in the engineer perspective—a lack of understanding of the impact on the supported commander's mission by ICS vulnerabilities—one among many of the reasons behind the comprehensive look by TFCS.

Doctrine: the Root of the ICS Disconnect

After recognizing the divergent perspectives of civil engineers and cyber professionals and their impact on networked ICS, it is prudent to look to doctrine to find a root cause. The following paragraphs suggest that the stove-piped civil engineer and cyber surety communities failed to acknowledge the importance of the relationship between IT and OT for decades due to inadequately updated doctrine. During the Air Force's recognition of cyberspace as a unique domain, civil engineers failed to acknowledge the fundamental differences in this digital battle space and cyber professionals failed to adequately address the connection between it and the physical universe.

In line with Joint engineer doctrine, Air Force civil engineer doctrine mentions cyberspace only in as much as it is a domain akin to air and space. Air Force Doctrine Annex 3-34, "Engineer Operations," recognizes cyber solely as a general engineering task, and not a domain through which the Air Force operates. On a positive note, Annex 3-34 does speak to the trade space between mission and infrastructure in stating, "The requirement is to balance mission effectiveness versus efficient performance of infrastructure supporting base activities…"[19] Unfortunately, the annex fails to recognize the full spectrum of cyberspace by only addressing that domain under the "operation" step in real property life cycle management, leaving out planning, acquisition, sustainment, and recapitalization.[20]

In contrast, Air Force cyber doctrine—set forth in Air Force Doctrine Annex 3-12, "Cyberspace Operations"— acknowledges the existence of a two-way relationship between cyber and physical infrastructure. However, the doctrine is lacking in that fails to elaborate on the connection beyond a figure adapted from a Department of Homeland Security document delineating three levels of infrastructure: physical, critical infrastructure/key resources, and cyber. Annex 3-12 uses this diagram as a jumping off point to explore cyberspace infrastructure (such as switches, routers, and cabling), but never returns to physical and critical infrastructure save a mention that physical protection of critical infrastructure alone is not sufficient.[21] Effectively, the civil engineer and cyber professional are left to figure out for themselves the way to manage the other two thirds of the IT related infrastructure.

A tiger team of engineers and cyber professionals huddle in the Combatant Command headquarters to consider how the operational effectiveness of strike missions in the ongoing conflict has been degraded due to loss of expeditionary electric power. The cyber surety officer regretfully admits, "If only the firewall had been better hardened, the adversary couldn't have penetrated the network, allowing access to the deployable generators." The engineer suggests that, "Perhaps, if each generator [now matrixed together in a smart-grid to save energy and reduce manpower] was protected by a bolt-on cyber filter, the mission would not be impacted." Both of these solutions, while logical, are infeasible in tomorrow's resource and time-limited reality and exemplify a default DoD failing: jumping directly to a costly material solution. What they are missing is a clearly defined link between the service provided, Agile Combat Support (ACS), and the mission of the operational commander.

Convergent Solutions

There are many solutions which could contribute to securing the Air Force's ICS. The following paragraphs will offer potential organizational and training solutions, in-turn, which are consistent with the conclusions of prior research. Whether or not the suggested courses of action are taken, there is an imperative to update both civil engineer and cyber surety doctrine.

Prior Recommendations on Air Force ICS Security

Others who have studied the Air Force have also recognized the disconnects inherent in the current management of ICS. One study in particular originating from Idaho National Labs makes solid recommendations that track with industry practice that should be considered, contextualized, and implemented as appropriate.

In 2011, Major Joseph Boling authored a significant study: *Analyzing Air Force Security Posture on Typical Industrial Control Systems Servicing Critical Infrastructures*. He recommended that:

- The Air Force needs to map out the interdependencies of its critical infrastructure's automated controls and a cross-functional standard needed to be published and funded

- The Air Force should improve communications between the disparate areas that control these critical infrastructures
- The Air Force should incorporate lessons learned in system upgrades and new system installations, carrying through to the procurement and contracting processes
- Civil engineering, cyberspace, security forces, and fuels management leadership should jointly press hard in establishing and enforcing policies that guide safer, more secure implementation of automated control systems on critical infrastructures.[22]

While some progress has been made toward these four recommendations, much work left to be done. There are two primary themes underlying all four recommendations: a cross-functional look at ICS coupled with an accurate mapping of systems to mission.

Joseph Weiss estimates, "…that there are less than several hundred people worldwide with expertise that falls in the realm of ICS cyber security experts."[23] With so few experts existing in the world, it is impossible to imagine that the Air Force could secure the talents of these individuals to work for the Service. The National Institute of Standards and Technology's *Guide to Industrial Control Systems (ICS) Security* offers a potential basis for furthering Boling's recommendations while accounting for the lack of ICS security professionals as identified by Weiss:

> In summary, the operational and risk differences between ICS and IT systems create the need for increased sophistication in applying cybersecurity and operational strategies. A cross-functional team of control engineers, control system operators and IT security professionals needs to work closely to understand the possible implications of the installation, operation, and maintenance of security solutions in conjunction with control system operation.[24]

The implications are that the IT and OT professionals must work together on a continuous basis to maximize the overlap in both the controls in section 1 and the OT and IT functionality represented by section 2 (Figure 1). It is in the trade space of sections 3 and 4 where relative risks and benefits of degraded functionality must be jointly weighed by a cross-functional team to provide the supported commander appropriate mission assurance.

Organizational Solution: RPIE-ICS Fusion Cell

A major flaw in Air Force ICS management to date has been its functionally isolated perspectives which offer Airmen at the unit level limited ability to provide the commander adequate advice on accepting risk in the trade space between OT and IT controls. A task-organized section, where individuals representing both disciplines collaborate on a daily basis, offers a positive solution to this dilemma.

The revolution of cyberspace as a domain, unlike air and space, has not been adequately recognized by the way Air Force units organize at the wing, or tactical level. For certain, airfields have been recognized as a potential target for conventional or unconventional attack—chemical weapons dispensed by ballistic missiles, bomblets scattered by low-flying aircraft, or sappers at the fence line attempting to breach the perimeter. The base is no longer just the launching platform from which air and space forces depart and recover, it is the battlefield itself though its ICS. Most commonly in the Air Force, the installation and operational command responsibilities are entrusted to one person, the wing commander. Air Force Instruction 38-101, *Air Force Organization*, recognizes the benefit of that dual hatting: "By pulling together the mission and support elements, a wing provides a significant capability under a single commander. It is often responsible for maintaining the installation."[25] It is thus the responsibility of the wing's subordinate squadrons—synthesized by its groups—to inform the wing

commander of the current risks to successfully achieving his assigned mission. In the arena of RPIE-ICS, those units are the civil engineer squadron and cyber unit (notionally) falling under the mission support group.

The Cyber Unit CONOPS recognizes that, "Cyberspace is a contested warfighting domain that demands a coherent, integrated approach." [26] This theory is consistent with previous discussion on industry best-practices indicating a mandate to bring together OT experts with their IT counterparts in some fashion. There are four potential solutions to providing a wing an integrated approach: migrating IT experts into the civil engineer squadron, a similar transition of OT experts in to the cyber squadron, creating a stand-alone unit, or leveraging a task-organized, matrixed section with personnel reporting to both squadrons.

At face value it would seem that Air Force guidance narrows the field to one of the first three organizational constructs. AFI 38-101 suggests, "…not [to] fragment a capability into multiple squadrons when a single squadron provides a parent wing or group commander the best approach in terms of a coordinated, focused capability under single direction."[27] However, when reminded of the unique nature of RPIE-ICS that links the real-property responsibilities of civil engineers with the IT responsibilities of cyber surety Airmen, one or the other of the capabilities would necessarily be sacrificed thus sub-optimizing mission assurance. The creation of a stand-alone unit would be worse in that neither the IT or OT experts would benefit from reporting to their functionally aligned squadrons.

A compromise solution would be to task organize. This option would matrix individuals, on a semi-permanent basis, to a RPIE-ICS Fusion Cell (Figure 4). During times of lower INFOCON, the preponderance of the effort would be on enabling the OT to control the

installation environment. For day-to-day operations, the duty location would be collocated with the civil engineer controls shop, tasked under the civil engineer squadron's operations engineering element. Not unlike key personnel relocating to a wing emergency operations center when a traditional FPCON threat rises, the RPIE-ICS Fusion Cell would relocate to the cyber unit's operations center for the duration of a heightened INFOCON alert when IT concerns would take precedence in the trade space defined earlier.

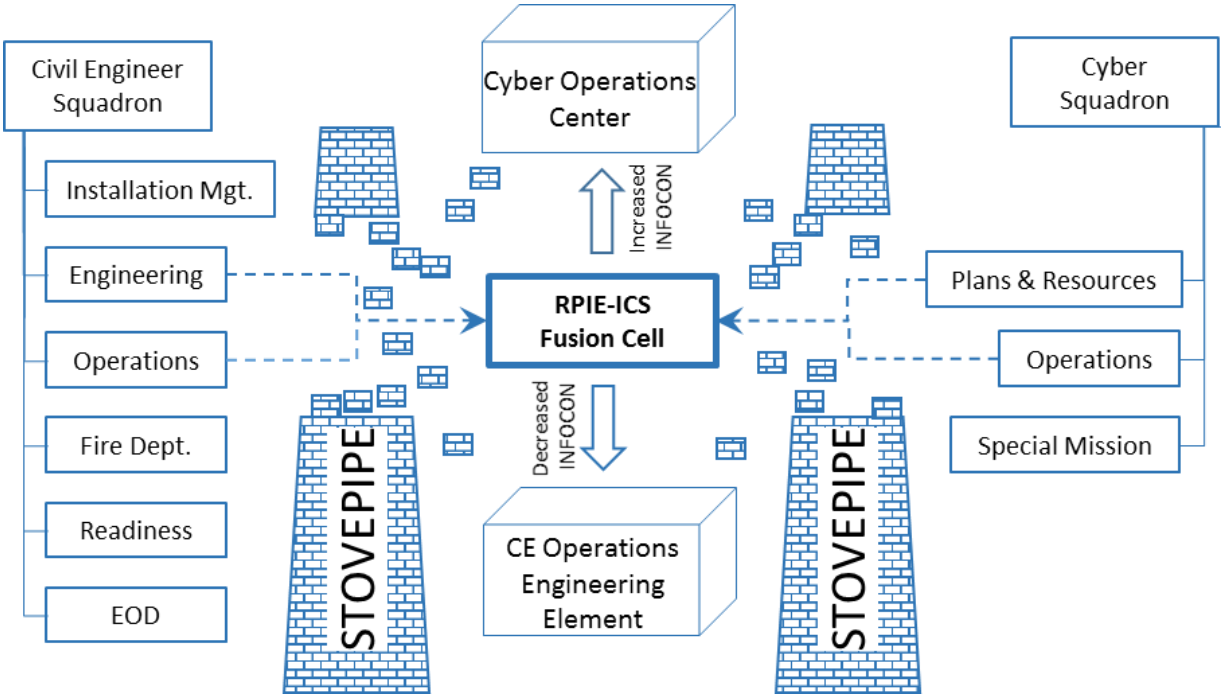

Figure 4. Illustration of Air Force functional stovepipes and proposed, matrixed wing RPIE-ICS Fusion Cell

Training Solution: Functional Mission Analysis-Cyber

A major flaw in both civil engineer and cyber attempts to operate and maintain ICS has been an inability to connect the resources demanded from a wing commander to the risk he is accepting. Functional Mission Analysis-Cyber (FMA-C) offers a systems engineering based approach to not only make that connection, but to prioritize limited resources to minimize risk and assure the mission. FMA-C is derived from System-Theoretic Process Analysis (STPA), a

causality-based model as described by Colonel William Young and Nancy G. Leveson which focuses strategically on system desired behavior rather than tactically on an overwhelming number of symptoms.[28] In other words training in FMA-C empowers Airmen to combat the fallacy: "if everything is important, then nothing is important."

A notional FMA-C analysis that would result in a look at the generator ICS from the paper's vignette would begin with mission statement from the Wing Commander: *generate strike sorties*. Next, an Agile Combat Support (ACS) doctrine-based system purpose template would identify the functions of *support* and *generate* as key system actions tying together *equipment* (generators, expeditionary airfield lighting, and the network connecting them) and *personnel* (airfield damage repair engineers). Such an analysis would recognize that the generators were connected in a grid, but would root out that the reason they were connected had little to do with the commander's mission, rather was driven by efforts to reduce manpower and conserve energy. The result of the analysis would be to present the commander the risk of losing airfield lighting and impacting sortie generation versus not meeting an energy goal or deploying an extra unit type code of power production engineers to manage the now stand-alone generators. In peacetime the commander might choose to accept the risk of connection to the network, whereas, in active conflict, the decision would likely be the opposite.

This small example illustrates the power in linking risk to mission based on the systems analysis of FMA-C. While gaining support in the Air Force cyber surety realm, the FMA-C model has yet to be explored by those who oversee the service's ICS. [29] There is potential that the methodology could not only link ICS risk to mission, but also achieve the ever elusive goal of linking risk to mission for the broader category of critical infrastructure.

When conducting a training exercise at home station, the matrixed members of the wing's RPIE-ICS fusion cell ponder a way to avoid the mission failure of a cyber-related power disruption they experienced on their last deployment. Now armed with a systems engineering analysis that links their commander's mission—generate strike sorties—with personnel, and equipment, the cell realizes that the solution was in their control the whole time. If they had only disconnected the smart-grid into individual generators and isolated them from the network, they could have eliminated the enemy threat. Their analysis showed that the networked connection of the generators had no impact on the commander's primary mission; rather it was a seemingly logical step influenced by industry and enforced by policy makers distanced from providing wartime ACS in a contested environment.

Recommendations

How do we organize, train, and equip Air Force forces to support the five core missions, in and through cyber? While changes can be made to the way units analyze systems or task organize under a wing, none of that will be effective until Air Force doctrine, both civil engineer and cyber surety, adequately recognizes the differences between cyberspace and the traditional physical domains of air and space. The TFCS infrastructure work group should prioritize revising both sets of doctrine to enable the force to view cyberspace for what it is, a digital battlefield that comes under fire every day, whether at home station or forward deployed. Without this revision, the limited mindset of Airmen in the field employing ICS enabled installations and the mission commanders they serve will never change. Therefore the Air Force should:

- Revise civil engineer & cyber doctrine to consider the unique aspects of cyberspace as it relates to the physical world through ICS
- Consider task organizing civil engineer and cyber Airmen at installations under an ICS fusion cell to provide commanders mission assurance
- Consider joint training of civil engineer and cyber Airmen on FMA-C to enable informed ICS security risk decisions by commanders

Conclusion

The argument presented suggests that Air Force doctrine inadequately addresses ICS security and as a result, the service is improperly organized and trained to secure missions across the domains of air, space, and cyberspace. In response, the Air Force must consider significant changes at the strategic, operational, and tactical levels to provide mission assurance to commanders.

Notes

[1] Lt Gen William J. Bender, *Task Force Cyber Secure Charter*, 1 June 2015, p. 1.

[2] "The basing system includes the infrastructure, people, materiel, and information needed to sustain operations for both the weapon and the weapon support system." Curtis E. LeMay Center for Doctrine Development and Education, *Annex 3-34, Engineer Operations*, 30 December 2014.

[3] "Mission assurance consists of measures required to accomplish essential objectives of missions in a contested environment. Mission assurance entails prioritizing mission essential functions (MEFs), mapping mission dependence on cyberspace, identifying vulnerabilities, and mitigating risk of known vulnerabilities." United States Scientific Advisory Board, *Report on Defending and Operating in a Contested Cyber Domain*, SAB-TR-08-01, August 2008, p. 1.

[4] National Institute of Standards and Technology, Special Publication 800-53 rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2003, p. B-21.

[5] *Gartner IT Glossary*. "Operational Technology (OT)," accessed 9 October 2015, http://www.gartner.com/it-glossary/operational-technology-ot/.

[6] Committee on National Security Systems, *Instruction Number 4009, National Information Assurance Glossary*, 26 April 2010, p. 38.

[7] Michael Sing, "The Fusion of Two Cultures…Information and Operational Technology Convergence," *Schneider Electric: Mining/Metals/Material* (blog), 10 July 2013, http://blog.schneider-electric.com/mining-metals-minerals/2013/07/10/the-fusion-of-two-cultures-information-and-operational-technology-conversion/.

[8] Adapted from Briefing, Task Force Cyber Secure, Team Infrastructure, subject: Strategic Advisory Board Info Update, 25 July 2015.

[9] National Institute of Standards and Technology (NIST) Special Publication 800-82 rev. 2, *Guide to Industrial Control Systems (ICS) Security*, May 2013, p. 2-1.

[10] Weiss includes these additional ICS to SCADA, DCS, and PLCs, however, they are primarily sub-components or applications of the three listed above. Joseph Weiss, *Protecting Industrial Control Systems from Electronic Threats*. New York: Momentum, 2010. p. ix.

[11] Since the publishing of ETL 11-1, DoD has mandated a revised categorization of what the department refers to as "Control Systems" or CS. For the purposes of this discussion, the mandated categories do not differ significantly enough from those in ETL 11-1 to alter the line of reasoning in the paper. As to the term "Control System" vs. the industry standard "Industrial Control System," to avoid adding further fog to the US military's understanding of the cyberspace domain, the acronym "ICS" will be used throughout this paper. Air Force Civil Engineer Support Agency, Engineering Technical Letter (ETL) 11-1, *Civil Engineer Industrial Control System Information Assurance Compliance*, 30 March 2011.

[12] A. J. Nowiejski, "The Base CE and Environmental Control." *Air Force Civil Engineer*, vol. 5 no. 1 (February 1964): pp. 6-8.

[13] Joseph Weiss, *Protecting Industrial Control Systems*, 2010. p. 25.

[14] Air Force Civil Engineer Support Agency, Engineering Technical Letter (ETL) 11-1, *Civil Engineer Industrial Control System Information Assurance Compliance*, 30 March 2011.

[15] AFI 32-9005 includes extensive tables that define what is considered as RPIE and what is not. Recently, DoD has mandated that ICS be considered "equipment." As the reason for this has more to do with budget accountability than reality, this paper will refer to ICS owned and maintained by Air Force civil engineers as RPIE-ICS. Air Force Instruction (AFI) 32-9005, *Real Property Accountability and Reporting*, 4 March 2015, p. 19.

[16] The author observed the lack of compliance in civil engineer squadrons during 2013 while serving as the Acting Director of the Air Force Civil Engineer Center, Operations Directorate, the organization charged with overseeing service-wide Certification and Accreditation (C&A) of Real Property Industrial Control Systems (RPIE).

[17] Headquarters United States Air Force. Program Action Directive 14-04, *Implementation of the Air Force Installation and Mission Support Center*, 25 February 2015. p. 1.

[18] ETL 11-1, Attachment 3, "Appointment of Platform Information Technology (PIT) Designated Accrediting Authority" exemplifies the delegation of security responsibility to an ICS "owner". Air Force Civil Engineer Support Agency, Engineering Technical Letter (ETL) 11-1, *Civil Engineer Industrial Control System Information Assurance Compliance*, 30 March 2011.

[19] Curtis E. LeMay Center for Doctrine Development and Education. "Annex 3-34, Engineer Operations," 30 December 2014. p. 9.

[20] Ibid.

[21] Curtis E. LeMay Center for Doctrine Development and Education. "Annex 3-12, Cyberspace Operations," 30 November 2011. pp 5-6.

[22] Maj Jonathan Boling, "Analyzing Air Force Security Posture on Typical Industrial Control Systems Servicing Critical Infrastructures." Research Report. (Maxwell AFB, AL: Air Force Fellows, 2011) pp. 19-21.

[23] Weiss, Joseph. *Protecting Industrial Control Systems,* 2010. p. 59-60.

[24]National Institute of Standards and Technology Special Publication 800-82 rev. 2. *Guide to Industrial Control Systems (ICS) Security*, May 2013. p. 2-17.

[25] Air Force Instruction 38-101, *Air Force Organization*, 16 March 2011, p. 12.

[26] Headquarters United States Air Force, *Cyberspace Squadron Concept of Operations [draft]*, 22 June 2015.

[27] Air Force Instruction 38-101, *Air Force Organization*, 16 March 2011, p. 13.

[28] William Young and Nancy G. Leveson, *An Integrated Approach to Safety and Security Based on Systems Theory*, Communications of the ACM, Volume 57, Number 2, February 2014.

[29] Col William Young, *Functional Mission Analysis-Cyber (FMA-C) Course Material*, as presented at Osan Air Base, 1-5 February 2016.

Bibliography

Air Force Civil Engineer Support Agency, Engineering Technical Letter (ETL) 11-1, *Civil Engineer Industrial Control System Information Assurance Compliance*, 30 March 2011.

Air Force Instruction (AFI) 32-9005, *Real Property Accountability and Reporting*, 4 March 2015.

Air Force Instruction 38-101, *Air Force Organization*, 16 March 2011.

Bender, Lt Gen William J., *Task Force Cyber Secure Charter*, 1 June 2015, p. 1.

Boling, Maj Jonathan, "Analyzing Air Force Security Posture on Typical Industrial Control Systems Servicing Critical Infrastructures." Research Report. (Maxwell AFB, AL: Air Force Fellows, 2011).

Briefing, Task Force Cyber Secure, Team Infrastructure, subject: Strategic Advisory Board Info Update, 25 July 2015.

Committee on National Security Systems, *Instruction Number 4009, National Information Assurance Glossary*, 26 April 2010.

Curtis E. LeMay Center for Doctrine Development and Education. "Annex 3-12, Cyberspace Operations," 30 November 2011.

Curtis E. LeMay Center for Doctrine Development and Education. "Annex 3-34, Engineer Operations," 30 December 2014.

Gartner IT Glossary, Operational Technology (OT), accessed 9 October 2015, http://www.gartner.com/it-glossary/operational-technology-ot/.

Headquarters United States Air Force, *Cyberspace Squadron Concept of Operations [draft]*, 22 June 2015.

Headquarters United States Air Force. Program Action Directive 14-04, Implementation of the Air Force Installation and Mission Support Center, 25 February 2015.

National Institute of Standards and Technology (NIST), Special Publication 800-53 rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2003.

National Institute of Standards and Technology (NIST) Special Publication 800-82 rev. 2, *Guide to Industrial Control Systems (ICS) Security*, May 2013.

Nowiejski, A. J. "The Base CE and Environmental Control." *Air Force Civil Engineer*, vol. 5 no. 1 (February 1964).

Sing, Michael. "The Fusion of Two Cultures…Information and Operational Technology Convergence," *Schneider Electric: Mining/Metals/Material* (blog), 10 July 2013. http://blog.schneider-electric.com/mining-metals-minerals/2013/07/10/the-fusion-of-two-cultures-information-and-operational-technology-conversion/.

United States Scientific Advisory Board, *Report on Defending and Operating in a Contested Cyber Domain*, SAB-TR-08-01, August 2008, p. 1.

Weiss, Joseph. *Protecting Industrial Control Systems from Electronic Threats*. New York: Momentum, 2010.

Young, William. *Functional Mission Analysis-Cyber (FMA-C) Course Material*, as presented at Osan Air Base, 1-5 February 2016.

Young, William and Nancy G. Leveson. *An Integrated Approach to Safety and Security Based on Systems Theory*, Communications of the ACM, Volume 57, Number 2, February 2014.