Booz | Allen | Hamilton

# MANAGING CYBER RISK AND BUILDING CYBER RESILIENCE FOR DEFENSE INDUSTRIAL CONTROL SYSTEMS

CONSULTING | ANALYTICS | DIGITAL SOLUTIONS | ENGINEERING | CYBER

Increasingly, military cyber attacks against physical infrastructure have been used to harass adversaries and prepare the ground for conventional attacks.

# UNDERSTANDING CYBER RISKS TO DEFENSE INDUSTRIAL CONTROL SYSTEMS

## THE EMERGING CYBER-PHYSICAL THREAT

The Department of Defense (DoD) relies on an estimated 2.5 million industrial control systems (ICS)—spanning across more than 500 installations and 300,000 buildings—to provide real-time automated monitoring, management, and control of industrial systems critical to military readiness and operations.[1] These ICSs control countless servos, switches, motors, actuators, valves, and relays—along with a myriad of sensors—to operate fuel pipelines, electricity distribution, facility security, waste management, and other services essential to the DoD mission. Every single ICS may consist of hundreds or even thousands of nodes, and the sheer volume of events they manage can only be choreographed efficiently with computer assistance.

As with any computer, an ICS can be the target of cyber attacks. When it emerged that the Stuxnet malware had successfully subverted an ICS to cause damage to Iranian centrifuges, it demonstrated that cyber attacks against ICSs can be highly effective, targeted, asymmetric weapons.[2] No other attack vector can reach so deeply into enemy territory with as little investment or physical risk to the attacker. A pipeline valve forced to malfunction can disrupt fuel supplies, cause environmental hazards, and endanger personnel without the enemies ever leaving their cubicle.

Increasingly, military cyber attacks against physical infrastructure have been used to harass adversaries and prepare the ground for conventional attacks. Because of the increasing frequency of these cyber-physical attacks, DoD leaders are keenly aware that mission-supporting ICSs will be attractive cyber targets in future conflicts. Congress has also taken notice. Recognizing the vast scope and scale of the ICS cybersecurity challenge across the military enterprise, Congress directed in the 2017 National Defense Authorization Act that the Secretary of Defense designate a single official to oversee “matters relating to integrating cybersecurity and industrial control systems for the Department of Defense.”[3]

1. *Michael Chipley, “Cybersecuring DoD Industrial Control Systems,” accessed October 7, 2019, https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1493737883.pdf; “Office of the Assistant Secretary of Defense for Sustainment Department of Defense Annual Energy Management and Resilience Report (AEMRR), Fiscal Year 2018,” last modified June 2017, https://www.acq.osd.mil/eie/Downloads/IE/FY%202018%20AEMR.pdf.*
2. *“What Is Stuxnet?” McAfee, accessed November 13, 2019, https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-stuxnet.html.*
3. *“National Defense Authorization Act for Fiscal Year 2017,” accessed October 7, 2019, https://www.congress.gov/114/plaws/publ328/PLAW-114publ328.pdf.*

Even as commanders and DoD leaders recognize the urgent need to address ICS cyber vulnerabilities, there is also momentum for connecting ICSs to larger information technology (IT) networks. This is desirable for a variety of reasons, including ease of remote access for maintenance, the ability to monitor for potentially malicious activity and improved situational awareness of key mission infrastructure. Unfortunately, many military ICSs predate modern systems that rely on internet protocol-based connectivity. These legacy ICSs are a patchwork of numerous subsystems and lack an effective security architecture. Although the legacy systems must be joined to the larger network, joining legacy ICSs with newer installations inevitably introduces new vulnerabilities, expands the attack surface, and vastly complicates the cyber challenge for the network as a whole.

## OPERATIONAL TECHNOLOGY SECURITY IS DIFFERENT THAN INFORMATION TECHNOLOGY SECURITY

Some might mistakenly view ICS security as an extension of information technology (IT) network security, which is well understood and for which there are countless tools available. But even though ICSs operate under an IT network layer, the hardware and software that operate the industrial controls—known as operational technology (OT)—present cybersecurity challenges quite distinct from those of traditional IT.

To begin with, IT security and OT security have different goals: whereas IT security tries to ensure the integrity and secure availability of data, OT security aims to ensure that physical industrial systems operate safely and reliably.

In addition, communication protocols between ICS components are often not standardized—unlike with IT—making automated security approaches difficult. Many industrial processes require precision coordination that cannot tolerate latency, making security features that are standard with IT such as encryption and packet authentication, problematic at best.

Moreover, changing any element of a functioning ICS introduces risk into the system in ways that are difficult to anticipate, so engineers often resist modifying, updating, or patching ICS components for fear of causing unexpected failures or introducing latency. This means that many basics of IT security (like aggressive firewalls, restrictive local user access policies, and frequent security patching) are often inappropriate for an ICS.

IT infrastructures have consistent, well-defined protocols that interoperate with relatively few distinct types of enabling hardware such as routers, network switches, servers, and workstations. This maturity and commoditization of network technologies means there are many cybersecurity tools available that can be used with almost any IT implementation. ICS ecosystems, on the other hand, are exponentially more diverse and there are far fewer commercial security tools available.

Because IT security models and tools cannot easily be applied to ICS environments because of their fragility, complexity, and diversity, installation commanders find themselves with few effective tools available to gain clear visibility of their ICS inventories, analyze ICS operations to determine what is normal baseline activity versus anomalous activity, and intercede in the face of attacks. For many installations, it can be a challenge to even know where to start risk mitigation efforts, given the scope and scale of their ICS operations. For many DoD components, it is becoming clear that the ICS security challenge requires a more holistic, tailored approach.

# ATTAINING ICS SECURITY AND RESILIENCE THROUGH A HOLISTIC, TAILORED APPROACH

Given the increasingly networked nature of ICS today, ICS cybersecurity requires going beyond traditional IT practices. Applying traditional cybersecurity tools and approaches will not fully secure the physical assets that comprise an ICS. Only a holistic and tailored approach to securing key ICSs can ensure continuity of operations in the event of a cyber attack.

Such an approach should consider all affected layers of the ICS operation: the military mission it supports, the industrial processes it controls, the IT network it may be connected to, the OT running the ICS and the security culture in which it operates. With this holistic approach, it is possible to systematically inventory, analyze, and remediate vulnerable systems, as well as introduce continuous monitoring tools that deliver deep visibility throughout the ICS. These actions not only manage risk but also build resiliency into the enterprise, enabling critical operations to persist in the event of a cyber attack.

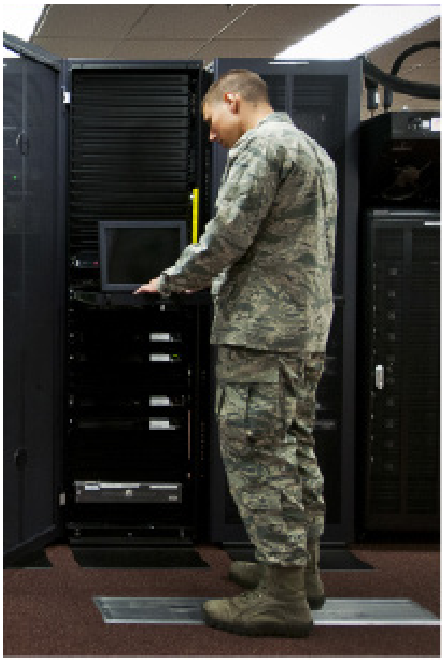
## GETTING STARTED BY SETTING PRIORITIES

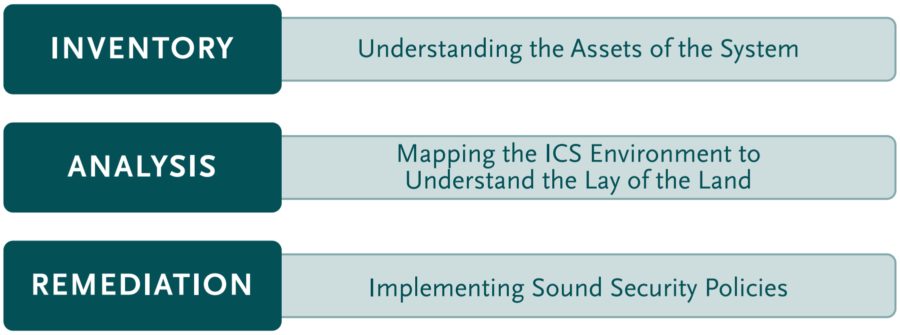
The impulse to secure everything is a natural but unrealistic goal. Fortunately, not every industrial process across an installation holds equal value to mission readiness, so it is possible to set informed priorities. With a deep functional understanding of the operations of the overall system, it is possible to identify and address those elements that pose the greatest risk to the mission. Which systems, if compromised, have the potential to compromise critical missions or mission-supporting tasks? Establishing functional priorities in this way allows planners to address individual system and subsystem vulnerabilities systematically and efficiently. Once mission-informed priorities are established, leaders should take a methodical inventory-analysis-remediation approach to addressing ICS vulnerabilities.

### Inventory: Understanding the Assets of the System

It is critical to first understand all the assets present so that their vulnerabilities can be identified and remediated. Because there is no standard process that is overseen by an ICS, this requires creating a detailed inventory that includes the make, model, configuration, and dataflow between components for every controller, sensor and final control element present in all critical systems. These inventories often require physical access to widely distributed assets and are extremely manpower-intensive, but to secure systems against a motivated attacker, those responsible for security must first understand what assets are present and how they work together.

These inventories can reveal a lot on their own through even a cursory review. For example, they can expose controllers that have built-in network software that





INVENTORY — Understanding the Assets of the System

ANALYSIS — Mapping the ICS Environment to Understand the Lay of the Land

REMEDIATION — Implementing Sound Security Policies

is not being used but have communication ports open by default—a common avenue for cyber attacks. Beyond highlighting basic security holes, an accurate inventory is the foundation for a detailed process map that can be used as a model for more sophisticated analyses. With a reliable model, it is possible to hypothesize vulnerabilities based on weaknesses of the cataloged connectivity, system protocols, types of data transmitted, and other individual security characteristics of assets.

### Analysis: Mapping the ICS Environment to Understand the Lay of the Land

This process map is what enables ICS security teams to mitigate risk by tailoring appropriate remedies to the affected ICS without disrupting ICS activities. With traditional networks, it is possible to demonstrate the efficacy of an attack through penetration testing without permanently disabling the target network. With OT however, any unexpected manipulation of physical controls can cause permanent damage or even injury—limiting the practicality of red teaming. An analyst with an ICS model in hand and an “adversarial mindset” can identify potential attack vectors and routes without needing to put the live system at risk.

This ability to think like an adversary is also essential for imagining nontraditional ICS vulnerabilities, such as attacks executed through seemingly less critical infrastructure. For example, a falsely triggered fire suppression system or hijacked HVAC unit could be used to sabotage carefully secured (even “air-gapped”) IT networks by damaging sensitive datacenters that support critical military operations. Collaboration between security teams and those who know the system best will help identify both traditional and nontraditional vulnerabilities—the engineers charged with programming, maintaining, and troubleshooting ICS are in the best position to understand how an enemy attacker can disrupt or disable a system.

Although fewer automated commercial off-the-shelf (COTS) technologies exist for protecting OT than are available for IT, the unique characteristics of OT do present opportunities when it comes to detecting anomalous behavior. The fact that OT is deliberately engineered, with its process and associated traffic explicitly defined, makes it easier to baseline and whitelist appropriate activity from the outset. OT traffic is limited in what inputs/outputs are possible and typically has less volume than what is found on IT networks, so a proper OT-centric baseline is useful for detecting system anomalies when they appear. Analytics can assist by tracking normal routes, frequency, and content of traffic through the system. Visualizations of this information then highlight threats and risks to the system that will then be candidates for remediation.

### Remediation: Implementing Sound Security Policies

By considering the unique role of each ICS and characteristics within a system, security experts can anticipate with acceptable confidence which components can be safely updated and when, where real-time network monitoring tools might be introduced, and which actions might instead lead to system jitter or unacceptable downtime. With meaningful knowledge of the affected processes, new monitoring tools can be embedded into the architecture without interrupting the mission. By consulting the detailed map of the system process and understanding the network traffic captured during normal activity, dangerous gateways can be identified and eliminated, and unintentional linkages can be severed. Where ICS and enterprise networks are linked—typically for logistics and enterprise resource planning (ERP) purposes—carefully monitored gatekeepers can be inserted to intermediate so that only appropriate messages are passed between the systems.

Continuous analysis of real-time data against the established baselines can verify that system responses that should be correlated, are correlated. For example, if a sensor indicates flow, but the tank at the end of the pipe is not registering an increase in fluid volume, the system can be made smart enough to alert operators to the discrepancy. The increasing use of smart devices that validate against the expected functioning of a system will make anomalous events easier to detect. Dummy components with no other purpose than to act as decoys can be strategically inserted into the process as tripwires to alert operators when malicious software is probing the OT.

## BEST PRACTICES STILL MATTER

Although current IT diagnostic tools are of limited value within OT networks, it is important to recognize that IT and OT security is not an either-or proposition: ICSs share all the attack vectors of both IT and OT, so IT security is critical to OT security. Proper IT security makes OT attacks more difficult and keeps attacks from spreading once they take hold. The most common and avoidable breaches in security are typically the unintentional consequence of an unauthorized USB drive or unvetted laptop connected to the network by outside technicians. No matter how malicious software first enters a system, once it is present, the enemy has a beachhead to work from. Even if the ICS has not been specifically targeted, malware such as ransomware that disrupts its enabling network can be devastating.

As tempting as it is to seek out pure technological solutions to every problem, they rarely provide security by themselves. Effective solutions will be a blend of people, processes, and technology. Maintaining security is difficult because it relies on the behavior of people, who do not act deterministically. But once baselines for a process are established, it is possible to define improved roles, responsibilities, and procedures that are aligned with operators' skillsets, dramatically contributing to the resilience of the enterprise. By developing updated standard operational procedures and incident response plans that are aligned with the real risks identified for the system, offline segments can be systematically brought back online according to priority, restoring mission readiness during an emergency.

## CONTINUOUS VISIBILITY KEEPS SECURITY UP TO DATE

Once identified vulnerabilities are remediated, ongoing security is maintained by providing operators with visibility into both the process and security environments. Where possible, it is optimal to integrate operational centers with security and network operations centers; an integrated operational view of both the IT and OT is useful because the most likely entry point for ICS cyber attacks is the point where they connect. But unless the available data is winnowed down intelligently before it reaches the operator, it can counterproductively reduce visibility, hiding important indicators of system compromise amidst less important data. Automated analytics can assist by monitoring activity logs for early warning signs of intrusion so that operators are provided meaningful alerts with a high percentage of signal-to-noise.

The unfortunate reality is that even with conscientious preparation, the enemy will sometimes breach a system's defenses. Continuous monitoring with remote policy enforcement will greatly contribute to system resilience by enabling defensive actions as soon as problems are detected—allowing for a more graceful isolation, removal, and eventual reentry of malfunctioning systems. This prepares the mission to bounce back from disruptions, bringing the system's performance back to an acceptable level in an acceptable amount of time. This two-pronged cyber defense—a security-aware architecture coupled with continuous operator visibility into the system—manages known risks while preparing for a resilient response in the event of an attack.

## HOLISTIC SECURITY, TAILORED TO THE MISSION

ICSs have been pushed into the front line of any likely conflict. Although the task of securing these critical systems seems daunting, it is a surmountable challenge. Security is a process, not an end state. Recognizing that ICS cybersecurity requires an understanding of both the specific at-risk engineering process and the broader mission is essential to properly securing DoD's automated infrastructure. By using insight into every layer of the IT and OT networks, along with deep knowledge of the engineering processes and military missions they serve, known threats can be identified, analyzed, and remediated, and new threats can be detected and managed. By taking a holistic, systematic approach to ICS cybersecurity, DoD leaders can effectively secure these systems and ensure mission continuity in the face of enemy attempts at disruption.

### About Booz Allen

For more than 100 years, military, government, and business leaders have turned to Booz Allen Hamilton to solve their most complex problems. As a consulting firm with experts in analytics, digital, engineering, and cyber, we help organizations transform. We are a key partner on some of the most innovative programs for governments worldwide and trusted by their most sensitive agencies. We work shoulder to shoulder with clients, using a mission-first approach to choose the right strategy and technology to help them realize their vision. With global headquarters in McLean, Virginia and more than 80 offices worldwide, our firm employs nearly 27,000 people and had revenue of $6.7 billion for the 12 months ending March 31, 2019. To learn more, visit BoozAllen.com. (NYSE: BAH)

## For more information, please contact our experts:

**David Forbes**
*Principal*
*forbes_david@bah.com*

**Jandria Alexander**
*Principal*
*alexander_jandria@bah.com*

**Kyle Miller**
*Chief Technologist*
*miller_kyle@bah.com*

**Shaun Long**
*Senior Lead Technologist*
*long_shaun@bah.com*

|