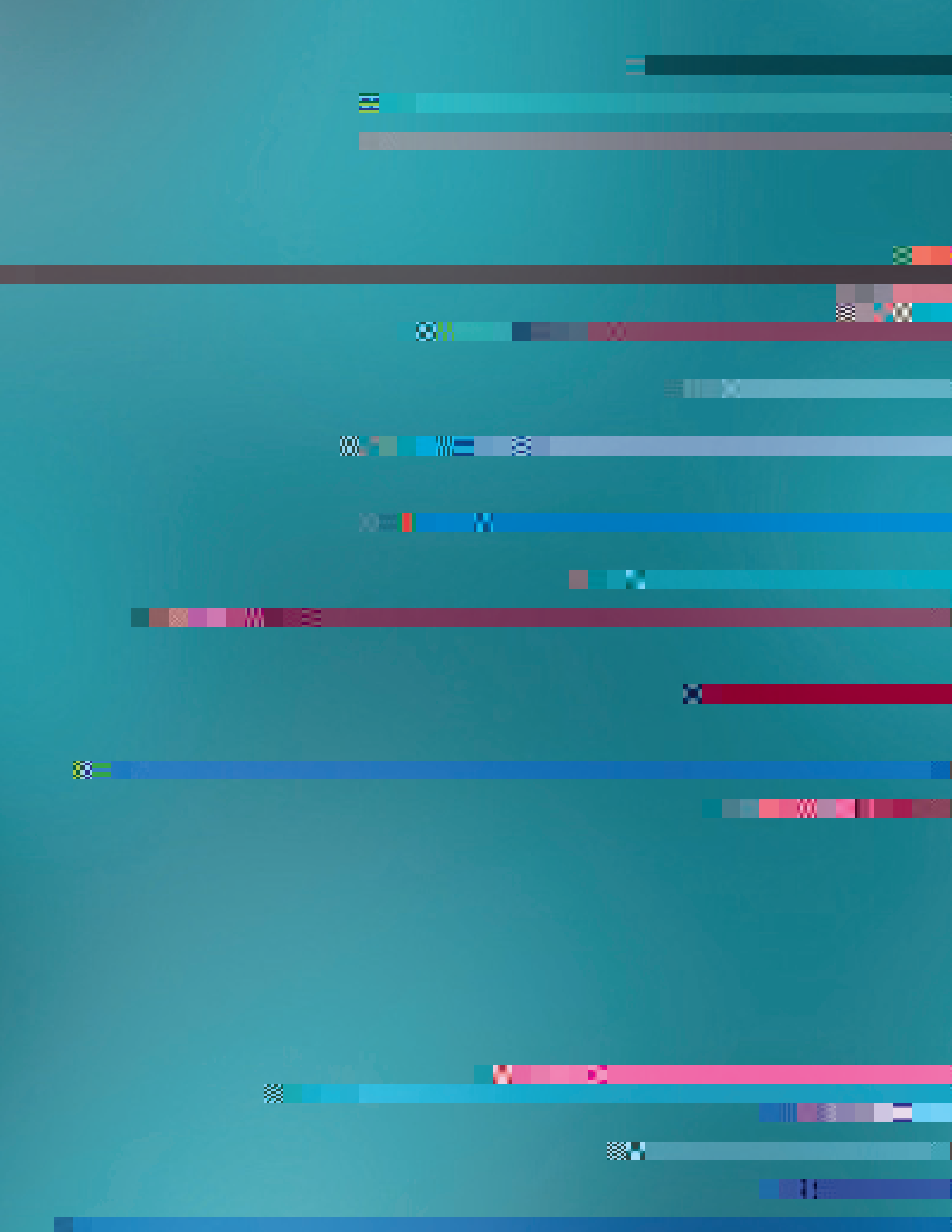


THE EMERGING CYBER-PHYSICAL THREAT

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,

Even as commanders and DoD leaders

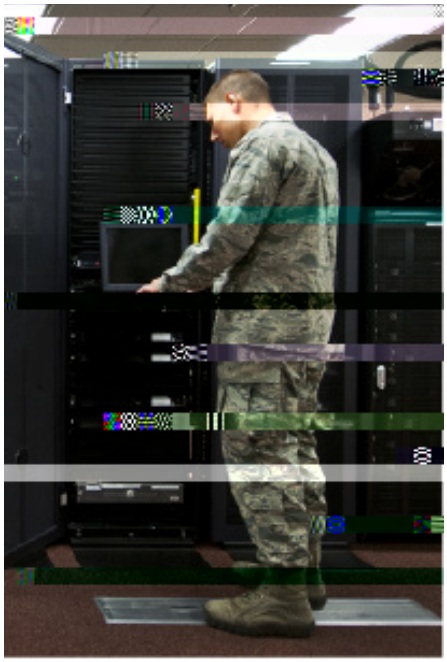
ATTAINING ICS SECURITY AND RESILIENCE THROUGH A HOLISTIC, TAILORED APPROACH

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 afected 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 e f ciently. Once mission-informed priorities are established, leaders should take a methodical inventory-analysis-remediation approach to addressing ICS vulnerabilities.



[illegible]

It is critical to frst understand all the assets present so that their vulnerabilities can be identifed 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, confguration, and datafow between components for every controller, sensor and fnal 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 frst 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

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 alert lt l.9 (3 (n)-1.-1.5 (t)-2 7.9 (r)[illegible]