The Importance of Modernizing and Cyber-Hardening Facility Related Control Systems in the Era of Multi-Domain Operations Warfare

Mark Duszynski
VP Johnson Controls Federal Systems, Inc.

AEA Engineer Regimental Information and Training Seminar

August 1, 2019
Facility-Related Control Systems (FRCS), which are a combination of control components (e.g., electrical, mechanical, hydraulic, or pneumatic, etc.), special purpose controlling devices, and standard IT that act together upon underlying mechanical and/or electrical equipment to achieve an objective (e.g., transport of matter or energy, maintain a secure and comfortable work environment, etc.). All automated control systems are considered PIT. Industrial Control Systems (ICS) are automated control systems that act upon industrial systems and processes. ICS is used as a general term that encompasses several – but not all - types of control systems. These include supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS) and other control systems, such as the Programmable Logic Controllers (PLCs) often found in the industrial sector and critical infrastructure.
Multi-Domain Warfare is here to stay…

Multi-Domain Operations

The U.S. Army in Multi-Domain Operations 2028, released on 6 December 2018, describes the Army’s concept for how to win future wars against near-peer competitors. According to the “Summary of the 2018 National Defense Strategy,” the joint force faces a more complex security environment “defined by rapid technological change, [and] challenges from adversaries in every operating domain.” Gen. Joseph Dunford, the chairman of the Joint Chiefs of Staff, wrote that “the U.S. military’s long-held competitive advantage has eroded” as adversaries have adapted to counter U.S. capabilities.

The central idea behind multi-domain operations is that Army formations, as part of the joint force, must be able to fight across all domains (land, maritime, air, space, and cyberspace), the EMS, and the information environment. Due to resource constraints and more dangerous adversaries, Army formations must maximize every capability, synchronize operations across domains, and mass at the decisive point to win future battles.
Multi-Domain Operations: Army Battlefield Framework

‘The spread of accurate and inexpensive weapons and the use of cyber tools have allowed state and non-state competitors to harm the US...they also enable adversaries to attempt to attack...in ways that could cripple our economy and our ability to deploy our military forces.’

- U.S. National Security Strategy / December 2017
"Army Installations must modernize to support the modernized Army of 2028"

"We cannot modernize the force without modernizing Army installations. Our infrastructure must include: abundant network bandwidth and speed; sensors and protection against cyber, physical, and aerial threats; strong defenses against threats to our energy and water systems, and the ability to streamline installation operations through data analytics."

Honorable Alex Beehler, Assistant Secretary of the Army for Installations, Energy & Environment (ASA IE&E)
The “Front Line” has moved inside the “Fence Line”

Mission success today depends more than ever on secure, integrated and efficient DoD installation facilities control networks

Most “ICS” and “FRCS” are vulnerable to compromise if not correctly specified at time of construction, or properly maintained over time

Integration of disparate ICS systems has many advantages but requires careful coordination among specifiers and subcontractors

New building specifications must address these issues, but the need to retrofit, upgrade and modernize existing FRCS networks is much more significant
Recommendations

1. Achieve policy and compliance consistency across the military services relative to FRCS cyber security requirements
2. Educate military command leadership about the critical mission alignment of control systems with battlefield success
3. Consistent hardening, modernization and on-going support of control systems through centralized goals and measurement at the installation management command level
4. Leverage industry to create specific technology master plans at the installation level that provide clarity on the most cost effective manner to upgrade and maintain systems compliance
Recommendations

5. Ensure that all networked control systems comply with UFGS standards

6. Create control system hardware “approved products lists”

7. Leverage commercially-proven Operational Technology standards (e.g. BACnet) and benchmarking approaches

8. Award separate systems integrator or technology contracts

9. Assess all FRCS at major DoD installations to determine inherent vulnerabilities

10. Develop long range modernization plans and secure needed funding
In the past, the Assistant Secretary of Defense for Energy, Installations and Environment (ASD(EI&E)) community used ICS in an even broader sense to represent all types of control systems (SCADA, DDC, DCS, building, vehicle, transportation, etc.). However, since most uses of the term ICS do not pertain to industrial systems or processes, the term “Control System” is used herein for this general category of PIT.

The EI&E community is responsible for all FRCS related to real property assets (facilities), including but not limited to:

- Control System Platform Enclaves (PE)
- Airfield Systems (AS)
- Pier Systems (PS)
- Environmental Monitoring (EM)
- Electronic Security Systems (ESS)
- Fire & Life Safety (FLS)
- Dam, Lock & Levee Systems (DLL)
- Medical Control Systems (MED)
- Traffic Control Systems (TCS)
- Transportation & Fueling Systems (TFS)
- Meteorological Control Systems (MET)
- Building Control Systems (BCS)
- Utility Control Systems (UCS)
- Utility Monitoring & Control Systems (UMCS)