SECMATION

Industrial Control Systems Secure Communications Module (SCM)

POC: Hal Aldridge, Ph.D., CEO, Secmation, hal@secmation.com, (919) 887-2560

Chelsea Meggitt, Business Development, Secmation, chelsea.meggitt@secmation.com, (919) 887-2560

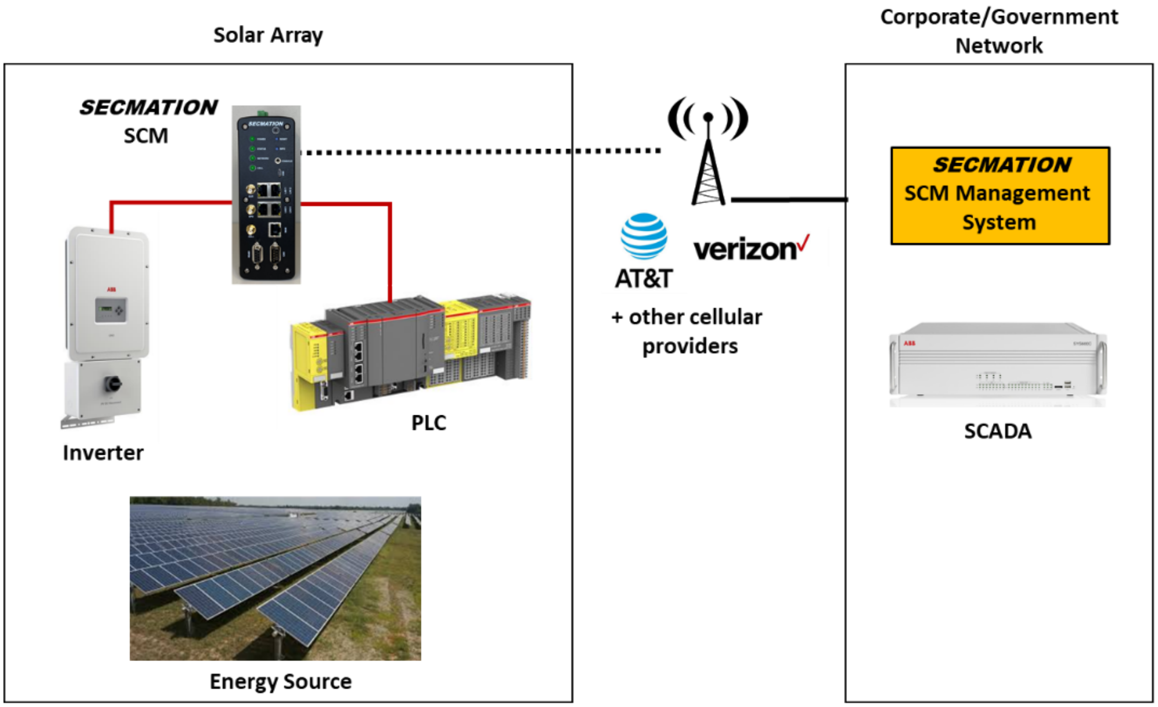
Sponsor: Navy Facilities Engineering Command (NAVFAC), Contract #N39430-18-C-2092

Problem Statement: Navy and DoD facilities (CONUS and OCONUS) use Industrial Control Systems (ICS) equipment to control and monitor infrastructure including energy generation/distribution, wastewater treatment, and building automation. ICS have become a target of modern cyber-attacks putting critical infrastructure and industrial operations at risk. For security reasons many of these systems are "air-gapped" making remote operation of these systems challenging. Cybersecure, resilient remote control/monitoring of these systems would enhance visibility to facility operations, enable optimization of functions to reduce operational cost, and reduce labor required to maintain the systems.

There are specific challenges in connecting these systems to Navy/DoD networks to enable remote monitoring/control. To join a DoD network, the ICS system must be DoD Risk Management Framework (RMF) certified. The RMF process assesses whether a computer system (in this case the ICS) provides adequate cybersecurity controls to limit the risk of it being used to compromise the DoD network. The RMF process is rigorous and requires significant resources/time to complete. Due to the purpose of the ICS data to control/monitor facility infrastructure, the data must be handled correctly. This data is considered "Sensitive but Unclassified" for most applications. DoD and US Government regulations require data of this type to be protected using NIST FIPS 140-2 certified cryptography. Like RMF the NIST certification process is rigorous and requires significant resources/time to complete.

In most cases, the COTS equipment (ex. Programmable Logic Controllers (PLC)) used to build new ICS systems and contained in legacy ICS systems have no/limited security features. If security features are available, it can be difficult to determine the quality/pedigree of the security (e.g. Where was it developed? How was it tested?). Few of these systems have the required RMF/NIST certifications. Equipment that has the needed security features would require significant participation from the equipment manufacturer to provide technical support and proprietary design information to enable either RMF or NIST certification of their equipment.

If the required security is available, many of these ICS systems are in remote locations at the facility making communications with these systems challenging without a significant infrastructure wired/wireless investment.



SCM provides a RMF Assessed and NIST FIPS 140-2 Certified security solution combined with multiple communications options including cellular enabling connectivity of ICS systems to DoD networks

Solution: The Secmation SCM and SCM Management System provide a secure, RMF/NIST compliant solution for connecting new and legacy ICS systems to DoD networks. The SCM features a robust security architecture designed from the ground up to protect ICS applications. These security protections are designed to operate with minimal overhead on system operation enabling compatibility with both new and legacy deployments.

The SCM is designed to be connected to nearby ICS equipment (e.g. the protected equipment) providing cybersecurity protections and wireless/wired communications to the DoD network. SCM is compatible with a wide variety of ICS equipment that use standard ICS protocols including Modbus, DNP3, and BACNet. The SCM allows local protected devices to connect to it via Ethernet or serial interfaces providing flexibility needed to support different ICS configurations.

The SCM uses FIPS certified cryptography to encrypt the ICS data from the protected equipment for transmission to the DoD network. This cryptography also authenticates the identity of the SCM sending the information and provides information for the receiver to confirm the data has not been tampered with or otherwise corrupted. Similar protections are enforced for data received by the SCM before it is provided to the protected equipment.

The SCM uses an advanced Intrusion Protection and Detection System (IDPS) to inspect standard ICS communications. The IDPS confirms that the communications used complies to the correct industry standard protocol and operational parameters defined

by the system operator. This confirmation provides a defense against an attacker using maliciously constructed data to affect system operation. If the IDPS detects that the communications do not meet the required standards it can block the communications and/or notify an operator. The IDPS enables an operator to define what types of communications are authorized and block unauthorized actions at a granular (e.g. coil) level.

In addition to cybersecurity, the SCM provides multiple options for communicating with the DoD network. The SCM provides a 100Mbps Ethernet port for wired network connectivity. The SCM also includes a cellular modem compatible with the new Internet of Things (IoT) cellular service options (e.g. LTE CAT M1, NB-IoT). These options provide cost effective connectivity using commercial cellular carriers. The SCM is authorized to connect with AT&T, Verizon, and multiple other CONUS/OCONUS carriers. The end-to-end data security provided by the SCM means that the carrier cannot access the information during transport providing a required level of security for sensitive data. The cellular communications can also act as a backup if the wired connectivity fails.

The SCM Management System enables centralized management of SCMs on or across facilities. The web-based operator interface enables configuration of network connectivity and security of remote SCMs. The Management System provides status of the deployed SCMs including security alerts. The Management System collects audit logs from remote SCM and can provide the logs a Security Information and Event Management (SIEM) system for analysis.

Program Status: Under the NAVFAC program the SCM has completed its Critical Design Review and is scheduled to begin integration and RMF assessment at Navy facilities in Q2FY21. The Navy assessment will use the Assess-Only process (e.g. through RMF Step 4) creating an approved data package for SCM documenting its security controls. This RMF documentation will enable a new/legacy ICS system properly incorporating SCMs to address most required security controls without re-assessment. As a result, new and legacy ICS systems can utilize SCMs to streamline the RMF certification process and connect to DoD networks. The Navy RMF assessment and NIST FIPS 140-2 certification are anticipated to be completed by the end of FY21 enabling SCM deployment in DoD operational systems.