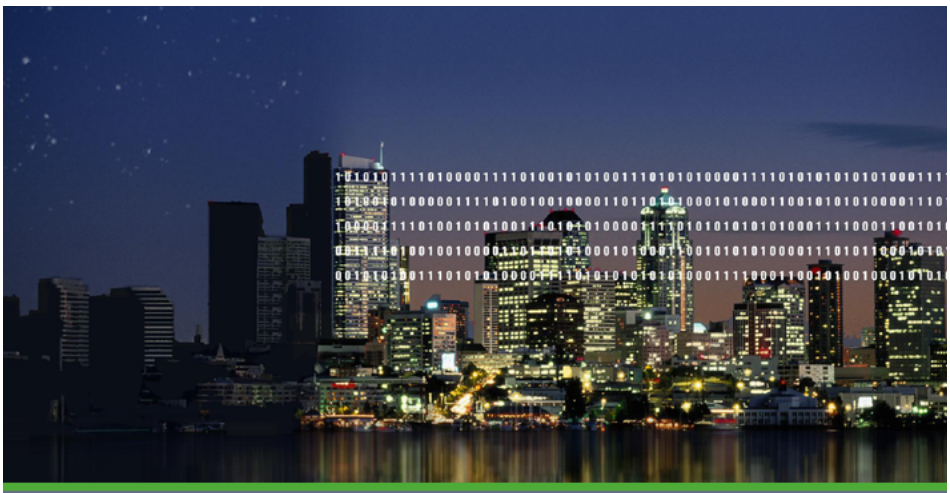
U.S. DEPARTMENT OF
ENERGY

Office of
ENERGY EFFICIENCY &
RENEWABLE ENERGY

Cyber-securing Facility Related Control Systems



Cyber security attacks can compromise physical systems and equipment. A wide range of actions can be taken to safeguard against cyber threats.
Image Credit: Pacific Northwest National Laboratory

Federal facilities are increasingly equipped with control systems that use information technology to ensure the safety and comfort of occupants, enhance efficiency, lower facility costs, and optimize operations. These facility-related control systems (FRCS) are automated, networked, and connected to other information systems and, in some cases, to the internet. Historically, the obscurity of proprietary FRCS and physical isolation from the outside world provided adequate protection. Today, increased connectivity requires diligence to secure these operational technology (OT) systems from cyber intrusions and attacks.

This fact sheet describes some cyber security strategies applicable to federal facilities gleaned from the experiences at several Department of Energy (DOE) national laboratories. The DOE national laboratories represent a diverse cross-section of facility types including research and development facilities, high security buildings, and traditional office space. The laboratories are cognizant of the importance of robust cyber security for FRCS and have developed implementation plans to adhere to federal regulations, guidance, and standards for cyber security (see Table 1).

A variety of cyber security objectives are considered. Techniques including benchmark assessments of building automation systems, penetration tests, and working to move FRCS and supervisory control and data acquisition (SCADA) systems to isolated networks can be used to develop roadmaps to address existing gaps and implement fixes.

IT systems are no longer the only cyber target

Cyber threats exploit vulnerabilities in systems or procedures in order to gain access to control system networks and components, obtain information and processes, and disrupt or gain control of the FRCS. Figure 1 shows the increasing frequency of cyber incidents targeting facilities that have been reported to the Industrial Control Systems Cybersecurity Emergency Response Team (ICS-CERT).

Implementing FRCS cyber security

There are numerous approaches to implementing effective cyber security measures. To determine what steps to take, a federal agency should consider the maturity of its existing cyber security practices, the agency's risk tolerance, available resources, and regulatory requirements.

Scope, prioritize, and orient

The starting point for FRCS cyber security is to identify responsible personnel, define objectives and priorities, and identify and understand the status of the FRCS inventory.

It is critical to create a cross-functional team and incorporate input from stakeholders throughout the organization because cyber security extends across business functions. This cross-functional team could include personnel from the following business function areas:

- Senior management - Advocates for cyber security as a strategic focus for the organization
- Facilities personnel – Manage daily operations of facilities and their associated FRCS
- IT – Manage cyber security, network hardware, and software assets across the enterprise
- Legal – Assist with interpreting cyber security requirements for regulatory compliance

- Contracts/procurement – Informs the acquisition process to ensure that the purchase of new equipment adhere to cyber security requirements
- Enterprise risk management – Track cyber security risk priorities
- Business continuity teams – Implement incident management procedures
- Finance/Budget personnel – Allocate funds and prioritize resources for cyber security
- FRCS equipment vendors and support integrators – Provide technology expertise

Collectively, the team determines which of the organization's functions and facilities need to be included in the cyber security program. For the functions or facilities included, a risk profile is developed to understand and articulate risk tolerances. Priority evaluations may be designated for highly sensitive facilities such as validated environments or facilities designated for contingency or emergency conditions.

Facilities personnel take the lead on producing an inventory of FRCS assets. The facilities personnel map how FRCS are shared across facilities and where multiple systems interact.

Table 1 - FRCS Cyber Security Drivers

Laws and Regulations	Federal Information Security Modernization Act of 2014 (FISMA)
	Executive Order 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (May 2017)
	Executive Order 13636: Improving Critical Infrastructure Cybersecurity (Feb 2013)
	Presidential Policy Directive 21: Critical Infrastructure Security and Resilience
	Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection
National Institute of Standards and Technology (NIST) Standards and Guidance	NIST Special Publication (SP) 800-18 Rev 1: Guide for Developing Security for Federal Information Systems (Feb 2006)
	NIST SP 800-37 Rev 1: Guide for Applying the Risk Management Framework to Federal Information Systems (Feb 2010)
	NIST SP 800-53 Rev 4: Recommended Security Controls for Federal Information Systems and Organizations (April 2013)
	NIST SP 800-82 Rev 2: Guide to Industrial Control Systems Security (May 2015)
	NIST SP 800-115: Technical Guide to Information Security Testing and Assessment (Sept 2008)
	NIST SP 800-184: Guide for Cyber Security Event Recovery (Dec. 2016)
Other Standards	ANSI/ISA-62443-2-1 (99.02.01)-2009: Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program

Facilities and IT personnel assess the topology of the FRCS networks, to determine if they share infrastructure with enterprise systems, operate on platform enclaves or virtual local area networks, or use isolated networks.

The cross-functional team members ascertain the relevant requirements, and standards that apply to the selected FRCS within their area of expertise. The team also determines if it is advantageous to perform self-directed evaluations using internal resources, or facilitated approaches using third party expertise.

For example, one of the DOE national laboratories created a multi-domain working group that included representation from across the organization. This working group has become the focus for change management efforts and has been critical in helping translate operational technology concepts to IT teams and vice-versa. The facilities personnel immersed the IT staff in FRCS in order to familiarize their IT counterparts with operational and technical details.

Operational Technologies (OT)

OT includes systems, components, and software that monitor and control the physical environment and can range from a simple stand-alone system with a few controllers connected to a single computer, to a campus-wide utility monitoring and control system with internet connections to the local utility.

Assess the current cyber security posture

Assessing the current cyber security posture involves identifying the level of sophistication of existing cyber security practices against established frameworks. There are many assessment methods available.

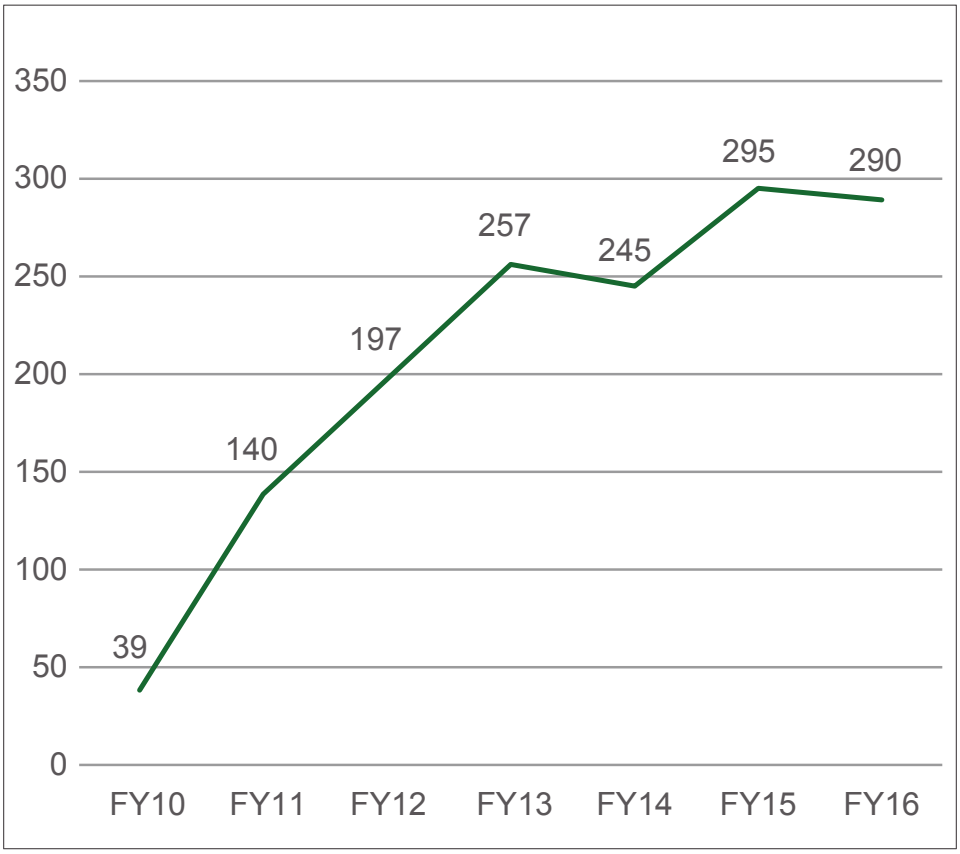


Figure 1 - ICS Incidents Reported to the Industrial Control Systems Emergency Response Team (ICS-CERT)

One assessment method is to map the current FRCS system characteristics, policies, and practices to categories within each of the five Functions in the NIST Cyber Security Framework (CSF) – Identify, Protect, Detect, Respond, and Recover. Alternatively, an organization may follow the steps in the Buildings Cyber Security Capability Maturity Model (C2M2) to evaluate the level of its maturity across the 10 cyber security domains (C2M2 is briefly described in the next section).

Conduct a risk assessment

Risk assessments are used to identify threats and vulnerabilities, impacts that threats may have on the organization, and the likelihood of adverse events occurring. In evaluating risk, FRCS may require additional considerations beyond traditional IT systems. Cyber-attacks on FRCS can have both digital and physical effects; risks can extend beyond the FRCS itself to the physical environment and associated processes.

One of the challenges encountered by a DOE national laboratory was that some of the FRCS could not be scanned for known vulnerabilities because the FRCS could not support the scanning, as it would lead to a denial of service on the system. These types of FRCS will have to be updated before a cyber vulnerability assessment can be performed.

Develop the target cyber security profile

Equipped with an understanding of the risks associated with the existing systems, and the relevant regulatory requirements, an organization can articulate the target profile for the FRCS and associated cyber security policies and procedures.

The profile may formulate specific target states for the functional categories within the NIST CSF categories, or could be articulated in terms of how the organization achieves higher levels of maturity in the C2M2 model.

For example, a real world cyber-attack on one DOE national laboratory's enterprise IT systems underscored the need for strong cyber security for the OT systems. As a result, the FRCS was moved off of enterprise IT networks and onto a dedicated secure network infrastructure.

Identify and prioritize gaps; develop and execute implementation plans

A comparison of the current FRCS cyber security profile to the target profile will help identify gaps and enable the team to evaluate consequences of failure to address those gaps. When prioritizing gaps consider their level of risk, operational impact, regulatory requirements, business objectives, and organizational constraints.

Real World ICS Impacts

"In more than 20 cases, Symantec says the hackers successfully gained access to the target companies' networks. And at a handful of US power firms…their forensic analysis found that the hackers obtained what they call operational access: control of the interfaces power company engineers use to send actual commands to equipment like circuit breakers, giving them the ability to stop the flow of electricity into US homes and businesses."

- Wired Magazine, 2017

The team can proceed to develop and execute a prioritized mitigation plan to progress from the current state to the target posture.

As one example, one of the DOE national laboratories consulted for this fact sheet integrated metering systems across OT and IT networks to track consumption. This configuration required the implementation of strong cyber security measures to protect the dispersed interconnected systems.

Example tools

The federal government and private sector have produced tools that provide evaluation and implementation instructions. Development of FRCS cyber security tools is on-going, thus agencies will need to stay engaged to be aware of the latest applicable tools. The following is a sampling of available tools and resources.

NIST Framework for Improving Critical Infrastructure Cybersecurity (NIST-CSF)

This document provides guidance for how organizations can assess and manage cyber security risk. It is not limited to any single sector, and is flexible enough for use by organizations with mature cyber security postures as well as those with less developed programs.

The CSF is organized around Core Functions that organize cyber security activities at a high level: Identify, Protect, Detect, Respond, and Recover.

Building Cyber Security Framework

Based on the NIST-CSF, this tool developed by DOE's Office of Energy Efficiency and Renewable Energy is a voluntary, set of risk-based standards and best practices to help facilities teams manage cyber security risks. It helps users describe their current posture and desired target state, identify and prioritize improvements, and assess and communicate progress to internal and external stakeholders.

DOE Building Cybersecurity Capability Maturity Model (B-C2M2)

The B-C2M2 provides a methodology to self-assess and improve cyber security capabilities for building IT and OT systems. It includes a toolkit that can be deployed in a single day or scaled to a more comprehensive evaluation effort.

B-C2M2 helps organizations express their capabilities through four maturity indicator levels across ten domains of cyber security practice:

- Risk management
- Asset, Change, and Configuration Management
- Identity and Access Management
- Threat and Vulnerability Management
- Situational Awareness
- Information Sharing and Communications
- Event and Incident Response, Continuity of Operations
- Supply Chain and External Dependencies Management
- Workforce Management
- Cyber Security Program Management

DHS Cyber Resilience Review (DHS-CRR)

This tool is a voluntary, no-cost non-technical assessment methodology used to evaluate an organization's cyber security practices. It assess programs across ten domains, consistent with those used by the C2M2.

ICS-CERT Cyber Security Evaluation Tool (CSET)

CSET is a software-based tool that provides a systematic approach to assess control system and network cyber security. The methodology is standards-based, allowing the user to evaluate their posture relative to a selected security level and identify opportunities for improvement.

Closing

The challenges of assessing FRCS cyber security at DOE National Laboratories highlighted the range of actions that need to be taken to improve our cyber security posture. There are many ways to tackle the FRCS cyber security challenge, with every small step helping in the overall goal. Cyber security for FRCS is a rapidly growing field, thus as agencies move forward, they should look for the latest available tools to facilitate the cyber security journey.

Acknowledgements

FEMP would like to acknowledge the contributions from Idaho National Laboratory, Los Alamos National Laboratory, National Renewable Energy Laboratory, Oak Ridge National Laboratory, and Pacific Northwest National Laboratory personnel who were consulted for this fact sheet.■

U.S. DEPARTMENT OF ENERGY

Office of ENERGY EFFICIENCY & RENEWABLE ENERGY

FEMP Federal Energy Management Program

For more information, visit:
energy.gov/eere/femp

DOE/EE – 1716 | Dec 2017