

# NIST SPECIAL PUBLICATION 1800-10A

---

## Protecting Information and System Integrity in Industrial Control System Environments: Cybersecurity for the Manufacturing Sector

---

### Volume A: Executive Summary

#### Michael Powell

National Cybersecurity Center of Excellence  
National Institute of Standards and Technology

#### Michael Pease

#### Keith Stouffer

#### CheeYee Tang

#### Timothy Zimmerman

Engineering Laboratory  
National Institute of Standards and  
Technology

#### Matthew Zopf

Stratavia  
Largo, Maryland

#### Joseph Brule

#### Chelsea Deane

#### John Hoyt

#### Mary Raguso

#### Aslam Sherule

#### Kangmin Zheng

The MITRE Corporation  
McLean, Virginia

FINAL

March 2022

This publication is available free of charge from

<https://doi.org/10.6028/NIST.SP.1800-10>

The first draft of this publication is available free of charge from

<https://www.nccoe.nist.gov/publications/practice-guide/protecting-information-and-system-integrity-industrial-control-system-draft>





cause damage to equipment and/or injuries to workers. Furthermore, these incidents could significantly impact productivity and raise operating costs, depending on the extent of a cyber attack.

**This practice guide can help your organization:**






- detect and prevent unauthorized software installation
- protect ICS networks from potentially harmful applications
- determine changes made to a network using change management tools
- detect unauthorized use of systems
- continuously monitor network traffic
- leverage anti-malware tools





## SOLUTION

The NCCoE, in conjunction with the NIST EL, collaborated with cybersecurity technology providers to develop and implement example solutions that demonstrate how manufacturing organizations can protect the integrity of their data from destructive malware, insider threats, and unauthorized software within manufacturing environments that rely on ICS.

The example solutions use technologies and security capabilities from the project collaborators listed in the table below. These technologies were implemented in two distinct manufacturing lab environments that emulate discrete and continuous manufacturing systems. This project takes a modular approach in demonstrating two unique builds in each of the lab environments.

The following is a list of the project’s collaborators.

Collaborator	Component
	Provides secure remote access with authentication and authorization support.
	Provides network and asset monitoring to detect behavior anomalies and modifications to hardware, firmware, and software capabilities.
	Provides network and asset monitoring to detect behavior anomalies and modifications to hardware, firmware, and software capabilities.
	Offers secure data storage on-prem.
	Provides network and asset monitoring to detect behavior anomalies and modifications to hardware, firmware, and software capabilities.

Collaborator	Component
 <b>OSIsoft.</b> <small>is now part of AVEVA</small>	Real-time data management software that enables detection of behavior anomalies and modifications to hardware, firmware, and software capabilities.
	Access control platform that secures connections and provides control mechanisms to enterprise systems for authorized users and devices; monitors activity down to the keystroke
	Provides network and asset monitoring to detect behavior anomalies and modifications to hardware, firmware, and software capabilities.
	Provides host-based application allowlisting (the blocking of unauthorized activities that have the potential to pose a harmful attack) and file integrity monitoring.

While the NCCoE used a suite of commercial products to address this challenge, this guide does not endorse these particular products, nor does it guarantee compliance with any regulatory initiatives. Your organization's information security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a solution.

## HOW TO USE THIS GUIDE

Depending on your role in your organization, you might use this guide in different ways:

**Business decision makers, including chief information security and technology officers,** can use this part of the guide, *NIST SP 1800-10A: Executive Summary*, to understand the drivers for the guide, the cybersecurity challenge we address, our approach to solving this challenge, and how the solution could benefit your organization.

**Technology, security, and privacy program managers** who are concerned with how to identify, understand, assess, and mitigate risk can use *NIST SP 1800-10B: Approach, Architecture, and Security Characteristics*. It describes what we built and why, including the risk analysis performed and the security/privacy control mappings.

**Technology professionals** who want to implement an approach like this can make use of *NIST SP 1800-10C: How-To Guides*. It provides specific product installation, configuration, and integration instructions for building the example implementation, allowing you to replicate all or parts of this project.

## SHARE YOUR FEEDBACK

You can view or download the guide at <https://www.nccoe.nist.gov/projects/use-cases/manufacturing/integrity-ics>.

Once the example implementation is developed, you can adopt this solution for your own organization. If you do, please share your experience and advice with us. We recognize that technical solutions alone

will not fully enable the benefits of our solution, so we encourage organizations to share lessons learned and best practices for transforming the processes associated with implementing this guide.

To provide comments, join the community of interest, or to learn more about the project and example implementation, contact the NCCoE at [manufacturing\\_nccoe@nist.gov](mailto:manufacturing_nccoe@nist.gov).

---

## COLLABORATORS

Collaborators participating in this project submitted their capabilities in response to an open call in the Federal Register for all sources of relevant security capabilities from academia and industry (vendors and integrators). Those respondents with relevant capabilities or product components signed a Cooperative Research and Development Agreement (CRADA) to collaborate with NIST in a consortium to build this example solution.

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia in order to acknowledge their participation in this collaboration or to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.