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

Joseph Brule*
Cyber Security Directorate
National Security Agency

Michael Pease
Keith Stouffer
CheeYee Tang
Timothy Zimmerman
Engineering Laboratory
National Institute of Standards and Technology

Chelsea Deane
John Hoyt
Mary Raguso
Aslam Sherule
Kangmin Zheng
The MITRE Corporation
McLean, Virginia

Matthew Zopf
Strativia
Largo, Maryland

*Former employee; all work for this publication done while at employer.

September 2021

DRAFT

This publication is available free of charge from
https://www.nccoe.nist.gov/projects/use-cases/manufacturing/integrity-ics

Executive Summary

Many manufacturing organizations rely on industrial control systems (ICS) to monitor and control their machinery, production lines, and other physical processes that produce goods. To stay competitive, manufacturing organizations are increasingly connecting their operational technology (OT) systems to their information technology (IT) systems to enable and expand enterprise-wide connectivity and remote access for enhanced business processes and capabilities.

Although the integration of IT and OT networks is helping manufacturers boost productivity and gain efficiencies, it has also provided malicious actors, including nation states, common criminals, and insider threats, a fertile landscape where they can exploit cybersecurity vulnerabilities to compromise the integrity of ICS and ICS data to reach their end goal. The motivations behind these attacks can range from degrading manufacturing capabilities to financial gain, to causing reputational harm.

Once malicious actors gain access, they can harm an organization by compromising data or system integrity, hold ICS and/or OT systems ransom, damage ICS machinery, or cause physical injury to workers. The statistics bear this out. The X-Force Threat Intelligence Index 2021 (ibm.com) stated that manufacturing was the second-most-attacked industry in 2020, up from eighth place in 2019.

One particular case study illustrates the long-lasting effects and damage a single cyber attack can inflict on an organization. It was reported that a global pharmaceutical manufacturer suffered a cyber attack that caused temporary production delays at a facility making a key vaccination. More than 30,000 laptop and desktop computers, along with 7,500 servers, sat idle. Although the company claimed that its operations were back to normal within six months of the incident, at this writing, news reports stated that the organization is locked in a legal battle with its insurers and is looking to reclaim expenses that include repairing its computer networks and the costs associated with interruptions to its operations. They are seeking more than $1.3 billion in damages.

To address the cybersecurity challenges facing the manufacturing sector, the National Institute of Standards and Technology's (NIST's) National Cybersecurity Center of Excellence (NCCoE) launched this project in partnership with NIST's Engineering Laboratory (EL) and cybersecurity technology providers. Together, we have built example solutions that manufacturing organizations can use to mitigate ICS integrity risks, strengthen the cybersecurity of OT systems, and protect the data that these systems process.

CHALLENGE

The manufacturing industry is critical to the economic well-being of our nation, and is constantly seeking ways to modernize its systems, boost productivity, and raise efficiency. To meet these goals, manufacturers are modernizing their OT systems by making them more interconnected and integrated with other IT systems and introducing automated methods to strengthen their overall OT asset management capabilities.

As OT and IT systems become increasingly interconnected, manufacturers have become a major target of more widespread and sophisticated cybersecurity attacks, which can disrupt these processes and

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 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
DISPEL	Provides secure remote access with authentication and authorization support.
DRAGOS	Provides network and asset monitoring to detect behavior anomalies and modifications to hardware, firmware, and software capabilities.
FORESCOUT	Provides network and asset monitoring to detect behavior anomalies and modifications to hardware, firmware, and software capabilities.
GreenTec™ www.GreenTec-USA.com	Offers secure data storage on-prem.
Microsoft	Provides network and asset monitoring to detect behavior anomalies and modifications to hardware, firmware, and software capabilities.
OSIsoft. is now part of AVEVA	Real-time data management software that enables detection of behavior anomalies and modifications to hardware, firmware, and software capabilities.

Collaborator	Component
tdi technologies	Access control platform that secures connections and provides control mechanisms to enterprise systems for authorized users and devices; monitors activity down to the keystroke
tenable	Provides network and asset monitoring to detect behavior anomalies and modifications to hardware, firmware, and software capabilities.
vmware	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.

IT 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 preliminary draft guide at https://www.nccoe.nist.gov/projects/use-cases/manufacturing/integrity-ics. Help the NCCoE make this guide better by sharing your thoughts with us. There will be at least 45 additional days for the comment period for this guide.

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.

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.