AUTOMATION 2021

VOLUME 2

OT/ICS Cybersecurity

- Closing IoT Security Gaps in the ICS
- Secure Edge Computing, Warehouse to Enterprise
- Open Secure Remote Operations
- Secure ICSs with Configuration Control
- And Much More

AUTOMATION.COM | ISA A subsidiary of the International Society of Automation

Introduction

AUTOMATION 2021 VOL 2

OT/ICS Cybersecurity

The future is here when it comes to connected plants, smart factories, and Industry 4.0/Industrial Internet of Things (IIoT) technologies, but securing today's industrial control system (ICS) networks is no small thing. Operational technology (OT) systems are very different from the automation networks of 10 years ago, and while the many IT systems and IIoT devices bring huge benefits to critical infrastructure and industrial organizations, they also bring new cybersecurity challenges. This edition of AUTOMATION 2021 shows you strategies and solutions for securing OT/ICS networks. Discover a useful security framework that presents information in matrices arranged by attack stages, how to use a risk assessment to start securing OT systems, and even how better management of code and configuration changes can reduce risk. Case studies examine how great strides in productivity and cost control in the oil and gas industry can be achieved with cloud computing and secure open technology platforms, as well as how edge programmable industrial controllers can work with connectivity options like OPC UA and secure gateway server functions to create secure automated packaging lines.

Renee Bassett
Chief Editor

SPONSORS

NOZOMI NETWORKS

OPTO 22
The Future of Automation.

1898 & CO.
PART OF BURNS & McDONNELL

BEDROCK®
OPEN SECURE AUTOMATION

tenable

ISA GLOBAL CYBERSECURITY ALLIANCE

About AUTOMATION 2021

The AUTOMATION 2021 ebook series covers Industry 4.0, smart manufacturing, IIoT, cybersecurity, connectivity, machine and process control and more for industrial automation, process control and instrumentation professionals. To subscribe to ebooks and newsletters, visit: www.automation.com/newslettersubscription.

AUTOMATION 2021 is published six times per year (February, April, June, August, October, December) by Automation.com, a subsidiary of ISA—the International Society of Automation. To advertise, visit: www.automation.com/en-us/advertise.

AUTOMATION.COM

groups/68581

automationdotcom

automation_com

ISA International Society of Automation
Setting the Standard for Automation™

groups/137598

InternationalSocietyOfAutomation

ISA_Interchange

Renee Bassett, Chief Editor
rbassett@automation.com

Chris Nelson, Advertising Sales Rep
chris@automation.com

Richard T. Simpson, Advertising Sales Rep
rsimpson@automation.com

Gina DiFrancesco, Inside Account Manager
GDiFrancesco@automation.com

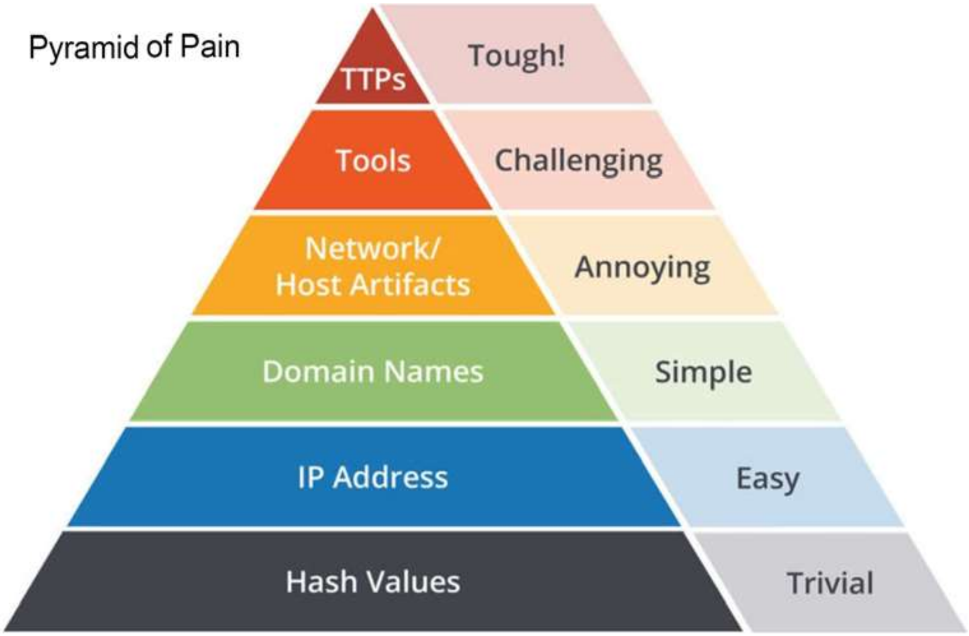
Cybersecurity Using ICS ATT&CK Strategies

By Jacob Chapman, Grantek

Protect smart manufacturing and IIoT systems using a security framework that presents information in matrices arranged by attack stages.

Risk assessments and mitigation are commonplace activities in the manufacturing environment, but as the number and type of cyberattacks increase in all industries, and connectivity continues to increase between information technology (IT) and operational technology (OT), it is necessary to take a practical, targeted approach to cybersecurity risk management of smart manufacturing and Industrial Internet of Things (IIoT) systems. The industrial control system (ICS) adversarial tactics, techniques, and common knowledge (ATT&CK) framework presents the information in matrices arranged by attack stages, from initial system access to data theft or machine control.

The tactics, techniques, and procedures (TTPs) describe patterns of activities associated with a specific threat actor or group of threat actors. By using the ATT&CK framework within a risk assessment process, organizations can identify risks and associate them to TTPs that adversaries are actually using today. This, in turn, helps identify the specific changes that can be made to the systems and network environment to disrupt those attacks and significantly reduce the OT environment's risk level.



Source: David J. Blanco, personal blog

The MITRE Corporation's federally funded cybersecurity R&D center helps to provide the nation's business infrastructure with effective and practical cybersecurity architectures and solutions. The ICS ATT&CK matrix is a knowledge base of adversary actions that focuses on adversaries whose goal is disrupting ICS. This open-sourced/community-driven knowledge base is accessible at https://collaborate.mitre.org/attackics/index.php/Main_Page.

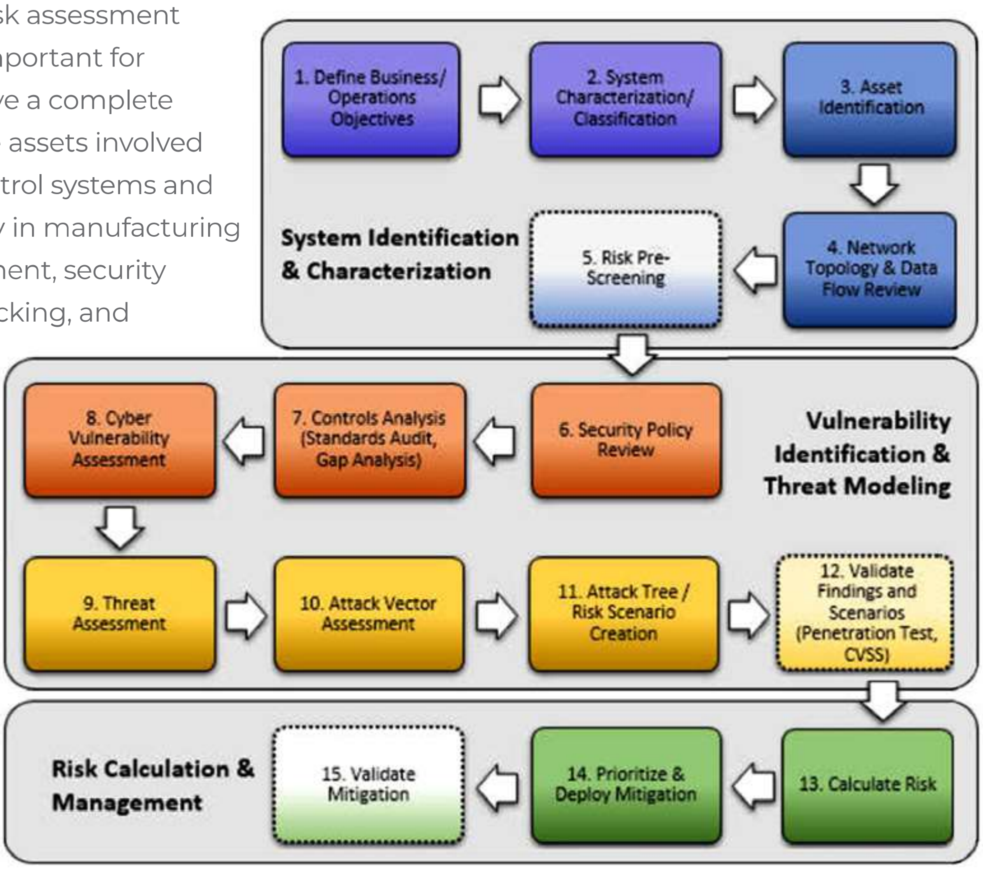
In the ICS ATT&CK matrix, disruptive tactics are mapped against mitigation techniques to give manufacturers practical actions to help prevent each type of threat. Information is also provided about adversary groups. Experts should know how to use the ATT&CK framework to create a roadmap that prioritizes mitigating the largest risks to an organization's smart manufacturing and IIoT systems.

Applying ATT&CK to risk management

Applying ICS ATT&CK to risk management involves identifying cybersecurity risks, determining the potential effect and likelihood of risk occurrence, and then determining the best way to deal with each risk with the resources available. Assessing this information helps manufacturers deploy the most efficient, cost-effective risk control and mitigation strategy and controls in a targeted way to reduce the most likely or highest-impact cybersecurity risks first.

In the typical risk assessment methodology, an estimate of risk probability is required. Unfortunately, there is no simple yet consistently accurate way to measure probability (likelihood of risk occurrence). Rather than relying on elaborate mathematical models or falling back on a guesstimate approach, ICS ATT&CK is a more practical approach. Some aspects of this include looking at localized data relevant to the specific environment. Risk assessment is more about prioritization than probability, so it is important to evaluate local attack vectors. It is also important to use facts and measurable data applicable to the facility's configuration and assets to estimate business impact rather than guessing or generalizing. Understanding the impact of a risk occurrence is more critical than its probability.

However, for a risk assessment to be effective, it is important for manufacturers to have a complete understanding of the assets involved in their industrial control systems and the network topology in manufacturing areas. Legacy equipment, security patches applied or lacking, and connectivity to business systems with more threat exposure must all be considered when evaluating cybersecurity risk. Typical steps involved with threat modeling and risk management are shown in the diagram.

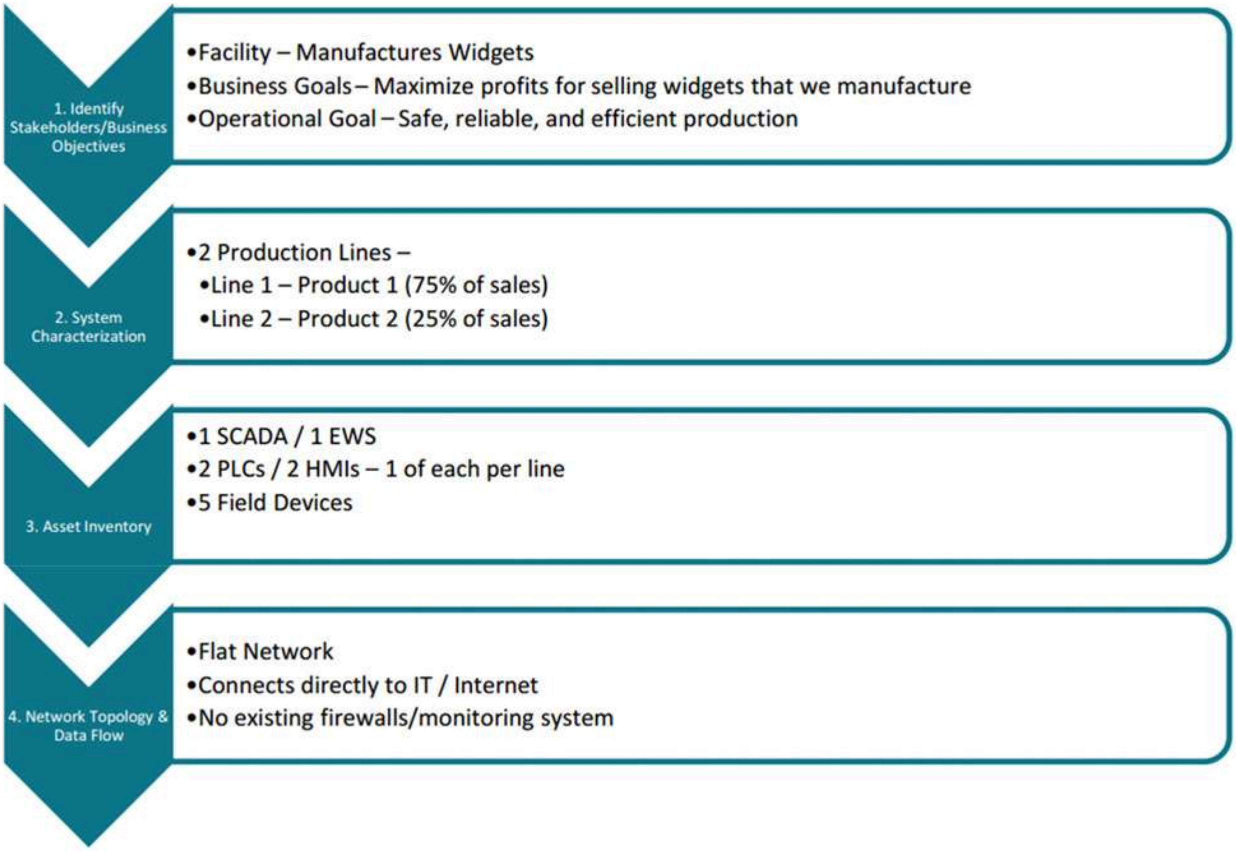

1. Define Business/ Operations Objectives
2. System Characterization/ Classification
3. Asset Identification
4. Network Topology & Data Flow Review
5. Risk Pre-Screening
System Identification & Characterization
6. Security Policy Review
7. Controls Analysis (Standards Audit, Gap Analysis)
8. Cyber Vulnerability Assessment
Vulnerability Identification & Threat Modeling
9. Threat Assessment
10. Attack Vector Assessment
11. Attack Tree / Risk Scenario Creation
12. Validate Findings and Scenarios (Penetration Test, CVSS)
13. Calculate Risk
14. Prioritize & Deploy Mitigation
15. Validate Mitigation
Risk Calculation & Management

Practical approaches to preventing cyberattack

The use cases of the ICS ATT&CK model assume that a breach will occur; thus planning and performing preventive maintenance is required to fortify an enterprise's perimeter and internal network to mitigate an attack. Proactive maintenance is always less costly than reacting after the fact, when time is of the essence and additional action may be needed to undo the damage caused by an intrusion. Risk assessment typically consists of three phases.

Phase 1 – Gather information on systems environment

System owners should evaluate the smart manufacturing and IIoT system assets as well as the ICS environment as a whole, including links to networks outside of manufacturing; software/firmware installed on each workstation, controller, or other equipment; and user permissions, with consideration for other factors such as corporate expansion plans or equipment upgrades. The following is an example presenting simplified findings of phase 1.



1. Identify Stakeholders/Business Objectives

- •Facility – Manufactures Widgets
- •Business Goals – Maximize profits for selling widgets that we manufacture
- •Operational Goal – Safe, reliable, and efficient production

2. System Characterization

- •2 Production Lines –
  - •Line 1 – Product 1 (75% of sales)
  - •Line 2 – Product 2 (25% of sales)

3. Asset Inventory

- •1 SCADA / 1 EWS
- •2 PLCs / 2 HMIs – 1 of each per line
- •5 Field Devices

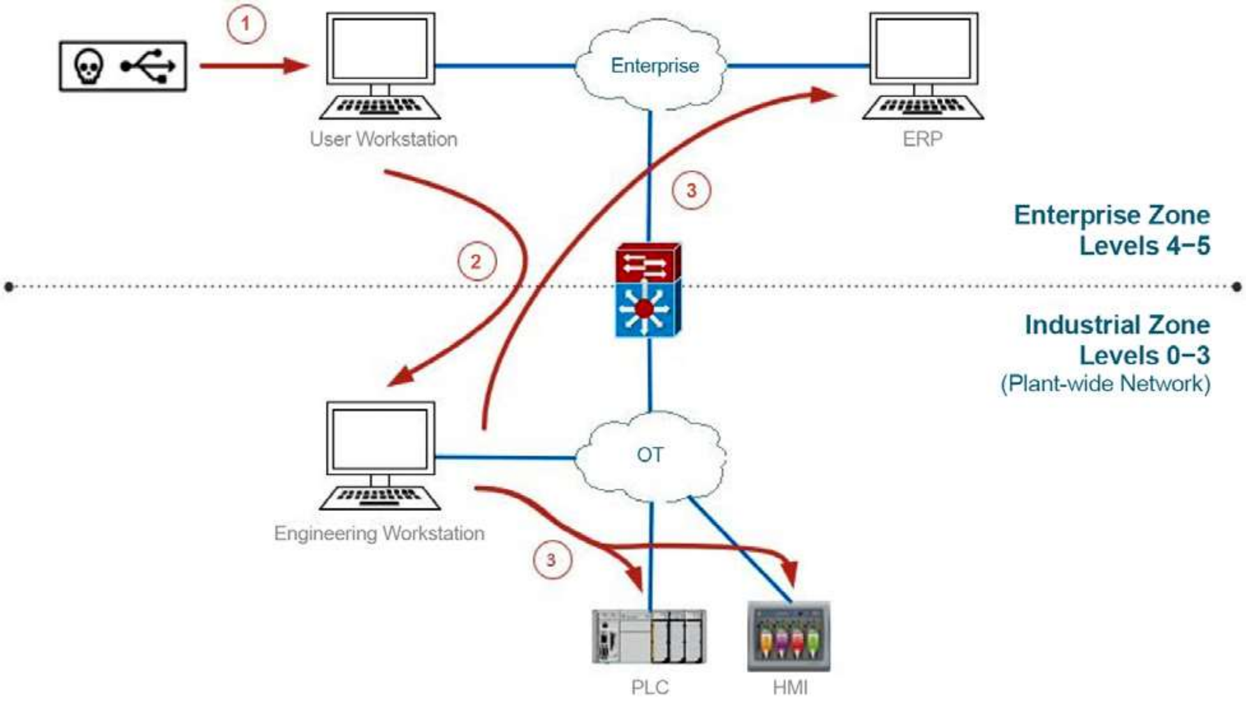
4. Network Topology & Data Flow

- •Flat Network
- •Connects directly to IT / Internet
- •No existing firewalls/monitoring system

Phase 2 – Create IIoT system attack tree using ICS ATT&CK framework

Define the risks for each piece of equipment and identify and prioritize appropriate mitigation techniques. For example, the figure below reflects an insecure network architecture with no security policies between the IT/OT zone and no industrial demilitarized zone (IDMZ). After analyzing the network, one attack tree may be a malicious USB connected at the enterprise network. Based on the flat network topology, the USB installs malware with the intent of gaining remote access to an engineering workstation (EWS). Once remote access is gained to the EWS, the adversary can use the manufacturing execution system (MES) software already installed to impair the facility's process or attack the business' ERP system.

Example of insecure network topology allowing malware spread between IT and OT

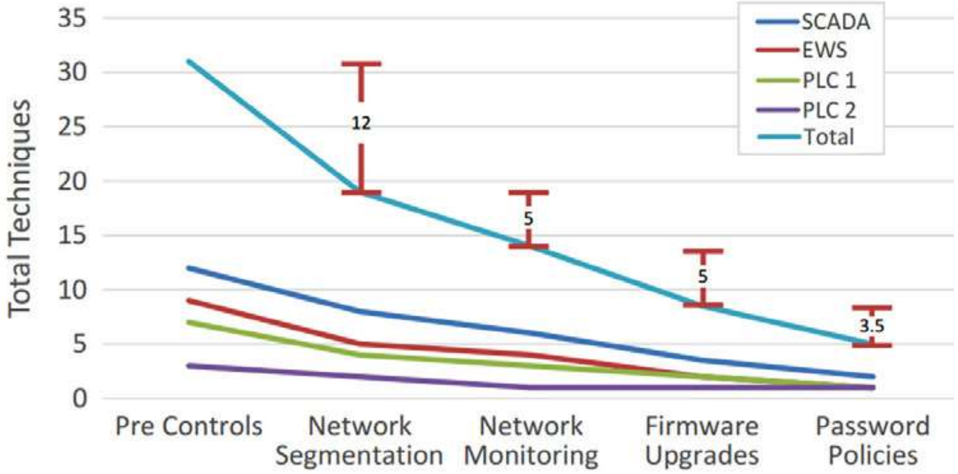


Phase 3 – Plan creation

Based on the findings of phases 1 and 2, ICS cybersecurity practitioners can calculate asset risk and identify the cybersecurity gaps that may allow unwanted adversarial activity. Using this information, they can create roadmaps prioritizing these risks while also visually modeling risk mitigation once these risk mitigation activities have been performed.

Technique Count Reduction

1. **Network Segmentation**
2. **Network Monitoring**
3. **Firmware Upgrades**
4. **Password Policies**



Realizing efficiencies

Many times, system owners have the opportunity to implement security enhancements in conjunction with other activities requiring planned system downtime. This minimizes the impact on production and of course is preferable to an unplanned shutdown caused by a cyberattack.

By incorporating security enhancements at the same time as system design changes, the security aspects of the system can be validated along with the rest of the system. System owners can also help ensure that any system expansions or improvements are planned and designed with cyberattack prevention in mind via defining minimum security requirements across the enterprise.

Enterprise-level considerations

Most security breaches are the result of intrusions or malicious attacks on the corporate side of the enterprise. In the past, networked manufacturing systems and equipment were separate from the rest of the enterprise and the outside world, and only communicated with each other. But in recent years, with the advent of smart manufacturing and IIoT systems such as MES, digital twins, and overall equipment effectiveness implementations, there is greater connectivity between the enterprise network and the manufacturing network. Though this improves efficiency and allows for better planning, it also allows more opportunities for intrusions, malware, and successful phishing attacks, and allows malware to spread to the production floor with potentially catastrophic results. A critical component for managing this connectivity is an industrial demilitarized zone to carefully control traffic between the industrial and enterprise zones.

The rapid adoption of the IIoT also has the potential to allow intrusion, as more and more devices are networked, often with inconsistent implementation without enough security measures. As the IIoT is increasingly adopted, it will increase the vulnerability of the control system network if robust security practices are not rigorously followed. Cloud-based tools and systems also pose new risks that increase the attack surface.

When a system owner performs a risk assessment and mitigation plan using the ATT&CK model, system assets should be classified based on criticality, not only from a manufacturing process perspective, but also from the perspective of the potential environmental, safety, and regulatory impacts from a security breach. For smart manufacturing and IIoT system breaches, which affect both the IT and OT environments, the stakes are higher.

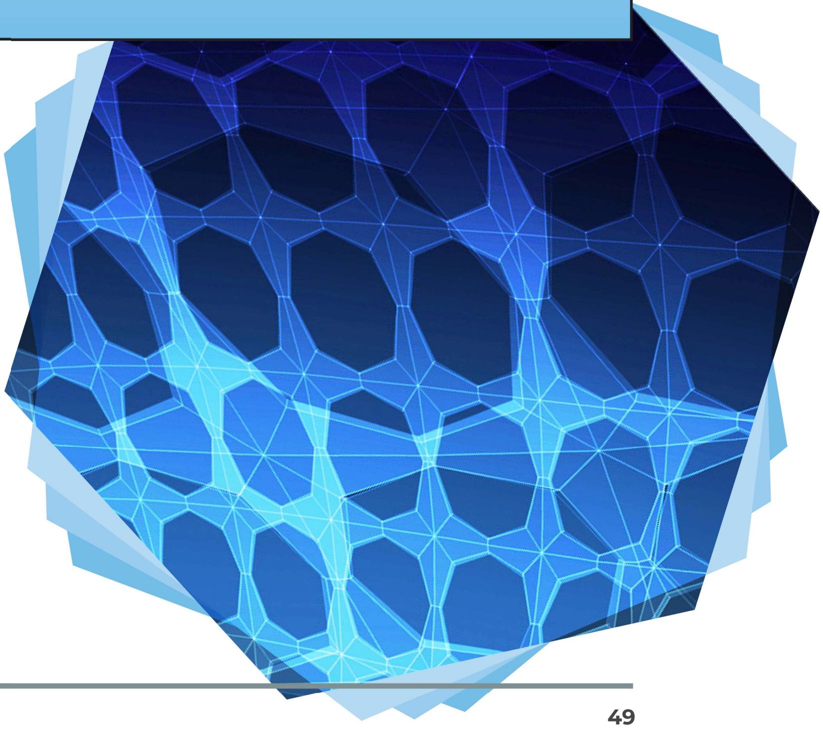
The ICS ATT&CK model is not a standard but provides a framework of known activities attempted by cybersecurity adversaries. It defines how adversaries have successfully attacked ICS such as smart manufacturing and IIoT systems and provides the mitigation steps to take for each type of known attack. System owners can then line up the mitigations with the standards applicable to each area for an industry-compliant mitigation. Approaches may be guided by closely following ISA-99 and IEC 62433.

What's coming next for defending IIoT systems?

MITRE ATT&CK provides an effective approach to understand risk and prioritize the security controls to protect smart manufacturing and IIoT systems. Baked into the framework are TTPs that can be applied to IIoT systems, such as initial access through Internet-accessible devices, execution through API, and exploitation of remote services. However, smart manufacturing and IIoT systems still pose unique challenges compared to traditional ICS security.

Webinar: Industrial IT & Cybersecurity Strategies for IT/OT Convergence

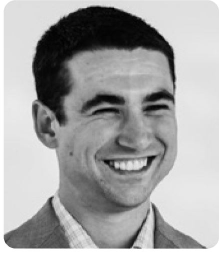
Technologies that make up a company's industrial operations are evolving faster than ever—and, in fact, they're accelerating. At the same time, research against Acatech's Industrie 4.0 Maturity Index shows that connectivity is the leading challenge holding back adoption of useful new industrial tech. That begs the question, how do we develop our Industrial IT infrastructure in order to prepare the organization for the future? And how should skyrocketing ICS Cybersecurity risks be factored into the equation? Jacob Chapman, Grantek's Director of Industrial IT & Cybersecurity, presented a webinar in conjunction with ISA - The International Society of Automation, that tackles these questions. It is available on demand. "Industrial IT & Cybersecurity Strategies for IT/OT Convergence" provides insights and real-world examples for manufacturers looking to grow their Industrial IT layer while also reducing their cybersecurity risk.



For this reason, experts and standard bodies are exploring ways to provide guidance for applying cybersecurity standards to these systems. For example, ISA99 recently communicated preliminary plans for adding standards to the IEC 62443 series dedicated to IIoT. In the future, we may see a consensus-driven answer to the question of how to apply cybersecurity standards to these systems.

MITRE is also exploring modifications to its framework to address the IT-OT combination of technologies that comprise smart manufacturing and IIoT systems. For example, articles and discussion are being had regarding a hybrid ATT&CK matrix visualization that combines ATT&CK for ICS and represents the IT portions of ICS attacks in ATT&CK for Enterprise. Should a hybrid matrix provide value in tracking attack pathways and effective mitigation measures it could become an improved approach for applying ATT&CK to smart manufacturing and IIoT systems.

ABOUT THE AUTHOR



Jacob Chapman has a background in automation engineering, project management, account management, industrial networking, and ICS cybersecurity expertise within the food and beverage, pharmaceutical, and energy generation sectors, among others. Chapman currently leads the industrial IT and cybersecurity solutions and services at Grantek, which helps manufacturers develop their facility infrastructures, including their industrial network architectures, local and cloud computing systems, and cybersecurity programs.

As Grantek's leader in the space, Chapman maintains involvement and leadership positions in international societies and standard bodies, including the Cybersecurity Committee chair of the ISA's Smart Manufacturing & IIoT Division, a registered U.S. expert to TC65 of the IEC, and a member of the ISA99 standards development committee.