Threats to Manufacturing Operational Technology

Critical Infrastructure (CI) | Fusion (FS)

April 20, 2022 09:19:26 PM, 22-00010505, Version: 1.0

Executive Summary

- Like many critical infrastructure (CI) sectors, manufacturing is an essential part of society. It provides goods to all other CI sectors. Disruptions in the manufacturing process can have long-term negative effects on a county's economy and peoples' lifestyle, leading to the importance of cyber security defenses to protect the operational technology (OT) systems of these facilities.
- Manufacturing systems face several security challenges similar to other CI industries, including outdated hardware/software, unsecured remote access, assets vulnerable to cyberattack, and common lack of security resources and knowledge.
- Asset owners should prioritize security strategies that thwart financially motivated crime as commodity-type attacks (e.g., ransomware) against utilities continue to be an enticing tactic for threat actors. Additionally, despite the relative low likelihood of a disruptive, physically destructive, or physically harmful cyberattack, asset owners should take precautions to prevent and mitigate these threats, given the potentially significant impact.

Threat Detail

Like many critical infrastructure (CI) sectors, manufacturing is an essential part of society. It provides goods to all other CI sectors, including transformers and protective relays for the energy sector, car parts and gasoline for transportation, valves and pipes for oil and natural gas, etc. While disruptions in manufacturing and the supply chain might not result in immediate negative impact, it can have long-term negative effects on a county's economy and peoples' lifestyle, reenforcing the importance of cyber security defenses to protect the operational technology (OT) systems of these facilities. This is especially true with the increased levels of automation and remote capabilities being introduced into manufacturing processes. This report summarizes a variety of potential cyber threats to OT networks in manufacturing facilities.

Manufacturing Reference Architecture

Manufacturing is the process of converting raw materials into finished goods, which are then shipped to various consumers. This includes smart phones, car doors, vaccines, computer processors, fire alarms, paint, etc.

While there are various types of manufacturing processes, the primary types are discrete and process manufacturing.

- Discrete manufacturing refers to the production of individual units constructed by assembling various parts and components together. This is the type of manufacturing that people are often most familiar with and produces a variety of solid-based products such as cars, furniture, and books.
- Process manufacturing refers to the production of a product by combining raw materials using a specific recipe and is often liquid-based and completed in large batches. This includes paints, gasoline, beverages, pharmaceuticals, etc.
- Other types of manufacturing include:
  - Repetitive manufacturing
  - Job Shop manufacturing
  - Batch manufacturing
  - Continuous manufacturing
  - Additive manufacturing

While the factory floor varies between manufacturing organizations to fit the needs of the produced product, many of them use similar equipment and processes. Key components of a manufacturing OT system can include:

- Industrial machines
  - Used in various places of the production process. This includes boring, cutting, drilling, turning, conveyor belts, and milling tools.
- Industrial robots
  - These assets are often mechanical "arms" that can automate a variety of repetitive tasks, such as handling product during manufacturing, loading pallets, cutting, welding, etc.
  - Some manufacturing plants are also incorporating autonomous robots into the factory floor, including self-driving drones and forklifts.
- Safety Instrumented Systems (SIS)
  - As manufacturing organizations often work with hazardous materials, large machinery, and dangerous situations, SIS help ensure that the process is operating appropriately and does not enter dangerous conditions.

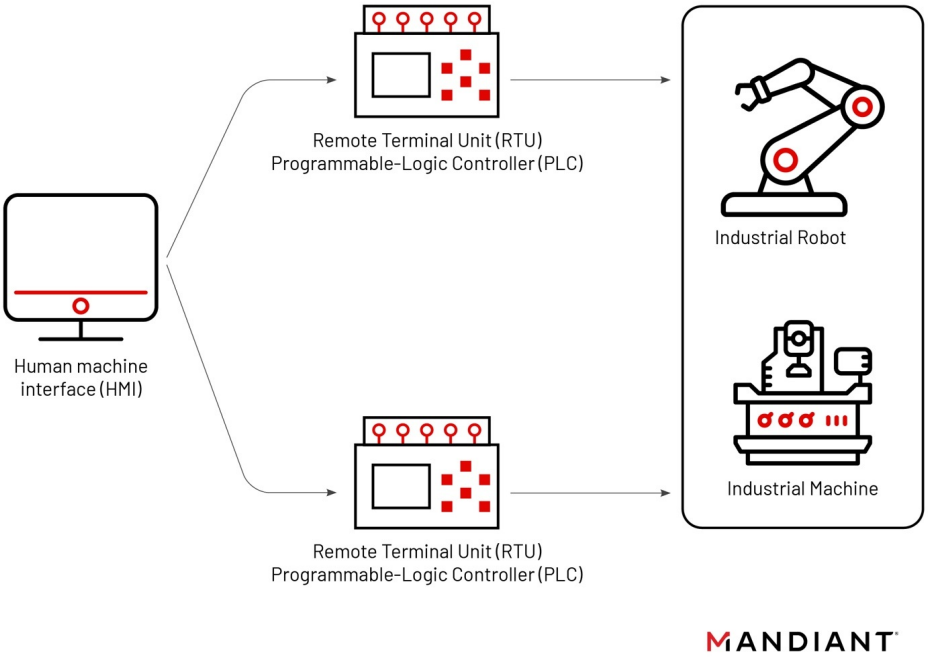

Figure 1: A simple network diagram of a manufacturing OT process

Attack Surface of Manufacturing Organizations

As the manufacturing sector includes a wide variety of products and processes, the attack surface can be quite broad, with the different facilities facing unique cyber security hurdles. However, there are also general threats that most manufacturing organizations face. These include unsecured remote access, attacks on industrial robots, and legacy devices, to name a few. While this report will not cover all attack vectors to unique facilities, we will examine common cyber threats manufacturing organizations may encounter.

- In December 2021, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) released an advisory warning of an increased risk of cyberattack against manufacturing organizations.
  - CISA reported that due to the COVID-19 pandemic, more manufacturing organizations have begun to use robotic process automation (RPA), which automates the controlled process and is managed by remote operators.
  - CISA warns that improper implementation of RPA can increase the organization's cyberattack surface due to poor network segmentation and a lack of proper cyber defenses (e.g., encryption and authentication).
- In manufacturing, data is often shared across a variety of physical production processes and business applications to facilitate demand-driven production. This could result in manufacturing organizations having more remote access for business reasons, which can broaden the sector's attack surface.
- Manufacturing organizations are also often privately owned versus government supported and operated. This can potentially result in a lack of security standards and regulations that are often more enforced in government operated facilities.
- For more information on threat actor interest in the manufacturing sector, see Industry Snapshot: Manufacturing (Q1 2022).

Industrial Robot Threats

In 2017, Trend Micro published the results of a collaboration project between its Forward-Looking Threat Research Team and Politecnico di Milano (POLIMI), examining the cyber security of industrial robots (17-00005266). The report examines five possible attack scenarios targeting industrial robots, resulting in either defective products, damages to assets, or risk of operator injury.

- IOActive also published a high-level report of robot security in 2017 describing a wide variety of issues discovered in robots from six vendors.
- While we have not observed threat actors target collaborative robots as part of their operations in the wild, threat actors have demonstrated a willingness to target organizations' industrial control systems (ICS) with the intent of physical degradation. For additional information on potential threats to industrial robots see Mandiant's Cyber Threats from Emerging Tech: Collaborative Robots.

Attack Class and Description	Concrete Effects	Requirements Violated
Attack 1: Altering the Control-Loop Parameters The attacker alters the control system so the robot moves unexpectedly or inaccurately.	Defective or modified products	Safety Integrity Accuracy
Attack 2: Tampering with Calibration Parameters The attacker changes the calibration to make the robot move unexpectedly or inaccurately.	Robot damages	Safety Integrity Accuracy
Attack 3: Tampering with the Production Logic The attacker manipulates the program executed by the robot to stealthily introduce a flaw into the workpiece.	Defective or modified products	Safety Integrity Accuracy
Attack 4: Altering the User-Perceived Robot State The attacker manipulates the status information so the operator is not aware of the true status of the robot.	Operator injuries	Safety
Attack 5: Altering the Robot State The attacker manipulates the true robot status so the operator loses control or can get injured.	Operator injuries	Safety

Figure 2: Trend Micro's description of attacks against industrial robots

Legacy Devices

Similar to other CI sectors, manufacturing organizations rely on equipment with lifecycles much longer than those of IT systems. Legacy devices represent a challenge given that they normally remain unpatched and are increasingly exposed to vulnerabilities over time.

- The low bandwidth of control devices used for manufacturing makes it difficult to apply additional security mechanisms such as authentication or data encryption.
- Legacy systems are often unpatched and not updated. This can be due to the downtime required to install the updates or that the system does not meet the required specifications to handle the update.

ICS Vulnerabilities

In 2021, the critical manufacturing sector had the highest number of ICS-specific vulnerability disclosures with 218 vulnerabilities (22-00001323).

- This is likely due to the fact that manufacturing, by nature, is a broad industry, providing a wide variety of products to various customers. This results in manufacturing also using a wide variety of devices and assets, increasing the sector's vulnerability threat landscape.

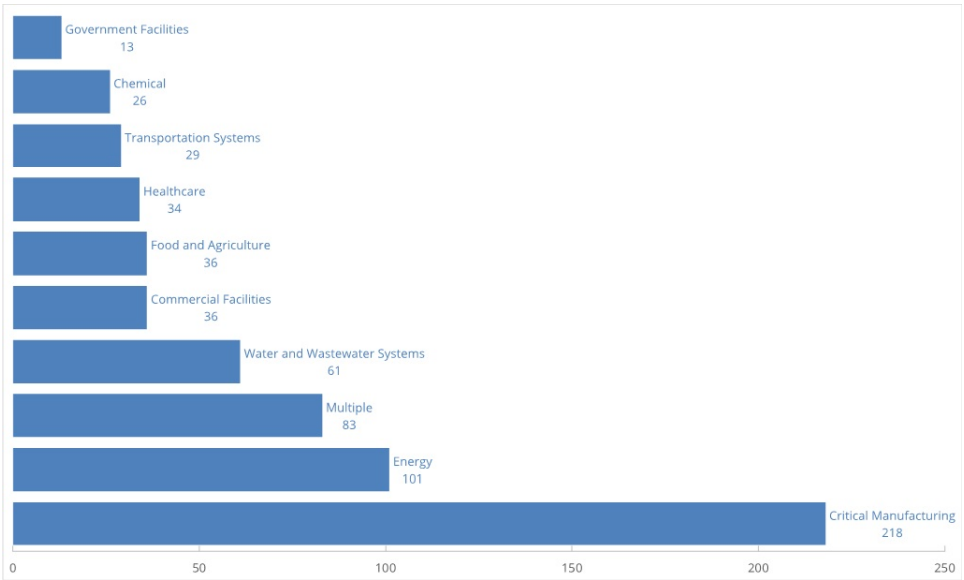

Figure 3: Top 10 affected industries by sector of ICS-specific vulnerabilities in 2021

Types of Attacks

Commodity Attacks

Commodity attacks are incidents where interfering with the OT process was not the primary goal of the threat actor.

These types of attacks are often financially motivated and include ransomware and cryptomining infections. While the incidents often do not target cyber physical processes, they can have direct and indirect effects on the processes by denying operators access to the process or taking necessary processing power away from a critical function.

- Since at least late 2019, there have been at least 652 cases of ransomware operators publishing stolen victim data in addition to encrypting victim files for critical manufacturing organizations, which as an industry also experienced the highest number of incidents (21-00011904). However, this may reflect the high number of organizations in the manufacturing sector as compared to other industries, as opposed to attacker interest in this sector.

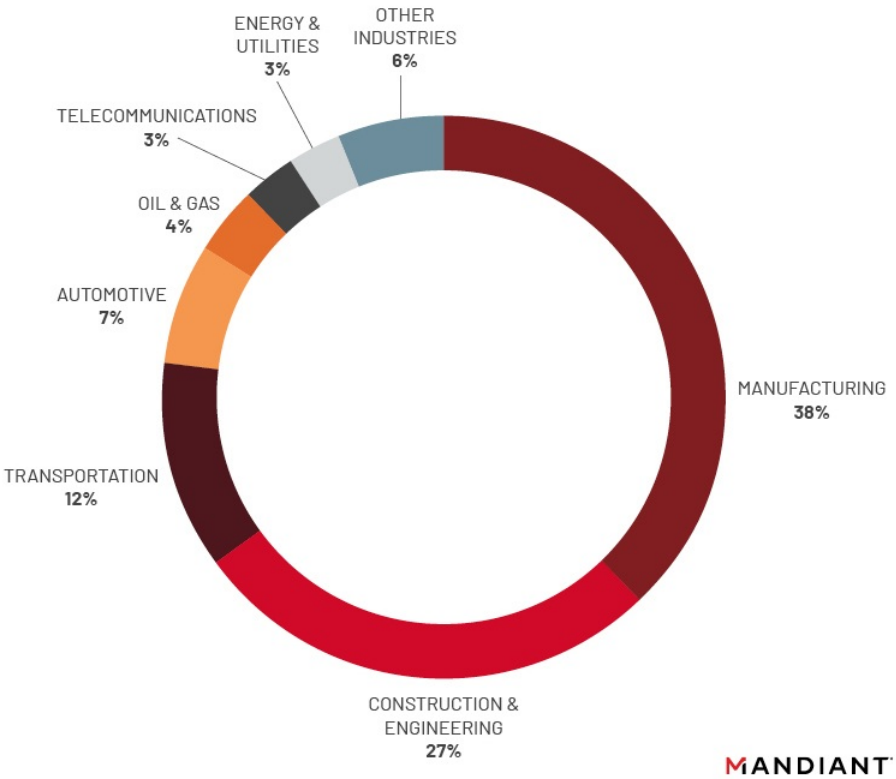

Figure 4: Victims appearing on extortion sites by industry between 2020–2021

- Manufacturing organizations can be prime targets for, and victims of, supply chain attacks. As manufacturing organizations provide goods to a variety of other sectors and companies, threat actors may target manufacturing organizations as a step toward their intended final target (18-00016598).
- Manufacturing organizations can also be targets for intellectual property theft as threat actors attempt to steal the recipes or processes used to produce the final product. While this type of threat is primarily IT-based, OT documentation would be a valuable target (20-00007004, 21-00016375).

Attacks on Manufacturing Processes

Targeting the OT processes of a manufacturing plant could sabotage the finished product, delay the delivery of product to consumers, and create a dangerous environment for engineers and operators.

- An attacker could sabotage the finished product by slightly altering the automated process. For example, a threat actor could slightly alter the trajectory of an industrial robot in charge of welding, possibly compromising the integrity of the finished product due to the weld not happening correctly.
- A threat actor could target the SIS of a manufacturing plant with the aim of disabling the safety systems, which could impede any alarms or corrective actions should the system enter dangerous conditions. The TRITON malware is an example of this type of attack (18-00009388).
- INCONTROLLER is another example of malware that could be used against manufacturing facilities (22-00008528). While the malware was not designed to specifically target manufacturing plants, the targeted equipment is used in manufacturing systems. INCONTROLLER could impact a manufacturing victim in several different scenarios (Figure 5).

Figure 5: INCONTROLLER attack scenarios

Outlook and Implications

Asset owners should prioritize security strategies that thwart financially motivated crime as commodity-type attacks against utilities continue to be an enticing tactic for threat actors. Additionally, despite the relative low likelihood of a disruptive, physically destructive, or physically harmful cyberattack, asset owners should take precautions to prevent these threats from occurring, given the potentially significant impact.

Specific mitigations and protections include:

- Raise employee awareness of cyber security.
  - Training employees to be aware of cyber security issues in general is effective mitigation that does not require a lot of money. Untrained employees are one of the largest security risks by either allowing cyber threats into the network or by not recognizing cyber threats after they are on the network.
- Employ strict access control policies for current and ex-employees.
- Apply application allow listing, particularly on intermediary systems.
- Embrace consistent encrypted back-up routines (cloud, offsite, local).
  - Test the back-up files to ensure they function correctly.
  - Store back-up configuration files separately so that if the most current system backup fails, the configuration files can still be used to bring an older system backup to operating condition.
- Conduct frequent asset inventories of OT systems and replace devices and equipment that fail to meet security standards.
- Isolate or "air gap" OT networks whenever feasible.
- Layer multiple security controls on top of common attack vectors.
- Deploy practical, network-wide firmware/software patching solutions.
- Use manufacturing information sharing programs.
- Implement regular penetration testing.

Please rate this product by taking a short four question survey

First Version Publish Date

April 20, 2022 09:19:26 PM

Threat Intelligence Tags

Affected Industries

- Manufacturing

Affected Systems

- Control Systems and Applications
- Equipment Under Control
- Operations Management
- Safety Protection
- Regulatory and Supervisory Control

- Communication Infrastructure
- Industrial Network Protocols
- Industrial Internet of Things

Version Information

Version:1.0, April 20, 2022 09:19:26 PM

MANDIANT ADVANTAGE