Securing Technology and Equipment (Operational Technology) Used for Medical Product Manufacturing

Issued by the

Office of Regulatory and Emerging Science
Office of the Chief Scientist

U.S. Food and Drug Administration

U.S. Department of Health and Human Services

June 2025

Executive Summary

The U.S. government has exerted significant effort to maintain and improve the nation's cybersecurity since the launch of the Comprehensive National Cybersecurity Initiative in 2008[2-5]. Data breaches, cyber incidents, and ransomware attacks on hospital systems, medical clinics, and U.S. industries have become pervasive in recent years, accelerating government and private sector work to mitigate vulnerabilities [7-16]. As these threats increase, manufacturing and supply chain attacks have the potential for even greater harm to patients, medical advancement, and public health security. The Department of Health and Human Services and FDA have particularly focused on cybersecurity for medical products, the U.S. healthcare infrastructure, and the public health supply chain in general (including manufacturing and shipping [6]).

Manufacturing infrastructure can be particularly vulnerable with connected devices, Industrial Internet of Things (IIoT), and smart technologies becoming more ubiquitous. These connected technologies, considered Operational Technologies (OT), have historically been designed to prioritize consistent functionality over cybersecurity. Consequently, it is sometimes difficult to tell what, when, and where communications are happening which has the potential to increase the risk of a cybersecurity incident.

To secure an industrial network, it is important to obtain visibility. Some connected hardware modules are embedded within other equipment and may be hidden from the end user. Once all devices are fully understood, they can be logically arranged on the network to maximize infrastructure security. Implementing zone and conduit architecture with three tiers (presentation, application, and data) greatly improves network security and overall network performance compared to a flat network where all devices share the same bandwidth.

Using its manufacturing and cybersecurity expertise, the FDA has integrated demonstration manufacturing lines including manufacturing execution, operations, and lifecycle management software which has allowed FDA to create a case study for a digitally integrated manufacturing system. In accordance with standard IT policies and procedures, this OT implementation followed the National Institute of Standards and Technology (NIST) Federal Information Product Standards (FIPS), Cybersecurity & Infrastructure Security Agency (CISA) guidelines, and strict network routing requirements. Unfortunately, many Commercial Off-the-Shelf (COTS) products may not natively comply with these security requirements and may need reconfiguration. Until these guidelines are industry standard practice, considerable vulnerabilities may be inherent in many OT configurations.

The FDA's recent experience provides an opportunity to identify potential considerations, vulnerabilities, and risks when implementing and securing network-enabled and smart operational technologies. These considerations fall into three categories: Technical Information Exchange, Security Standards and Compliance, and Security by Design.

There is a balance to be struck between creating an operational environment that is easy to use and one that secures operations against as many threats as possible. Overemphasizing either security or ease of use can have serious ramifications to public health, patient access to care, availability of cutting-edge products, and pandemic preparedness. Much like a quality assurance program, a strong cybersecurity process is one of the pillars that support the safe, effective, and reliable production of medical products.

Introduction

FDA regulates over $3.6 trillion worth of food, tobacco, and medical products or 21 cents of every $1.00 spent by US consumers[1]. As such, it is critical to the FDA's public health mission to help ensure reliable supplies of high quality, safe and effective medical products are available to U.S. patients and a safe and healthy food supply is available to U.S. consumers. The ability of the U.S. to respond to public health emergencies, pandemics, and other threats, hinges on continued access to essential medical products. Consequently, if the cybersecurity of manufacturers or other supply chain participants are compromised, it could drastically affect the health of thousands or millions of patients and consumers.

Advancements in design and manufacturing technologies across medical industries allow the development of more sophisticated products, create more efficient processes, reduce waste, and improve supply chain resilience. Concurrently, the same advancements are connecting, digitizing, and automating manufacturing. All connected industrial pieces of equipment, devices, and technologies that make up a production facility are considered "operational technology." As such, operational technology (OT) has become a strategic enabler to increase domestic manufacturing and supply chain resilience. However, adding new technologies and retrofitting old equipment can introduce new vulnerabilities, therefore, securing OT has become a high priority for both public and private sectors. Since the launch of the Comprehensive National Cybersecurity Initiative in 2008, the U.S. government has increased its efforts to maintain and improve the nation's cybersecurity[2-5]. In recent years, the Department of Health and Human Services, including FDA, has particularly focused on cybersecurity for medical products, the U.S. healthcare infrastructure, and the public health supply chain (including manufacturing and shipping [6]).

Manufacturing infrastructure can be particularly vulnerable to cyber incursions or corporate espionage as the use of connected equipment, components of the Industrial Internet of Things (IIoT), and other smart technologies becomes more ubiquitous. In addition, each of these pieces of equipment may contain components from multiple manufacturers, each of which may in turn have their own cybersecurity risk profiles. Updating or changing manufacturing equipment or software may mitigate some of these risks, but it can be hard for manufacturers to determine what to update. In regulated industries, such as medical products, manufacturing processes are validated by the manufacturer and reviewed by FDA to ensure they are capable of manufacturing safe, effective, and high-quality products. Additionally, FDA regulatory frameworks include requirements for updating equipment or processes when issues such as cybersecurity vulnerabilities are discovered, however business needs, lack of visibility into software, or other conditions can delay a manufacturer from updating their software and equipment.

In the area of medical device cybersecurity, FDA has recognized cybersecurity as a patient safety concern, and has long reviewed medical devices to ensure they are designed, developed, and maintained cyber securely. This includes implementing explicit cybersecurity regulatory authorities, publishing guidance documents, and working with partners, including other agencies, third party researchers, patients, and others to manage cyber risk to devices. Medical device cybersecurity is the domain of other programs within the FDA and will not be discussed here, but lessons can be learned from their experience. Similar to securing devices, securing medical product manufacturing cannot be done by individuals or single companies. It requires coordinated efforts from all involved parties across public and private sectors.

Each FDA Center takes a concerted look at the technologies that affect its products and collaboratively approaches topics like cybersecurity which affect all of FDA's product areas. FDA's Office of the Chief Scientist's Office of Regulatory and Emerging Science (OCS/ORES) is collaborating with the Office of Digital Transformation to apply the Agency's expertise to create a demonstration manufacturing line including software for manufacturing execution, operations, and lifecycle management, and digital hardware. The FDA is not using this system to manufacture any products, but to identify and research cybersecurity and advanced manufacturing topics. Implementing such a system has allowed FDA to create a case study for a digitally integrated manufacturing line within a secure network. The program has compiled a basic list of standards and guidelines for good operational technology security practices and presents a case study of vulnerabilities and risk mitigation strategies.

Cybersecurity Incidents

A 2019 survey across hundreds of companies led a cybersecurity industry group to estimate that the global cost of cybercrime would top $10.5 trillion in 2025[7]. These are not theoretical concerns. As far back as 2013, Iranian cyber threat actors took control of the Supervisory Control and Data Acquisition (SCADA) systems for the Bowman Dam in Rye, New York, which allowed access to the dam's computerized floodgates[8, 9]. In 2017, the NotPetya cyber incident targeted essential companies and systems such as the shipping company Maersk, a Pennsylvania Hospital system, and the pharmaceutical manufacturer Merck & Co among many others[10, 11]. The White House estimated at the time that the financial toll of the attack was approximately $10 Billion[12].

According to a study by Forrester and Tenable, 94% of executives surveyed said that their firms had experienced a cyber-incursion that impacted their business within the last 12 months[13]. A 2023 attack on Applied Materials, a semiconductor industry supplier, reportedly caused supply chain delays and $250 million in lost revenues. Industrial control and automation supplier, Johnson Controls was attacked in 2024 by a ransomware gang, which was able to download over 27 terabytes of internal company and customer data. In February 2024, the U.S. Cybersecurity & Infrastructure Security Agency (CISA) warned of persistent access to critical infrastructure systems by a Chinese state-sponsored hacking group known as Volt-Typhoon[14]. Though the FBI reportedly disrupted some of the group's operations, Volt-Typhoon had compromised thousands of devices across different international critical infrastructure sectors and the extent of infiltration into U.S. critical infrastructure is still being determined.

On July 19, 2024, cybersecurity firm CrowdStrike pushed a routine but flawed update to a single portion of a single security software, causing global outages cancelling flights, shutting down airports, delaying care at hospitals, and locking up government systems. It is estimated that the impacts caused at least $5 billion in direct losses over 4 days[15]. The pre-release testing system used by CrowdStrike did not catch the fatal flaw in that July 19th release, which was recalled less than two hours later, only after it was downloaded by millions of systems. While the CrowdStrike incident was not a malicious act, merely an extremely costly mistake, the incident highlights the importance of rigorous testing in multiple environments before release.

Data breaches and ransomware attacks of hospital systems and medical clinics have become more ubiquitous in the last few years, leading to significant efforts by HHS, other government departments, and the private sector to mitigate the damages and reduce the effectiveness of these attacks[16-19]. As high profile as these attacks are, manufacturing and supply chain attacks have the potential for even greater harm to patients, medical advancement, and public health security. FDA is developing policies, guidance, strategies, and regulatory science tools for OT security and supply chain resilience to meet its public health mission.

Physical and Digital Landscape

OT Cybersecurity starts with awareness of the physical and digital landscape of each production line and the wider enterprise infrastructure. The manufacturing equipment, sensors, plumbing, and electrical systems that make up any production facility create the operational environment. Digital technologies and controls often connect to a larger building, facility, or corporate networks that allow remote oversight and operation of production. A comprehensive understanding of all these elements and their connections is integral to creating a secure OT environment.

Operational Technology Environments

Operations environments can include almost any industrial asset (such as valves, actuators, drivers, robots, power breakers, etc.) managed by industrial control system (ICS) devices, such as programmable logic controllers (PLCs), remote terminal units (RTUs), intelligent electronic devices (IEDs), distributed control systems (DCSs). These devices often must work continuously for months or years in potentially harsh or severe conditions. Consequently, many OTs were designed to prioritize consistent functionality over cybersecurity and did not anticipate the constantly connected, internet accessible conditions of modern industry. As such, they are more vulnerable to modern cyber threats such as distributed denial-of-service (DDoS) or vulnerability exploits. Moreover, it is sometimes difficult to tell what, when, and where communications are happening. Two primary issues can cause challenges for organizations attempting to secure their industrial networks:

- **Lack of visibility:** ICS devices and OTs are often embedded within other systems. A piece of equipment for one unit operation (e.g., chromatography, bioreactor, annealing furnace) may contain embedded control and automation devices from another manufacturer. Legacy technology may also have communications needs that are built into the "baseline" requirements for an internal network. This means that organizations often do not have an accurate inventory of: a) what is on the network and b) how each device is communicating on the network. Without these, manufacturers have limited ability to understand their risks and take precautions to mitigate and secure their network architecture.
- **Lack of control**: Many pieces of equipment assume a certain amount of connectivity when they are placed on a network. They may use this to contact other related devices to exchange data, to communicate with a home server to check for updates, or to fulfill many other functions. Some of these connections are integral to the function of equipment and devices, others are nice to have to increase functionality or ease of use. However, these connections are not always disclosed by the manufacturer to the end users. If they are, they also may not be alterable by the user. If an organization does not know the nature of all incoming and outgoing communications, it cannot effectively control and secure its networks.

Situations with reduced transparency only worsen the lack of control of OTs. The first step then, to securing an industrial network, is to obtain visibility. To truly begin securing any operational environment, it is incumbent on manufacturers to understand what devices are on their networks, what they are communicating, why they are communicating, and where those communications lead.

A hardware bill of materials and software bill of materials (SBOM) provided by the vendor can be useful in understanding relevant devices and software. The manufacturing system vendor may also consider identifying the digital storage requirements and intended installation locations for each system component. Additionally, SBOMs should be able to provide a complete summary of the frequency and volume of communications and the infrastructure requirements for implementation [20]. These factors impact security in a manufacturer's technology environment and allow organizations to ensure that vulnerabilities can be catalogued and understood for all manufacturing system components within the environment. For medical device manufacturers specifically, this is now a requirement established under the Consolidated Appropriations Act, 21 USCS § 360n-2(b)(3) (2023) [21].

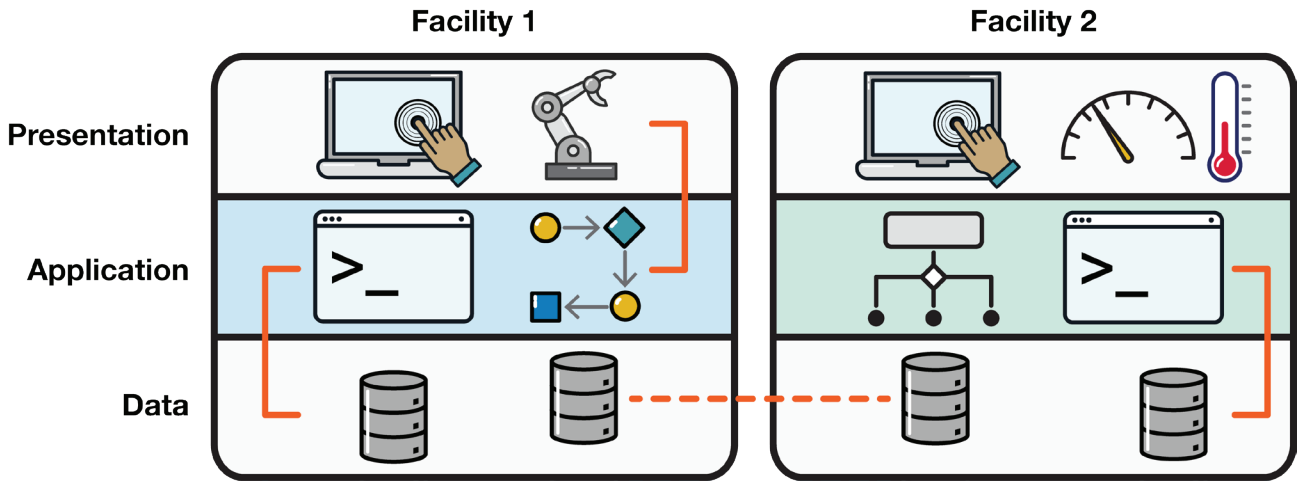
Reference Architecture

Once the devices and assets are fully understood, they can be logically arranged on the network to maximize infrastructure security. Modern network architecture standards aim to keep pace with the development and deployment of technology from cloud-based processing to edge computing. ISA-95/IEC-62264, developed in the 1990s, provides baseline standards for overall enterprise architecture and security. ISA-99/IEC-62443 provides updated security standards for smart and connected networks, recommending industrial networks be segmented into zones and conduits. The objective is to restrict communications between assets to keep cyber threats from spreading and disrupting the entire production infrastructure.

A zone is a collection of assets that have common security requirements. Conduits allow and control communication between zones. Under the least privilege principle, OT assets can communicate only with assets in their zone. If assets need to communicate outside of their zones, security policies must be defined, and communication can occur only through specified communication conduits. For example, a single facility may have multiple fill-finish production lines. It is not expected that equipment from one fill finish production line would need to interact with equipment from the other lines. However, information about the products being filled and capacity utilization may be transmitted between different lines. Placing each in its own zone, with specific conduits of communication, limits system-wide impacts if equipment in one zone is compromised. Implementing zone and conduit architecture greatly improves network security and overall network performance, compared to a flat network where all devices share the same bandwidth. It also, however, requires an accurate inventory of all connected assets and a clear understanding of their roles and communication needs within the industrial process.

A common way to improve cybersecurity is to implement a three-tier architecture. A three-tier architecture is a modular, well-established computing application architecture that organizes applications into three logical and physical computing tiers: the **presentation zone** manages the user interface; the **application zone** handles business logic; and the **data zone** stores and manages persistent data. With it, physical interfaces, external communications, and long-term storage can then be managed individually and securely.

Example of Zones and Conduits in a Three-Tiered Infrastructure



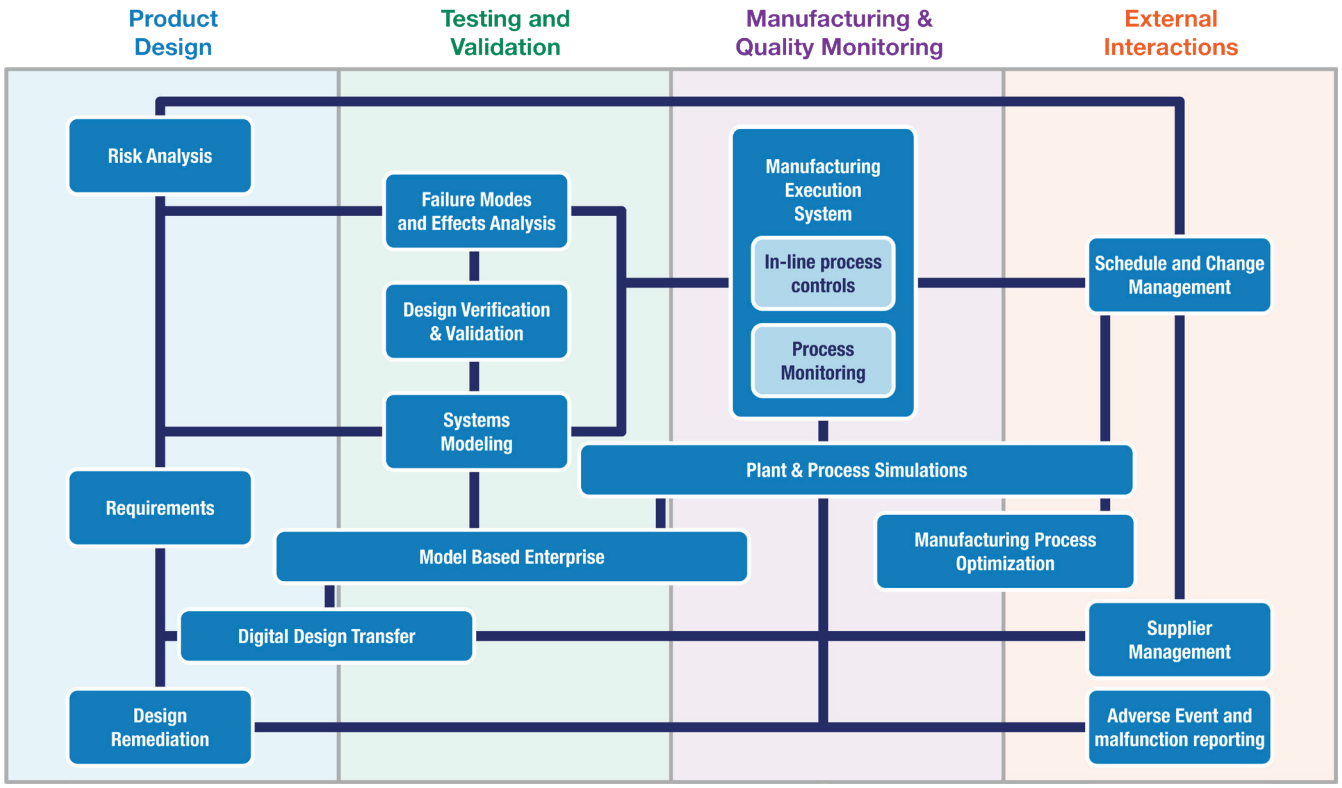
The chief benefit of three-tier architecture is that isolation of each tier makes development, updates, and security independent for each, enabling different technical teams to work on them without impacting other tiers.

A Demonstration of Manufacturing OT at FDA

The FDA, like other federal agencies, is a high-profile target for cyber threats because of the scope of the products it regulates and the types of data that it keeps[7]. In 2021, the White House issued an Executive Order on Improving the Nation's Cybersecurity calling for transformative changes to the U.S. government's approach to IT and OT systems[5]. Subsequently, NIST launched programs to standardize and implement zero-trust architectures[1]. To protect a modern digital enterprise, organizations need a comprehensive strategy for secure "anytime, anywhere" access to their corporate resources (e.g., applications, legacy systems, data, and devices) regardless of where they are located[7, 22-26].

Programs across FDA focus on the various aspects of medical products and manufacturing that maintain safety, efficacy, and security. The Agency continually updates its guidelines and strategies for industrial automation, artificial intelligence (AI), and connected manufacturing systems[22-25]. Specifically related to the manufacturing of regulated products, FDA's Office of the Chief Scientist's Office of Regulatory and Emerging Science has implemented a demonstration manufacturing line including software for manufacturing execution, operations, and lifecycle management, and digital hardware that has allowed FDA to create a case study for a digitally integrated manufacturing line within a secure network. Several practices and key considerations were identified that may be equally applied by government and industry stakeholders.

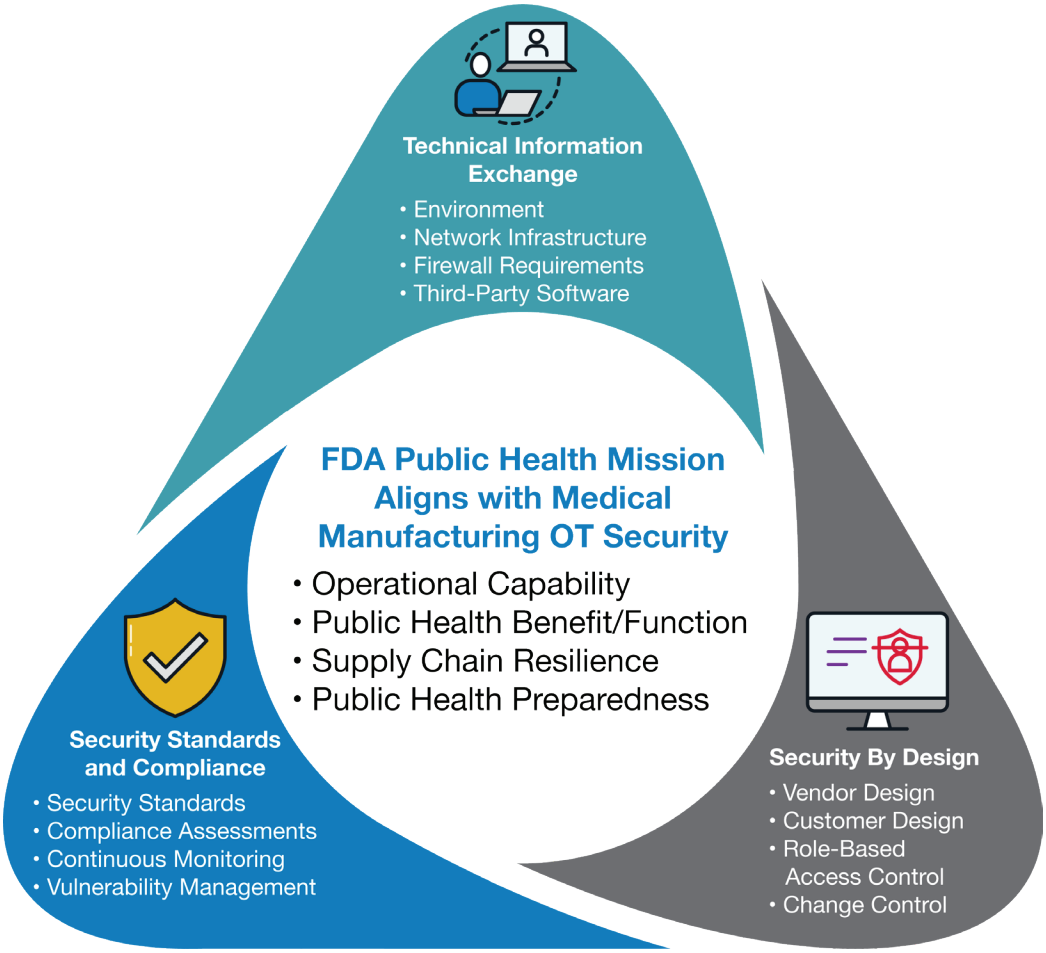
Digital workflows connect all elements of the product lifecycle together, creating connections between previously siloed business processes



1 "Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned). Authentication and authorization (both subject and device) are discrete functions performed before a session to an enterprise resource is established." (NIST SP 800-207)

For this demonstration, FDA followed cybersecurity expert recommendations including NIST Special Publications including Federal Information Product Standards (FIPS 140-2 and 140-3) and NIST SP 800-82, CISA guidelines, and strict network routing requirements to safeguard networks. In the short term, it can be easier and tempting to make exceptions or set permissive network rules. However, this would create an unacceptable long-term cybersecurity risk for government networks and similarly for medical manufacturing facilities. Many Commercial Off-the-Shelf (COTS) products may not natively comply with these security requirements and may require some reconfiguration to function. Even if it may not be current industry standard practice to comply with FIPS or similar security guidelines, the benefit to implementing them quickly and comprehensively can far outweigh short-term inconveniences.

Until these guidelines are considered industry standard practice, there may be considerable vulnerabilities inherent in many OT configurations. The availability of security by default may change as industry demands security as a baseline for manufacturing excellence. Until then, FDA is using this recent experience as an opportunity to identify potential considerations, vulnerabilities, and risks that industry should be aware of when implementing and securing network-enabled and smart operational technologies.



These considerations fall into three categories: Technical Information Exchange, Security Standards and Compliance, and Security by Design. The practices outlined in this document are abbreviated and consolidated considerations based on the references provided. Lessons are also draw from FDA's experiences with industry as well as its experience implementing non-manufacturing OTs.

Technical Information Exchange

Adoption of connected, digital, and smart manufacturing systems often entails extensive retooling, retrofitting, or acquisition of equipment. Visibility and certain levels of control are important to securing a network. Every automated unit operation, smart material handling unit, connected sensor, edge computer, and software cloud has the potential to contain multiple:

- software packages– such as functional modules, middleware, scripting, webservices
- hardware iterations – chipsets, printed circuit board (PCB) configurations
- firmware versions – software on read-only hardware chips that must be periodically updated

These all affect how OTs communicate and function, but they are not always controlled by the equipment vendor. For instance, branded PLCs from one vendor can be embedded within a piece of manufacturing equipment from another, which may rely on a separate software component from a third vendor to communicate with the manufacturing execution system. It is important for the team responsible for integrating the system into a manufacturing line to know exactly what and how hardware and software products are being used to achieve expected functionality, for example through a hardware bill of materials and SBOM.

Integration teams, which may include short term contractors or vendor personnel, require special access to manufacturer systems to complete product deployment. Preserving the same security training and standards for both permanent personnel and for short-term access needs is critical to maintaining network security. This includes automatic and confirmed removal of temporary privileged accounts when deployment activities are completed. Legacy accounts, passwords, and access points can provide easy access for potential cyber threats.

Before deployment even begins, both the vendor(s) and manufacturer OT specialists, should have a complete technical understanding of the extent and routing of system traffic within zones, between zones, and externally. This will help identify any potential conflicts with existing network security measures or communications standards and ensure the system will function as intended once it is deployed. For example, if a network is only able to communicate externally using one specific port, then any deployed software will have to be configured to use that port, even if the software does not enable it by default. If a manufacturer's system uses a specific version of infrastructure software (e.g., a database) then the OT vendor should match this within reasonable limits. This means that there may be some additional effort for the software developer in supporting different communication ports or protocols for multiple customers. Communications and cybersecurity standards can help alleviate some of these problems by decreasing uncertainty and variability between installations. They can also increase cybersecurity overall by ensuring that all parties understand the expectations for all OT systems.

The full complement of OTs used to perform manufacturing operations will rarely, if ever, come from a single vendor who has developed all the products in house. Even when a single vendor is providing resources, there may be products from other business units or intermediate vendors that are not always considered when planning a deployment. Mapping, discussing, and understanding every OT and connected subcomponent will improve the OT deployment experience and increase network security overall.

Security Standards and Compliance

Securing hardware and software becomes more straightforward with specific guidelines and standards that can be followed across industries. Federal standards, such as FIPS, must be applied by federal agencies handling sensitive or confidential data as well as other organizations that must comply with specific rules such as the Health Insurance Portability and Accountability Act (HIPAA). These standards can also provide a strong basis for securing other networks with connected OTs. Other essential security and privacy standards are published under NIST Special Publication (SP)-800 and IEC 62443 (See Appendix A for Example Standards). Additionally, CISA maintains a list of discovered vulnerabilities and exploits for common software and OTs that is useful for maintaining vigilance.

Not all commercial and industrial OT products, even from the same vendor, will have built-in compliance to FIPS or other security standards. FIPS and similar security standards may take additional time and resources to implement, but they can provide a much stronger bulwark against cyber-intrusion – protecting the nation's critical public health supply chains. Ransomware attacks, cyber-induced production stoppages, or other externally prompted supply chain disruptions can have much greater costs and graver consequences to the public health of all Americans.

To ensure compliance with these security standards when implementing enterprise systems or OTs on government networks, federal agencies require the solutions deployed on their systems to receive Authorizations to Operate (ATOs)[27]. For external cloud systems, the FedRAMP program (FedRAMP.gov) ensures a similar level of security at the federal government level, after which the agency must accept the FedRAMP authorization and conduct an agency ATO on the agency system hosted in that cloud service provider. These processes help the vendors and agencies:

- Determine the potential security impact level.
- Establish a security and privacy plan.
- Perform an assessment of system security implementation.
- Develop a continuous monitoring and improvement plan to maintain security.

The ATO process ensures all parties have a clear understanding of the system, its components, and required communications. It helps to identify standards compliance as well as issues and gaps that need to be addressed before commencing operations. In addition to security vulnerabilities, the issues and gaps can include specifically allowed or prohibited activities based on an individual network's configuration, enterprise needs, or software version controls. A portion of this process is completed through documentation review, and network inspection tools are used to probe critical systems and communication conduits. For instance, an OT may utilize hardware from a third party, which includes firmware that automatically tries to communicate externally. This may not come up on an initial mapping of the communications needs and conduits but would be discovered during the security scans.

Finally, an ATO assessment will provide compliance gaps and issues which should be addressed to reach compliance. The ATO assessment results may require action from the organization or the OT vendor and they provide a clear starting point for discussions.

Security by Design

The 2021 Executive Order on Improving the Nation's Cybersecurity (EO 14028) specifically calls out the risks to the IIoT and the need for education and procedures to secure them[5]. It is ultimately easier to build OTs with technical and physical security safeguards in mind from the outset. In the design phase of any product, mapping clear communications pathways, integrating security standards, and implementing best practices can reduce the time and resource costs associated with OT deployment. It is advantageous to engineer the network infrastructure and enterprise procedures with security in mind when implementing off-the-shelf or commercially marketed OTs.

Large public and private organizations are made up of many operating divisions with varied operational and technological requirements that operate on a combination of individual and shared resources. Frequently, in addition to traditional network resources, these include on-premises and external cloud services. When implementing any project on a shared enterprise resource, a change control board (CCB) may help to maintain operational visibility and bring up any potential shared concerns. CCB stakeholders will represent specific interest and may then review each proposed change before it is implemented to ensure that there will be no unintended effects that could break or adversely affect other projects. Ultimately, this is often a technique that can significantly reduce downtime and increase organizational productivity.

Commonly used and critical services, such as Single Sign On, database servers, user portals, manufacturing quality assurance systems, or remote process monitoring applications, can all represent potential critical vulnerabilities if compromised by another application sharing its resources. It falls to the groups implementing OTs to be vigilant about enterprise cybersecurity design and implementation until all OTs comply with the latest security standards and cybersecurity best practices by default.

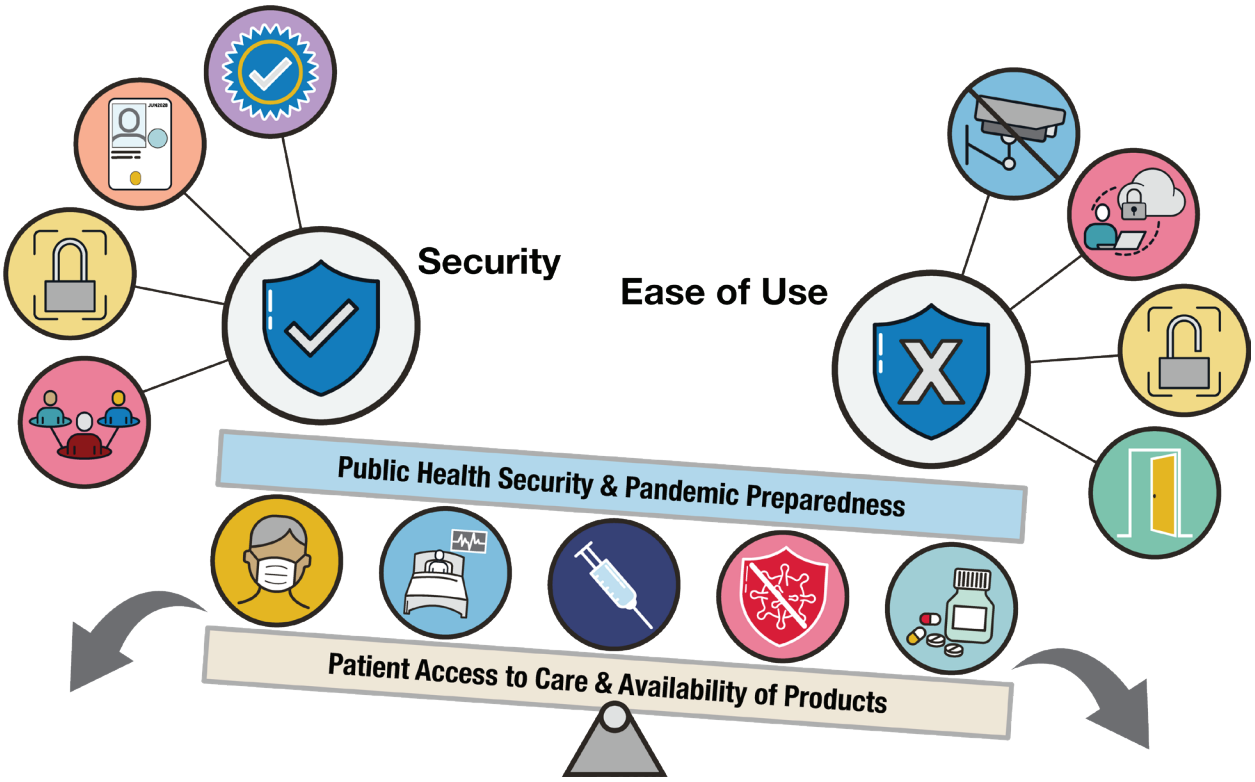
In some cases, a security function or feature may not be available for a particular product. The group implementing the OTs can always ask their vendor(s) to add the security features they need. The option for high security assurance OTs can be an advantage for all parties, but vendors may not know exactly what features their customers want until they receive a large enough number of requests. Requesting conformance to federal or consensus standards may help organization to choose an appropriate level of security. This may seem like a significant workload; however, these security updates can avoid costly security breaches and would bring assurance to many customers and to the federal government.

> **"Requesting conformance to federal or consensus standards may help organization to choose an appropriate level of security."**

Designing an OT security plan requires a thorough understanding of cybersecurity processes and operational technology business requirements. This is a risk-based proposition where all cybersecurity measures may not be needed in every case, but a comprehensive understanding of organizational and operational needs is required to make that determination. Cybersecurity experts working on federal systems find compliance to FIPS, conformance to CISA guidelines, and use of the latest consensus cybersecurity standards to be essential to its daily operation. Under these security conditions, many federal agencies have been able to implement OTs, including the demonstration manufacturing line at FDA that replicates a digitally integrated small manufacturer.

Balancing Security, Ease of Use, and Innovation

Some people believe that innovation is hampered by implementing rigorous cybersecurity. Innovative products and manufacturing processes can create intellectual property for companies, bring novel medical therapies to U.S. patients, and improve U.S. medical supply chain resilience. All of these benefits can be easily and quickly undone if cyber threat actors steal intellectual property, contaminate medical products, or disrupt production at critical times. Much like quality assurance programs, strong cybersecurity processes are one of the pillars that support the safe, effective, and reliable production of medical products.



There is still a balance to be struck between creating an operational environment that is easy to use and securing operations against all possible threats or misuse. Overemphasizing either security or ease of use can cause have serious ramifications to public health, patient access to care, availability of cutting-edge products, and pandemic preparedness. Risks can be managed by mapping potential hazards, implementing fixes and mitigations, and continuous threat monitoring. When standard protocols and procedures are used, it is even easier for new OTs to be developed and integrated. Federal standards and guidelines provide a baseline for original equipment manufacturers, software developers, and manufacturers to implement Security by Design. Innovative processes can then be implemented with greater assurance that the system will not be compromised.

FDA has implemented manufacturing OTs within its secure network, demonstrating the feasibility of maintaining high levels of security, standardization, and monitoring while running a digital manufacturing line. FDA's ongoing research into advanced manufacturing and emerging technologies will help keep the Agency up to date with industry activities, continue to identify best practices for implementing novel and innovative technologies, and ensure regulatory science tools are available to generate needed validation data. The FDA encourages innovation in all aspects of product development and manufacturing to enhance U.S. public health security and to ensure that U.S patients have consistent access to the latest medical products available.

Appendix A: Resources and Standards for Securing Manufacturing Technology and Industrial Automation

Federal agencies and standards development organizations provide a variety of documents that provide expert and consensus-derived guidelines for methods to determine the level of risk a facility, process, or end user; designing cybersecurity into a system; and adapting or maintaining cybersecurity. These baseline good cybersecurity practices and hygiene (activities that reduce the overall vulnerabilities to cyber incidents without targeting specific threats) can help companies and agencies build a robust, secure, and dynamically connected manufacturing technology infrastructure.

Cybersecurity & Infrastructure Security Agency (CISA): CISA is the operational lead for federal cybersecurity and the national coordinator for critical infrastructure security and resilience. They work with partners to defend against today's threats and collaborate to build a more secure and resilient infrastructure for the future. CISA publishes guidelines, best practices, standards, and training courses to help stakeholders create safe cyber environments for their systems. They also publish a list of known vulnerabilities and exploits that is constantly updated as new ones are found.

- Known Exploited Vulnerabilities Catalog: For the benefit of the cybersecurity community and network defenders—and to help every organization better manage vulnerabilities and keep pace with threat activity—CISA maintains the authoritative source of vulnerabilities that have been exploited in the wild. https://www.cisa.gov/known-exploited-vulnerabilities-catalog

- Cybersecurity Best Practices: Information on cybersecurity best practices to help individuals and organizations take preventative measures and manage cyber risks. Content ranges from recommended cyber hygiene tasks to specific threat mitigation activities. https://www.cisa.gov/topics/cybersecurity-best-practices

- Cyber Hygiene Services: CISA provides services that help partners reduce the risk of a successful cyber incident. The services include vulnerability scanning, web application scanning as well as interaction with CISA cybersecurity professionals. https://www.cisa.gov/cyber-hygiene-services

International Electrotechnical Commission (IEC): The IEC develops a range of standards that are highly relevant to securing manufacturing technologies in the context of medical products:

- ISA-95/IEC 62264 series – Enterprise-control system integration: These standards were first established in the 1990s and have been regularly updated to assist in integrating logistics systems with manufacturing control systems. Technology and business processes are organized into layers defined by the activities taking place with methods to allow communication between the layers. It can be applied and adapted for use with smart / connected manufacturing systems, especially when used with the newer ISA-99/IEC 62443, which was specifically created to address their unique needs. https://www.isa.org/standards-and-publications/isa-standards/isa-95-standard

- ISA-99/IEC 62443 series - Industrial communication networks - Network and system security: The IEC 62443 series of standards focus on cybersecurity for industrial automation and control systems, which includes manufacturing technologies used in medical device production. These standards provide guidelines and requirements for securing networked systems, addressing vulnerabilities, and implementing cybersecurity controls to protect against cyber threats. https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF): The NIST CSF provides a framework of cybersecurity best practices, standards, and guidelines that can be customized and implemented by organizations, including medical products manufacturers. It consists of core functions (Identify, Protect, Detect, Respond, Recover) and categories that help organizations manage and mitigate cybersecurity risks across their operations, including manufacturing and operational technologies. Several NIST standards are relevant for securing manufacturing technologies in the context of FDA-regulated medical products, including:

- NIST SP 800-53: Security and Privacy Controls for Federal Information Systems and Organizations: This publication provides a comprehensive catalog of security and privacy controls for information systems and organizations, including those used in medical device manufacturing technologies. It covers a wide range of security controls that can be tailored to manage cybersecurity risks associated with electronic systems, data handling, and network security.
  https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final
- NIST SP 800-82: Guide to Industrial Control Systems (ICS) Security: Although focused on industrial control systems, NIST SP 800-82 provides guidance on securing critical infrastructure and control systems, which may include manufacturing technologies used in medical device production. It covers cybersecurity considerations such as network security, access control, and system monitoring relevant to manufacturing environments.
  https://csrc.nist.gov/pubs/sp/800/82/r3/final
- NIST SP 800-171: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations: While initially developed for protecting sensitive information in nonfederal systems, the controls outlined in NIST SP 800-171 are relevant for safeguarding manufacturing technologies that handle sensitive data related to medical devices. This includes controls for access control, incident response, and system and communications protection.
  https://csrc.nist.gov/pubs/sp/800/171/r3/final
- NIST SP 800-172: Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171: This special publication provides enhanced security requirements beyond NIST SP 800-171 for protecting critical programs and high-value assets. While specific to certain high-risk environments, it offers additional guidance that can be adapted for securing manufacturing technologies handling critical medical device data.
  https://csrc.nist.gov/pubs/sp/800/172/final

References

1. FDA. *FDA at a Glance from the Office of the Commisioner*. 2024 3/5/2024; Available from: https://www.fda.gov/about-fda/economics-staff/fda-glance.
2. The White House, *Executive Order 13636*, in *Improving Critical Infrastructure Cybersecurity*, Federal Register, Editor. 2013. p. 217-223.
3. The White House, *Executive Order 13800*, in *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, Federal Register, Editor. 2017. p. 22391-22397.
4. The White House, *Executive Order 13691*, in *Promoting Private Sector Cybersecurity Information Sharing*, Federal Register, Editor. 2015. p. 1-5.
5. The White House, *Executive Order 14028* in *Improving the Nation's Cybersecurity*, Federal Register, Editor. 2021. p. 26633-26647.
6. The White House, *National Cybersecurity Strategy*. 2023. p. 39.
7. Morgan, S.S., Calif *2024 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics*. The past, present, and future of cybercrime. 2024 June 24, 2024; Available from: https://cybersecurityventures.com/cybersecurity-almanac-2024/.
8. U.S. Department of Justice, *Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector*. 2016.
9. Berger, J., *A Dam, Small and Unsung, Is Caught up in an Iranian Hacking Case*, in *New York Times*. 2016. p. 4.
10. British Broadcasting Corp. *Global ransomware attack causes turmoil*. 2017; Available from: https://www.bbc.com/news/technology-40416611.
11. Vanderford, R., *Merck's Insurers On the Hook in $1.4 Billion NotPetya Attack, Court Says*, in *The Wall Street Journal* 2023. p. 3.
12. Greenberg, A., *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, in *Wired*. 2018. p. 28.
13. Forrester, *The Rise of the Business-Aligned Security Executive*. 2020. p. 39.
14. Cybersecurity and Infrastructure Security Agency, *PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure*. 2024. p. 50.
15. Fung, B. *We finally know what caused the global tech outage - and how much it cost*. 2024; Available from: https://www.cnn.com/2024/07/24/tech/crowdstrike-outage-cost-cause/index.html.
16. U.S. Department of Health and Human Services, *Breah Portal: Notice to the Secreatary of HHS Breach of Unsecured Protected Health Information*. 2024; Available from: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.
17. U.S. Department of Health and Human Services, *Healthcare Sector Cybersecurity*, in *Introduction to the Strategy of the U.S. Department of Health and Human Services*. p. 1-6.

18. Advanced Research Projects Agency for Health. *Upgrade: Universal Patching and Remediation for Autonomous Defense*. Available from: https://arpa-h.gov/research-and-funding/programs/upgrade.

19. U.S. Department of Justice, *Justice Department to Implement Groundbreaking Executive Order Addressing National Security Risks and Data Security*, in *Executive Order Will Focus on Countries of Concern Accessing Americans' Bulk Sensitive Personal Data and U.S. Government-Related Data*. 2024. p. 5.

20. Cybersecurity and Infrastructure Security Agency. *Software Bill of Materials*. 2024 [cited 2024 11/18/2024]; Available from: https://www.cisa.gov/sbom.

21. FDA, *FDA's Medical Device Cybersecurity Program and SBOM*, CDRH, Editor. 2023. p. 14.

22. FDA, *Artificial Intelligence& Medical Products: How CBER, CDER, CDRH, and OCP are Working Together*. 2024. p. 7.

23. FDA, *Distributed Manufacturing of Drugs: Stakeholder Feedback and Action Plan*, C.f.D.E.a. Research, Editor. 2023. p. 18.

24. FDA, *FDA outlines cybersecurity recommendations for medical device manufacturers*. 2016.

25. FDA, *Artificial Intelligence in Drug Manufacturing*, C.f.D.E.a. Research, Editor. 2023. p. 17.

26. NIST National Cybersecurity Center of Excellence. *Implementing a Zero Trust Architecture*. 2024 [cited 2024; Available from: https://www.nccoe.nist.gov/projects/implementing-zero-trust-architecture

27. U.S. General Services Administration. *An Introduction to ATOs Understand the Authority to Operate Process*. 2024. 8.


FDA
U.S. FOOD & DRUG
ADMINISTRATION