Manufacturing Cybersecurity Systems Operator

Section 1: *Job Role Identifier Section*

Role Title: Manufacturing Cybersecurity Systems Operator

Role Impact: Pioneer

Summary Scope

Transforming to a smart manufacturing factory means integrating security practices and technology into plant processes via interconnected machinery, automation, data driven operations, communications, and software. The systems and roles that protect these increasingly digital operations and resources are essential. Of these roles, who can assist determining what and if something changed from a cybersecurity perspective – a configuration setting, firmware version, new port opened, new device connected to the network, etc.? Who is a junior part of the prevention, detection, and resolution capability when there is a production outage that is impacting the plant's ability to make product? Keeping the human, physical, and digital assets secure is the responsibility of both the operating technology and information technology areas and many job roles at all levels that ensure secure operations.

So, which of these roles is the entry-level operations role who is the "on the ground eyes, ears and voice" for IT (Information Technology) and OT's (Operational Technology) shared interests, closest to the operating environment and its security protections? The Manufacturing Cybersecurity Systems Operator has a primary focus to monitor, record, detect, and report security system performance and functions. Who is the role that may overlap into other adjacent cyber roles as experience and skill increases, but usually does not take on tasks associated with production or assembly operations? The Manufacturing Cybersecurity Systems Operator is not a conventional equipment operator but a systems operator who uses security software and processes for protecting factory floor automation and control technology assets, information, processes, and employees. On a daily basis, these systems operators watch and report the security status in diverse industrial and product settings: they monitor and escalate OT and IT concerns crossing plant automation and control platforms, components, IoT devices, access points, network connections, and more.

Who can be a bridge with IT and help advance old paradigms of plant isolation, creating better practices and improved performance? As an entry level cybersecurity "utility player", these System Operators can more broadly support plant engineering, production management, quality and ICS by leveraging varying worker backgrounds and experiences. And who then can help to revert that change back so that the process is back to operating at a functional, productive state?

This Manufacturing Cybersecurity Systems Operator role may be an internal role of a manufacturer and may have other IT and/or OT responsibilities; it also may be a role employed at a manufacturer, through a third-party vendor, systems integrator, or factory automation technology provider. The scope of systems that an operator works with can be proprietary or third-party, including across multiple manufacturers, software packages, network architectures, and/or industrial components. Systems and technologies under the umbrella of OT that relate to this role are Industrial Control Systems (ICS), SCADA, DCS, PLC, etc.

As experience increases, this role - which can start as a Level I and progress to a Level II or III operator - may add analysis and detection tasks, engage more deeply with related functions, and participate in cyber testing and exercising. Also, this role may serve as an incident SME if a specific threat, incident or breach occurs and the operator is needed for further response, recovery, and restoration.

With numerous available certifications and training programs available to learn and practice, and then supported on-the-job by technology and further training, this role is a solid opportunity to bring or transition diverse backgrounds into both the manufacturing and cybersecurity environment, a win-win for the workforce and manufacturers.

Outcomes

Business Needs Addressed

From a core business perspective, this role produces or supports the production of these valued outputs:

- Reduction of cyber threat risks and improved defenses for Industrial Control zones and production and product assets.
- Increased cyber compliance.
- Realization of the same security benefits for OT that are enabled for other business and administrative IT systems.
- Ensured confidentiality.
- Protection of the control logic; first line monitoring to avoid changes or improper communications with OT systems without proper procedures or authority.
- Improved prevention, detection, and recovery efforts.
- Safeguarded device, component, process, and control logic and configuration data.
- Lowered production time stoppage due to improved incident response and recovery.
- Increased timeliness and accuracy of version control.
- Maintained safety.

Some technology or production stakeholders may connect this role to the notion of 'Shadow IT' - the classic term for where a line of business (not central IT) purchases, implements, and uses new tech for its own processes. Shadow IT presents issues when it's a symptom of disconnected tech strategy and operations. Here it is 'shadow IT' in the best of both worlds as this role is one that formalizes the system operations essential to manufacturers converging OT and IT. It is core to success that this role is both IT-oriented (systems use, monitoring information and reporting) and OT-oriented (direct and deep interaction with the cybersecurity systems operations on the plant floor).

Compliance Requirements and Employer Profile

Federal agencies including the Department of Defense (DoD) have put implementing strong cybersecurity practices into every aspect of production and procurement as a top priority on their list of critical activities. In this effort, the Office of the Under Secretary of Defense for Acquisition and Sustainment has created the Cybersecurity Maturity Model Certification (CMMC) which will require a Third-Party Assessment Organization (C3PAO) to certify applicable defense contractors participating in the DoD supply chain. CMMC accreditation builds upon existing regulation (DFARS 252.204-7012) by adding a cybersecurity verification component. Businesses providing products and/or services to the DoD must prepare for compliance with CMMC guidelines in anticipation of the requirements being included on future RFPs, anticipated beginning in early 2021. For additional detail on CMMC requirements, visit https://www.acq.osd.mil/cmmc/.

Domain Profile

This role aligns with Operating Technologies & Convergence domain and the Automation & Controls subdomain.

Business Case Contribution

The true value of this role is in the routine completion of convergence and shared cyber solutions practices most closely associated with plant and physical production and processing equipment. These operators will make their everyday work the integrated security operations and systems use. This role helps ensure accurate information is delivered to people, machines, switches, sensors and devices at the right time and in the best format; and helps to minimize complexity and lower the operating costs of siloed IT and OT.

From a talent perspective, this role provides human capital value in meeting workforce objectives such as:

- Providing an opportunity to place IT candidates/professionals in the core business and production environment of manufacturing.
- Offering an opportunity to diversify the cyber workforce with candidates from varied incoming experiences.
- Serving as an example of modern manufacturing and factory of the future opportunities and messaging.
- Lowering academic degree requirement enhances community and technical college connections with manufacturing employers for a steadier influx of new workers with new skills.
    - Note: This role may be a suitable consideration for an Industry-Recognized Apprenticeship Program (IRAP), designed to enhance the workforce in rapidly-expanding sectors of the economy, such as cybersecurity, by providing individuals with opportunities to obtain relevant workplace knowledge and progressively advanced skills.
- Creating a potential career pathway opportunity through reskilling for military veterans and professionals with IT and cybersecurity training and experience, as well as relevant security clearances, into the manufacturing workforce.
- Serving as an excellent feeder role into other areas of cybersecurity, based on its generalist exposure to, informational technologies, operational technologies and the convergence between them for improved cybersecurity performance,

Section 2: *Key Responsibilities*

Activities

Summary Activities:

This role contributes to the achievement and maintenance of confidentiality, integrity, and availability of production/processing controls and communications that guard physical, financial, human, and customer assets.
A Manufacturing Cybersecurity Systems Operator routinely:

1. Performs security systems operations tasks on the plant/factory floor as this role's primary day-to-day work environment and also works at SOC or ICS command center systems monitoring stations and/or a remote operations console.
2. Interprets and translates system operations requests into operational duties and tasks.
3. Operates and maintains diverse facility and process specific systems and platforms working between hardware controllers, sensors, and related communication protocols connecting to business and enterprise software across internal and external networks.
4. Interacts with many other OT roles and IT roles as convergence efforts and solutions increase; supports plant engineering, quality, production management and other key manufacturing functions.

Additional detailed tasks aligned to the NIST Cybersecurity Framework stages include:

Identify

1. Applies and improves asset inventory tracking and knowledge of the asset/device/equipment/system layout
2. Assists with creating and managing any exceptions to cyber security standards or system usage/configurations as required.
3. Ensures all work fits within the broad cyber systems architecture while meeting local facility operational functions and goals.
4. Understands that any local variances would impact the ability to scale the system or extend it to other facilities.

Protect

1. Understands, applies, and improves assessments of vulnerability and risks; updates the risk profile from networks and or IT devices to the controls level.
2. Maintains, tunes, and upgrades related systems and software.
3. Monitors preventative controls in place to enforce communication patterns; observes data on the industrial processes and protocols to ensure and enforce authorized communication between devices and/or networks
4. Assists in establishing and defending ICS security zones with appropriate countermeasures.
5. Supports and implements coordinated efforts with supply chain on remote access, data sharing and security process calibration.

6. Supports the enforcement of expected communication patterns or data flows with network segmentation.
7. Supports acceptable changes to varied devices such as controllers, HMI's, RTU's, engineering workstations, operator workstations, routers, switches, databases, and firewalls.
8. Uses or maintains older and/or proprietary software with heightened awareness of existing and previous changes, workarounds, or undocumented patches.
9. Schedules and completes maintenance and patch activities in a way that minimizes production impacts.
10. Monitors data transfer performance between automation, production, and administrative systems with business systems (MES, ERP, etc.).
11. Maintains system reference information and documentation.
12. Maintain system logs and other reports and records.

Detect

1. Applies a standardized set of security product and system requirements and produces metrics to report performance against those requirements.
2. Detects security risks, responds to product security incidents and works with customers, plant engineers, and other related functions regarding security issues.
3. Monitors system operations and reacts to events in response to triggers and/or observations of trends or unusual activity.
4. Monitors device data flows, what is expected and what is abnormal.
5. Monitors and address real time variances and alarms.

Respond

1. Responds to alarms and complete initial analysis, response, and notification; coordinate and escalate as needed and per cyber and plant management guidelines.
2. Reviews and processes appropriate incident tickets.

Recover

1. Contributes to roadmaps for cybersecurity actions and improvements.
2. Assists with security code reviews.
3. Assists and supports Engineering, ICS, IT, IS, ESH, etc. and fuller life cycle activities related to planning, improvements, and communications of recovery activities.

Section 3: *Competencies*

Representative Capabilities

This role is often a generalist role, encompassing a range of tasks, responsibilities, and competencies of a cybersecurity systems operator. As a transitional role requiring 2 years or less of additional training in related IT/OT and cyber areas, this is an excellent entry point into cybersecurity for individuals who may not possess a four-year degree but have sufficient and appropriate experience, training, and/or education to begin an operator progression.

(See also the Experience and Education Section 4 and the connections to progression levels of the Cybersecurity Operator Role (Level I, II, and III).

At a minimum, this role at entry levels requires:

1. Fundamental knowledge of production and processing activities and industrial controls and communications.
2. Foundational knowledge of cybersecurity principles, processes, and practices.
3. Familiarity with related cybersecurity regulations, compliance and standards (industry, company, supplier, customers).
4. Increasing hands-on experience with applicable systems and interfaces.

The role also requires increasing levels of knowledge and skill in the application of these competencies:

Systems and Equipment Monitoring, Troubleshooting and Reporting	Cyber-Physical Asset Management
Routine Systems Testing and Maintenance	Industrial Controls Security
Facility and Process Security and Operations	Supply Network Cyber Compliance
Network Security and Operations	Knowledge Management and Analysis
Wireless Network Testing	Incident Handling & Analysis
Intrusion Detection and Prevention	Regulatory Compliance & Audit
Automation and Controls	Basic programming proficiency of PLCs, HMIs, and SCADA systems

Other general, business and personal competencies include:

1. Drive and eagerness to learn with a strong interest in expanding personal cybersecurity skillsets.
2. Increasing knowledge of plant production/processing information, automation and controls environments, and impacts of related physical and digital security concerns.
3. Appropriate and necessary human and environmental safety knowledge and training for particular plant/operational environments.
4. Customer experience mindset for representing both IT and OT concerns; curiosity and ability to bridge production and security concerns and opportunities.
5. Increasing capability in clearly communicating related technical issues and operations in business language to various stakeholders, and vice versa.
6. Ability to work independently and collaboratively.
7. Strong verbal communication skills.
8. Attention to detail and troubleshooting.

Section 4: *Experience And Education*

The Cybersecurity Systems Operator role is structured as a skilled technical worker role also referred to as a “new-collar job,” or “middle-skill job.” It requires certain technical skills, knowledge and experience but does not necessarily require a four-year college degree (or an extensive cyber or industrial work history) to enter. Over time and with expansion, the role can work into both higher-level operator roles and other professional roles, some of which will require a four-year degree. At the onset of entering the Operator progression, apprenticeships and other high-simulation education and development experiences will be essential to early success for this role due to its overall high degree of applied, hands on responsibilities.

Depending on the cybersecurity and plant automation profile of the IT/OT environment where the role would be employed, multiple position levels of the operator role exist for advancement. This overall profile is directed initially at the Operator I level as a transition role for production or industrial controls workers interested in more technical careers or other new(er) to cyber work candidates with diverse backgrounds supplemented with appropriate education and/or certification.

Most duties, outputs, and value in the profile would also hold for an Operator II and III level. Increasing independent responsibility and broadened proficiency in areas of security operations and team coaching and/or customer responsibility, support to other IT, OT and plant operations or network security could come with progression. As a result, the education and experience needs will vary for the Level I, II and III Cybersecurity Systems Operator role.

Section 4: *Experience And Education*

Education

Level I:

Entry-level to Intermediate-level education and or demonstrated training or work experience program completion:

- Minimum high school diploma or GED required.
- Completion of Cyber Systems Operations Initial Skills course, background investigation and Basic Military Training if military transitioning to civilian roles.
- Cybersecurity Operations Apprenticeship or equivalent hands on experience and development.

Level II:

Intermediate-level community college or equivalent education and or demonstrated training or work experience program completion.

As above with Associates Degree and hands on experience and development required;

Bachelor's degree preferred (Cybersecurity, Manufacturing Automation Engineering, Computer or Information Science, Computer Engineering, or a related technical field).

Level III:

Continuing education and/or demonstrated training or work experience program completion.

As above, with Bachelor's degree highly preferred and often required, continuing hands-on experience. (Cybersecurity, Manufacturing Automation Engineering, Computer or Information Science, Computer Engineering, or a related technical field).

Certifications

These are representative certifications that may be desirable or required for particular employers. Some certifications are vendor-specific, and some are vendor-neutral; some may have specific experience requirements and others do not require specific experience requirements. All of them with as much hands-on or applied practice will be important.

	Level I	Level II	Level III
Micro-credentials in related areas (see competencies for topic areas)	●	●	●
Formal Certifications such as:			
CISSP			●
CISM			
CCT, CCNA	●	●	●
CSSP			●
CCSK			●
SSCP		●	●
CompTIA Sec+, NW+	●	●	●
CCA, CCST or related general industrial controls certifications	●	●	●
GICSP, GRID, GCIP or other Industrial controls security certifications	●	●	●

Manufacturing Cybersecurity Systems Operator

Cybersecurity Systems Operations & Development Pathway Overview

Path A
Path B
Path C

Role 1

Manufacturing Cybersecurity Systems Operator

Role 2

Cybersecurity Operations Specialist

Role 3

Industrial Controls Network Security Specialist

Embedded Code Developer-Secure Systems (> SW Developer/Engineer)

IT/OT Integration Engineer
(see Hiring Guide for this path)

Introduction to Career Pathway:

The Cybersecurity Systems Operator is an example of one of the cybersecurity operations roles supporting IT/OT convergence and likely one of those roles that CyberSeek.org indicates are part of the 21% of cyber job openings that require less than a bachelor's degree. These job roles require technical cybersecurity learning and development and experience that can be gained via micro credentials, initial skills courses, bootcamps, apprenticeships and certifications. These apprenticeships and the follow-on actual job experience should also provide professional and early leadership skills. Progression into a more advanced and independent operations specialist would further enable experience in more complex integration, automation and security scenarios; and that additional time and widened experience as a Specialist along with additional certification and experience can open up several higher-level routes. Branching into deeper and more complex Network Security specialization, or into engineering arenas such as Software/Hardware code development, or broader IT/OT integration engineering are all possible when starting as a generalist cybersecurity Systems Operator. Also possible are technical and people leadership routes.

Cyber Risk Management & Governance Pathway A

Path B

Role 1

Manufacturing Cybersecurity Systems Operator

Role 2

Cybersecurity Operations Specialist

Role 3

Embedded Code Developer-Secure Systems

	Manufacturing Cybersecurity Systems Operator	Cybersecurity Operations Specialist	Embedded Code Developer-Secure Systems
Education (Credentials, Certification & Certificates)	• High school/GED required; some additional related coursework highly preferred (towards associate degree or evidence based micro credentials) • Technical training and development • Certifications such as CCT, CCNA, CompTIA Sec+ or NW+ • CCA, CCST; GICSO, GRID, GCIP or other industrial controls related • Specific systems training as required by local operations • Relevant Military Training	• Associates Degree and progress towards Bachelor's degree in Cybersecurity, Computer Science, Information Technology or related area. • Continued or completed professional certification as previous plus additional such as SSCP or movement from Associate certifications into fully granted certifications	• Bachelor's Degree in a relevant field. Cybersecurity, Computer Science, Information Technology or related area. • Additional secure software development certifications from MTA to Azure • CCDH; • CISSP and other Info Security and Cyber certifications; • PSD1 (Srum) and PMP-ACD (Agile Certified) professional certifications • Associate to full certification as experience enables
Experience	• Previous production, technical support or general business experience preferred • Apprenticeships and other applied/hands-on experiences and development required	• Minimum 3-5 years' Systems Operator experience, with progression to Level II and III and related increased independence, complexity and responsibility • Other equivalent experience/ specialized IT and OT Operations experience • Other professional and early leadership skills	• Minimum 6 years' experience (4 years with Master's level or higher degree) in executive program analysis and direct support. • Experience with policy development
Considerations	• Interest in continued development of IT and OT integration and modernized operations • Fundamental knowledge of production/processing activities and industrial controls and communications. • Foundational knowledge of cybersecurity principles, processes, and practices. • Familiarity with related cybersecurity regulations, compliance and standards (industry, company, supplier, customers). • Increasing hands-on experience with applicable systems	• Problem solving, multi tasking & other soft skills • Cross function initiatives and practices • Broad knowledge and increasing experience with various DoD and or other security compliance and standards experience	• Ability to work with other computer and information science roles, hardware engineers and automation experts to secure data and ensure performance. • Increasing ability to support entire Secure Software Development Life Cycle • Strong understanding of industry and product cybersecurity guidelines and regulations