CYMANII the cybersecurity manufacturing innovation institute

SECURE TOGETHER

SECURING THE FUTURE:
2026 Manufacturing & Critical Infrastructure Threat Landscape

Innovations, Risks, and Practical Solutions for U.S. Manufacturers

MARCH 2026

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Manufacturing remains the most attacked industry in the United States, driven by its high-value intellectual property (IP) and critical role in supply chains of other industries. Small and medium manufacturers (SMMs), often hindered by limited resources and outdated legacy systems, are particularly at risk.

This report outlines the current state of manufacturing weaknesses introduced by the complexities of modern environments, including cloud services and Internet of Things (IoT) devices, with particular attention paid to the unique vulnerabilities encountered by SMMs. It also highlights CyManII's strategic initiatives and collaborative solutions to mitigate these risks and strengthen the cybersecurity posture of the manufacturing ecosystem.

Emerging cyber threats in today's manufacturing environments include improper input validation, memory safety weaknesses, authentication and access control weaknesses, and third-party weaknesses, providing insights into the evolving landscape of cyberattacks. Even technological advancements—such as rapid artificial intelligence (AI) adoption, cloud computing, and additive manufacturing (AM)—can create opportunities for exploitation. This report calls for manufacturers to prioritize cybersecurity as a core component of their operational excellence strategy. It also discusses the integration of Cyber-Informed Engineering (CIE) and Secure-by-Design (SbD) principles as essential strategies for addressing risks and enhancing resilience within critical operations.

Additionally, this report emphasizes the importance of sustained collaboration between industry stakeholders, including initiatives led by CyManII, to advance workforce development and strengthen cybersecurity best practices. Coordinated training, shared technical guidance, and sector-wide implementation of proven controls enable manufacturers to enhance resilience and reduce systemic risk across the industry.

Utilizing data from 2025 to inform forward-looking mitigation strategies, this report provides manufacturers with a clear understanding of both current and emerging cybersecurity threats, as well as practical opportunities to strengthen their cyber ecosystems. The following sections detail key vulnerabilities and threat vectors, along with actionable mitigation strategies, many of which have been developed or piloted through CyManII-led efforts. A thorough understanding of these risks and mitigation strategies is essential for manufacturers seeking to strengthen the security and resilience of their manufacturing operations.

MESSAGE FROM THE CEO

CyManII exists to bring new verifiable innovations in cybersecurity to manufacturers, ranging from original equipment manufacturers (OEMs) to SMMs.

We don't just use existing tools; we generate new tools and approaches. Hence, CyManII has made many outstanding accomplishments over the past months. We deployed our cybersecurity innovations to industry and greatly expanded our education and workforce development (EWD) programs by adding efforts around an operational technology (OT)/industrial control system (ICS) bootcamp, as well as on-site training for manufacturers, critical infrastructure (electrical grid, water utilities, etc.), and city governments and municipalities. This report highlights a few select examples of these accomplishments.

This year we are also introducing the **U.S. Manufacturing and Critical Infrastructure Cyber Threat Landscape** section to our report. Our analysis provides private industry—and manufacturers in particular—with objective and relevant information on the evolving nature of cyber risks facing their companies. We augment this non-classified information with forward-leaning information on how CyManII will continue to support the Department of Energy (DOE), especially its nuclear energy mission and the Genesis Mission. The Genesis Mission is a national initiative to build the world's most powerful scientific platform to accelerate discovery science, strengthen national security, and drive energy innovation. Later in this publication, we outline how CyManII is supporting this critical national initiative.

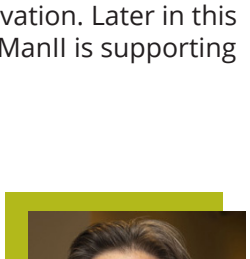
Most importantly, I want to acknowledge the extraordinary team that is making this a reality. The CyManII team, ranging from world leaders in cybersecurity, manufacturing, and workforce development to a stellar operations team, excels day in and day out. Their collective expertise drives the innovation produced by CyManII.

As you digest this information, please remember that we are in the beginning phase of a massive transition in cybersecurity—the incorporation of AI tools into the threat landscape.

CyManII must, and is, transitioning in response to the advent of AI-enabled cyber threats. This is a comprehensive effort that includes:

- *Our work with DOE's Genesis Mission*
- *Our efforts to design radically new approaches to EWD that train operators how to engage their own AI tools to address AI-enabled threat vectors*
- *Our embedding of agentic AI approaches into our Cyber Weakness Enumeration strategy and our Cyber Physical Passport tools*

Stay tuned for the **"2027 Manufacturing & Critical Infrastructure Threat Landscape"** update for more information on how AI is upending the cybersecurity threat landscape, but also know that we are already working with industry to secure U.S. manufacturers.



As always, let us "Secure.TOGETHER."

Dr. Howard Grimes
CyManII CEO

ABOUT CYMANII

The Cybersecurity Manufacturing Innovation Institute (CyManII—Cī-man-ē) was launched by the Department of Energy (DOE) in 2020 to advance cybersecurity for U.S. manufacturing and strengthen U.S. global competitiveness. CyManII is focused on pursuing fundamental research and development (R&D) that advances our understanding of the evolving cybersecurity issues that threaten U.S. manufacturers. The results of this research are improving efficiency in manufacturing industries, inspiring the development of new cybersecurity technologies and innovations, and enhancing cybersecurity knowledge and awareness within the broader community of U.S. manufacturers.

OUR VISION & MISSION

CyManII's vision to be the most innovative cyber-defense team in the world with a mission to innovate—to make U.S. manufacturing **Secure.TOGETHER**—and the deployment of innovative technologies that empower a skilled workforce is now more important than ever.

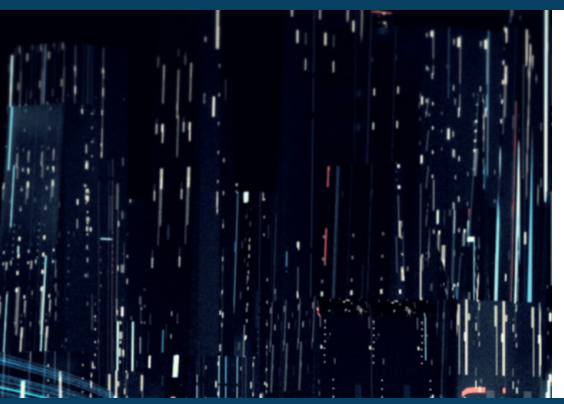
In previous years, CyManII delivered on this mission by introducing a suite of innovative technologies leading to verifiable cybersecurity of data and physical processes, revolutionizing the approach to addressing cyber vulnerabilities, training a workforce in cybersecurity, and building an ecosystem of manufacturing industry stakeholders. CyManII continues to accelerate the maturity of several fundamental innovations that lay a new foundation for delivering robust capabilities for all U.S. manufacturers, and especially SMMs.

CyManII leverages this fundamental research to advance the state of secure U.S. manufacturing in the following three areas:

Innovation with Industry

- Research and develop new technologies and solutions that support cybersecurity, energy efficiency, and decarbonization.
- Train and upskill U.S. workers in information technology (IT) and operational technology (OT) security.
- Inform stakeholders of cyber vulnerabilities and mitigations.
- Increase risk awareness of cyber threats among business decision makers.
- Accelerate adoption of technologies and solutions through industry engagement, demonstrations, and a measurable return on investment (ROI).

Industry Engagement



- CyManII is focused on engaging with and influencing the entire U.S. manufacturing ecosystem. SMMs constitute more than 80% of new institute members within the last year.
- CyManII's engagement strategy is centered on collaborating with partners with different roles and vantages within the manufacturing ecosystem, including original equipment manufacturers (OEMs), integrators, SMMs, and service providers.
- SMMs cannot be secured at scale one-by-one. SMMs must adopt and deploy Secure Defensible Architecture (SDA) principles and tools in order to ensure their security and resiliency.

Education and Workforce Development for Industry and State/Federal Government

- A cyber-informed workforce is essential to secure the U.S. manufacturing ecosystem—and its supply chains—now and for the future.
- CyManII drives the development of a cyber-informed manufacturing workforce with the necessary skills to anticipate, identify, and prevent cyberattacks against information technology (IT) and operational technology (OT) systems.
- CyManII paves the way for a cyber-informed workforce by upskilling and reskilling current and future workers, expanding access to cybersecurity skills for all, and empowering the manufacturing ecosystem to attract and develop a cyber-informed workforce.

OUR IMPACT ON INDUSTRY

Manufacturing dominance and energy security are critical elements of U.S. national security and global competitiveness. For the United States to dominate global manufacturing output, our national assets must be cybersecure and AI-resilient. CyManII is providing industry-focused deployment frameworks to grow the U.S. manufacturing ecosystem and create energy supply chains that are robust, highly productive, and competitive. The urgent challenges facing U.S. manufacturers demand rapid access to the strongest talent, expertise, and capabilities from best-in-class research universities, National Laboratories, and industry.

CyManII has created a direct pipeline to channel innovations to market and strengthen the cybersecurity of industry, fostering collaboration with key National Labs, including Oak Ridge (ORNL), Sandia (SNL), and Idaho (INL), as well as more than 60 U.S. manufacturing organizations such as General Electric (GE Vernova), Lockheed Martin, Cisco, Corsha, Dynics, Humtown, Foley & Lardner, Mazak, and DOE's Manufacturing Demonstration Facility (MDF).

CyManII is piloting solutions to secure legacy systems as well as developing the next generation of secure defensible architectures for U.S. manufacturing dominance and national defense.

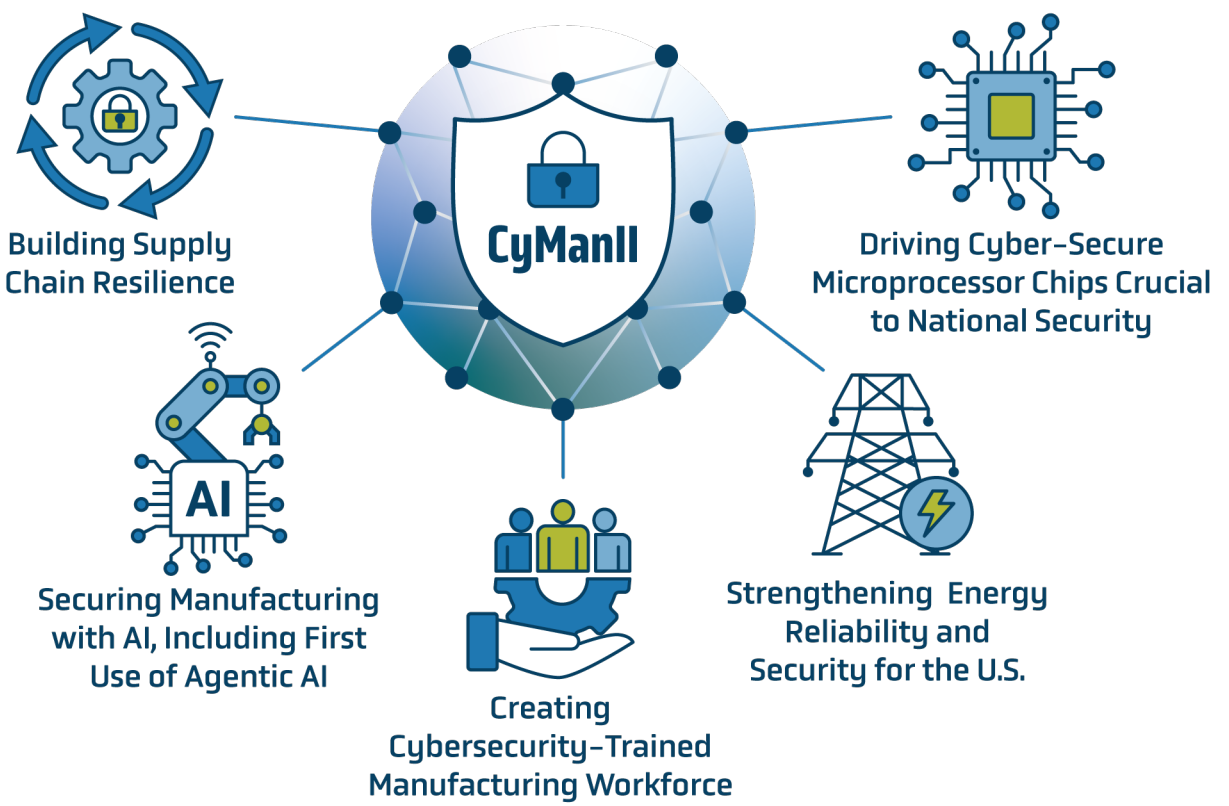
Some of CyManII's solutions, discussed in more detail in Section 4, include:

- *Born-qualified supply chains through use of the Cyber Physical Passport (CPP)*
- *Hardened manufacturing control units supported by a new type of firmware fuzzing*
- *The use of AI to address fundamental weaknesses*
- *Formalized vulnerability and mitigation analysis through CyManII's new data model, the Compositional Attack-Defense Annex (CADA)*
- *Empowering small-to-medium manufacturers*

Looking Ahead

With approval of continued funding, CyManII will continue to accelerate the development and deployment of these innovations in partnership with key industries and processes in the U.S. supply chain, such as: critical and rare earth materials, advanced materials in energy systems, small modular reactor components, power electronics, and semiconductors.

Driving U.S. Manufacturing Resilience + Productivity with Transformative, Secure-by-Design, Cyber-Informed Innovations



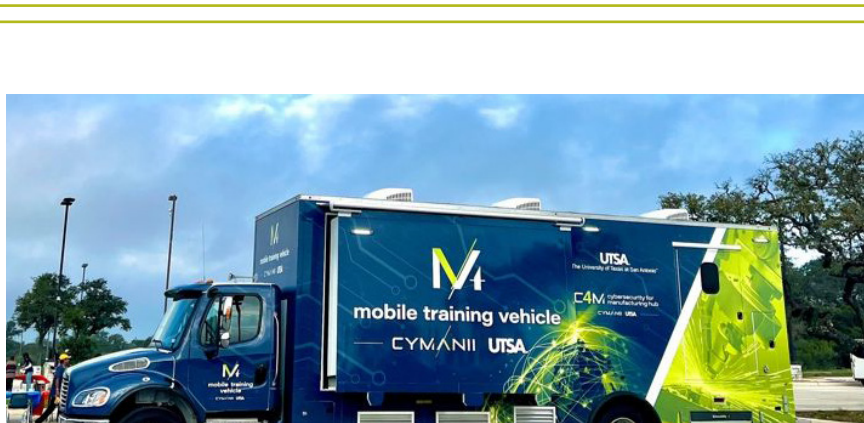
CYMANII'S FACILITIES AND RESOURCES

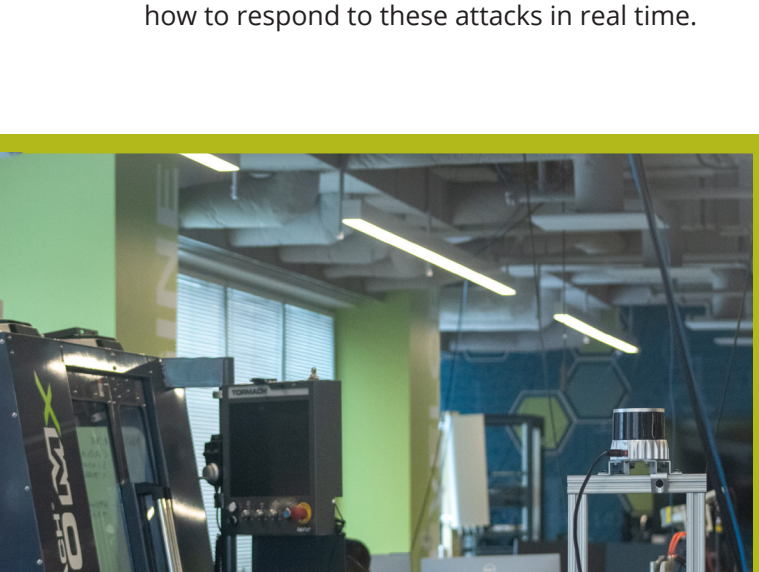
Cybersecurity for Manufacturing (C4M) Hub

Located in the heart of Port San Antonio, the Cybersecurity for Manufacturing (C4M) hub is a 17,000-square-foot training and technology demonstration facility that supports manufacturers by providing access to applied research, engineering support, and hands-on workforce training in secure smart manufacturing. Through partnerships and memberships, CyManII has grown its capabilities to further enhance our cybersecurity training, including hosting events and creating a strong communications link between the hub and Port San Antonio. C4M provides an open venue to host industry in piloting and deploying new cybersecurity innovations on their machines and operations.

Mobile Training Vehicle (MTV)

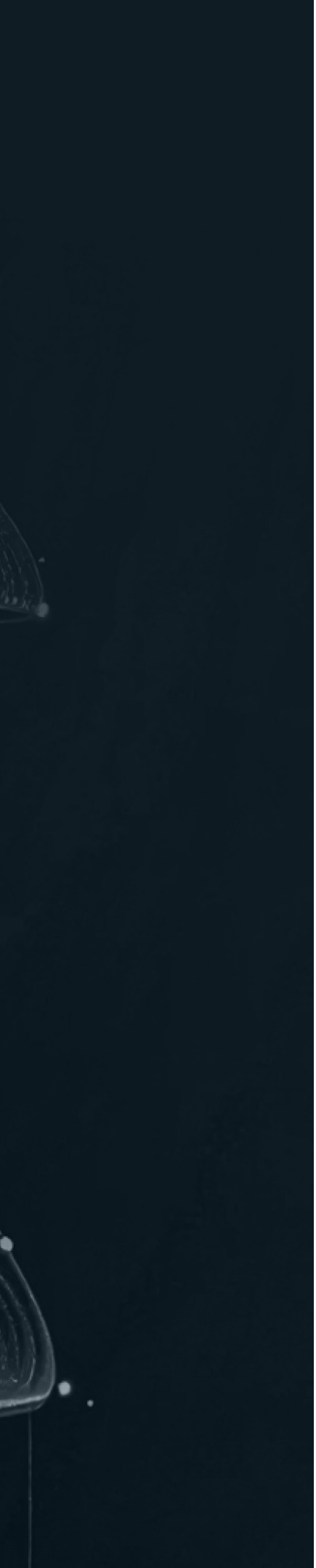
The Mobile Training Vehicle (MTV) is a movable, state-of-the-art cyber range built and operated by CyManII. This Cyber-MTV provides hands-on training "on site," meeting SMMs, manufacturers, and young learners where they are. Team training, individual on-demand labs, and a crisis simulation experience are offered to upskill the workforce in cybersecurity awareness. One of the most popular trainings simulates a live ransomware attack and teaches manufacturers how to respond to these attacks in real time.





University of Texas at San Antonio (UTSA) and George Mason University

CyManII is headquartered in the North Paseo Building on the main campus at UTSA and has an additional HQ annex on the George Mason campus in Arlington, Virginia. These locations, along with C4M, allow us to aggregate scientists, engineers, and leaders from across the nation to tackle the hard challenges of cyber securing the industry of manufacturing. Because we are a "hyper distributed organization" with staff across the United States, we deploy a very agile and efficient work ethic that relies on communication rather than physical proximity.



2

EMERGING TECHNOLOGIES **AND THE SHIFTING LANDSCAPE OF U.S. MANUFACTURING**

For manufacturers, the common theme across 2025's emerging challenges was that digital transformation has brought both opportunity and risk.

Artificial intelligence (AI), digital twins, cloud platforms, additive manufacturing, and robotics are revolutionizing production—*but each one comes with its own set of risks.*

The lesson is clear: cybersecurity is no longer just an IT responsibility; it is a core part of quality, safety, and business continuity in manufacturing and procurement. Companies that treat cybersecurity as part of their operational excellence strategy will be better positioned to innovate safely and remain competitive in 2026 and beyond.

ARTIFICIAL INTELLIGENCE (AI) AND MACHINE LEARNING (ML)

AI is now deeply embedded in factories, helping predict equipment failures, optimize energy use, and spot defects in products. But the same tools that improve efficiency can also be tricked or misused. Researchers have shown that if attackers manipulate the data feeding AI models, the AI might approve faulty parts or miss early warning signs of breakdowns. In other cases, attackers can tamper with the training data that teaches AI how to make decisions, leading to inaccuracies and poor performance that is hard to trace back to its source.

The greatest current value of AI in cybersecurity lies in its ability to support human cybersecurity professionals—reducing alert fatigue, accelerating response times, and automating repetitive tasks. Increasingly, cybersecurity response will involve humans using AI tools to more efficiently mitigate attack vectors. However, as AI capabilities evolve, *so do the risks.*

Ensuring secure artificial intelligence and machine learning implementation is critical to avoid introducing new weaknesses while solving existing ones.

In 2025, manufacturing environments were contending with vulnerabilities arising from the convergence of OT-, IT-, and AI-driven decision support tools.

As highlighted in CyManII's recent paper "Practically Leveraging LLMs for Manufacturing Cybersecurity," large language models (LLMs) can both mitigate and introduce new vulnerabilities in manufacturing systems.[1] The paper highlights how multi-modal models struggle to reliably interpret diagrams, floor plans, and configuration tables, which leads to inconsistent or hallucinated outputs that could misguide operators. When used without expert oversight, these errors introduce operational risk, particularly for resource-constrained manufacturers that often lack specialized cybersecurity staff. At the same time, adversaries are already exploiting generative AI's creative tendencies through misinformation, model poisoning, and prompt injection attacks, creating weaknesses not just in physical machinery but in the very digital assistants meant to safeguard them.

The field of AI is vast and multifaceted, extending far beyond the domain of LLMs. It encompasses various subfields such as computer vision, which empowers machines to interpret and understand visual information; robotics, which involves designing intelligent robots capable of performing complex tasks; and reinforcement learning, where agents learn to make decisions through trial and error.

1 Curtis Taylor, et al., "Practically Leveraging LLMs for Manufacturing Cybersecurity," ACSAC ICSS Workshop 2024, http://acsac.org/2024/workshops/icss/Matthew%20Luallen-LLMs-Cyber-ICCS24.pdf.

DOE'S GENESIS MISSION

The challenges and complexities presented by AI demand a national initiative on a scale equal to the opportunity. The solution is DOE's Genesis Mission, a national initiative to build the world's most powerful scientific platform to accelerate discovery science, strengthen national security, and drive energy innovation.

The Genesis Mission will utilize AI to focus on three priority areas:

- *Achieving American energy dominance through accelerated development of advanced nuclear and fusion energy*
- *Advancing discovery science by building the quantum ecosystem for future innovations*
- *Ensuring national security by developing AI technologies for defense missions and maintaining the nuclear stockpile.*

It has outlined 26 distinct areas of focus, with the first being "Reenvisioning Advanced Manufacturing and Industrial Productivity."

By collaborating with the Genesis Mission, CyManII will help to harness the transformative power of artificial intelligence to drive scientific discovery and better protect manufacturers and members of the energy sector from cyberattacks. This presents an opportunity for CyManII to dramatically accelerate and scale its core mission of securing U.S. manufacturing through enhanced computational resources, expanded partnerships, and national prioritization of manufacturing cybersecurity.

In this environment, maintaining the provenance of AI models and the integrity of the data they utilize is paramount—and CyManII's Cyber Physical Passport (CPP) was designed to address exactly these kinds of concerns.

One of the greatest threats to AI is data poisoning, a type of cyberattack in which adversaries corrupt or manipulate training examples to compromise model behavior. The 2025 NIST Adversarial Machine Learning taxonomy (NIST.AI.100-2e2025)[2] formally recognizes model sanitization as the leading mitigation for availability poisoning attacks, citing foundational work that includes sanitization techniques first proposed in CyManII's CTO's doctoral research. This positions CyManII with rare, recognized depth in exactly the vulnerability class most threatening to AI supply chains used in energy and national security contexts.

The CPP framework (discussed in detail in Section 4) should incorporate model verification and sanitization as first-class lifecycle events. Specifically, every model version's passport should be a record of: sanitization audits performed on training data (with methodology, date, and attesting organization); performance metric baselines used to detect poisoning-induced degradation (precision, recall, F1, AUC); any anomalies detected and the remediation taken; and re-certification attestations following updates or fine-tuning. This transforms model sanitization from a one-time training-stage activity into a continuous, auditable lifecycle record—closing the gap between what NIST recommends and what industry currently tracks.

Furthermore, the Genesis Mission's framework for public-private partnerships, standardized cooperative research agreements, and competitive fellowship programs will enable CyManII to expand its reach beyond its current membership base, accessing advanced AI capabilities from leading technology companies while maintaining the stringent cybersecurity and supply chain security standards the Institute has developed.

2 Apostol Vassilev, et al., "Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations," NIST, Mar. 2025, https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-2e2025.pdf.

DIGITAL TWINS AND SIMULATION ENVIRONMENTS

Digital twins—virtual copies of machines and production lines—are becoming a staple within modern manufacturing. They allow teams to test new processes, optimize output, and anticipate problems before they happen. However, digital twins are only as good as the data that feeds them. If a twin is compromised, it could give operators false confidence or mask problems in the real plant. Cloud-hosted twins also carry risks if access is not well-controlled.

Digital twins can speed up decision-making and innovation, but they must be protected like any other production tool. Strong access controls, secure data sharing, and regular validation that the twin matches real-world conditions are critical to prevent costly mistakes.[3]

INDUSTRIAL ROBOTICS AND AUTONOMOUS SYSTEMS

Robots and autonomous guided vehicles are transforming factories, making them faster and safer. However, they rely on complex software and sensors that can be manipulated.

If attackers interfere with a robot's instructions or sensors, it could move unpredictably, create faulty products, or even put workers at risk. Since robotic systems often run for years without major updates, they are especially vulnerable to long-term threats. Robotics will keep advancing, but safety and reliability must include cybersecurity. Asking vendors about update practices, monitoring robots for unusual behavior, and training staff to recognize issues can help prevent both accidents and sabotage.

3 JP Perez-Etchegoyen, "Business-Critical Applications Under Attack: The Rise of SAP, Salesforce, and Oracle Breaches," *Onapsis*, Nov. 6, 2025, https://onapsis.com/blog/sap-salesforce-oracle-attacks-rising-2025-report/.

ADDITIVE MANUFACTURING (3D PRINTING)

3D printing and additive manufacturing are moving from prototypes to production parts in the aerospace, automotive, and healthcare industries. But the direct link between digital designs and physical products creates opportunities for sabotage. Researchers have shown it is possible to subtly alter print instructions or machine settings to disguise flaws. In industries where safety is critical, this could have devastating consequences. The integration of advanced automation, embedded software, and IoT-enabled smart devices on the factory floor has expanded the attack surface, rendering traditional perimeter security measures inadequate.[4] In particular, "digital-first" technologies like additive manufacturing (AM) carry inherent cyber risks because if a 3D printer's design files or settings are maliciously altered, the resulting product may be defective in ways that are difficult or impossible to detect or fix after production.[5] An adversary having the potential to alter a product design file immediately before or during printing is a threat to product integrity, IP privacy, and service uptime, making cyber sabotage a major concern and slowing the adoption of AM technologies.

Protecting design files, using only trusted machine firmware, and adding quality checks beyond visual inspection are essential. Manufacturers adopting additive manufacturing should treat cybersecurity as part of quality assurance, not just IT overhead.

INDUSTRIAL CLOUD AND REMOTE MANAGEMENT

Many equipment vendors now offer cloud platforms that let manufacturers monitor and manage machines remotely. Cloud platforms save time and provide valuable insights into the manufacturing floor, but they also create a single point of failure if organizations rely too heavily on digital monitoring.

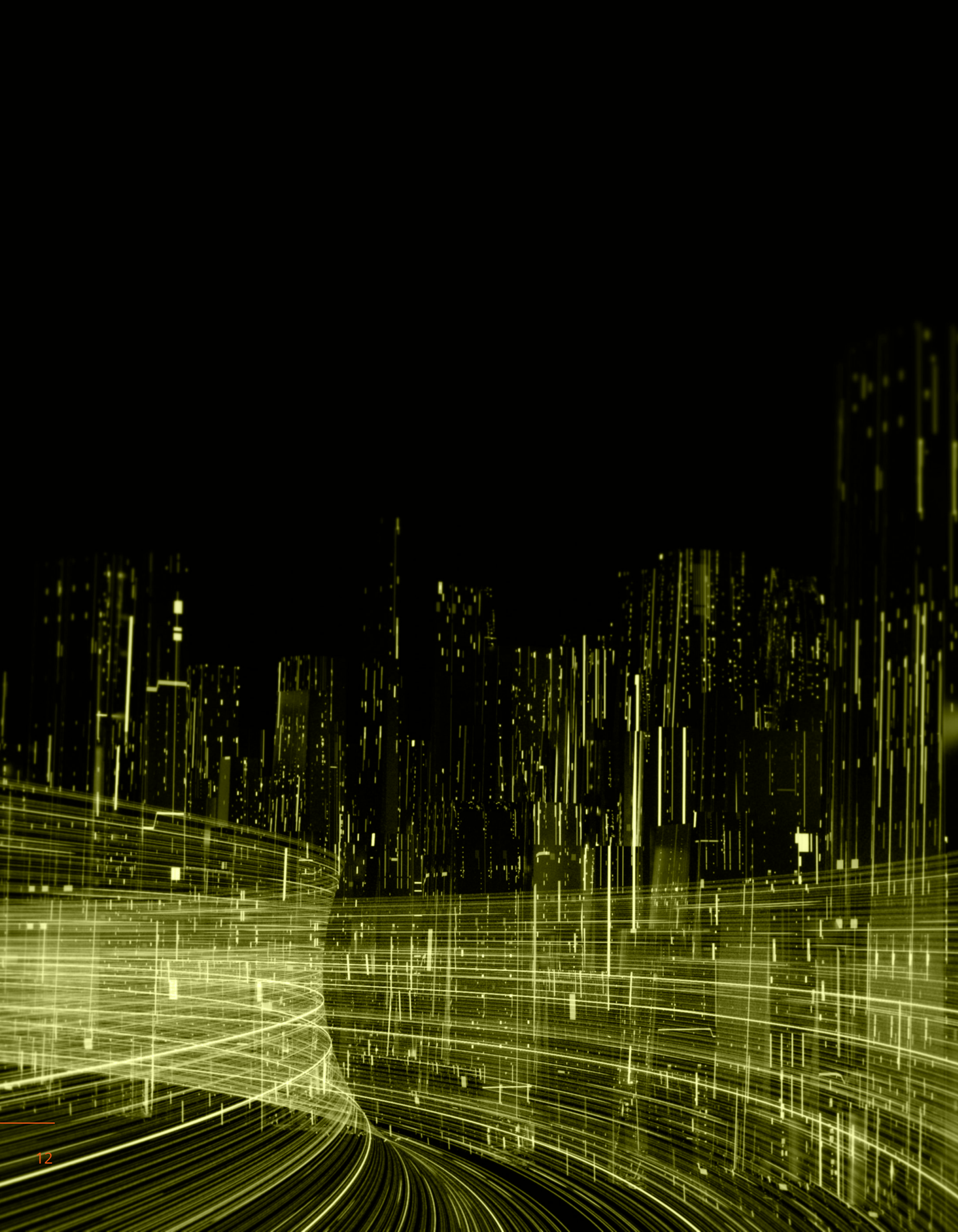
A vendor platform breach could affect multiple factories at once. High-profile cyber incidents in other industries have shown how quickly cloud-based disruptions can cascade across supply chains, halting production, and creating widespread operational and financial impacts.[6] Manufacturers should require vendors to document how remote access is secured, how sessions are authenticated and monitored, and what controls allow immediate suspension of access if anomalous activity is detected. These expectations should be formalized through secure procurement requirements and contractual provisions such as defined cybersecurity obligations, audit rights, incident notification timelines, and access control standards.

A well-structured vendor relationship, grounded in enforceable security terms and continuous oversight, can significantly reduce operational risks.

4 "IBM X-Force 2025 Threat Intelligence Index," IBM, https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/2025-threat-intelligence-index.

5 "Model-based security analysis in additive manufacturing systems," CyManII, https://cymanii.org/resource/model-based-security-analysis-in-additive-manufacturing-systems/.

6 JP Perez-Etchegoyen, "Business-Critical Applications Under Attack: The Rise of SAP, Salesforce, and Oracle Breaches," *Onapsis*, Nov. 6, 2025, https://onapsis.com/blog/sap-salesforce-oracle-attacks-rising-2025-report/.



3

U.S. MANUFACTURING AND CRITICAL INFRASTRUCTURE CYBER THREAT LANDSCAPE

The manufacturing sector stands at the forefront of technological innovation and economic development and is essential for sustained growth and global U.S. competitiveness. Yet, it faces unprecedented security challenges that threaten its growth and stability.

The manufacturing sector has emerged as the most targeted industry for cyber adversaries and holds the unfortunate distinction of being the most attacked sector for four consecutive years.[7] Manufacturers make particularly compelling targets for cyber adversaries due to their high-value intellectual property (IP), the critical role they play in supply chains, and their low tolerance for operational downtime.[8]

Complex supply chains for hardware and electronics expand the attack surface for U.S. manufacturers while dependencies on overseas components, contract manufacturers, and third-party software can introduce hidden vulnerabilities, malicious code, or unsupported components into critical systems. Components from foreign entities of concern (FEOCs) can introduce backdoors or other exploitable flaws, features, and malicious code, undermining security from the outset.[9] These risks are amplified by multi-tier subcontracting structures, limited transparency into sub-suppliers, and insufficient oversight of vendor security practices. Manufacturers are increasingly concerned about scenarios in which supply chain dependencies could be leveraged to disrupt operations directly, including denied firmware updates, malicious or corrupted software patches, or the activation of remote management features that function as de facto kill-switches capable of halting production lines. Recent nation-state campaigns have demonstrated that sophisticated adversaries deliberately target trusted hardware and software suppliers to compromise update mechanisms and distribute malicious code to multiple downstream customers simultaneously.[10]

SMMs face unique challenges in this landscape. Often lacking the resources and unified solutions necessary to effectively prevent, detect, and respond to cyberattacks, many SMMs continue to operate legacy OT equipment that features minimal connectivity and few security controls. These legacy systems were not designed with cybersecurity in mind, resulting in environments that are frequently under-monitored, unpatched, and inadequately segmented from business networks.

Like SMMs, many critical infrastructure owners and operators rely on legacy equipment that is not easily protected against modern attacks, leaving them equally vulnerable to attacks on their OT and ICS systems.[11] This situation creates significant gaps where intrusions can go unnoticed, directly impacting production and safety. The rapid digital transformation of the manufacturing sector—characterized by the integration of cloud-connected equipment and AI-driven processes—has outpaced cybersecurity, leading to a "perfect storm" of vulnerabilities and weaknesses.

7 "IBM X-Force 2025 Threat Intelligence Index," IBM, https://www.ibm.com/reports/threat-intelligence.

8 "Supply Chains Under Siege: Top 3 Cyber Threats to Manufacturing," *Bitsight*, Aug. 13, 2025, https://www.bitsight.com/blog/inside-cyber-threats-in-manufacturing-2025.

9 "Information and Communications Technology Supply Chain Security," Cybersecurity and Infrastructure Security Agency, https://www.cisa.gov/topics/information-communications-technology-supply-chain-security.

10 Anna Ribeiro, "CISA releases 2025 SBOM Minimum Elements outlining minimum requirements for software transparency," *Industrial Cyber*, Aug. 25, 2025, https://industrialcyber.co/cisa/cisa-releases-2025-sbom-minimum-elements-outlining-minimum-requirements-for-software-transparency/.

11 Callie Guenther, "Five ways to protect critical infrastructure ops that run on legacy IT," *SC Media*, Dec. 23, 2024, https://www.scworld.com/perspective/five-ways-to-protect-critical-infrastructure-ops-that-run-on-legacy-it.

MANUFACTURING RANSOMWARE ATTACKS IN 2025

Cyberattacks on manufacturing and industrial companies surged in 2025, with ransomware the most prevalent threat. Attackers recognize that even brief production outages can cost millions in lost revenue, making manufacturers high-payoff targets for extortion.

While this report focuses on the evolving ransomware threat to manufacturing and OT environments, detailed prevention, mitigation, and recovery guidance is provided in CyManII's Ransomware Preparation Guide. The playbook translates these threats into practical actions for manufacturers, emphasizing workforce readiness, secure data backups, and OT-aware incident response practices across all phases of a ransomware event.

RECENT DATA SHOWS A SHARP RISE IN BOTH THE FREQUENCY AND IMPACT OF ATTACKS.

7,419

Global ransomware incidents in 2025

51% of these (3,810) were carried out on U.S. organizations

The United States saw a 33% increase in the number of attacks from 2024.[12]

Statistics from 2025 confirm that ransomware remains a persistent and growing threat to manufacturing. Disrupting individual ransomware groups has not reduced overall activity; new actors routinely emerge, many using ransomware-as-a-service models to sustain the ecosystem.[13] Many ransomware groups now employ multi-layered extortion strategies that combine system encryption with data theft and threats to publicly release proprietary information if payment is not made. In 2024–2025, a notable increase in "encryption-less extortion" was observed, in which groups such as Cl0p focused solely on exfiltrating sensitive data and demanding payment without deploying file encryption.[14] This approach is particularly effective against manufacturers, as the risk of IP exposure, competitive harm, contractual liability, and regulatory penalties can be just as damaging as production downtime.

The exploitation of newly converged IT and OT networks in manufacturing remains a major concern. As noted earlier, the traditional isolation (airgap) of factory control systems has eroded; many OT systems are connected to corporate IT or cloud services for efficiency. Ransomware groups have taken advantage of these gaps by breaching IT (often via phishing or stolen credentials) and then pivoting to OT. In one case, a U.S. manufacturer suffered major production delays when a ransomware attack on the corporate IT network spread to plant floor systems. This convergence means a cyber incident can no longer be "contained" to just office computers; it can disrupt industrial control systems (ICS), halt production lines, and directly affect physical equipment and product output.[15]

12 Rebecca Moody, "Worldwide ransomware roundup: 2025 end-of-year report," *Comparitech*, Jan. 13, 2026, https://www.comparitech.com/news/worldwide-ransomware-roundup-2025-end-of-year-report/.

13 Michael Lester, "Top manufacturing cyber risks of 2025," *WTW*, Dec. 6, 2024, https://www.wtwco.com/en-us/insights/2024/12/top-manufacturing-cyber-risks-of-2025.

14 "CISA and FBI release advisory on CL0P ransomware gang exploiting MOVEit vulnerability," Cybersecurity and Infrastructure Security Agency, Jun. 7, 2023, https://www.cisa.gov/news-events/news/cisa-and-fbi-release-advisory-cl0p-ransomware-gang-exploiting-moveit-vulnerability.

15 Shane, "Industrial Ransomware Surge: Dragos Q1 2025 Analysis Reveals Critical Threats to Manufacturing and Infrastructure," *CinchOps*, Jun. 9, 2025, https://cinchops.com/dragos-q1-2025-analysis-reveals-critical-threats/.

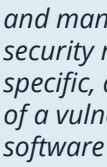
TOP CYBER WEAKNESSES OBSERVED IN 2025

In addition to ransomware attacks, manufacturing environments continue to face a concentrated set of software and supply chain weaknesses that create elevated cyber and operational risk, particularly within ICS and OT. CyManII analysis of publicly disclosed weaknesses from November 2024 through November 2025 shows that a small number of recurring weakness categories account for a disproportionate share of high-impact manufacturing vulnerabilities.

The most significant risks stem from improper input validation, memory safety failures, authentication and access control weaknesses, and third-party supply chain exposures. These weaknesses appear frequently in manufacturing-specific advisories and often map to high-severity exploitation outcomes, including remote code execution, unauthorized access to cyber-physical systems, data exfiltration, production disruption, and safety impacts to human operators.

The findings rely on a structured ranking methodology that combines frequency of occurrence with severity, using MITRE's Top 25 Most Dangerous Software Weaknesses[16] framework and Common Vulnerability Scoring System (CVSS) data.[17] This approach enables prioritization of weaknesses that are both prevalent and operationally consequential in manufacturing contexts.

Manufacturers face a variety of weaknesses that can impact their operations, supply chains, and overall business performance. Top manufacturing weaknesses in the supply chain are critical concerns that need to be addressed to ensure the security and resilience of ICS and OT. These weaknesses include cyber threats, supply chain disruptions, compliance issues, and third-party risks.



The distinction between Common Vulnerabilities and Exposures (CVE) and Common Weakness Enumeration (CWE) is essential for understanding and managing software security risks. A CVE refers to a specific, documented instance of a vulnerability discovered in software or hardware.

The CVE ID is an assigned unique identifier for tracking and remediation. In contrast, a CWE comprises a broader category or pattern of software and hardware weaknesses that can lead to vulnerabilities, such as improper input validation or insecure authentication mechanisms.

While CVEs represent real-world, exploitable issues, CWEs provide insight into the underlying coding or design flaws that cause them. CVEs map to one or more CWE, making both systems complementary tools in vulnerability management and secure software development.

16 "CWE Top 225 Most Dangerous Software Weaknesses," MITRE, https://cwe.mitre.org/top25/.

17 "CVSS (Common Vulnerability Scoring System," *BitSight*, Oct. 14, 2025, https://www.bitsight.com/glossary/cvss-common-vulnerability-scoring-system.

Weakness Identification Methodology

For the purposes of this report, the CyManII team gathered publicly released CWEs from the Cybersecurity and Infrastructure Security Agency (CISA) Common Security Advisory Framework (CSAF) GitHub and vendor self-reports.[18] Additionally, MITRE's Top 25 Most Dangerous Software Weaknesses methodology was used alongside the CWEs to rank and identify the most dangerous weaknesses from November 2024 to November 2025.[19]

This scoring system assigns a danger score to each CWE based on its frequency and severity:

(Frequency x Severity) x 100 = Danger

In the following sub-sections, we highlight manufacturing weaknesses that have some of the highest danger scores of all reported manufacturing weaknesses from November 2024 to November 2025.[20]

Figure 1 highlights additional CWEs gathered through our research methodology.

Frequency Score:

The frequency score is calculated by taking the total number of times a weakness has been reported and subtracting the minimum frequency of weaknesses in the dataset. This result is then divided by the difference between the minimum and maximum frequencies of weaknesses in the dataset.

Severity Score:

The severity score is determined by subtracting the lowest CVSS score recorded of all the recorded CWEs in the dataset from the average CVSS score for all instances of that CWE. This difference is then divided by the range of CVSS scores (the difference between the minimum and maximum CVSS scores).

Danger Score:

The frequency and severity scores for each CWE are multiplied together, and the result is then multiplied by 100 to produce the danger score.

Top 10 Most Dangerous Manufacturing CWEs, Nov. 2024–Nov. 2025

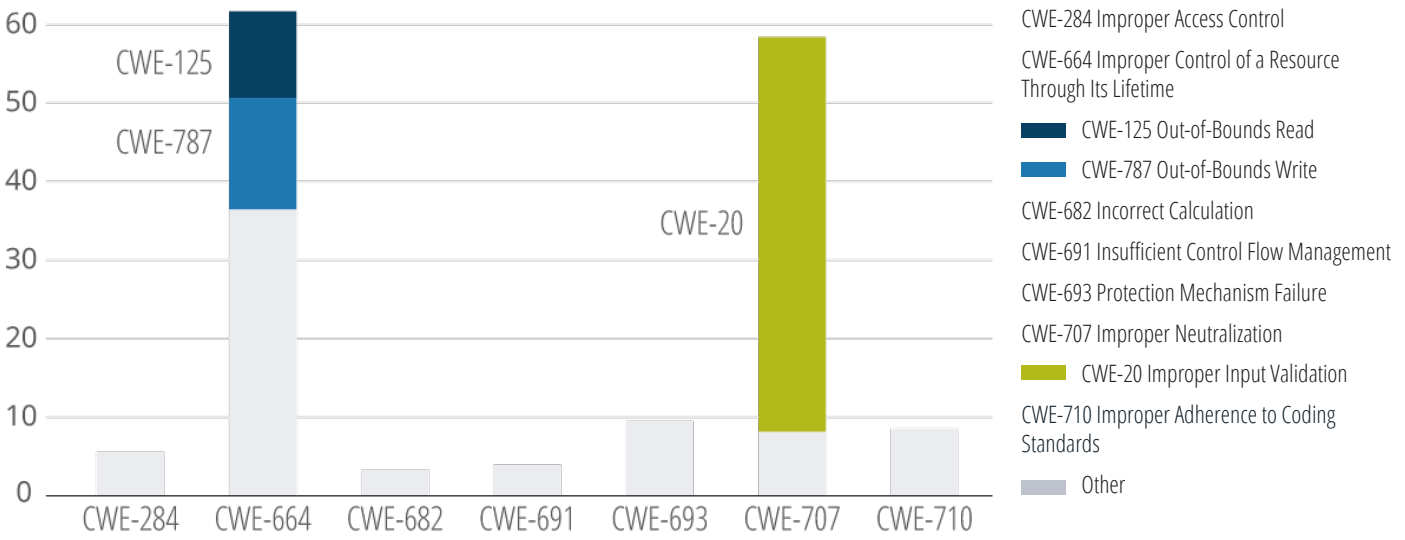


Figure 1. *This figure contains the top ten most dangerous manufacturing weakness categories identified from November 2024 to November 2025. The top 25 weaknesses have been categorized into 10 parent weaknesses based on the Research Concepts CWE view, and the top three most dangerous weaknesses have been identified.*

18 "CSAF OT white files," GitHub/CISA, https://github.com/cisagov/CSAF/tree/develop/csaf_files/OT/white.

19 "2024 CWE Top 25 Most Dangerous Software Weaknesses: Methodology," MITRE, https://cwe.mitre.org/top25/archive/2024/2024_methodology.html.

20 "CISA CSAF repository," GitHub/CISA, https://github.com/cisagov/CSAF.

Improper Handling and Data Validation

Applying MITRE's Top 25 Most Dangerous Software Weaknesses calculation to publicly reported manufacturing-specific vulnerabilities from 2024–2025, the most dangerous manufacturing weakness is CWE-20: Improper Input Validation. CWE-20 emerged as the most dangerous manufacturing CWE due to its medium to high severity and remarkably high frequency. The Improper Input Validation weakness occurs when input data is not validated or is incorrectly validated to check that the inputs are safe and will be safely processed within the code or other components of the system. CWE-20 can result in an attacker exploiting this weakness, causing the system or device to unexpectedly expose confidential information, modifying data on the system or device, enabling arbitrary command execution, or providing unexpected commands that cause the system to crash. If CWE-20 is present in a manufacturing environment, the potential consequences of an adversary performing a cyberattack may result in compromised intellectual property and sensitive information, significant loss of revenue if a machine must be shut down, or significant injury or loss of life to an employee.

Memory Safety Weaknesses

Some of the more critical and prevalent CWEs identified in the past year relating to memory safety are those surrounding out-of-bounds reads and writes. Memory safety weaknesses are created during the development of software and tools but can go unnoticed because the vulnerability does not occur until the software runs and the memory is not properly processed. These vulnerabilities provide unauthorized privileges, allowing attackers to execute malicious code, steal sensitive data, or cause system instability leading to potential data corruption and unexpected program behavior. Some contributing factors for these weaknesses include insecure coding practices, not using memory-safe languages, and improper input validation. To prevent memory safety vulnerabilities altogether, memory-safe languages, such as Rust and Go, should be used.

An out-of-bounds write occurs when an app can write to memory outside of the permissible bounds for writing to memory. This vulnerability is a memory and buffer overflow–related weakness and is a descendent of CWE-664: Improper Control of a Resource Through Its Lifetime. This weakness allows a bad actor to write unauthorized code that could cause memory corruption or unexpected results. If an out-of-bounds write is present in a manufacturing environment, specifically on a programmable logic controller (PLC), an attacker could erase the device configuration and corrupt the firmware, halting production. Existing memory safety vulnerabilities can be mitigated by non-executable memory, control flow integrity, address space layout randomization, sandboxing, and hardening memory allocators.[21]

21 "The Case for Memory Safe Roadmaps," Cybersecurity and Infrastructure Security Agency, Dec. 2023, https://www.cisa.gov/sites/default/files/2023-12/The-Case-for-Memory-Safe-Roadmaps-508c.pdf.

Authentication and Access Control Weaknesses

Authentication-related weaknesses, such as hard-coded credentials, missing authentication for critical functions, and weak password requirements remain a category of weaknesses with high danger scores in manufacturing environments. These authentication weaknesses allow adversaries to gain unauthorized access to systems and data. In manufacturing-specific contexts, authentication vulnerabilities may provide attackers access to personally identifiable information (PII), IP, sensitive company information, and potentially restricted or export-controlled data, as well as access to cyber-physical systems—which can jeopardize the safety and security of human operators, damage machines, and compromise the quality of the product. These weaknesses can arise from insecure coding practices, system misconfiguration, and poor password hygiene.

Authorization-related CWEs put systems at risk of being accessed by unauthorized users, leading to potential data breaches and risk systems being viewed or changed without proper restrictions. Access control, authentication, and authorization weaknesses can significantly increase the damage a potential attacker can do within a system. Many of these weaknesses can be mitigated with strong password policies, cybersecurity training, and changing root passwords. A practical example is 3D printers, where anyone with physical access can update the firmware or enable network root access using local controls.

DEFENDING AGAINST WEAKNESSES

To defend against these challenges, manufacturers are adopting both technology and strategy improvements.

On the technology side, many firms are investing in threat detection and response capabilities tailored to OT environments, including network monitoring of industrial protocols and anomaly detection within control systems. Organizations are also strengthening segmentation between IT and OT networks and adopting zero-trust architectures that continuously verify user and device access before granting connectivity.

Artificial intelligence and advanced analytics show promise in detecting deviations in production behavior that may signal sabotage, manipulation, or malware activity. In parallel, manufacturers are implementing engineered fail-safes designed to maintain safe operating conditions even if digital control systems are compromised. These controls help ensure that a cyber intrusion does not automatically translate into unsafe physical consequences.

Industry stakeholders are increasingly embracing Secure-by-Design (SbD) principles and Cyber-Informed Engineering (CIE), which focus on designing systems that can tolerate cyber disruption without catastrophic operational failure. For example, engineering controls may include mechanical overrides or analog safety interlocks that activate if digital controls are manipulated, preventing unsafe states in systems such as high-speed production lines.

Industry collaboration also plays a central role in strengthening resilience. Organizations such as CyManII are disseminating practical guidance, workforce training, and implementation of resources tailored to manufacturers, particularly SMMs. These efforts emphasize achievable actions, including updating legacy equipment where feasible, enforcing strict access controls, improving network segmentation, establishing supply chain provenance through mechanisms such as Cyber Physical Passports (CPPs), and developing incident response plans specifically adapted to manufacturing environments.[22]

Together, these technical and strategic measures (further detailed in Sections 4 and 5) help manufacturers move beyond reactive cybersecurity and toward a more resilient, consequence-focused approach.

22 "CyManII Cyber Readiness Training Helps Manufacturers Face Daunting Digital Future," Manufacturing USA, Aug. 15, 2025, https://www.manufacturingusa.com/news/cymanii-cyber-readiness-training-helps-manufacturers-face-daunting-digital-future.

CYMANII SOLUTIONS

CyManII has developed next-generation solutions to help manufacturers, from education and workforce development (EWD) tools and trainings to network guards and digital twins, and special solutions tailored specifically to SMMs.

Over the past 18 months, CyManII has been facilitating Industry Use Cases (IUCs) among manufacturers to harden their systems by identifying and addressing common weaknesses in past and future manufacturing systems.

IUCs are essentially pilot projects meant to demonstrate the real-world potential of CyManII's research and innovation and are just one of the many ways CyManII works with industry to bring new technologies to market. Each IUC project is co-led by a member of the CyManII team and a representative from the company that owns the system in which the pilot will be deployed. Each project is designed to advance larger objectives—such as ensuring the provenance of physical parts for specialized manufacturing devices or validating the cybersecurity of digital components retrofitted to legacy systems—while also driving development of the supporting technological capabilities needed to implement and deploy the pilot project.

The projects highlighted below reveal several themes and innovative approaches to securing manufacturing IT and OT systems.

STRENGTHENING THE CYBER WORKFORCE THROUGH ASSESSMENTS AND EXPERIENTIAL LEARNING

Most cyber intrusions are due to human error.[23] A robust training program can significantly decrease the volume and veracity of cyberattacks. CyManII has developed an extensive range of training options—for everyone from floor operators to the C-suite—to assist manufacturers in preventing and mitigating cyberattacks. By providing the tools, support, and training to educate and upskill the workforce in IT/OT cybersecurity, CyManII has made EWD a central aspect of its work.

CyManII provides a range of EWD solutions for common cybersecurity challenges, from in-person training at the CyManII Cyber Range to on-site lessons and simulations with the Mobile Training Vehicle (MTV). CyManII's Learning Library offers a deep catalog of self-led modules, and our EWD program also offers hands-on Cyber Maturity Model Certification (CMMC) preparation and assessments.

Training solutions to improve IT and OT cybersecurity worker readiness extend beyond manufacturing, and CyManII now provides cybersecurity readiness assessments and exercises for local governments and critical infrastructure owners and operators. In 2025, CyManII offered live cyberattack simulations in Eagle Pass and Mission, Texas, to help city officials and infrastructure operators assess their readiness posture and develop the muscle memory to respond quickly and efficiently in the event of a compromise.

Over a six-month period, CyManII trained 140 critical infrastructure professionals across five Texas counties and eight critical infrastructure sectors, including both technical staff and C-suite members. This cohort is responsible for critical infrastructure used by 3.6 million people.

23 A 2024 report by Mimecast attributes 95% of all data breaches to human error. See Mimecast, *The State of Human Risk 2025*, accessible at: https://www.mimecast.com/resources/ebooks/state-of-human-risk-2025/; J. Coker, "95% of Data Breaches Tied to Human Error in 2024," *Infosecurity Magazine*, Mar. 11, 2025, https://www.infosecurity-magazine.com/news/data-breaches-human-error/.

SECURING THE FULL PRODUCT LIFECYCLE WITH CYBER PHYSICAL PASSPORTS (CPPs)

Modern manufacturing depends on globally distributed, digitally mediated supply chains. A single industrial product can incorporate millions of components sourced from hundreds of suppliers, often spanning multiple jurisdictions. While this model enables scale and efficiency, it introduces systemic risk: manufacturers frequently lack a reliable, verifiable way to confirm where a component came from, how it was produced, whether it was altered, or whether it still meets safety and security requirements once deployed.

CyManII has developed five separate technologies for cyber-securing our nation's critical supply chains—collectively integrated into the Cyber Physical Passport (CPP).[24] The CPP goes well beyond any existing "passport," such as those developed by the European Union, to secure every transaction in a manufacturing process and establish provenance across the supply chain, including for emerging technologies such as digital twins and AI. CPPs can apply to all manufacturing processes and are being implemented and tested by Manufacturing Demonstration Facility (MDF) and our industry collaborators across multiple sectors. Through an IUC, GE Vernova is currently piloting the CPP with suppliers to provide a consistent framework-validating provenance—performing security verifications formally and analytically—and to provide both quality and security guarantees for critical energy components manufactured in the United States.

A CPP functions as a persistent digital object that is bound to a specific physical artifact or process and evolves as that artifact moves from design to production to deployment and into operation. Unlike static documentation, CPPs are append-only and hierarchical. They capture evidence at each stage of the manufacturing lifecycle, including but not limited to:

- *Design baselines and design tool chains*
- *Software, firmware, and hardware bills of materials*
- *Manufacturing process parameters and transformations*
- *Test, evaluation, and verification results*
- *Operational state changes and updates over time*

Each update to a CPP is identity-bound and digitally signed, creating a tamper-evident record that can be independently validated. This structure allows manufacturers to verify not just what a component claims to be, but whether it has remained trustworthy throughout its lifecycle.

The CPP directly supports five of the nine priorities outlined by U.S. Secretary of Energy Chris Wright to unleash American energy, with active participation from industry partners.[25] By applying modern AI to manufacturing supply chains, CPPs strengthen supply chain assurance, improve visibility into vulnerabilities and mitigations, and protect critical energy infrastructure, advancing both national security and reliable energy production.

24 "Cybersecurity resources for advanced manufacturing," *AdvancedManufacturing.org*, https://www.advancedmanufacturing.org/resources/cybersecurity/.

25 Exec. Order No. 14154, 90 Fed. Reg. 8353 (Jan. 20, 2025), https://www.federalregister.gov/documents/2025/01/29/2025-01956/unleashing-american-energy.

CPPs are already being piloted and deployed across multiple CyManII IUCs, spanning large OEMs and SMMs. They are central components to many IUC projects, demonstrating their versatility:

Energy Sector:

In energy sector deployments, CPPs are used to track the provenance and configuration state of ICS components from fabrication through commissioning and operation. This enables operators to verify that controllers and firmware match approved baselines and have not been altered through unauthorized updates or supply chain compromise.

Additive Manufacturing:

In additive manufacturing environments, CPPs aggregate design data, machine telemetry, in-situ monitoring outputs, and post-build inspection results into a single, verifiable record per part. This approach directly addresses the risk of subtle cyber-induced defects that may not be visible through traditional quality assurance methods but can materially affect performance and safety.

Small and Medium Manufacturers:

For SMMs, CPP deployments have demonstrated value beyond cybersecurity alone. By consolidating production data, quality evidence, and process history into a unified structure, CPPs have supported improved diagnostics, reduced rework, and enabled stronger supplier–customer trust relationships, all while operating within resource-constrained environments.

These highlighted use cases show that CPPs function as both a security control and a manufacturing optimization mechanism, reinforcing their relevance to DOE priorities that link security, productivity, and energy efficiency.

PROTECTING LEGACY "BROWNFIELD" SYSTEMS

The Kry10 IUC project focuses on legacy industrial systems connected to the internet without adequate protection. They developed a network guard based on a formally verified microkernel (seL4) that filters network traffic, restricting it to known endpoints and safe commands, thereby providing a secure solution without requiring a full system replacement.

IMPLEMENTING SECURE-BY-DESIGN

Secure-by-Design (SbD) is a cybersecurity principle advanced by CISA that directs technology manufacturers to deliver products that are secure by default rather than relying on post-deployment configuration by customers.[26] For decades, many software and hardware products shipped with permissive default settings, exposed services, and weak authentication controls. Vendors often prioritized feature velocity, market share, and interoperability. Security hardening became the customer's responsibility. That approach proved unsustainable as threat actors scaled exploitation of common weaknesses such as default credentials, injection flaws, and memory safety errors. CISA's position is direct: manufacturers should eliminate entire classes of vulnerabilities during design and development instead of depending on patches and downstream mitigations. The 2020 SolarWinds supply chain intrusion illustrates the systemic risk created by opaque software dependencies.[27] Malicious code inserted into a trusted update propagated to roughly 18,000 customers, including federal agencies and critical infrastructure operators.[28]

A Purdue University IUC project is demonstrating an SbD approach by replacing the controller in a commercial 3D printer with one built using a tamper-resistant microcontroller. This hardware-based approach ensures firmware integrity and enables secure-by-default communication protocols, mitigating an entire class of vulnerabilities from the start.

NON-INVASIVE MONITORING FOR THREAT DETECTION

Several projects focus on detecting attacks without modifying the target machine. The UTSA-led STRAP-AM IUC project is exploring the use of radio frequency (RF) signal emissions, energy consumption data, and camera feeds of the human-machine interface (HMI) to monitor additive manufacturing machines for anomalies. Similarly, an Ohio State University project is developing a low-cost powerline monitoring solution for legacy AM machines to track build-to-build signatures.

TAILORING SOLUTIONS FOR SMMS

SMMs are finding a wealth of new benefits and efficiencies in digitization—but digitization can introduce new cyber risks, which CyManII is working to mitigate. One of CyManII's IUC projects demonstrated the success of CyManII technologies in securely digitalizing a composite rebar thermal curing process to improve efficiency through a cybersecurity blueprint. The project was led by Michigan Technological University in collaboration with an SMM (Neuvokas Corp), a solution provider (Corsha Inc), and two manufacturing organizations (Automation Alley and SME). The SESAME project designed a practical and affordable "anomaly catcher" to detect threats at the physical, network, and logical levels for SMMs with varying levels of infrastructure.

26 "Secure by Design," Cybersecurity and Infrastructure Security Agency, https://www.cisa.gov/securebydesign.

27 "SolarWinds Orion (CVE-2020-10148)," IBM, May 10, 2024, https://www.ibm.com/docs/en/randori?topic=2022-solarwinds-orion-cve-2020-10148.

28 "SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response (infographic)," U.S. Government Accountability Office, Apr. 22, 2021, https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic.

ADDRESSING ADDITIVE MANUFACTURING (AM) SECURITY

The unique vulnerabilities of AM are a major focus. The Authentise "AM-Verify" IUC project uses in-situ monitoring cameras and Manufacturing Execution System (MES) data to detect maliciously introduced defects during a 3D printing process.

BRIDGING WEAKNESSES AND ATTACK PATTERNS

Through an IUC, the University of Texas at El Paso developed AWEB, a novel framework to connect MITRE CWE with ATT&CK by embedding both datasets into a shared representation space. Using graph structures and text-based embeddings, AWEB uncovers associations between common software weaknesses and adversarial tactics, techniques, and procedures (TTPs). This mapping enables end-users to move beyond isolated vulnerability catalogs and gain actionable insight into how specific weaknesses are exploited in real-world attack scenarios, ultimately supporting more proactive risk assessments and targeted mitigations.

ADVANCING AI-ENHANCED DIGITAL TWINS

CyManII's BP3+ Lab Foundational Sprint focuses on advancing AI-enhanced digital twins as a practical mechanism for reducing cyber and operational risk in advanced manufacturing environments. Traditional digital twin model physical systems for performance optimization or predictive maintenance. The BP3+ approach extends this concept by integrating cybersecurity, provenance, and verification into the digital twin itself.

The sprint explores multiple classes of digital twins in parallel, including data-driven twins, specification-based twins, and first-principles physics models. The core objective is not to select a single modeling paradigm, but to combine these approaches into a composite digital twin framework that is robust, verifiable, and adaptable across manufacturing contexts. Artificial intelligence is used to correlate multi-source data streams, identify deviations from expected behavior, and surface risk indicators that would be difficult for human operators to detect in real time.

This approach allows manufacturers to test design changes, process configurations, and security controls in a safe, virtual environment before deployment. For DOE-relevant manufacturing domains, including energy systems and nuclear components, this capability supports faster iteration while preserving safety, reliability, and security expectations.

CYMANII'S AMATROL TESTBED FOR MANUFACTURING CYBER R&D

CyManII has piloted the Malcolm tool stack at the C4M industry incubation hub to support and enhance R&D within the manufacturing sector. The initiative offers a dynamic learning environment where academia, researchers, and manufacturers can gain hands-on experience with Malcolm, an open-source intrusion detection system (IDS). Malcolm accepts network traffic data either uploaded via a browser-based interface or captured live and forwarded to the platform with a network sensor. It then organizes network traffic into a digestible, user-friendly interface, allowing users to identify unusual behavior and patterns. This integration of simulated manufacturing hardware and software technologies aims to equip industry and academia with practical skills and insights to react to a simulated cyberattack, while showcasing how Malcolm's network traffic interface can detect vulnerabilities within a simulated manufacturing environment.[29]

By introducing Malcolm to the manufacturing sector, CyManII aims to encourage manufacturers to IDS tools for better visibility of manufacturing environments. This initiative will provide targeted training and resources, enabling manufacturing professionals to learn how to adapt and integrate Malcolm into their operations for better network visibility.

FORMALIZED VULNERABILITY & MITIGATION ANALYSIS

CyManII has created an analysis methodology and software toolset that provides precise understanding of the system architecture, component interactions, and control flows that are critical to security assurance in automation systems.

The Compositional Attack-Defense Annex (CADA) is CyManII's new data model that extends the Architectural Analysis & Design Language (AADL) Assume-Guarantee Reasoning Environment (AGREE) tool to build system models for analysis of both legacy systems and new designs. CyManII's CADA identifies and categorizes potential attack vectors and techniques, highlighting initial access points and post-compromise lateral movement possibilities using the MITRE ATT&CK framework as a guiding structure for provable analysis that is repeatable as new threats emerge.

Working with a small additive manufacturer subjected to past ransomware attacks, CyManII performed a comprehensive attack path analysis of a complex manufacturing system composed of interconnected components such as programmable logic controllers (PLCs), motor controllers, embedded industrial PCs, and network devices to systematically mitigate vulnerabilities and permit more rapid analysis against future threats.

29 "Malcolm: Network traffic analysis tool suite," GitHub/Idaho National Laboratory, https://github.com/idaholab/Malcolm.

NOVEL CYBER DEFENSE CAPABILITIES: NEW FIRMWARE FUZZING

The CyManII team developed novel cyber defense capabilities (a new type of firmware fuzzing) to analyze and secure control systems used in plant floor equipment to prevent remote tampering and attacks. These innovations are now being deployed in DOE's Cyber Testing for Resilient Industrial Control Systems (CyTRICS) program to secure the U.S. energy grid, sponsored by DOE's Office of Cybersecurity, Energy Security and Emergency Response (CESER).[30] In August 2025, CISA reported the use of CyManII's innovative technology to identify a series of previously unknown cyber vulnerabilities in devices that are widely used by industry.

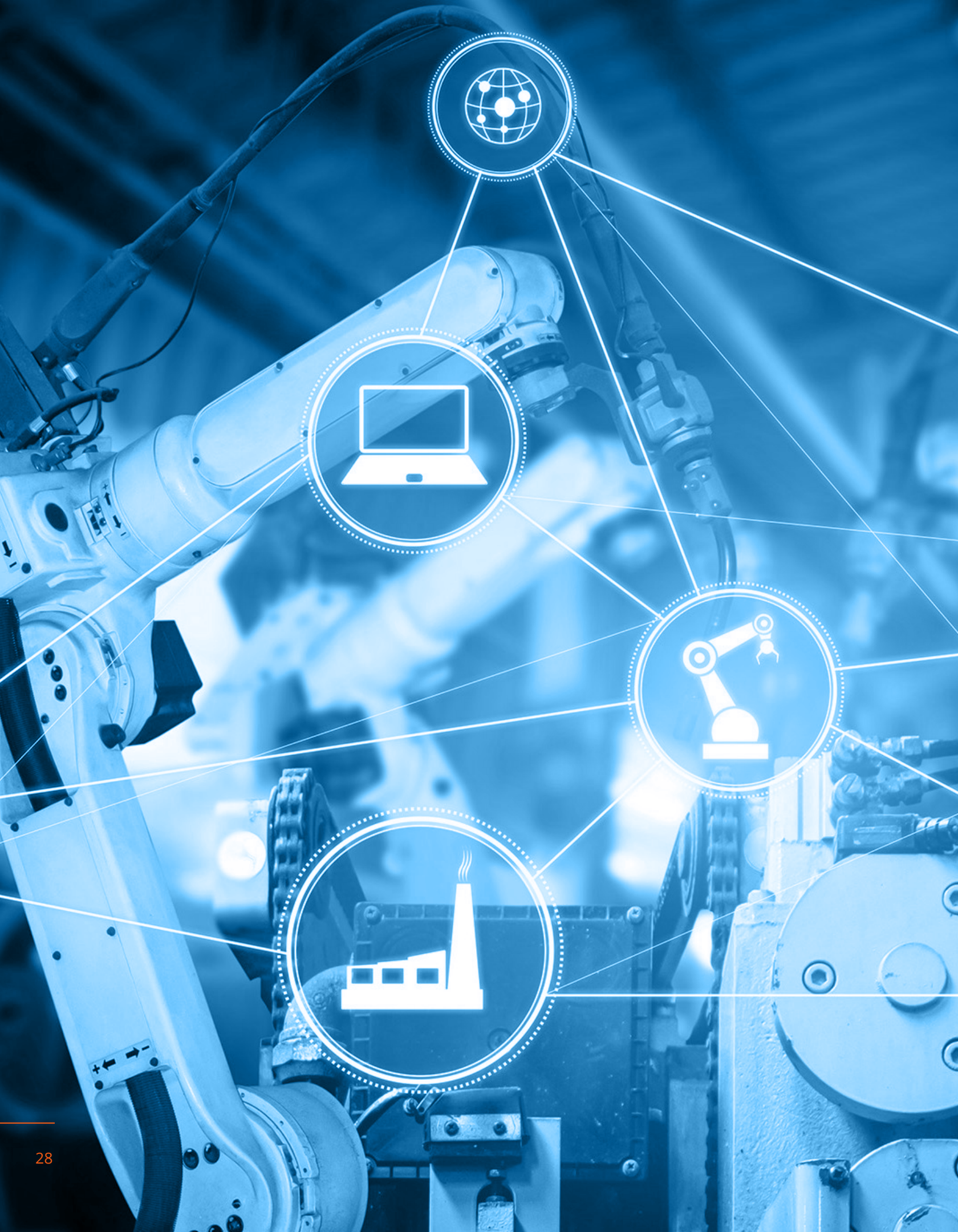
AI TO ADDRESS FUNDAMENTAL WEAKNESSES

CyManII is leading efforts to scale vulnerability detection and mitigation by transforming security tools to focus on the fundamental weaknesses that create many individual vulnerabilities. To ensure broader impact on the ecosystem, CyManII defined those critical cyber weaknesses in manufacturing and control systems and published the approach with IEEE in collaboration with the Common Weakness Enumeration (CWEs).[31]

Based on this foundational work, CyManII is now using AI to analyze energy-cyber-physical components of manufactured parts for security gaps and productivity inefficiencies and provide recommendations to manufacturers. By analyzing all three elements of a manufactured part, CyManII provides guarantees that components are productivity-efficient and cyber-secure, enhancing the cyber resiliency of entire manufacturing systems and supply chains.

30 "Cyber Testing for Resilient Industrial Control Systems (CyTRICS)," U.S. Department of Energy, https://cytrics.inl.gov.

31 "CWE," MITRE, https://cwe.mitre.org/.



5

MITIGATION OPTIONS FOR MANUFACTURERS

Providing manufacturers with mitigation strategies is the key to solving many of the challenges described in this report.

This section dives into key mitigation strategies identified by CyManII to help manufacturers enhance their security measures, with an emphasis on Cyber-Informed Engineering, Secure-by-Design, software bill of materials, memory-safe languages, network segmentation, human factors, and digital modeling concepts. This list is not exhaustive; manufacturers should consider additional mitigation strategies depending on their unique environment.

CYBER-INFORMED ENGINEERING (CIE)

The increasing sophistication of cyberattacks—from those targeting hardware, global supply chains, and the reliability of the nation's critical infrastructure—highlights the need for an engineering-based approach. Cyber-Informed Engineering (CIE) encourages engineers to address cybersecurity considerations at the earliest stages of system engineering, long before the incorporation of software and security controls.[32] CIE can help manufacturers proactively address cyber-physical risks by simplifying system designs and building in engineered safeguards from the start. The CIE implementation guide provides key questions engineering teams should ask during each phase of a system's lifecycle.[33]

SOFTWARE BILL OF MATERIALS (SBOM)

Tracking component versions through maintaining an accurate inventory of software and firmware in a software bill of materials (SBOM) is increasingly necessary to identify and remediate vulnerabilities before attackers do. The U.S. government and industry groups have recognized this and, in 2025, released updated SBOM guidance to improve software supply chain transparency.[34] In practice, having an SBOM allows manufacturers and developers to quickly decide whether to use a library or controller firmware that just got reported as vulnerable or to identify an alternative. This push for software transparency goes together with a broader strategy to re-shore and diversify manufacturing sources. Notably, some suppliers bind buyers with contracts that restrict disclosing discovered vulnerabilities or swapping out components, leaving manufacturers stuck with insecure parts until the vendor provides a fix.

32 "Cyber Informed Engineering," Idaho National Laboratory, https://inl.gov/national-security/cie/.

33 "Cyber-Informed Engineering Implementation Guide," U.S. Department of Energy, Aug. 7, 2023, https://www.osti.gov/biblio/1995796.

34 "ANSI/ISA-62443-3-3-2013: Security for industrial automation and control systems," International Society of Automation, 2013, https://www.isa.org/products/ansi-isa-62443-3-3-2013-security-for-industrial-au.

MEMORY-SAFE LANGUAGES

Memory-safe programming languages have arisen as a method of addressing memory-related weaknesses in products such as embedded firmware, control logic, and industrial software. Traditional languages like C and C++ remain dominant in ICS but lack protections against common memory-related issues such as buffer overflows, use-after-free errors, and heap corruption. These weaknesses have historically accounted for the majority of ICS and embedded system exploits.

In response, memory-safe languages such as Rust, Ada/SPARK, Go, and more are gaining traction for high-assurance software, such as manufacturing use cases. Rust, for example, eliminates entire classes of memory errors at compile time and is being explored for developing safe, high-performance firmware for Industrial Internet of Things (IIoT) and embedded industrial systems. Despite the advantages of memory-safe languages, adoption in manufacturing is extremely limited due to legacy tooling, vendor lock-in, and the complexity of recertifying new language ecosystems under industrial safety standards.

PROPER NETWORK SEGMENTATION AND MONITORING

Improper network segmentation is a critical cyber risk for manufacturers because it undermines the ability to isolate, contain, and defend OT from threats that originate in the IT domain or external networks. Without proper segmentation, malware or ransomware can move laterally from IT systems (email, enterprise resource planning) to production lines. Flat networks allow threat actors to compromise PLCs, HMIs, or safety systems after breaching a user's endpoint or virtual private network (VPN) gateway.

The importance of network segmentation stems from its ability to protect safety critical systems on a manufacturing floor. Manufacturing networks often include safety instrumented systems (SIS), robotic arms, or pressurized control loops. A compromised business system can indirectly trigger unsafe commands or halt production. ISA/IEC 62443-3-3 requires segmentation via zones and conduits to enforce trust boundaries and isolate critical assets.[35] The main purpose of secure network architecture is to limit communications across boundaries, and to limit, monitor, inspect, and record all communications within the boundaries.

Unsegmented networks make incident containment extremely difficult. Shutdowns affect all lines simultaneously. Segmented networks can isolate infected systems while allowing unaffected lines to continue operating.

Best practices for manufacturers include (but are not limited to):

- *Zone creation (e.g., enterprise IT, DMZ, OT network, safety systems) and conduits, per ISA/IEC 62443 (networks should be organized by the Purdue levels).*
- *Firewall and data diode usage to control inter-zone traffic.*
- *Deploy intrusion detection systems (IDS) at inter-zone boundaries with protocol-aware inspection (e.g., Modbus/TCP, Profinet). Malcolm is a free open-source IDS tool available on Github.*[36]
- *Set the IDS to monitor and alert for unauthorized lateral movement or suspicious access attempts across segments.*

35 "ANSI/ISA-62443-3-3-2013: Security for industrial automation and control systems," International Society of Automation, 2013, https://www.isa.org/products/ansi-isa-62443-3-3-2013-security-for-industrial-au.

36 "Malcolm." Malcolm, https://malcolm.fyi/.

Manufacturers can find practical guidance and hands-on support for network segmentation through established federal and industry resources. NIST provides manufacturing-specific cybersecurity and segmentation guidance, including tailored resources for SMMs through the NIST Manufacturing Extension Partnership (MEP) network, which offers direct technical assistance nationwide.[37]

CISA publishes clear, implementation-focused guidance for IT and OT network segmentation to reduce lateral movement and contain cyber incidents.[38] For industrial environments, the ISA/IEC 62443 standards remain the global benchmark for designing segmented, zone-based industrial control system architectures aligned with risk.[39]

HUMAN FACTORS IN MANUFACTURING CYBERSECURITY

Human factors remain a critical yet under-addressed dimension of cybersecurity in manufacturing and other ICS/OT environments. Security failures often arise not solely from technical flaws but from the complexity, ambiguity, or impracticality of the standards and practices intended to prevent them. For instance, guidance in frameworks such as the NIST Cyber Security Framework (CSF)[40] or IEC 62443[41] presumes resources and expertise that smaller organizations and overextended operators often lack, resulting in misinterpretation, misconfigurations, workarounds, or non-compliance.

Usability metrics such as operational fit, interpretability, actionability, and error resilience should be considered when developing security practices. Operators may struggle with unclear alerts, IT/OT administrators with overly abstract policies, or managers with recommendations that conflict with business continuity demands.

Despite widespread recognition of these challenges, the integration of human factors into ICS/OT cybersecurity standards remains limited. Current guidelines emphasize system architecture but often neglect user behavior, training, and recovery support. Bridging this gap requires embedding usability as a design principle from the outset, ensuring that security measures align with real-world workflows, resource constraints, and the varying levels of expertise of industrial personnel.

To accelerate adoption of ICS/OT cybersecurity standards and practices, SMMs may choose to implement an incentive program that rewards employees for proactive engagement in cybersecurity practices. For example, operators who successfully identify and report ambiguous alerts, administrators who streamline policy implementation for clarity, or teams that achieve measurable improvements in error resilience can be recognized through bonuses, professional development opportunities, and public acknowledgement. This approach not only encourages compliance but also transforms human factors from a point of weakness into a driver of continuous improvement. By aligning incentives with usability-focused security outcomes, organizations foster a culture where staff and suppliers view cybersecurity not as a burden but as an integral part of safe, efficient operations.

37 "Manufacturing Sector," NIST, https://www.nist.gov/itl/smallbusinesscyber/guidance-sector/manufacturing-sector; "Manufacturing Extension Partnership (MEP)," NIST, https://www.nist.gov/mep.

38 "Industrial Control Systems," Cybersecurity and Infrastructure Security Agency, https://www.cisa.gov/topics/industrial-control-systems.

39 "ISA/IEC 62443 Series of Standards," International Society of Automation, https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards.

40 "Cybersecurity Framework," NIST, https://www.nist.gov/cyberframework.

41 "ISA/IEC 62443 Series of Standards," International Society of Automation, https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards.

DIGITAL MODELING AND SIMULATION

The growth and adoption of digital models of physical systems (e.g., AADL, CADA, and digital twins) allow manufacturers to test and trial how new software, virtual configurations, and physical changes to manufacturing systems will interact. Digital modeling, especially detailed models such as digital twins, allow cyber professionals to have greater visibility into what is connected to a system and how OT software affects and interacts with the physical world. A combination of digital models and CPPs, SBOMs, or hardware bills of materials (HBOMs) can provide cyber professionals with greater insight into the manufacturing system and greater visibility on what parts of a system may be affected by a vulnerability release.[42] Manufacturers may use digital models to test changes to their systems, whether software updates, switching out hardware, or reconfiguring operational processes, in a low-stakes environment that won't affect their production systems.

SECURE PROCUREMENT AND CONTRACTING

The manufacturing sector is at an inflection point. Competitive pressure, workforce challenges, and global supply chain volatility are accelerating the modernization of production systems. Facilities that were once dominated by standalone mechanical equipment are now built around tightly integrated, networked, and software-defined systems—industrial control systems (ICS), programmable logic controllers (PLCs), distributed control systems (DCS), robotics, machine vision, industrial networking, and plant-wide data platforms. These digital systems deliver clear benefits in efficiency, throughput, quality, and predictive maintenance, but they also significantly expand the cyber and supply chain attack surface within plants and across multi-site operations.

Modern manufacturing increasingly relies on complex, globalized supply chains for the components that underpin operations. However, these assets can come from a multitude of suppliers, including from foreign entities of concern (FEOCs).[43] When integrated into the production line, these assets can put the entire digital manufacturing ecosystem at risk if there has been a failure to consider cybersecurity and supply-chain risk at the procurement and contracting stage. Because of these challenges, manufacturers should treat cybersecurity and supply chain risk as core procurement requirements, not technical afterthoughts.

This is not legal advice, nor is it a substitute for professional counsel. Always consult a qualified attorney in your jurisdiction regarding your specific situation.

At a minimum, procurement and contracting teams should focus on three areas:

1. Define clear cybersecurity expectations in RFPs.

Require vendors to meet baseline controls for authentication, remote access, patching, vulnerability disclosure, and secure development practices. Specify transparency requirements such as SBOM and HBOM. Make security capabilities a scored evaluation factor, not a secondary consideration.

2. Conduct risk-based vendor assessments.

Prioritize assessments for higher-risk assets such as PLCs, safety systems, remote access platforms, and cloud-connected production software. Evaluate country of origin, foreign ownership or control exposure, use of third-party libraries, and lifecycle support models. Align assessment depth to operational impact; a safety-critical control system warrants more scrutiny than a non-critical monitoring tool.

3. Embed enforceable security obligations in contracts.

Include requirements for vulnerability disclosure, patch timelines, secure remote support, update integrity controls, incident notification, and lifecycle support commitments. Define ownership of security responsibilities during commissioning, maintenance, and end-of-life. Tie non-compliance to contractual remedies.

For additional information, see Foley.com/insights.

42 "Digital twins," Manufacturing Futures Institute, https://engineering.cmu.edu/mfi/research/digital-twins.html.

43 An act to provide for reconciliation pursuant to title II of H. Con. Res. 14, H.R. 1, 119th Cong. (2025), https://www.congress.gov/bill/119th-congress/house-bill/1/text.

VULNERABILITY MANAGEMENT AND PRIORITIZATION THROUGH COMMON WEAKNESS ENUMERATION (CWE)

Effective vulnerability management is foundational to cybersecurity resilience. However, with thousands of vulnerabilities disclosed each year, organizations must prioritize what to patch—and when. To effectively manage vulnerabilities, it is important to understand how they are disclosed.[44]

1. **Discovery:** Vulnerabilities can be found by researchers, vendors, customers, independent third parties, or threat actors.
2. **Disclosure:** Responsible disclosure involves notifying the vendor and coordinating a fix before public release to an impartial third party, such as NIST. Some disclosures are coordinated through entities like a computer emergency response team coordination center (CERT/CC) or CISA.
3. **Publication:** Once disclosed, vulnerabilities are assigned to a Common Vulnerabilities and Exposures Identifier (CVE ID) and published in databases like the National Vulnerability Database (NVD) or MITRE.
4. **Exploitation:** If a vulnerability is weaponized, it may be added to the Known Exploited Vulnerabilities (KEV)[45] list or flagged by threat intel sources.

Organizations should monitor multiple sources of threat information (such as vendor advisories, KEV updates, and threat intelligence feeds) to stay ahead of emerging risks.

CWE provides a useful abstraction layer that groups related software and hardware weaknesses into broader categories. This higher-level perspective allows organizations to move beyond patch-by-patch triage and instead prioritize mitigation strategies around classes of vulnerabilities most relevant to their environment. Each CVE is typically mapped to one or more CWE in databases such as NVD, enabling analysts to trace from a specific vulnerability instance to the underlying weakness it represents. By leveraging these mappings, security teams can identify recurring weaknesses (e.g., improper authentication, injection flaws, insecure defaults) and design mitigations that reduce entire classes of security weaknesses, rather than addressing each CVE in isolation.

Multiple methods of vulnerability and weakness prioritization exist, such as the Exploit Prediction Scoring System (EPSS), Likely Exploited Vulnerabilities (LEVs), or the Common Vulnerability Scoring System (CVSS), among others. When determining which vulnerability scoring system to use, organizations should determine which system works with their data and measure factors most important to the organization. Such factors may include:

- *Dependence on opaque or high-risk technology sources, including FEOCs or vendors with limited security maturity.*
- *Inability to identify and prioritize vulnerabilities in embedded software, firmware, and hardware across production assets.*
- *Contractual gaps that leave manufacturers without clear mechanisms to demand remediation, transparency (e.g., SBOM/HBOM), or lifecycle support when security issues emerge.*

44 "CVEs and the NVD Process," NIST, https://nvd.nist.gov/general/cve-process.

45 The CISA Known Exploited Vulnerabilities (KEV) Catalog provides a curated list of vulnerabilities that have been confirmed to be exploited in the wild. These are not theoretical risks—they represent active threats and should be treated as top-priority for patching and should be addressed immediately.

6

CONCLUSION

The U.S. manufacturing sector faces a sustained and evolving cyber threat environment shaped by IT–OT convergence, expanding supply chains, legacy system dependencies, and rapid adoption of AI, cloud platforms, and additive manufacturing. The information presented in this report—including continued ransomware growth and the concentration of risk in recurring weakness categories such as improper input validation, memory safety flaws, weak authentication, and third-party exposures—makes clear that these challenges are systemic. They cannot be addressed through reactive patching or isolated technical controls alone.

CyManII is addressing these challenges by focusing on practical, deployable measures that reduce systemic cyber risk across manufacturing environments. Through structured IUCs, the institute pilots secure-by-design approaches that eliminate recurring weaknesses in controllers, firmware, and embedded systems, while also developing compensating controls such as network guards and non-invasive monitoring for legacy brownfield equipment that cannot be easily replaced. By combining technical innovation, supply chain transparency, structured analysis, and workforce development, CyManII is working to help manufacturers strengthen resilience, reduce systemic exposure, and sustain secure industrial growth in an increasingly contested digital environment.

For manufacturers, the central takeaway is that cybersecurity must be treated as a core element of operational excellence, product integrity, and supply chain reliability. A single exploited vulnerability can halt tightly coupled production lines, expose sensitive IP, and introduce latent defects into digitally driven processes such as additive manufacturing. By integrating secure-by-design principles, CIE, structured vulnerability prioritization, supply chain transparency mechanisms such as SBOMs and CPPs, disciplined procurement and contracting practices, manufacturers can shift from reactive mitigation to engineered resilience. In modern manufacturing environments, where a digital intrusion can halt production, compromise safety systems, and trigger cascading financial losses, cybersecurity is not an afterthought; it is essential to sustaining reliable and globally competitive U.S. manufacturing.

APPENDIX A

ACRONYMS

AADL	*Architectural Analysis & Design Language*
AGREE	*Assume-Guarantee Reasoning Environment*
AI	*Artificial intelligence*
AM	*Additive manufacturing*
BP	*Budget period*
C4M	*Cybersecurity for Manufacturing*
CADA	*Compositional Attack-Defense Annex*
CERT/CC	*Computer emergency response team coordination center*
CESER	*DOE's Office of Cybersecurity, Energy Security and Emergency Response*
CIE	*Cyber-Informed Engineering*
CISA	*Cybersecurity and Infrastructure Security Agency*
CMMC	*Cyber Maturity Model Certification*
CPP	*Cyber Physical Passport*
CSAF	*Common Security Advisory Framework*
CVE	*Common Vulnerabilities and Exposures*
CVE ID	*Common Vulnerabilities and Exposures Identifier*
CVSS	*Common Vulnerability Scoring System*
CWE	*Common Weakness Enumeration*
CyManII	*Cybersecurity Manufacturing Innovation Institute*
CyTRICS	*DOE's Cyber Testing for Resilient Industrial Control Systems*
DHS	*U.S. Department of Homeland Security*
DOE	*U.S. Department of Energy*
EPSS	*Exploit Prediction Scoring System*
EWD	*Education and workforce development*
FEOC	*Foreign entity of concern*
HBOM	*Hardware bill of materials*
HMI	*Human machine interface*
ICS	*Industrial control system*
IDS	*Intrusion detection system*
INL	*Idaho National Laboratory*
IIoT	*Industrial Internet of Things*
IoT	*Internet of Things*
IP	*Intellectual property*
IT	*Information technology*
IUC	*Industry use case*
KEV	*Known Exploited Vulnerabilities Catalog*
LEV	*Likely Exploited Vulnerabilities*
LLM	*Large language model*
MDF	*Manufacturing Demonstration Facility*
MEP	*Manufacturing extension partnership*
MES	*Manufacturing execution system*
ML	*Machine learning*
MTV	*Mobile training vehicle*
NIST	*National Institute of Standards and Technology*
NVD	*National Vulnerability Database*
OEM	*Original equipment manufacturer*
ORNL	*Oak Ridge National Laboratory*
OT	*Operational technology*
PII	*Personally identifiable information*
PLC	*Programmable logic controller*
R&D	*Research and development*
RF	*Radio frequency*
SbD	*Secure-by-Design*
SBOM	*Software bill of materials*
SDA	*Secure Defensible Architecture*
SIS	*Safety instrumented systems*
SMM	*Small and medium-sized manufacturers*
SNL	*Sandia National Laboratory*
TTPs	*Tactics, techniques, and procedures*
UTSA	*University of Texas San Antonio*
VPN	*Virtual private network*

CYMANII the cybersecurity manufacturing innovation institute

SECURE TOGETHER

MARCH 2026

SECURING THE FUTURE:
2026 Manufacturing & Critical infrastructure Threat Landscape

Innovations, Risks, and Practical Solutions for U.S. Manufacturers