



## Emerging Liability Exposures in Advanced Manufacturing: **AI and Robotics**

Advanced manufacturing is evolving exponentially. Companies across sectors now use AI-driven inspection, automated controls, predictive maintenance, and digital twins to increase speed, accuracy, and uptime. The result is a new kind of factory where machines make real-time decisions alongside, and sometimes instead of, human workers.

These technologies deliver real gains. However, they also create new forms of liability that most risk programs were not designed to handle. As AI and robotics become standard equipment on the factory floor, responsibilities and exposures are shifting in ways that demand attention.



### With AI, Liability Has Shifted

When a product liability claim or regulatory action occurs, all parties in the supply chain are still named. What has changed is the number of decision-makers involved and the difficulty in identifying who made the decision. In an advanced manufacturing facility, a single event can involve:

- + The manufacturer
- + The robotics or automation vendor
- + The AI or software provider
- + Sensor, vision, or data platform suppliers
- + The systems integrator or maintenance contractor

Collaborative robots (cobots) now work directly alongside human operators, handling repetitive or dangerous tasks and adapting to changing production conditions. Autonomous mobile robots move materials across the floor. Manufacturing execution systems coordinate everything from raw material intake to finished product shipping. When outcomes are driven by these interconnected systems instead of people, fault becomes fragmented and root cause analysis takes longer, which can delay resolution and escalate defense costs.

Workplace injuries add another dimension. Incidents involving workers and malfunctioning or inadequately guarded robotic systems are rising. When a cobot injures a worker, the question of fault is rarely a simple answer. The chain of responsibility can include any or all of those involved in making, operating, programming, owning, and overseeing the cobot. Even if a standard workers' compensation coverage responds, product liability claims against the robot manufacturer or integrator may apply. While there is abundant reporting of fatal incidents involving robots, data involving robots and non-fatal accidents has been sparse before a 2015 OSHA mandate.<sup>1</sup> Because insurance needs several years of data to build coverages and terms, manufacturers should expect a continuation of broad chain of responsibility until more is understood about AI in autonomous manufacturing.

## The Duty of Care Is Also Evolving

AI systems used for early detection, such as defect recognition, anomaly alerts, and process drift, raise expectations about what a company knew and when. Increasingly, regulators and courts look at whether:

- + An alert was generated
- + The alert was reviewed
- + A decision was overridden
- + That decision was documented

This creates a bit of a Catch-22. Failure to act on AI-generated insights, or explain why they were ignored, is being treated as a potential control failure. The standard is shifting from reactive problem-solving to credible prevention and oversight. This shift doesn't remove people from responsibility; it raises the bar on human accountability.

Demonstrating human oversight with clear escalation channels, documented overrides, model governance, and active monitoring is moving from best practice to a baseline expectation in advanced manufacturing environments.

## The AI Insurance Gap

While companies have used robots since the 1960s, manufacturers have increased the implementation of cobots over the last 15 years. There were significant incidents, such as the death of a Grand Rapids worker by a cobot whose wife subsequently sued the five companies responsible for manufacturing the robot.<sup>2</sup> Insurers responded with specialized insurance programs designed for the manufacturing, use, and programming of cobots.

The integration of AI with cobots changes the equation. Specialized insurance markets are growing rapidly to cover AI and automation.<sup>3</sup> For manufacturers, deploying AI in automation robotics and cobots creates real opportunities and also increases exposure across several lines of coverage:



### GENERAL LIABILITY/PRODUCT LIABILITY

When AI systems drive quality control, process decisions, or equipment behavior, algorithms become part of the operation itself. Traditional policies may not respond as expected when an AI system or robotic component is implicated in a defect, equipment failure, or injury. The Insurance Services Office (ISO), which develops standardized insurance policy forms, recently released new endorsements that insurers can add to general liability policies. These endorsements are designed to exclude coverage for losses that result from generative AI. In this context, generative AI is broadly defined as any data-trained, machine-based system capable of producing outputs such as text, images, audio, video, or computer code.



### TECHNOLOGY ERRORS & OMISSIONS (TECH E&O)

As software and automation become inseparable from production, failures in code, data, or system logic can trigger physical loss. A software error in a manufacturing execution system or robot control platform can cascade into equipment damage, defective output, or facility-wide shutdowns. Tech E&O coverage addresses wrongful acts or performance failures tied to technology — gaps that general liability and cyber policies often leave open.





## CYBER



The interconnected nature of smart factories — where IoT sensors, AI platforms, robotics controllers, and cloud systems are tightly linked — means a single vulnerability can cascade across the entire operation. A cyberattack or act of data poisoning can corrupt AI models, disable robotic systems, halt production, and trigger simultaneous business interruption and third-party liability claims.



## WORKERS' COMPENSATION AND EMPLOYER'S LIABILITY

As cobots and autonomous systems take on more tasks near human workers, the potential for serious injury increases when safety protocols fail or equipment malfunctions. Workers' compensation will likely respond, but employer's liability exposure grows when inadequate safety integration or a failure to act on known system warnings is part of the injury narrative.

Underwriters are drilling down on questions such as:

- + Who owns and controls training data?
- + How often are models reviewed or audited?
- + What happens when systems disagree with human decisions?

Manufacturers struggling to provide clear answers are facing stricter conditions from insurers, including tighter terms, higher retentions, and reduced capacity.<sup>4</sup>

## Final Thought

Automation has already increased exposure in manufacturing. What matters now is ensuring your contracts, controls, and insurance keep pace with your evolving production environment. For manufacturers deploying AI and robotics, aligning a risk strategy with an automation strategy is no longer optional, it is part of running a defensible operation. For more information on how your risk portfolio aligns with your automation strategy, contact your broker or risk advisor.



## Where to Start: A Practical Checklist

Advanced manufacturing companies do not need to solve everything at once. But they do need a clear starting point. The following checklist focuses on actions that matter most from a liability and insurance perspective.

### GOVERNANCE AND OVERSIGHT

- Document when and how humans can override automated systems.
- Define escalation paths for AI-generated alerts.
- Require written rationale for overrides and ignored alarms.
- Maintain version control and change logs for models in production.

### VENDOR AND CONTRACT RISK

- Review AI, software, and automation contracts for liability caps.
- Identify risk transfer gaps between vendors and the manufacturer.
- Confirm indemnification language aligns with real operational risk.
- Understand who bears responsibility for model failure or data issues.

### INSURANCE COVERAGE ALIGNMENT

- Map AI use cases against existing policies, not job titles.
- Identify where GL, cyber, and workers' comp policies may stop responding.
- Evaluate standalone Tech E&O or AI-specific endorsements.
- Confirm cyber coverage addresses data integrity, not just breaches.

### INCIDENT RESPONSE READINESS

- Integrate AI system data into incident response and injury investigation plans.
- Ensure cyber, operations, safety, and legal teams are aligned.
- Test how alerts, logs, and analytics will be handled after an event.

### UNDERWRITER READINESS

- Prepare clear explanations of AI governance for renewal meetings.
- Show how models are monitored, reviewed, and corrected.
- Demonstrate that automation decisions are understood — not blind.



### SOURCES

1. Sanders, N., Sener, E., and Chen, K. (2024, November). *Robot-related injuries in the workplace: An analysis of OSHA Severe Injury Reports*. Science Direct. <https://www.sciencedirect.com/science/article/abs/pii/S0003687024001017>
2. Walsh, Juliann. (2017, May 2). Rise of the Cobots. <https://riskandinsurance.com/rise-of-the-cobots/#:~:text=AIG's%20Lexington%20Insurance%20introduced%20an,we%20want%20that%20to%20continue.%E2%80%9D>
3. Koop. (2024, March 18). *Two Hottest Topics in Insurance: AI & Robotics and Climate*. Koop. <https://www.koop.ai/blog/two-hottest-topics-in-insurance-ai-robotics-and-climate>
4. Duff-Brown, Beth. (2026, January 6). *AI-driven insurance decisions raise concerns about human oversight*. Stanford Report. <https://news.stanford.edu/stories/2026/01/ai-algorithms-health-insurance-care-risks-research>

This material is for general information only and should not be considered as a substitute for legal, medical, tax and/or actuarial advice. Contact the appropriate professional counsel for such matters. These materials are not exhaustive and are subject to possible changes in applicable laws, rules, and regulations and their interpretations.