

Connected Manufacturing: Will IoT risks take your plant offline?

Manufacturing companies can prepare for the risks and opportunities from the Internet of Things (IoT)



Insights for manufacturing companies on IoT opportunities and risks

Leading a manufacturing company requires awareness of a number of factors, each of which can be changing at any given moment. Government regulation, customer sales and service requirements, supply chain challenges, production and quality techniques, workforce safety demands, energy management, attracting skilled labor, and information security all consume mindshare and impact the bottom line. To further complicate this picture, the emerging and rapidly expanding Internet of Things (IoT) cuts across each of these factors, presenting opportunity and, if done incorrectly, significant risk.

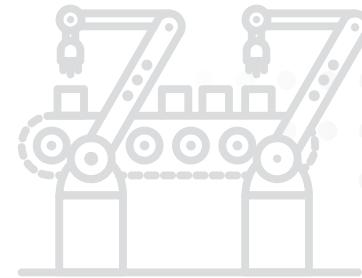
As the technology advances, IoT offers the potential for reduced costs, greater convenience, enhanced products and improved safety. Increasingly powerful software can multiply firms' IoT return on investment by capturing more and better insights from a growing number of increasingly sophisticated connected devices. Inevitably, however, the complexity and ubiquity of these devices may result in an occasional misfire, potentially leading to a data breach, customer or employee injury, property damage, or third-party economic loss.

Firms in more traditional manufacturing sectors may not be able to isolate themselves from new manufacturing trends such as IoT. While high-tech manufacturers may be impacted most, suppliers and customers increasingly interface with traditional manufacturers through IoT technology. Additionally, IoT is finding its way onto the manufacturing floor and into the hands of the manufacturing workforce in ways that are often underestimated or misunderstood by traditional manufacturers.

The emergence of IoT represents a turning point for manufacturing firms. Whether deployed into factory production lines or integrated into finished goods, IoT devices can be the gateway to a competitive market advantage. But with every new technology, firms must reevaluate their operational risks. Manufacturing leaders who understand both will be positioned to reap the greatest rewards.

Erika Melander

TRAVELERS MANUFACTURING INDUSTRY PRODUCT DIRECTOR



Introduction

Factors driving adoption of IoT in manufacturing

Areas of application

IoT-related risks to manufacturers

Actions to consider for minimizing risk from IoT

Insurance considerations for IoT in manufacturing

How Travelers can help

Introduction

IoT technologies have perhaps been most visible in the consumer market. Applications that once seemed futuristic are now almost commonplace. Consumers order groceries and household supplies by speaking at a voice-enabled connected device. Wearable smart watches and activity trackers help consumers meet their fitness goals. Homeowners can keep tabs on their house or apartment while they're miles away and use a smartphone to turn up the heat, arm the security system, and even feed pets.

IoT also impacts a wide range of sectors outside of the technology industry, including healthcare, transportation, construction, retail and others. Companies integrate connected devices into their operations to improve economics, safety, convenience and other factors.

The manufacturing industry, where IoT is often referred to as the “industrial internet of things” (IIoT), is no exception to the trend. Integrating IIoT technologies into manufacturing operations can help companies produce goods at a higher quality and lower cost, with greater control over the production process. IIoT can lead to more efficient resource allocation, with less waste of time and materials. IoT industry analysts, including Gartner and International Data Corporation, predict an IoT device count in the tens of billions across all industries by 2020,¹ while Intel anticipates that the manufacturing industry could account for as much as 40% of them.² Throughout this white paper, we will use the term “IoT” as a convention to reference the Internet of Things whether or not it is used in an industrial or consumer setting.





The pages that follow examine both the opportunities and risks related to the use of IoT by manufacturing companies. First, we consider the factors driving the adoption of IoT and the increasing number of ways in which manufacturing firms leverage IoT in their operations. Then, we identify and explore specific types of IoT-related risks that can negatively impact manufacturing firms, and we highlight for consideration several specific actions to minimize such risks. Finally, we conclude by sharing insurance considerations that manufacturing companies can discuss with their independent agent or broker as they evaluate the IoT opportunity.

Factors driving adoption of IoT in manufacturing

Several key factors are converging to bring IoT to manufacturing. Companies that understand these factors will be better positioned to capitalize on the opportunity and to manage the risks this presents.



A) TECHNOLOGICAL ADVANCEMENTS

Enabling a wider range of device functionality, technological advancements facilitate the expanded use of IoT in manufacturing:

- **Widespread internet availability:** Improvements in high availability internet mean that more connected products can transmit data in more physical locations. Widespread cellular, satellite and Wi-Fi internet connectivity has given manufacturers exactly what they need: extreme mobility. There are now very few places a connected production device can go where it cannot find an internet connection.
- **Moore's law and the miniaturization of technology:** Gordon Moore, founder of Intel and Fairchild Semiconductor, wrote a paper in 1965 noting a doubling in the number of transistors per integrated circuit every year. This observation, which came to be known as "Moore's Law," was remarkably accurate for decades and had a profound impact on the research and development goals of digital electronics, leading to smaller devices with greater power.
- **Materials engineering advances:** Progress in developing new advanced materials has facilitated advancements in sensors, actuators, casings and other components used in IoT technology. In many cases, this allows IoT devices to maintain high performance in the wide range of conditions they encounter in manufacturing and industrial applications.
- **Cloud computing:** The cloud accepts IoT-generated data into virtual storage, allowing IT teams to efficiently capture terabytes of data for later manufacturing optimization analysis.
- **Big data analytics:** IoT produces large amounts of unstructured or semi-structured data on a continual basis. Data scientists and other analytics professionals "mine" the data to extract insights that can improve factory operations.



B) CONVENIENCE

IoT makes viable what was previously unpleasant, unsafe, remote or repetitive. Production, maintenance and engineering tasks that involve physical risk for employees can now be partially or completely transferred to IoT devices. Machine-to-machine communication simplifies monitoring and reporting, and in many cases, software can automatically change a device's behavior, based on sensor inputs. In this way, IoT devices can regulate themselves and collaborate with other internet-connected devices throughout the production cycle.

Robotics is one area where many manufacturers are finding quantifiable business benefits. Robotic arms and assembly mechanisms can be programmed to perform complex assembly operations with low cost and greater accuracy, freeing up factory workers for other tasks. And with onboard IoT sensors, robots can detect tolerance thresholds and notify maintenance teams when human intervention is required.

With information gleaned collectively from these devices, companies gain visibility into what is happening on the factory floor. As the company continues to analyze and learn from the information gathered, managers can make decisions more quickly and easily about how to adjust operational processes as well as other business functions.



C) ECONOMICS

Manufacturers are betting that IoT will help them reduce costs and capture new revenue opportunities. Connected inventory systems allow manufacturers to keep on hand smaller quantities of components and spare parts. As stock levels deplete, connected devices can send reorder messages to purchasing managers or automatically invoke replenishing orders via purchasing software. Likewise, industrial equipment can self-assess performance and signal the need for routine maintenance or repair. With overall improvements in efficiencies, throughput may be improved and downtime reduced by these internet-enabled sensors.



D) SAFETY

Some devices can offer distinct opportunities for preventing injuries or death by their ability to detect activity of both humans and machines. For example, if a worker strays too close to a hazardous area of production, the device triggers an alert to avoid an accident. Devices can detect malfunctions of the equipment itself to turn it off before an accident occurs. Information collected from machines helps management determine what actions to take to improve operational inefficiency. That information can be shared with other company plants that use similar operating procedures. Besides helping protect workers from harm, connected devices present the potential to monitor products once they've reached consumers to identify when service is needed.



Areas of application

Manufacturing companies are applying IoT technologies to their operations, both inside and outside the plant. Connected devices are an increasing feature of daily life for manufacturing employees, suppliers and customers. In many cases, these devices are also becoming less directly visible, even as their span of control increases. Industry leaders should understand the following ways in which companies are integrating IoT in their manufacturing operations.



1

EQUIPMENT MAINTENANCE

Traditionally, a factory's maintenance crew performs its work on scheduled shifts, which may or may not sync with actual requirements. Performing maintenance before it is needed may drive costs up and slow productivity, while waiting too long can be catastrophic. Industrial firms looking for a way to accurately predict when they should take their equipment offline for preventive maintenance may be able to leverage IoT technology to save time and money.

IoT sensors embedded into industrial machines can stream data points such as heat, vibration and oil viscosity. When filtered through analytical software, this vital information gives maintenance crews better insights into when a machine needs their attention. Companies that have implemented production line sensors have experienced significant decreases in downtime and maintenance costs.

C U R R E N T U S E S

Salt Lake City-based Spectra Symbol leverages the Altizon with Datonis® IoT platform for remote monitoring. The technology connects to remote oil wells and collects operational data to keep them running smoothly. Altizon's application features industrial sensors that detect tank levels in oil wells while temperature and configurable strain sensors deliver maintenance data over the web in real time. As a result, customers keep their wells pumping reliable streams of crude oil through optimized supply lines.³

In the tech sector, Dell was able to correct a consistent problem in microchip production that relied on automatic solder dispensing equipment. Every so often, a solder machine would fail to deposit any solder at all, resulting in faulty circuit boards that had to be scrapped. Engineers traced the problem to fluctuating vacuum levels in the solder dispensers. By correlating machine sensor readings with other web-connected machines on the production line, Dell monitors and controls their board assembly more effectively, resulting in fewer defects and greater throughput.⁴

2

INVENTORY AND SUPPLY CHAIN MANAGEMENT



IoT devices use a variety of methods to collect and share information. Radio Frequency Identification (RFID) tags are tiny elements inserted into parts, shipping containers or other material that act as beacons – relaying their location in real time. For example, devices can transmit GPS coordinates so a factory knows that a part needed for Wednesday's production run is 300 miles away on Monday, but should arrive by Tuesday afternoon.

With enhanced visibility into the location of all the needed materials, companies can optimize their inventory and increase their fulfillment execution. IoT devices can use visual signals as well as radio, Wi-Fi and GPS for real-time data transmissions.

CURRENT USES

Swedish automaker Volvo has connected sensors in its supply chain to cloud services on a global scale. Now the company can track its inventory en route, regardless of what country the supplier ships from. As a result, the manufacturer now enjoys greater flexibility than with previous on-premises supply systems.⁵

The German company Würth has developed internet-connected video cameras placed adjacent to supply bins. The cameras monitor the bins' quantities and send the data to an Enterprise Resource Planning (ERP) system programmed to alert when reorder points have been reached. The company can then place orders to replenish stock on any number of parts.⁶

3

PRODUCTION PROCESS AND QUALITY CONTROL



While many manufacturing processes allow for a tolerance for inaccuracy in the production process, others require very high tolerances to be met.

In addition, sensors in the production line can direct changes in operations if needed. If a sensor in a paint booth of a General Motors assembly line detects higher-than-acceptable humidity levels, it automatically adjusts ventilation in the booth or reroutes work to another location in the plant.⁷

IoT can help manufacturers walk this tightrope by correlating production benchmarks with historical staffing levels. The resulting insights can help manufacturers forecast hiring needs more accurately, bringing them closer to the goal of production workforce optimization.

CURRENT USES

Raytheon, a maker of missile systems for the Department of Defense, has no room for error in its production assembly functions. So, the company has implemented its Manufacturing Execution System, or MES, to help automate production quality control. The software uses sensors to capture highly detailed factory floor data right down to the number of times a screw has been turned.⁸ By subdividing and analyzing these data elements, the company can deliver defense products that adhere to the strictest of manufacturing standards.

Human resources can be a large expense for manufacturing firms. If manufacturers hire more workers than they need, they incur cost overruns due to idle personnel. If they hire too few, they might miss important production deadlines and shipping commitments.

4 WORKFORCE SAFETY



In the workplace, robots blend into operations with employees to better manage repetitive and potentially hazardous tasks. Products can be stacked so high in warehouses that retrieving them could expose employees to dangerous and unnecessary risks. To alleviate this hazard, IoT devices relay bin location data to plant robots. They fetch the products and deliver them to the employees, who then sort the items for delivery.⁹ By relieving humans from risky tasks, IoT devices can decrease the frequency of expensive worker injury claims.

More dynamically connected devices can detect the conditions leading to equipment failures and provide warnings and/or automatically shut down the production line if necessary.

Wearable devices are making their way into the modern manufacturing workplace. In the oil and gas industry, hard hats are equipped with sensors and a flip-down visor that show a heads-up display. When a field worker approaches an oil well, the sensor identifies the well and presents the worker with all of the schematics necessary to go to work immediately.

CURRENT USES

Accenture, along with AeroScout, Cisco and Industrial Scientific, has developed new technology to detect gas exposure and alert plant managers to remote safety incidents.¹⁰ The devices can monitor the safety of thousands of employees across a large plant in real time from a central location.¹¹

5 CUSTOMER AND PRODUCT DEVELOPMENT INSIGHTS



Real-time automation and process integration across the supply chain can help manufacturers respond more quickly to consumer demand. The enhanced connectivity can also help strengthen design efforts with data on how their products are being used. This allows them to make adjustments to existing products that benefit the consumers and improve sales.

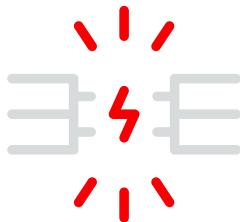
CURRENT USES

A coffee machine manufacturer can embed a tiny connected device within its coffee makers to collect information about when consumers turn the machine on and off, how many cups they make in each setting, and any ancillary features the customer may use. The device sends this data via wireless internet back to the manufacturer who then can use it to design new features based on a better understanding of how consumers actually use their products.

Another innovative manufacturer has already found a clear payoff for connected device deployments. Automobile company Tesla faced a recall of some 30,000 vehicles in 2014 due to onboard software issues. Ordinarily, such a recall would have required customers to bring their cars into a dealer, wait for the software update to be done or even leave the car overnight for service. But Tesla's IoT application executed the repair over wireless internet, saving car owners a considerable amount of trouble and spared the company significant costs they would have otherwise incurred from a conventional recall.¹²

6

ENERGY MANAGEMENT



The industrial sector accounts for nearly one-third of U.S. energy consumption – nearly \$200 billion every year. However, nearly 30 percent of that energy goes to waste, taking a large bite out of already-thin manufacturing profit margins.¹³ IoT has the potential to provide management with the insights necessary to decrease energy waste and improve manufacturing profitability.

Using sensors to control energy usage is nothing new for manufacturing. But new sensory technology can communicate real-time energy performance indicators over the internet to powerful backend optimization algorithms and controls. Plants can now automatically turn down lights and adjust factory room temperature when workers leave the factory floor, then readjust ambient conditions when workers clock in for the next shift. Likewise, connected sensors in pipelines can detect potential leaks and notify maintenance crews in time to avoid a major outage.¹⁴

7

SECURITY



Every manufacturer, regardless of size, faces the challenge of physical plant security. Manufacturing professionals must ensure the safe arrival of parts and materials, and secure production processes to protect against theft and accidents. IoT offers unique ways to automate plant security against theft, tampering, unauthorized access and to track/recover goods.

Firms can also leverage their sensor-generated information to predict future security encroachments. Data scientists can capture and analyze historical surveillance data to detect patterns in the movements and techniques of unauthorized personnel. Companies can then utilize these patterns to predict when and where a future attack might occur and deploy larger numbers of security personnel to defend against it.

IoT-related risks to manufacturers

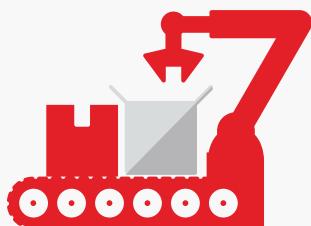
Because of their many applications, IoT devices are finding their way into every sector of manufacturing. The inherent risks of these technologies, however, are often underestimated and misunderstood. There are many different ways in which IoT can impact finished goods, property, workplace safety and cybersecurity.



Risk 1: Manufacturing defect

IoT technology has the potential to introduce unintended defects into manufactured products. This can happen when new technologies inadvertently cause finished goods to depart from their intended design, resulting in products that do not function as customers expect.

MANUFACTURERS ERRORS AND OMISSIONS is one type of manufacturing defect risk. A purchaser of a manufacturer's products may sustain economic losses from the failure of the product to work as intended, due to an error, omission or negligent act.



Risk 2: Property

Property risk refers to the risk of physical damage to, or loss of use of, buildings, business personal property and loss of business income and extra expense. Integrating IoT technology improperly into your operations could damage your physical plant, raw materials or finished goods, any of which could negatively impact your bottom line.



Risk 3: Workplace safety

The factory floor can expose employees and managers to the risk of injury, but IoT may present new risks that manufacturers have never faced before. IoT machines, equipment and devices that don't perform as they should in a manufacturing environment can lead to employee injuries. For any company trying to keep pace with customer needs, these incidents can pose an important threat.



Risk 4: Cyber

Cyber risk can be understood in terms of threats to the confidentiality, integrity or availability of information systems and data. When IoT devices are used in manufacturing, those threats could include stolen production plans or data, or impaired operations caused by a malfunctioning IoT device. Moreover, as IoT devices become more widespread, they increase the overall exposure of a company's network to cyber risk by increasing the number of possible vulnerabilities that can be exploited by an attacker.

Manufacturers are already taking precautions to guard against cyber risks by establishing firewalls to protect their data. But IoT opens up other avenues of attack, so factories and other manufacturing facilities will need to take extra precautions to keep the hackers at bay.

The following scenarios are hypothetical. Each serves to illustrate the kinds of risks associated with IoT technology if proper security practices and product reliability are not built into IoT systems up front.

DISGRUNTLED FOR DESTRUCTION

An employee leaves his company to join a startup competitor. In an effort to increase market share, this individual hacks into his former employer's network and gains access to production line control systems. The employee makes slight changes to sensor tolerances so that the products do not conform to design specifications. The company begins to lose market share due to the unreliability of its products and reputational damage.

STAMPING HAZARD

A stamping press is connected to an integrated production line where sensors are used to synchronize the placement of raw metal into the press. The stamping press, conveyor and material handling robot are made by different manufacturers. The settings for the robot are adjusted remotely by the manufacturer, improving its energy consumption but throwing off the synchronization with the stamping machine. The operator of the press, unaware that any changes have been made, inserts his hand into the press area to remove a part just as the robot inserts a metal blank, causing a hand injury.

MACHINE MAINTENANCE MISCALCULATION

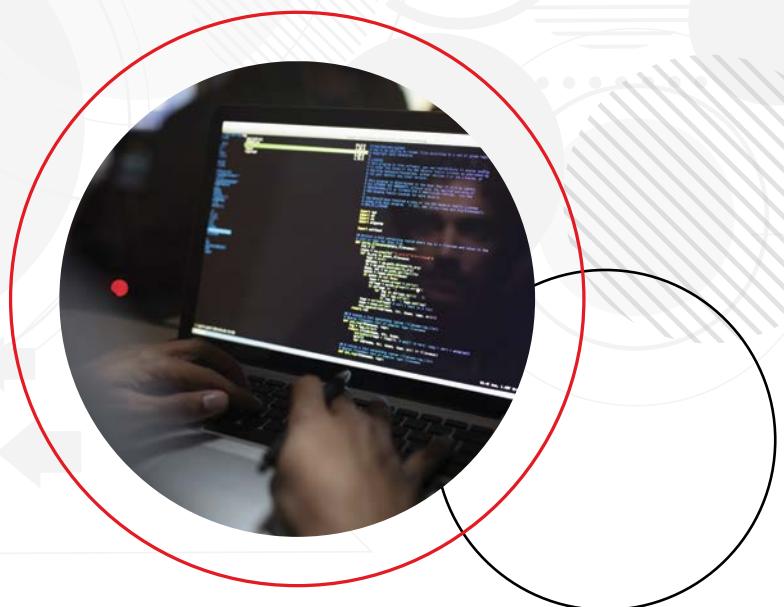
An aluminum fabrication plant uses several metal extrusion machines that perform shaping of rolled metal according to customer specifications. The machines are equipped with heat, vibration and usage sensors to detect when the machines should be taken offline for preventive maintenance. One of the machine's usage sensors contains a faulty firmware calculation that results in erroneous alerts for service far sooner than needed, wasting maintenance personnel's time and resources.

SELF-GUIDED MATERIAL HANDLING ROBOT

An electronics manufacturer uses autonomous material handling vehicles to deliver parts from staging areas to production cells as well as assembled goods to the warehouse. The vehicles are guided by an IoT sensor system that uses guidance beacons that form a map of the production floor. The guidance system was hacked causing the vehicle to veer from the expected path, striking a warehouse rack, causing damage to products ready for shipment. As a result, stock was either destroyed or had to be reworked, and customer orders were delayed.

VIDEO VULNERABILITY

Hackers take advantage of a vulnerability in an internet-connected video surveillance system to connect to the manufacturer's network. After exploring the server, they choose to alter the inventory management system to disrupt the company's operations. As a result, the erroneous data triggers the company's auto-reordering system to buy materials the manufacturer already has on hand and delay ordering of needed supplies.



Actions to consider for minimizing risk from IoT

The IoT offers manufacturing companies two distinct and exciting opportunities to deliver superior value. First, by integrating connected IoT systems into their manufacturing operations, they can increase quality, decrease unit costs and more accurately track inventory throughout their entire supply chain. Second, by incorporating internet-connected devices directly into their finished goods, they can provide connected data features that customers have come to expect from innovative manufacturers.

However, as manufacturers continue to harness the IoT's new capabilities, they may unknowingly expose their companies to significant risks. Should a production line sensor or its connected software fail to function properly, people could be injured and sensitive data compromised. Fortunately, there are several steps that manufacturers can consider to minimize their exposure to these risks.

REINFORCE CYBERSECURITY

Information security is a topic of concern for manufacturers worldwide. Yet, despite all the packaged security solutions on the market today, breaches still occur. In addition to costing manufacturers millions in liability costs every year, the net reputational damage could prove insurmountable. The good news, however, is that there are actions manufacturers can take to reduce their exposure to IoT-based cyber threats and keep liability costs down.

Companies that use IoT devices in their production facilities should consider the following steps to help minimize IoT-based risk exposure:

Maintain an IoT inventory

An inventory of all network devices, including IoT devices, can help companies understand the potential risks for network intrusion. A device as mundane as a network printer can harbor a vulnerability that would allow an attacker to secure administrative privileges or spread malware throughout a network.

Change default passwords

Companies often overlook the need to change default passwords on IoT devices. Leaving default passwords in place can provide an easy way for attackers to steal data or to change settings on an IoT device.

Implement IoT patch management

It can be difficult to ensure that patches are applied properly to IoT devices. In the first place, some IoT devices do not support remote or automated patching. In addition, installing patches on IoT devices that are critical to a manufacturing operation can be disruptive. Nevertheless, it is important for a company to apply patches as needed, and to provide compensating controls when IoT devices with known vulnerabilities cannot be patched.

Segregate IoT-related network traffic

When IoT devices are critical to a business's operations, or when they are used to capture or process sensitive data, segregating IoT network traffic from the rest of the corporate network can help to improve security.

Conduct an IoT risk assessment

For companies that have widely deployed IoT devices, an IoT-focused risk assessment can help ensure that the unique risks associated with those devices are adequately understood and properly mitigated.

Firms that design their finished goods with embedded connected devices face a unique set of security concerns. Because the physical product is no longer within firewalls of the manufacturer's facility, security professionals should consider the following points:

Design with security in mind

When designing a network-connected device, the appropriate level of security should be built in from the start. This can include software-level considerations, such as providing for a secure "boot" sequence, as well as hardware considerations, such as minimizing unnecessary ports.

Encrypt sensitive data

If the device is intended to be used for collecting or processing sensitive data, manufacturers should consider using encryption to protect against unauthorized access to the data while it is at rest or in transit.

Support remote, automated patching

As noted previously, the "always on" nature of IoT devices can make patch management and software updates particularly challenging. Manufacturers of IoT devices should strive to allow patches and updates to be installed with as little business impact as possible, e.g., by supporting remote and automated patching.

CONSIDER APPROPRIATE QUALITY AND RISK MANAGEMENT SYSTEMS

Companies that use connected devices in their manufacturing processes should be aware of and adhere to appropriate quality and risk management systems. This will help to ensure that their finished products consistently meet requirements and specifications. In addition to adopting effective product requirements, manufacturers should consider altering legacy procedures and design methods to make the most of this groundbreaking new technology. Manufacturers that take these actions to heart may avoid crippling liability costs from a high-profile negative event.

Conduct robust hazard analysis

Methods such as fault tree analysis (FTA), failure mode and effects analysis (FMEA), and hazard and operability analysis (HAZOP) can be used by manufacturers to assess potential hazards at different points in their production lines. Companies should not ignore issues that can be introduced during processes such as manufacturing, packaging, labeling, storage or transport.

Companies that integrate connected devices in their merchandise cannot visually monitor how their products are actually being used. However, they should still consider actions to minimize risk when their goods reach the end consumer. And it all starts with designing risk management before the production process begins.

Conduct routine design reviews

Firms that produce goods with IoT devices embedded in the final product should assess the frequency and severity of all identified potential hazards the IoT devices could cause. All firms in the development and production chain should seek to eliminate high-severity hazards and reduce the potential for medium-severity hazards. One review approach includes assembling a diverse team that includes personnel outside of the design process to generate potential mitigation solutions.

Conduct extensive testing

Product manufacturers should not only test IoT devices within their production contexts, but also any peripheral hardware their devices may need to communicate with. Insist that device vendors offer continuous integration to detect bugs as early as possible in the build phase where they may be easiest and least costly to fix.

Develop clear safety and use instructions with conspicuous warning labels

Companies should provide users with clear, unambiguous written instructions on the full range of use for devices on production lines. This may include providing visual depictions of proper device use, as well as instructions on maintenance and what to do if the device malfunctions.

EVALUATE COMPANY CONTRACT PRACTICES

Even well-designed products fail to perform as expected from time to time. In those rare cases, a deficiency resulting from new IoT technology in your production plant – or elsewhere in your supply chain – could have unfortunate side effects that result in high-dollar liability claims. Companies can manage their exposure to errors and omissions risk by ensuring that they use effective contract practices. Manufacturing companies should consider the following specific contract provisions whether they use IoT devices in their production processes or integrate them into their finished goods:

Limitation of liability

This provision disclaims liability for certain types of damages – usually incidental, consequential or special damages. In the event of threatened litigation, these provisions can become very useful.

Damage caps

These provisions limit the amount of recoverable damages. The limitations can be defined in terms of a specific dollar amount or an amount to be determined, depending on specific factors set forth in the contract.

Disclaimer/limitation of warranties

This provision identifies the warranties provided, disclaims or limits those warranties not provided, and identifies the remedies available in the event the product or work does not comply with the warranties provided.

Integration

This provision identifies the documents that comprise the parties' contract and will also limit the parties' reliance on documents and information outside of the contract.

Contractual risk transfer and defense/ indemnity provisions

Provisions like these can shift risk to other parties.



Insurance considerations for IoT in manufacturing

Manufacturers face special challenges as they adopt IoT technology that presents unknown risks. The adoption of any new technology has its own unique set of risks, many of which are unknown because there is no track record associated with this technology. Likewise, many production lines were designed decades ago, long before the age of sensor-enabled manufacturing, so the net effect of these devices from one implementation to the next is uncertain.

Safety features, data protection measures, effective risk management and good design decisions can help manufacturers reduce their exposure to some of the risks we see today. However, given the rapid pace of technological change, many are unlikely to ever fully understand and eliminate their current or emerging exposures. To prepare, companies should investigate their insurance options for the categories of risk described in this white paper.

 Risk type	 Relevant insurance coverage to evaluate with an agent or broker
Cyber	Cyber coverage provides coverage for critical cyber risks. Coverage options vary, but most include privacy and security liability, media liability, and regulatory proceedings coverage. Firms can also opt for many first-party coverages including forensics, data restoration, business interruption, computer fraud, funds transfer fraud, cyber extortion, crisis management expenses and security breach notification expenses.
Bodily Injury Liability for Your Products	Product liability coverage provides coverage for your liability to pay damages because of physical harm to a person arising out of a product manufactured, sold, handled, distributed or disposed of by you.
Manufacturing Errors & Omissions	Errors & Omissions (E&O) liability coverage protects against damages that you must pay because of economic loss arising out of your products that fail to perform the function or serve the purpose intended, or your work, that are caused by an error, omission or negligent act.
Property	Property insurance provides coverage for buildings, business personal property, and loss of business income and extra expense.
Workplace Safety	Workers compensation coverage can help protect both you and your employees after a work-related injury or illness. For the injured employee, workers compensation provides medical care, lost wages and more. For the employer, workers compensation provides a sole remedy, avoiding expensive civil litigation, plus peace of mind knowing your employees will get the help they need to recover and return to work.

As IoT technology spreads through the manufacturing industry, the potential for large-loss events also increases. Travelers helps companies protect their business, brand and reputation from such events. For large losses beyond what your primary insurance can cover, evaluate with your agent or broker an extra layer of protection with umbrella and excess liability coverage.

How Travelers can help

Travelers stays ahead of manufacturing industry risks. We continually update our risk management products and services, to help manufacturing companies manage their existing and emerging risks. Travelers has served manufacturing companies for more than 150 years. As IoT continues to proliferate within the industry, our expertise will be there to help companies prepare for the risks.



For more information, contact your independent insurance agent or broker,
or visit us on the web at travelers.com/manufacturing.

References

- ¹ <https://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated>
- ² <https://www.intel.com/content/dam/www/public/us/en/images/iot/guide-to-iot-infographic.png>
- ³ <http://altizon.com/smart-manufacturing-spectra-symbol-leverages-altizon-iot-platform-for-remote-asset-monitoring-solutions/>
- ⁴ <http://i.dell.com/sites/doccontent/shared-content/solutions/oem/en/Documents/intel-dell-blueprint-331705-001.pdf>
- ⁵ <https://internetofbusiness.com/8-real-life-examples-iot-supply-chain/>
- ⁶ https://www.wuerth-industrie.com/web/en/wuerthindustrie/cteile_management/kanban/lbin_intelligenterbehaelter/lbin.php
- ⁷ <http://connectedlife.blogspot.com/>
- ⁸ <https://sameerdhanrajani.wordpress.com/2016/06/13/sameer-dhanrani-smart-manufacturing-enabled-by-data-sciences/>
- ⁹ https://www.accenture.com/t20160119T041002_w_us-en_acnmedia/PDF-5/Accenture-804893-Smart-Production-POV-Final.pdf
- ¹⁰ Ibid.
- ¹¹ <https://newsroom.accenture.com/subjects/technology/accenture-lifesafety-solution-named-new-product-of-the-year.htm>
- ¹² <https://www.scs-luettgen.com/en/internet-things-manufacturing/>
- ¹³ <http://blogs.constellation.com/energy4business/6-ways-manufacturers-can-reduce-industrial-energy-costs>
- ¹⁴ https://www.accenture.com/t20160119T041002_w_us-en_acnmedia/PDF-5/Accenture-804893-Smart-Production-POV-Final.pdf



Travelers understands the unique needs of manufacturing firms. We often insure what other carriers won't, because we've been protecting manufacturing companies longer than most. So, as manufacturing companies expand globally, Travelers will be there to help manage their risks with the right insurance products.



travelers.com

The Travelers Indemnity Company and its property casualty affiliates. One Tower Square, Hartford, CT 06183

This material does not amend, or otherwise affect, the provisions or coverages of any insurance policy or bond issued by Travelers. It is not a representation that coverage does or does not exist for any particular claim or loss under any such policy or bond. Coverage depends on the facts and circumstances involved in the claim or loss, all applicable policy or bond provisions, and any applicable law. Availability of coverage referenced in this document can depend on underwriting qualifications and state regulations.

© 2018 The Travelers Indemnity Company. All rights reserved. Travelers and the Travelers Umbrella logo are registered trademarks of The Travelers Indemnity Company in the U.S. and other countries. BCMWH.0009-P New 4-18