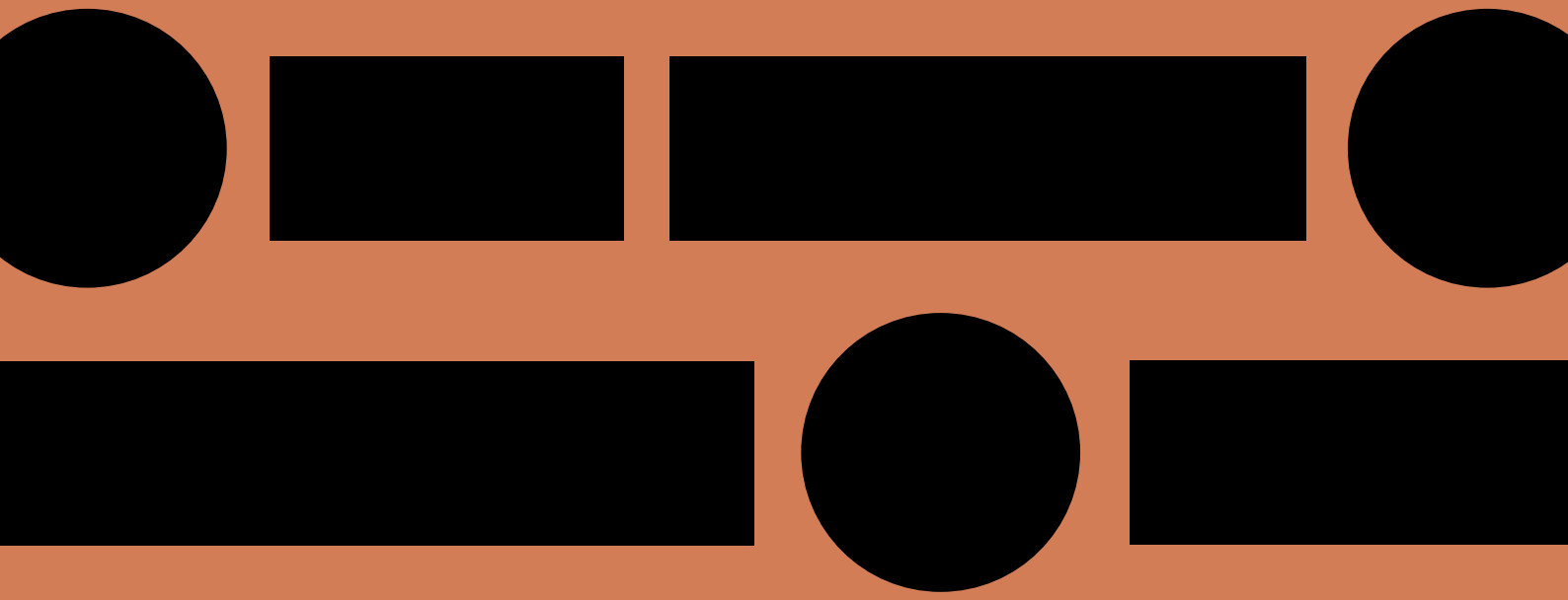
WHITEPAPER

IIoT: The Gateway to Efficiency for Smart Manufacturing

Unlocking the potential of Industry 4.0



SECOMEA

About Secomea

Founded in 2008, Secomea has been catering to the OT remote access needs of manufacturers and machine builders for over 15 years.

Secomea is a Secure Remote Access (SRA) solution purpose-built for industrial networks and OT equipment. Over 9,500 customers around the world use it every day across thousands of sites to manage remote access to their machines, reduce cybersecurity risks, and prevent downtime.

© Secomea 2024, All rights reserved. The content provided in this publication is intended for general informational purposes only and not to be relied upon as legal or other professional advice. Although we endeavor to provide correct and timely information, we cannot guarantee its accuracy as of the date it is received since it may not be up to date with the most recent legal or technical developments. Secomea would be pleased to advise readers on how to apply the principles set out in this publication to their specific circumstances. For additional information, please visit secomea.com.

Securing the future

Seizing IIoT opportunities

Harnessing the power of IIoT

Manufacturing leaders may feel overwhelmed trying to choose amongst the plethora of digital solutions that promise to improve operational performance.

Still, one of the most essential areas they are investing in is the **Industrial Internet of Things (IIoT)**, as they are seeing its game-changing value for manufacturing operations and overall production process monitoring. And that is proved by the fact that the Industrial IoT market is expected to reach $325.8 billion in 2024[1].

So, to maintain a competitive edge, an increasing number of industrial processes are anticipated to include IIoT technology as it undergoes perpetual evolution.

But alongside the promise of innovation comes the looming specter of cyber risks.

Manage risks, maximize rewards

Ransomware organizations, such as LockBit and ALPHV, had a surge in activity from the second half of 2022 to the first half of 2023, leading to a 53% rise in attacks against the manufacturing industry[2].

Manufacturing is now the most targeted sector, even more so than financial enterprises.

Security challenges in IIoT differ significantly from those in IoT across multiple aspects - such as attack surface, connectivity, interoperability, and integration with **Operational Technology (OT)**.

For manufacturing businesses to enjoy the positive effects of digitalization, they must become cyber-resilient and ready to face the dynamic threat environment.



To support you in this process, we have compiled this whitepaper covering the main pillars of IIoT in manufacturing alongside cybersecurity concerns and best practices.

Read on to

- Discover the **innovation triad** made of IIoT, Industry 4.0, and Smart Manufacturing.
- Explore the components of the **IIoT ecosystem** you can implement in your production facilities to drive overarching business improvements
- **Understand the risks** faced by modern manufacturers in the current IIoT cyber-threat landscape
- **Implement risk management** best practices to mitigate and prevent IIoT cybersecurity risks.

Table of Contents

01 IIoT, Industry 4.0, Smart Manufacturing
Exploring the innovation triad 5

02 The Transformative Power of IIoT
Reshaping Manufacturing Operations 12

03 IIoT Cyber Risks Unveiled
Safeguarding Manufacturing Infrastructure 15

04 IIoT Cybersecurity Best Practices
Risk Management Strategies for Manufacturers 22

05 How Secomea can help you embark on your IIoT journey
Discover the industry-leading SRA solution 26

01

IIoT, Industry 4.0, Smart Manufacturing

Exploring the innovation triad

A new outlook for the manufacturing industry

Integrating IIoT with Smart Manufacturing and Industry 4.0 principles is dynamically reshaping the manufacturing landscape.

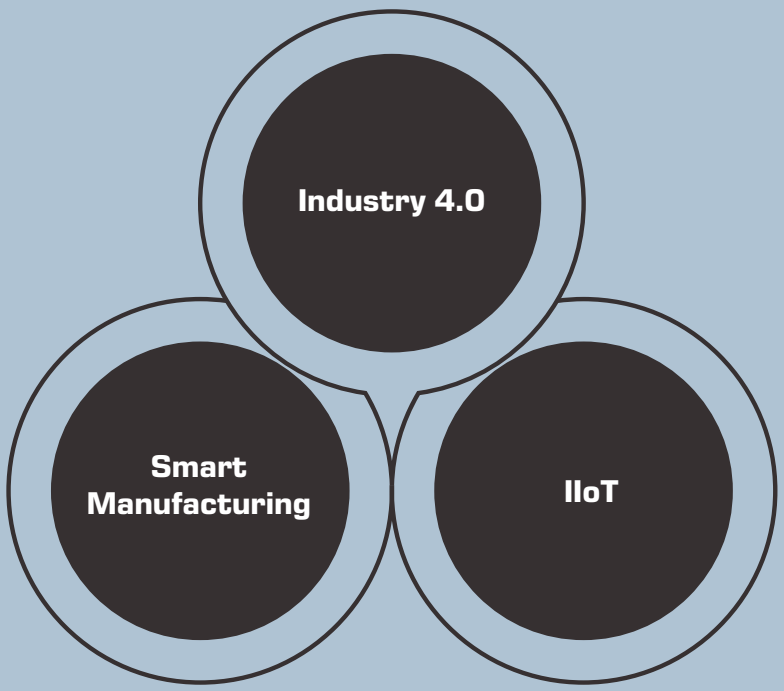
IIoT facilitates seamless connectivity among devices, enabling smarter manufacturing processes.

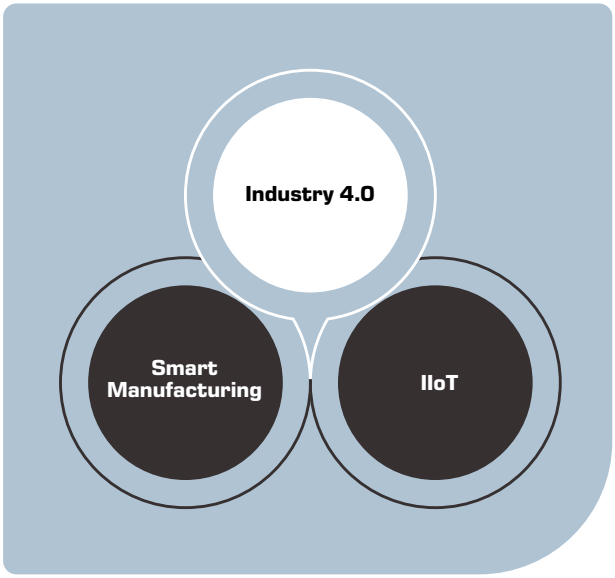
Through automation and real-time analytics, Smart Manufacturing strengthens production efficiency.

Meanwhile, Industry 4.0 principles integrate advanced digital technologies into traditional manufacturing, driving improvements in productivity.

Each pillar of this convergence set new, modern standards for innovation, providing the outlook for a future where intelligent systems redefine manufacturing processes.

Let's cover the basics by exploring what each of them entails.







Industry 4.0: The next frontier in manufacturing evolution

From steam power to cyber-physical systems: a historical journey to Industry 4.0

Since the introduction of the concept of “Industry 4.0” in 2011, the purported fourth industrial revolution has already occurred.

For enhancing industrial productivity, safety, efficiency, and transparency, this revolution is distinguished by its reliance on Cyber-Physical Systems (CPS), which are capable of communicating with one another and making autonomous, decentralized decisions.

A trip down memory lane

For centuries, technological advancements have been responsible for redefining the way we live as a society – experiencing what we call industrial revolutions. Industry 1.0, emerging in the late 1700s, marked the advent of water and steam-powered machines in manufacturing. Industry 2.0, commencing in the early 20th century, introduced electricity and assembly lines.

By the latter part of the 20th century, Industry 3.0 emerged, characterized by the integration of computers into manufacturing processes.

Over the past decade, incorporating innovative technologies into manufacturing processes and operations has ushered in a new age of industrial growth known as **Industry 4.0**.

Transitioning to Industry 4.0 demands disruptive technologies like IoT, cloud computing, big data, digital twin, augmented reality, 3D printing, artificial intelligence, and new generation CPS to enable autonomous communication among industrial devices.

Through distributed communication architectures beyond centralized models, companies must prioritize cybersecurity considerations due to the critical impacts of breaches on business models and competitiveness.

Workers, being the most flexible component of cyber-physical production systems, will be entrusted with a growing suite of responsibilities[3], from strategy verification to monitoring and specification. Empowered by the latest technology, employees can reach their maximum potential and become strategic decision-makers and adaptable problem solvers.

In various research papers[4], the eight key factors outlined below consistently emerge as pillars of Industry 4.0.



Exploring the pillars of Industry 4.0

Autonomous Robots
Vital components of Industry 4.0, autonomous robots provide diverse services, including task completion, safe human interaction, and learning from human input.

Additive Manufacturing
By producing customized products in small batches, it reduces transportation and inventory costs, enhancing Industry 4.0 performance.

Horizontal & Vertical System Integration
Facilitating swift delivery, it directly connects companies and suppliers, accelerating the production process.

Industrial Internet of Things (IIoT)
Foundational to Industry 4.0, IIoT enables real-time responses and enhances productivity through centralized sensor-equipped machines.

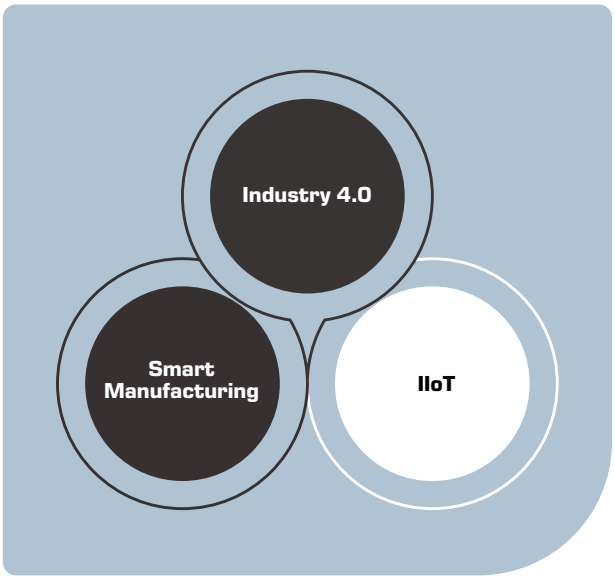
Cloud Technology
Key for managing vast data in Industry 4.0 setups, cloud technology enhances data storage and retrieval cost-effectively.

3D Simulation
Integral to Industry 4.0, 3D simulation optimizes machine settings before production, reducing time and enhancing quality.



Augmented Reality
By providing real -time information for quick decision -making, it improves industrial processes.

Big Data & Analytics
By analyzing vast untapped data, it enables product quality optimization, service improvements, and energy savings.





Elevating industry performance: the role of IIoT in manufacturing

IIoT innovation: shaping the future of industrial connectivity

Industrial IoT can only be understood with a brief overview of the fundamentals of the Internet of Things.

The Internet of Things (IoT) refers to a network comprising physical objects that are sensor-enabled and Internet-connected[5], facilitating data collection and exchange.

IIoT is a version of the Internet of Things that aims to **improve safety, security, and communication** in critical industrial settings so that they can continue their ongoing, continuous operation. Proprietary maintenance and effective management of industrial assets and activities remain the key focuses of IIoT[6].

"The Industrial Internet of Things is made up of a multitude of devices connected by communications software. The resulting systems, and even the individual devices that comprise it, can monitor, collect, exchange, analyze, and instantly act on information to change their behavior or environment intelligently – all without human intervention[7]."

The IIoT shares several core technologies with the broader Internet of Things (IoT) - such as cloud computing, sensors, connectivity solutions, machine-to-machine (M2M) communication, and data analytics.

However, the deployment contexts and objectives significantly diverge between the two.

IoT technologies improve daily living in agriculture, healthcare, consumer products, and smart cities through smart gadgets like wearable fitness trackers and automated home systems.

In general, these new applications do not entail any severe risks if they fail.

In contrast, IIoT is built for industrial applications in manufacturing, oil and gas, utilities, etc. System breakdowns or downtime might pose safety risks or incur many costs, so IIoT solutions focus on operational efficiency, safety, and system health.

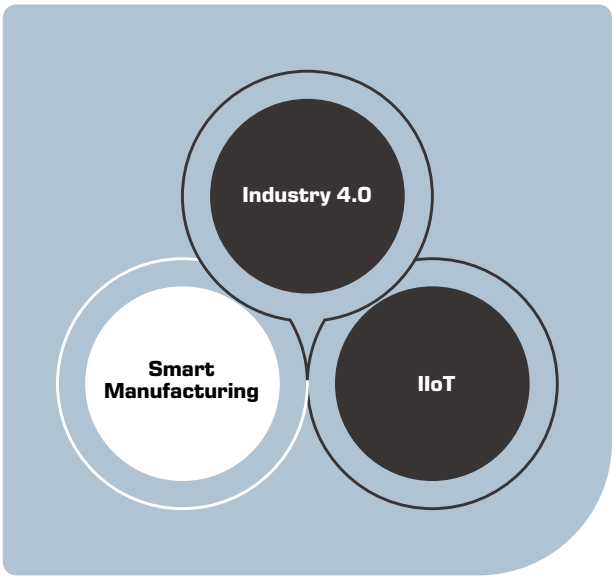
When integrating IIoT elements, manufacturers face crucial decisions on technology across three levels: platform, cloud, and ecosystem.

The critical dimensions of IIoT

Platform
At the platform level, they must integrate IIoT with OT, often requiring a redesign of traditional manufacturing systems. This involves assessing current setups, creating future target states, potentially partnering for implementation, and managing cybersecurity challenges.

Cloud
Cloud solutions offer significant business benefits, including access to AI and machine-learning engines and a sandbox environment for experimentation. Manufacturers should strategically migrate applications to the cloud, implement robust governance measures, and establish infrastructure teams for efficient management.

Ecosystem
Uniting all the disparate components, ecosystems are vital for IIoT success. Whether building their own or joining an existing one, manufacturers need a solid platform to manage applications, analytics, and data. Ensuring a diverse set of partners with varied skills and value propositions is crucial, with leading companies establishing industrial business-development teams to leverage ecosystem contributions effectively.





Breaking barriers: implementing Smart Manufacturing strategies

From concept to reality: connecting processes in Smart Manufacturing

Smart Manufacturing represents the tangible manifestation of the IIoT's impact on traditional manufacturing.

For designing, simulating, and configuring the controllers of the manufacturing machinery, most of the process preceding the actual manufacturing phase is entirely digital and dependent on computer networks and computational resources. Hybrid manufacturing, additive, and subtractive machinery may comprise the Digital Manufacturing (DM) system.

Connectivity is a prerequisite for this process transfer across the entire process chain. Yet, connectivity presents a security risk that must be mitigated[8] through the implementation of both conventional and innovative cybersecurity solutions that span multiple stages of the process flow.

02

The Transformative Power of IIoT

Reshaping Manufacturing Operations

Below is an overview of the complex web of technology that can allow contemporary manufacturing organizations to be more efficient, productive, and innovative.

Connected Devices
Containing sensors and communication capabilities, these devices adeptly collect and transmit data about their operational states and surroundings. Authorized personnel is then granted access to and analysis of the data via a centralized IIoT platform.

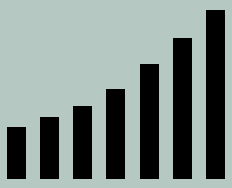
Analytics and Applications
Data from IIoT devices is gathered, stored, and analyzed through applications and analytics. Subsequently, the data can be utilized for process optimization, maintenance demand prediction, and production monitoring. Even more, the overall quality of products and services may also be enhanced with the assistance of this information.

Communications Infrastructure
Every device in an IIoT system is connected to the network via the Data Communications Infrastructure. Devices are able to communicate data in real-time because of this architecture, and it is also possible to access and manage devices remotely. Both public and private networks facilitate fluid information exchange across the ecosystem's nodes.

Data Storage Solutions
Repositories designed to accommodate the vast amounts of data generated by IIoT devices ensure the availability of such data for analysis and reference. By employing distributed storage architectures, redundancy mechanisms and data replication organizations can ensure fault tolerance and high availability, minimizing the risk of data loss or downtime.

Human Interaction
As with any digital system, humans are in charge. Specialists and operators can engage with the IIoT ecosystem, leveraging their expertise to interpret data, make informed decisions, and take action based on the insights provided. Users may also access and administer devices remotely via IIoT systems.





Driving efficiency and security: how IIoT enhances operational performance in manufacturing

IIoT enables manufacturers to collect reliable and accurate data to know how they are doing and where they are falling short, and then act on that data to make their production processes more efficient. Let's explore some more ways in which IIoT impacts organizations.

Tangible ways in which IIoT impacts manufacturing

Operational efficiency enhancement
IIoT technologies enable manufacturers to boost efficiency significantly through automation and optimization. Robotics and automated systems increase precision and speed, thereby enhancing productivity and streamlining manufacturing processes.

IIoT tools and platforms allow for fine-tuning production workflows, leading to increased output and improved profitability while also elevating product quality through precise monitoring.

Sharing knowledge across plants
Sharing knowledge across plants is essential for organizational success. Institutionalizing knowledge within the workforce preserves critical information over time and promotes process standardization.

Centralized knowledge is invaluable for continuous improvement efforts, allowing experts to address issues regardless of location.

Better interfaces for operators
Connected software empowers operators, engineers, and managers to monitor data through intuitive Human-Machine Interfaces (HMIs).

As a whole, these interfaces consolidate data from various sources, facilitating access and analysis for personnel with varying levels of IT proficiency.

This centralized approach enables personnel to master tools without extensive training or dependence on IT staff.



Accident prevention & safety improvements

Continuous monitoring and data analysis from industrial machinery enable the prediction and prevention of equipment failures and hazardous incidents.

Predictive maintenance software, analyzing sensor data from machinery, identifies and rectifies potential mechanical failures before they lead to accidents.

Real-time asset monitoring & management

IIoT's role in remote manufacturing includes critical asset monitoring using sensors to track production activities and update relevant personnel.

Such capabilities extend to comprehensive asset management, providing a sophisticated platform for optimizing asset use and supporting proactive manufacturing decisions.

Real-time tracking of machinery and product conditions through IIoT facilitates production schedule refinement, inventory cost reduction, and logistics enhancement.

IIoT-driven asset tracking aids in preventing quality issues and enables the precise location of misplaced or stolen assets, offering a transformative approach to asset utilization in manufacturing.

Process & behavior monitoring

Process and behavior monitoring drive performance enhancements in manufacturing. Data collected from IoT-enabled devices and software offers invaluable insights into employee performance. Managers leverage this data to identify bottlenecks and areas for improvement, such as recurring mistakes or defects during specific steps.

Process engineers utilize this information for root cause analysis, guiding improvements, and serving as a benchmark for progress.

Improved predictive maintenance

Production facility breakdowns lead to exorbitant repair bills. But predictive maintenance, facilitated by AI, may help businesses save millions.

Still, industrial machine learning methods are useless without accurate information on the hardware under consideration.

Sensors connected to the Industrial Internet of Things may gather data from a collection of machines in a network. Following this data, it will be possible to determine which equipment needs preventative maintenance and when. In addition to assessing electricity consumption, temperature, and vibration, these sensors may predict eventual machinery failure points.

03

IIoT Cyber Risks Unveiled

Safeguarding Manufacturing Infrastructure

Reaping the benefits of IIoT while counteracting cyber risks

Now more than ever before, manufacturers are placing a premium on security.
The World Economic Forum[9] drew some alarm bells by pointing out that “manufacturing has been the most targeted sector by cyberattacks.” IBM[10] estimated that **in 2022, over 30% of extortion happened in the manufacturing sector due to the low tolerance for downtime**.

Midway through 2023, the SonicWall Cyber Threat Report[11] found that there was a **37% increase in IoT malware**, with 77.9 million assaults recorded, compared to 57 million in the same period in 2022.
As a domino effect, the risks that ensue are systemic in nature, easily transmissible, and frequently exceed the understanding or authority of an individual entity.

Each producer within the manufacturing ecosystem is also a consumer, and production facilities are dispersed across the globe. Thus, a cyberattack directed at a single organization can generate catastrophic repercussions throughout the entire ecosystem.

High failure probabilities in these settings could expose IIoT resources to cyberattacks, leading to everything from losing confidential information to significant revenue losses.



Compared with conventional networks like IoT, **IIoT paradigms are notably more sensitive due to their vast scale, complexity, robustness, and the critical role they play.**

Traditional networks comprise IT infrastructure components like servers, workstations, routers, and switches. IIoT, on the other hand, broadens the attack surface by including a variety of industrial devices such as control systems, sensors, actuators, SCADA systems, field devices, and industrial communication protocols.

Strong IIoT security functions as a shield for the intelligent machinery and devices utilized in industries. In the same way that we protect our homes with locks and alarms, IIoT security consists of a collection of procedures and technologies that safeguard industrial systems and machinery against cyberattacks and other digital risks.

By choosing the right IIoT providers, manufacturers and machine builders can stay ahead of the curve and successfully overcome these cyber risks.



Fortifying manufacturing security: avoid common mistakes when implementing IIoT

Although they provide unquestionable benefits for operations productivity, IIoT devices are appealing targets for cybercriminals because of the numerous security holes they pave the way to[12]. Once they gain access, hackers may go laterally and access other servers, devices, and private information.

Smart factories have expanded attack surfaces, meaning that a large number of “entry points” to the commercial or industrial infrastructure are readily discoverable by adversaries.

Potential security threats include the exploitation of vulnerabilities, malware deployment, and both DoS and DDoS attacks. Properly introducing a solid security strategy across OT security and physical safety necessitates a cohesive approach by Smart Manufacturing organizations.

Originally, the industrial environment was not designed with cybersecurity considerations, and this transition to IP-based cyber-physical systems has introduced significant vulnerabilities.

As systems convert from closed to connected cyber-physical configurations, new vulnerabilities emerge - and they require urgent attention.

Despite the critical need for advanced cybersecurity measures, many manufacturers’ cybersecurity maturity is not yet sufficient to combat these risks effectively.

Below are the most common mistakes to look out for to ensure a secure IIoT implementation.

Most common errors to avoid when implementing IIoT

Insufficient security features in IoT devices
IoT devices often include basic security functionalities that are inadequate for blocking sophisticated cyber threats.
Vulnerabilities in these devices can become conduits for attackers to penetrate broader enterprise networks.

Lagging behind in updating and patching devices
Failing to update and patch IoT devices consistently exposes them to attacks, as cybercriminals often target known vulnerabilities.
Regular updates are essential for protecting against these threats.

Neglecting encrypted traffic inspection
While employing encryption is a vital security measure, it can also veil malicious activities.
Failing to scrutinize encrypted traffic leaves organizations at risk of overlooking threats hidden within encrypted communications.

Flawed authentication protocols
Weak authentication and authorization mechanisms rank among the top vulnerabilities in IoT infrastructures.
Utilizing easily guessable or default passwords, not implementing MFA, and poor access control measures can enable unauthorized access.

Excessive trust in devices
Placing undue trust in IoT devices, especially those unauthorized or lacking robust security measures, introduces risks.
Such shadow IoT devices, not complying with organizational security policies, create additional avenues for security breaches.

Gaps in network visibility
Ensuring comprehensive visibility over an expanding network of connected devices presents a substantial challenge.
Lack of visibility into which user is connected to which device and their activities leaves organizations vulnerable to threats that remain undetected within their networks.

Knowing what you're up against is half the battle

Any network might be vulnerable to any of the following cyberattacks. But with the rise of the IoT, these dangers operate on a whole new dimension.
Their cyber roots may now have real-world effects, particularly in the IIoT space where **IT and OT are converging.**

On the next page, we prepared an overview of the most common types of cyber-attacks you should be mindful of and how you can prepare to protect your manufacturing organization.



Main types of cyber attacks		Takeaways for manufacturers
DoS and DDoS Attacks	DoS and DDoS attacks disrupt services by overwhelming networks or devices, as exemplified by the IoT botnet Mirai's significant online disruption[13]. The availability of DDoS-as-a-service and the release of Mirai's source code suggest an increasing threat to IIoT infrastructure.	Strengthen network resilience and prepare for potential DDoS attacks with advanced threat detection and mitigation strategies.
Man-in-the-Middle (MitM) Attacks	MitM attacks intercept communications between devices or systems within a smart factory, potentially altering transmitted data or stealing sensitive information. This risk is exacerbated by insecure communication protocols, which could allow attackers to manipulate data in transit.	Secure all communication channels and employ encryption to prevent unauthorized data interception and manipulation.
Vulnerability Exploitation	Smart factories connect numerous devices into a unified network, creating potential entry points for cyberattacks through any single vulnerability. The Stuxnet worm[14] illustrated this by exploiting specific vulnerabilities to target critical infrastructure, highlighting the necessity of robust security measures like consistent software updates.	Prioritize regular security updates and comprehensive vulnerability assessments to safeguard every connected device within the network.
Malware Deployment	Threat actors frequently deploy malware to compromise industrial control systems (ICS). The specialized trojan Triton[15] further demonstrates the risks, having been designed to disrupt industrial safety systems. Moreover, a European water facility's recent breach via cryptocurrency-mining malware[16] underscores the evolving nature of threats.	Implement comprehensive malware defenses and promote cybersecurity awareness among employees to counteract the varied malware tactics employed by attackers.
Surveillance and Information Theft	Attackers may stealthily steal data or surveillance systems, targeting exposed human-machine interfaces (HMI) to access customer databases or personally identifiable information (PII). The unauthorized network access for stealing operational data emphasizes the need for effective intrusion detection and prevention.	Enhance network security with robust intrusion detection systems and secure sensitive data against unauthorized access.
Device Hacking	Since there are multitudes of connected devices within smart factories, they present numerous targets for hacking, where a single compromised device can jeopardize the entire network. Physical device tampering also poses a significant risk to operational integrity.	Ensure comprehensive device security, both for digital threats and physical tampering, to maintain operational continuity and network integrity.

Revenue loss and safety risks: the expensive consequences of overlooking cybersecurity

Failing to protect systems, processes, data, and thereby enabling exploitation, can cause significant financial and operational harm and shatter a company's image.

For a manufacturing organization, a cyber-incident could lead to equipment failures, unplanned downtime, supply shortages, or other issues.

When production ceases, revenue generation comes to a halt, causing immediate economic impacts. Additionally, the interruption can strain relationships with partners due to disrupted supply chains.

Besides, manufacturing downtime significantly elevates the risk of workplace accidents. Research indicates a significant increase (about 40%) in workplace accidents during production startups and shutdowns, underscoring the importance of avoiding downtime to maintain a safe working environment.

Numbers don't lie: calculating the real cost of downtime

According to Siemens' 2023 report, the cost of downtime has significantly increased over the past two years (2021-22), with unplanned downtime now costing Fortune Global 500 companies 11% of their yearly turnover (almost $1.5 trillion).

The cost of a lost hour now ranges from an average of $39.000 to more than $2 million depending on industry (with the highest in Automotive). In Oil & Gas, the cost of an hour's downtime has more than doubled in just two years to almost $500,000.

The total losses to downtime are also rising sharply. The cost for an average large plant in the sectors surveyed is now $129 million a year, up 65% in just two years.
Among respondents, the average manufacturing facility suffers 20 monthly downtime incidents – six fewer than two years ago.

When a manufacturer experiences downtime, the financial impact can be significant and is usually calculated based on two main categories: direct costs and indirect costs.

Direct costs encompass tangible expenses directly related to the downtime event. This includes the value of lost production during the downtime period, the wastage of raw materials that occurred while production was halted, and any expenses associated with repairing or restoring equipment to operational status.

Indirect costs, on the other hand, are less tangible but equally important. These include factors such as missed sales opportunities due to the inability to fulfill orders during downtime, additional expenses incurred from having to pay overtime to employees to catch up on lost production time, and potential damage to the company's reputation or brand image resulting from delayed deliveries or poor customer service.

Combining these two categories, the overall cost of downtime can be estimated by considering factors like the duration of the downtime event, the financial impact per unit of time (such as the cost per minute of downtime), lost revenue opportunities, overtime labor expenses, and potential reputational damage.

While these considerations provide a simplified framework for estimating downtime costs, the actual financial impact will vary depending on the unique circumstances of each manufacturing operation. You can evaluate the potential cost of downtime in your organization **using our calculator**.



04

IIoT Cybersecurity Best Practices

Risk Management Strategies for Manufacturers

From risk to resilience: cyber hygiene in manufacturing

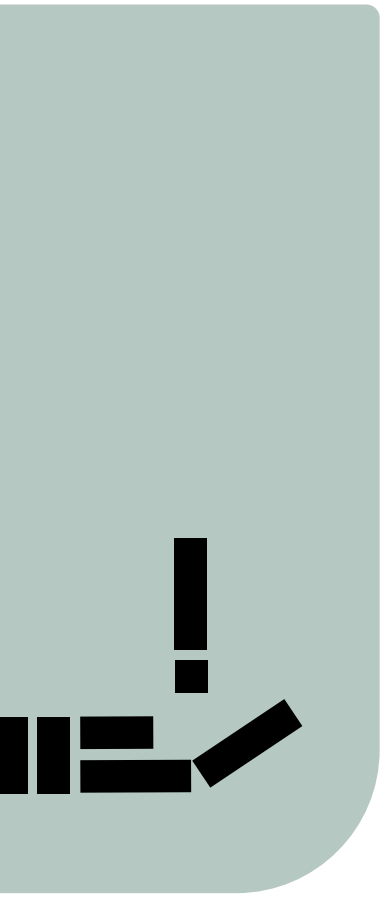
The reality that we can't influence every single detail of any given circumstance is a major theme in risk management.

The information landscape, including both internal and external factors, is dynamic and subject to constant change.

Therefore, keeping an eye on potential dangers may verify assumptions and determine if a risk is becoming more likely to materialize than originally anticipated or whether it is already a major problem.

In the following pages, you'll find a list of risk management best practices to protect your manufacturing organization from IIoT cybersecurity risks.





Recommendations for proactive risk management

Integrate a zero-trust approach

Adopting a Zero-Trust Architecture is a strategic move to enhance the security of IIoT systems.

This approach operates on a fundamental principle: trust no one and verify everything – hence, the zero-trust principle.

Access is granted strictly on a need-to-know basis, significantly reducing the risk of unauthorized entries and potential cyber threats.

Conduct risk assessments

Addressing cybersecurity risks in IIoT requires a clear plan, starting with a detailed risk assessment.

A risk assessment helps understand what might go wrong, how likely it is to happen, and the impact if it does happen. It looks at IIoT devices, sensors, and how IT and OT communicate.

After identifying and ranking the risks, steps can be taken to reduce them.

Introduce a Secure Remote Access solution

Secure Remote Access (SRA) solutions facilitate secure connections for remote users, including employees and third-party vendors, to access a company's infrastructure and systems from outside the corporate network. Therefore, SRA solutions are essential for remote maintenance, enabling access to devices from anywhere, at any time, while adhering to your organization's security protocols and compliance policies.

While each SRA solution may provide specific capabilities, make sure to opt for one including VPNs, SSL/TLS, or other secure protocols for data transmission, MFA or SSO for simplified user access, Secure Tunneling, and Access Control to define and enforce policies that restrict access based on user roles, devices, or locations – and mechanisms to approve access requests.

Equipping your production facilities with a secure remote access solution will go a long way in improving your cybersecurity posture - as well as driving cost-efficiency and overall performance enhancements.



Cultivate a strong cyber culture
After all, the security of IIoT systems depends on staff members actively practicing good security habits.

Organizations need to employ targeted training and awareness programs that educate employees, covering the best practices - such as utilizing strong, distinctive passwords, multi-factor authentication, and so on.

Build structured update processes
As IIoT environments become increasingly complex, the challenge of keeping devices updated has intensified. Where manual updates were once feasible, the vast deployment of devices now makes this impractical.

Companies must prioritize structured update processes, opting for systems that support automatic updates and have a long operational lifetime to ensure devices remain secure throughout their use.

Preserve network segmentation & device management
Separating networks for connected machines from general office or guest networks is essential for enhancing security.

Access to these specialized networks should be tightly controlled, with credentials limited to necessary personnel only, to prevent unauthorized access and potential security breaches.

Implement strong controls
Access control, authentication, and encryption are fundamental for securing network communication channels. It is non-negotiable to guarantee the security of all communications, including data transmission and remote access between IIoT devices and control systems.

Step by step, the network is fortified against unauthorized intrusion, and the integrity of data in transit is preserved.

Assure software maintenance
Despite the challenges in scheduling device or machinery updates and restarts, regular software maintenance is essential. It is also a fundamental defense mechanism against cybersecurity attacks.

Firmware also requires attention, with updates often addressing security vulnerabilities.

Use secure messaging platforms
Adopting secure messaging protocols like MQTT for IIoT communication offers additional security layers.

MQTT is designed to be secure, allowing only subscribed clients to receive messages - and, when combined with Transport Layer Security (TLS) encryption, it preserves the confidentiality and integrity of data in transit.

Sustain the viability of cyber policy management
Centralizing visibility and policy management is essential for effective cybersecurity across an organization's IT network and IoT/OT process network.

A unified monitoring and management platform allows security teams to observe the entire cyber kill chain and swiftly implement controls and policies across IT and OT sites.

Leverage hardware security modules
Incorporating Hardware Security Modules (HSM) into an organization's security strategy enhances the protection of hardware components. HSMs are specialized devices designed to secure cryptographic keys and sensitive data, preventing unauthorized access and tampering.
Their integration into the security infrastructure reduces the risk of data compromise.

Bonus tips

Formulate common goals for all teams

To bridge the gap between OT, IT, and SecOps teams, a unified approach to cybersecurity is paramount.

Traditionally, OT teams prioritize reliability and availability for production continuity, while cybersecurity teams focus on safeguarding information confidentiality and data integrity. Despite these differing priorities, common objectives such as maximizing uptime and risk mitigation can serve as a foundation for collaboration.
OT personnel should be made aware of cyber risks and the significance of maintaining cyber hygiene to prevent attacks, thereby easing the responsibilities of cybersecurity teams.

At the same time, cybersecurity and IT professionals need training in OT operations. Mutual support and joint efforts are today necessary to ensure smooth communication and successfully **improve the IT-OT dynamics**.

Choose the right partner

If manufacturing businesses want to keep their industrial networks and OT equipment secure, choosing a reliable cybersecurity partner is imperative.

Therefore, one last but crucial piece of advice is to entrust compliant providers that have clear security policies in place.

Your choice should fall on a provider that can prove its commitment to security through certifications based on third-party audits.
Some **cybersecurity standards** are internationally recognized best practices for securing operational technology in automation and control systems. **IEC 62443**, for example, proves that a provider has implemented a secure-by-design methodology in the product development process, which includes complete security lifecycle management and patch management. So they can successfully identify and respond to vulnerabilities and mitigate their risks.

05

How Secomea can help you embark on your IIoT journey

Discover the industry-leading SRA solution purpose-built for OT environments



Towards IIoT excellence: how Secure Remote Access empowers manufacturers

Secure Remote Access solutions: your go-to choice for IIoT management

A Secure Remote Access solution is an essential component of a comprehensive IIoT cybersecurity strategy. By centralizing multiple remote access approval processes under one interface, activity authorization, monitoring, and logging actions can be made through a single portal, gifting manufacturers complete control. Such tools are especially useful for large companies that use IIoT systems to safeguard multiple production sites at once, efficiently and comfortably from a single office.

For an IIoT setup to work efficiently and drive improvements in performance and safety, manufacturing organizations need to enable remote access and maintenance to IT and OT equipment for a distributed workforce. And that's what IIoT remote access solutions like Secomea specialize in.

A new era of manufacturing connectivity with IIoT Secure Remote Access

Supporting a wide range of use cases, Secure Remote Access solutions offer multiple benefits to organizations seeking to improve their OT cybersecurity profile, as outlined below.

Benefits of including a Secure Remote Access (SRA) solution in your IIoT setup

Allowing companies to support remote work and secure access to corporate resources from anywhere with an internet connection, SRA solutions enable **flexibility** – which is especially valuable during emergencies or in a global workforce.

For the same reason, SRA solutions play a crucial role in **business continuity** plans, ensuring that operations can continue even when employees cannot physically be present due to unexpected events like natural disasters or pandemics.

Besides, enabling remote access leads to **cost and time savings** – as there is no need to pay and wait for a technician's trip to the location where the device in need of assistance is located.

What's more, it allows companies to tap into a global talent pool by hiring remote workers from various geographic locations, accessing specialized skills, and **reducing the impact of skill shortages**.

Introducing Secomea's IIoT solution: how we help you defend your factory floor

Offices in Denmark (HQ), US, China, Japan

Represented in 35 countries through our 70+ Distributors, Alliance Partners and OEM Partners

+9.500 customers, over 300.000 SiteManagers installed in thousands of production sites worldwide

Manage remote access in a few clicks

Plug-and-play for ICS: PLC, HMI, SCADA

High security by design

Purpose-built for OT equipment

Global reach, local support

Easy to use for you and for your technicians

Implementation at record speed

Supports all protocols: RDP, VNC, SSH, Telnet

New platform built on a zero-trust architecture

Secomea solution overview: your turnkey IIoT platform

Secomea Prime
Gain full oversight over your remote access sessions

IIoT Gateway
Connect hardware/ install software to any OT asset

IIoT Server
Seamlessly manage user access to assets

Access Client
Easy access to assets by authorized users

Why Secomea is trusted by over 9.500 manufacturers and machine builders worldwide since 2008

Secomea is a Secure Remote Access (SRA) solutionpurpose-built for industrial networks and OT equipment. It includes all the software and hardware components needed for performing remote access and maintenance tasks—from remote programming and troubleshooting to data-driven decision-making.

As a turnkey solution, Secomea can be implemented at record speed, and it's ready to use with ease, even by non-IT people. With Secomea, you can manage your technicians' access with a few clicks, allowing them to intervene on any of your machines immediately, wherever they are. This minimizes response time, reduces security risks, and prevents downtime.

Our brand-new platform built on a zero-trust architecture, **Secomea Prime**, gives you complete oversight over your remote access sessions.
The **IIoT Gateway** is the key component of the solution, which, in combination with the **IIoT Server** and **Access Client**, connects you transparently to machines anywhere in the world.

Together we make manufacturing the most secure industry in the world.





Sources

[1] https://www.statista.com/outlook/tmo/internet-of-things/industrial-iot/worldwide

[2] https://www.reliaquest.com/blog/cyber-threats-to-manufacturing-industry-1h-2023/

[3] https://ieeexplore.ieee.org/abstract/document/6945523

[4] https://www.techscience.com/csse/v37n3/41714

[5] https://link.springer.com/book/10.1007/978-1-4842-2047-4

[6] https://www.sciencedirect.com/science/article/abs/pii/S0045790618329550

[7] https://link.springer.com/chapter/10.1007/978-3-319-42559-7_1

[8] https://ieeexplore.ieee.org/abstract/document/9247392

[9] https://www.weforum.org/agenda/2023/03/why-cybersecurity-in-manufacturing-matters-to-us-all/

[10] https://www.ibm.com/reports/threat-intelligence

[11] https://www.sonicwall.com/2023-mid-year-cyber-threat-report/

[12] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8200965/

[13] https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/

[14] https://www.csoonline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html

[15] https://www.technologyreview.com/2019/03/05/103328/cybersecurity-critical-infrastructure-triton-malware/

[16] https://www.securityweek.com/cryptocurrency-mining-malware-hits-monitoring-systems-european-water-utility/



www.secomea.com