What is the industrial internet of things (IIoT)?

The industrial internet of things (IIoT) refers to the extension and use of the internet of things (IoT) in industrial sectors and applications. With a strong focus on machine-to-machine (M2M) communication, big data, and machine learning, the IIoT enables industries and enterprises to have better efficiency and reliability in their operations. The IIoT encompasses industrial applications, including robotics, medical devices, and software-defined production processes.

The IIoT goes beyond the normal consumer devices and internetworking of physical devices usually associated with the IoT. What makes it distinct is the intersection of information technology (IT) and operational technology (OT). OT refers to the networking of operational processes and industrial control systems (ICSs), including human machine interfaces (HMIs), supervisory control and data acquisition (SCADA) systems, distributed control systems (DCSs), and programmable logic controllers (PLCs).

The convergence of IT and OT provides industries with greater system integration in terms of automation and optimization, as well as better visibility of the supply chain and logistics. The monitoring and control of physical infrastructures in industrial operations, such as in agriculture, healthcare, manufacturing, transportation, and utilities, are made easier through the use of smart sensors and actuators as well as remote access and control.

In the context of the fourth industrial revolution, dubbed Industry 4.0, the IIoT is integral to how cyber-physical systems and production processes are set to transform with the help of big data and analytics. Real-time data from sensors and other information sources helps industrial devices and infrastructures in their “decision-making,” in coming up with insights and specific actions. Machines are further enabled to take on and automate tasks that previous industrial revolutions could not handle. In a broader context, the IIoT is crucial to use cases related to connected ecosystems or environments, such as how cities become smart cities and factories become smart factories.

The consistent capturing and transmitting of data among smart devices and machines provide industries and enterprises with many growth opportunities. The data allows industries and enterprises to pick up on errors or inefficiencies in the supply chain, for example, and immediately address them, thus pushing for day-to-day efficiency in operations and finance. Proper integration of the IIoT can also optimize the use of assets, predict points of failure, and even trigger maintenance processes autonomously.

By adopting connected and smart devices, businesses are enabled to gather and analyze greater amounts of data at greater speeds. Not only will this enhance scalability and performance, but it can also bridge the gap between the production floors and general offices. Integration of the IIoT can give industrial entities a more accurate view of how their operations are moving along and help them make informed business decisions.

What are the security considerations and challenges in adopting the IIoT?

Adoption of the IIoT can revolutionize how industries operate, but there is the challenge of having strategies in place to boost digital transformation efforts while maintaining security amid increased connectivity.

Industries and enterprises that handle operational technologies can be expected to be well-versed in such aspects as worker safety and product quality. However, given that OT is being integrated into the internet, organizations are seeing the introduction of more intelligent and automated machines at work, which in turn invites a slew of new challenges that would require understanding of the IIoT's inner workings.

With IIoT implementations, three areas need to be focused on: availability, scalability, and security. Availability and scalability may already be second nature to industrial operations, since they could already have been established or in the business for quite some time. Security, however, is where many can stumble when integrating the IIoT into their operations. For one thing, many businesses still use legacy systems and processes. Many of these have been in operation for decades and thus remain unaltered, thereby complicating the adoption of new technologies.

Also, the proliferation of smart devices has given rise to security vulnerabilities and the concern of security accountability. IIoT adopters have the de facto responsibility of securing the setup and use of their connected devices, but device manufacturers have the obligation of protecting their consumers when they roll out their products. Manufacturers should be able to ensure the security of the users and provide preventive measures or remediation when security issues arise.

Even more, the need for cybersecurity is brought to the fore as more significant security incidents surface over the years. Hackers gaining access to connected systems do not only mean exposing the business to a major breach, but also mean potentially subjecting operations to a shutdown. To a certain extent, industries and enterprises adopting the IIoT have to plan and operate like technology companies in order to manage both physical and digital components securely.

Adopters are also faced with the challenge of properly integrating industrial operations with IT, where both connection and information need to be secured. Users' data should be processed in accordance with applicable privacy regulations, such as the European Union (EU) General Data Protection Regulation (GDPR). While gathered data plays an important role in generating insights for the devices and infrastructures, it is imperative that personal information be segregated from general log data. Information like personally identifiable information (PII) should be stored in an encrypted database. Storing unencrypted information together with other relevant activity in the cloud could mean businesses running the risk of exposure.

One of the major concerns that have been surrounding the IoT is technology fragmentation, and the IIoT, by extension, isn't exempt from the coexistence of different

standards, protocols, and architectures. The varying use in IIoT systems, for example, of standards and protocols such as Message Queuing Telemetry Transport (MQTT) and Constrained Application Protocol (CoAP) may hinder IIoT systems' interoperability.

What are the risks to IIoT systems?

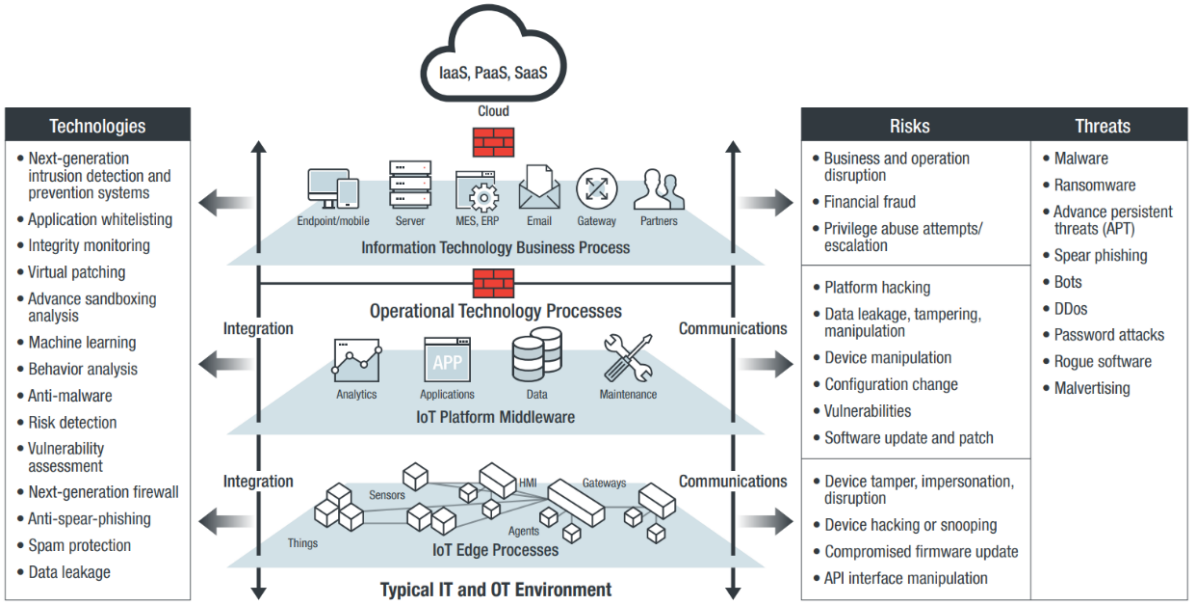
Many security problems associated with the IIoT stem from a lack of basic security measures in place. Security gaps like exposed ports, inadequate authentication practices, and obsolete applications contribute to the emergence of risks. Combine these with having the network directly connected to the internet and more potential risks are invited.

Businesses may have grown familiar with the probable business impact of having IT systems go down because of cybercrime or malware infection. However, the convergence of IT and OT introduces a new significant risk factor: real-world threats that could affect even civilians.

Unsecure IIoT systems can lead to operational disruption and monetary loss, among other considerable consequences. More connected environments mean more security risks, such as:

- Software vulnerabilities that can be exploited to attack systems.
- Publicly searchable internet-connected devices and systems.
- Malicious activities like hacking, targeted attacks, and data breaches.
- System manipulation that can cause operational disruption (e.g., product recalls) or sabotage processes (e.g., production line stoppage).
- System malfunction that can result in damage of devices and physical facilities or injury to operators or people nearby.
- OT systems held for extortion, as compromised through the IT environment.

A notorious example of an OT system compromised through the IT environment is the December 2015 cyberattack against a power grid in Ukraine, where the adversary was able to infect the IT infrastructure to shut down critical systems and disrupt power in thousands of households.



Basic security reference architecture in the new IT/OT environment

How should industries and enterprises go about securing the IIoT?

While pushing for productivity in operations is essential for IIoT systems, security should be regarded as much. Connecting OT to the internet could make businesses more viable, with the help of the many sensors and connected devices at work and the real-time data that they generate. But failing to invest in cybersecurity could undermine the benefits. This is where security by design and embedded security approaches should come in.

Having a security operations center (SOC) is critical in proactively monitoring and defending against the broad range of threats that affect connected environments. This centralized unit allows industries and enterprises to oversee the significant number of alerts that they may encounter and to enable quick response. SOCs are especially beneficial for facilities in need of better visibility and continuous analysis of their security posture. It is the goal of SOC teams to detect security incidents or any anomalous activity and be able to immediately address issues before any compromise could occur. This approach addresses the challenges that could come with legacy systems, low system visibility, and slow response times. With an SOC, alerts will be prioritized and threat correlation will be more optimized to enable enterprises to manage both IT and OT.

However, shifts in the threat landscape as well as industrial infrastructures require organizations to adapt their protection for the new and unknown threats that they may encounter. Adopters of the IIoT could put emphasis on having a dedicated team for tackling security in an OT environment, given that it's a specialized area. Recruiting security experts who can understand different kinds of threats and take quick action in

mitigating the effects of attacks should be top of mind for industries and enterprises if they are to thrive amid the IT/OT convergence.

Having a full stack of protection purposely built into the different layers of IIoT implementations would enable industries and enterprises to securely conduct their operations. These security layers include the device, the network, and the cloud.

The device layer usually comprises the IIoT devices and applications that are brought in from different manufacturers and service providers. IIoT adopters should be able to know how their manufacturers and service providers transmit and store data. And in the event of a security issue, manufacturers and service providers should also be able to actively notify enterprises of what needs to be taken care of.

On the network area, there is the gateway, which gathers data from devices. This is the part where organizations should have next-generation intrusion prevention systems (IPSs) in order for them to monitor and detect potential attacks. The gateway is also where there is usually a control center that issues commands to different devices. The control center is the most critical place where organizations should implement security hardening to ensure protection against malware infection or hackers gaining control of it.

Finally, the cloud is where providers should have security implementations that run server-based protection to mitigate the risk of hackers taking advantage of servers and stored data. This reiterates the concern that organizations are subject to applicable data protection retributions.

Securing IIoT systems therefore requires connected threat defense and end-to-end protection, from the gateway to the endpoint, that are able to provide:

- Regular monitoring and detection in case of malware infection.
- Better threat visibility and early detection of anomalies.
- Proactive prevention of threats and attacks between IT and OT.
- Secure data transfer.
- A next-generation IPS to prevent attacks from exploiting vulnerabilities.
- Server and application protection across the data center and the cloud.