HIVEMQ

Building Industrial IoT Systems in 2024

What's driving and delaying the business impact of IIoT?

Table of Contents

HIVEMQ

The State Of Industrial IoT in 2024

Industrial IoT is fueling improved productivity and efficiency for organizations in manufacturing, transportation and logistics, automotive, and energy worldwide. As technologies advance, more companies are executing IIoT initiatives to minimize downtime, reduce costs, and become more agile to respond to changing market conditions, making IIoT essential to long-term competitiveness.

Digital transformation and deployment of IIoT projects need alignment, ownership, and support to be successful. A staggering **80% of IoT projects fail to scale** due to the complexity of integration and the inability to support scaling systems. If these challenges are not adequately addressed and accounted for at the onset, the implementations are destined to fail.

What can companies expect when implementing an IIoT strategy that can scale to the data demands of the business and prove ROI quickly? HiveMQ partnered with IIoT World on a survey of 350 IIoT professionals to delve into the challenges they are facing, which technologies they are adopting, and how they plan to show the business impact of IIoT in 2024. These are the key themes that emerged.

IIoT has significant business impact
Professionals agree that IIoT can increase productivity, improve Overall Equipment Effectiveness (OEE), and reduce overhead costs.

Stakeholder buy-in is critical
Top challenges to implementing IIoT systems include leadership support, lack of budget and uncertain ROI, and cybersecurity.

If you don't have an IIoT strategy you're falling behind
74% of the companies surveyed have already deployed or are in the process of developing an IIoT strategy.

The time is now to integrate IIoT data for AI and ML
Nearly half of respondents are integrating Machine Learning and AI applications and services into their IIoT strategy.

MQTT continues to lead as the industry-standard protocol
60% of respondents have deployed, plan to deploy, or consider MQTT as their protocol of choice for IIoT systems.

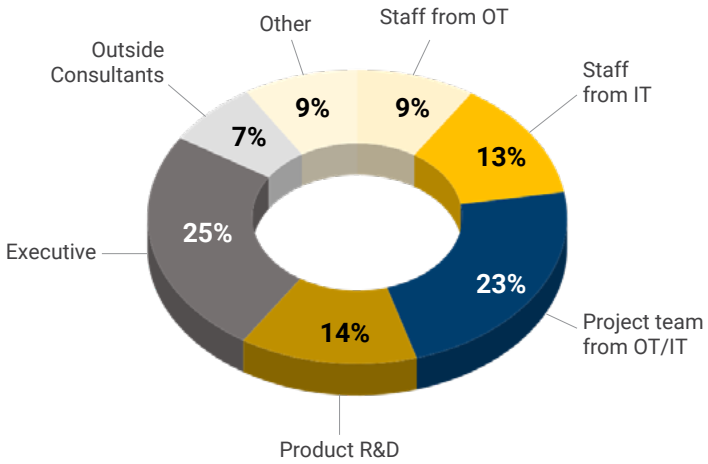
Lack of Alignment and Ownership of the IIoT Strategy

> "People and processes must shift to capture the benefits of the data-driven insights IIoT can generate and maximize the technology's value. This requires the commitment of leadership to ensure that IIoT is not simply an IT or OT initiative but, rather, an organization-wide effort."
>
> *-McKinsey*

The success of any business-wide project starts with alignment and ownership. Determining who should own the IIoT strategy can be a complex decision. Is it the realm of the Executive team, the Operational Technology (OT) team, the Information Technology (IT) team, or a collaborative effort?

The answer is not so straightforward for many organizations. A quarter of survey respondents believed that executive leadership (25%) should own the project while nearly a quarter of respondents (23%) believe that a project team combining both OT and IT expertise should spearhead the IIoT strategy.

Who is leading your IIoT Strategy?



It's no surprise that professionals across industries view the implementation and ownership differently. Several factors come into play when making this choice, ranging from the industry's regulatory environment to the specific business objectives.

Here are some factors that can influence who should own the IIoT strategy:

Business goals and objectives

Align ownership with the primary business goals. If the objective is to improve operational efficiency, it may make sense for the OT team to take the lead. The IT department might play a more significant role if the goal is to leverage IIoT for data-driven decision-making.

Supportive executive leadership

The IIoT strategy may rest with executives, such as the CIO or COO, who oversee both IT and OT. Executive support is critical to success and 38% of survey respondents said leadership vision and management support was a challenge to implementing an IIoT system.

Collaboration between IT and OT

IT is often responsible for connectivity, data management, and analytics, while OT focuses on operations and control systems. In many successful IIoT implementations a cross-functional team or project group is the ideal owner of the strategy.

Regulatory compliance

Industries with strict regulatory requirements, such as healthcare, pharmaceuticals, or utilities, might need to consider compliance a top priority. In such cases, the ownership may be driven by the team responsible for ensuring adherence to industry-specific regulations.

ROI Uncertainty Threatens IIoT Implementations

With clear ownership of the initiative confirmed, the next challenge for implementing an IIoT system is proving ROI. Over a third of respondents (31%) said a key challenge for implementing IIoT systems is a lack of budget and uncertain ROI. What is the return on investment that the company can expect by introducing new technology and processes to the business?

The key to showing ROI for any IIoT initiative is identifying the key KPIs, measuring the baseline before the project starts, and then continuing to measure them incrementally upon deployment. Many teams fail to track the right KPIs and start initiatives to “digitally transform” but without clear and specific metrics in mind to show ROI.

To prove a financial return on the investment for an IIoT system, consider these KPIs:

Overall Equipment Effectiveness

OEE is a metric that assesses the efficiency of manufacturing equipment, and improving OEE can be a win for any IIoT project’s ROI.

Downtime reduction

Measure the reduction in unplanned downtime by monitoring equipment health and predicting maintenance needs.

Asset utilization

Monitor and optimize the utilization of industrial assets such as machinery to ensure they are operating at their maximum capacity.

Energy efficiency

Track and analyze energy consumption to identify opportunities for optimization and cost savings.

Quality improvement

Monitor and improve product quality by using IIoT data to identify and address issues in real time, reducing defects and waste.

Supply chain visibility

Improve visibility into the supply chain by tracking the movement of raw materials, work-in-progress, and finished goods in real time.

Cycle time reduction

Monitor and optimize the time it takes to complete a manufacturing cycle, leading to increased efficiency and market agility.

Customer satisfaction

Measure improvements in customer satisfaction resulting from improved product quality, delivery times, or other benefits facilitated by IIoT.

Accounting for Cybersecurity Risks is a Top Concern

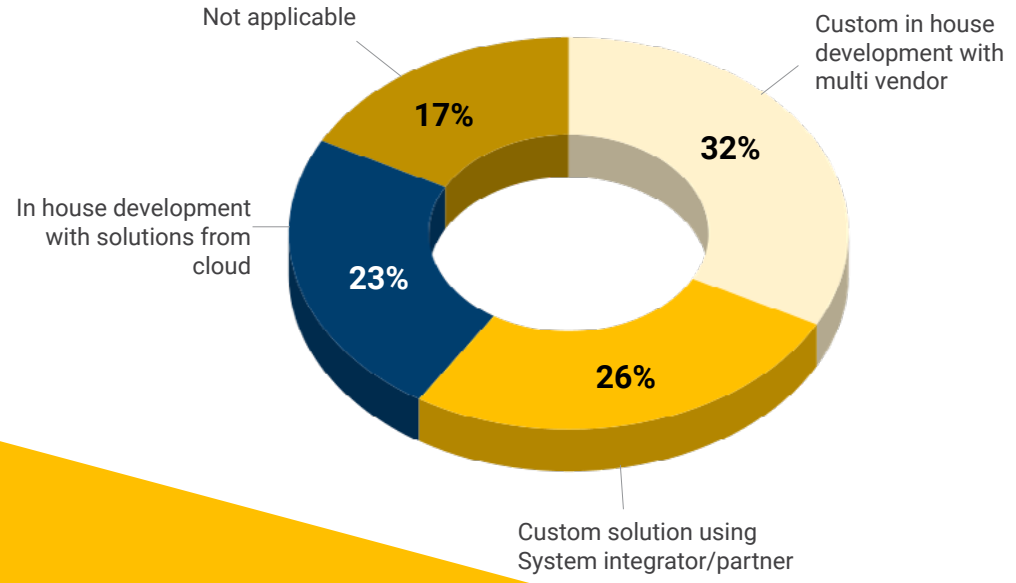
In the IIoT World survey, cybersecurity (35%) was cited as a key challenge for implementing a new IIoT system. Security breaches continue to make headlines, and ensuring enterprise-grade security is paramount to winning customer loyalty and maintaining corporate responsibility. The security risks for IIoT include practices such as device hijacking, data siphoning, data breaches, and device spoofing. There are a few ways to bring the highest security standards to your IIoT strategy and maintain the integrity, confidentiality, and availability of critical industrial systems.

Important features like device authentication and authorization should be employed. Organizations should use vendors with strong authentication mechanisms for devices and users accessing the IIoT network. This includes the use of secure credentials, multi-factor authentication, and proper authorization controls. Data encryption should be used both in transit and at rest to protect sensitive information from interception or unauthorized access. Encryption is particularly important for data transmitted between IoT devices, edge devices, and cloud services.

Any hardware used in IIoT should be secured using hardware security modules (HSM). Regular system security audits should be performed to ensure that system security is up to industry standards, especially in highly regulated industries. Of note, IIoT messaging using MQTT is inherently secure because there are no inbound connections, only clients subscribed to specific topics receive the messages and use TLS encryption.

Consider how you will implement your IIoT strategy as you plan a security approach. Deploying in the cloud, for instance, has different risks than deploying on-premise.

How have your implemented your IIoT strategy?



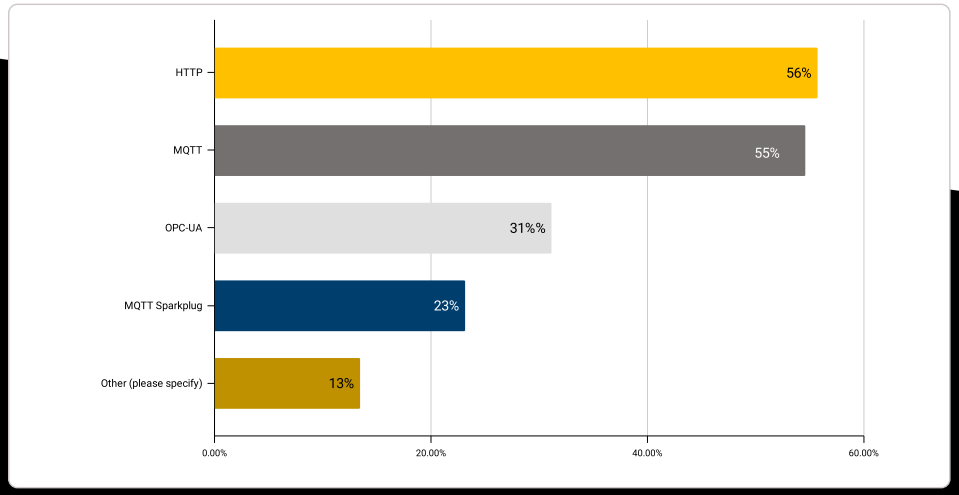
Enabling IIoT with the Ideal Technology Protocol

MQTT continues to rise in popularity as companies seek a lightweight, reliable messaging protocol for device and data communication. MQTT has been identified as a key enabler for IIoT projects and is rapidly complementing machine data frameworks such as OPC-UA and Modbus, while Sparkplug is an up-and-coming data framework.

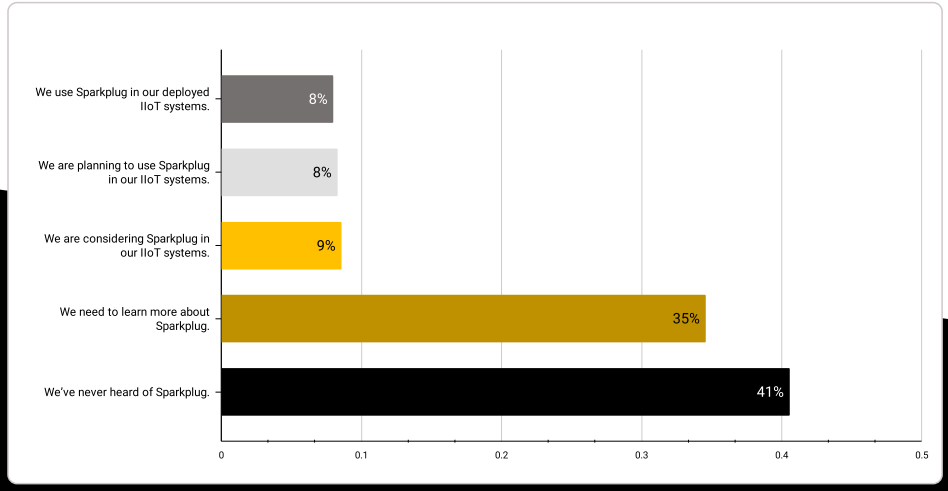
While the technology requirements vary from industry to industry, survey respondents indicated their strong preference for both MQTT and HTTP.

MQTT Sparkplug is still in its infancy but 25% of companies say they have deployed or are looking at using Sparkplug, while 35% say they need to learn more about it. Sparkplug is an open-source software specification for MQTT helping the manufacturing industry to seamlessly integrate data from their applications, sensors, devices, and gateways.

Which of the following data movement tools do you consider essential to fulfill your IIoT strategy?



What best reflects your experience with Sparkplug?



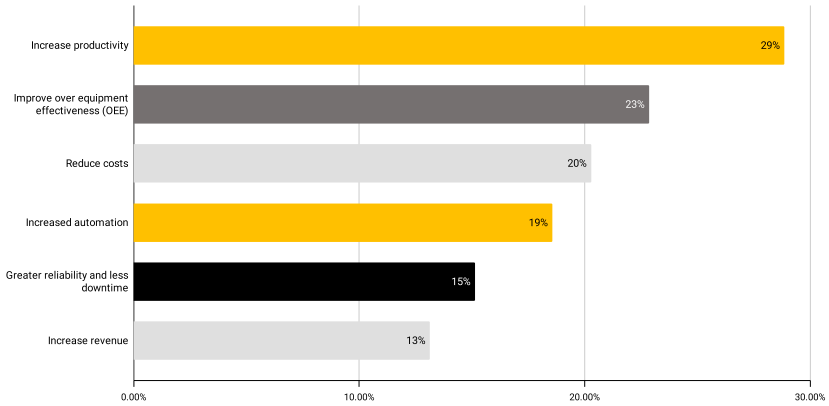
"MQTT has been gaining momentum as the protocol of choice for the last-mile connectivity of OT assets to IT/cloud systems."

- IoT Analytics

No matter the choice of technology, accurate and reliable data plays an important role in the success of the implementation. Data collected from IIoT devices must be useful and trusted for decision-making. Making use of approaches such as **Unified Namespace (UNS)** to create a single source of truth for all data on the Edge and in the Enterprise is important for the success of any IIoT project.

IIoT Investment Pays Off With Efficiency and Productivity Gains

As companies invest in and deploy IIoT projects, they are seeing much-needed improvements and competitive advantages in the form of efficiency and productivity gains. Automating manual tasks, for instance, turns into more time for highly skilled workers to allocate to more strategic tasks. This boost in productivity was the top benefit survey respondents (29%) indicated they expect from an IIoT implementation. A close second to productivity was improved Overall Equipment Effectiveness (OEE) (23%).



What best describes the greatest benefits you expect from implementing IIoT systems?

The continued focus on OEE can help companies learn why machine downtime happens, highlight delayed changeovers or setup times, and bring more visibility to productivity statistics. A company using OEE as a KPI can then optimize processes - improving production on the same equipment, better allocation of resources, and identifying areas of surplus capacity.

OEE and productivity translate into other tangible business impacts as well — in the form of reduced costs and increased revenue. When IIoT is implemented for long-term success, companies can expect the optimization of data connectivity to **save them up to tens of millions of dollars** and **deliver hundreds of millions in revenue**.

To realize these types of benefits and ROI, organizations need to combat the most common IIoT challenges to ensure their deployments are future-proof and battle-tested. Let's dive into some of those challenges.

"Smart factories are set to boost the global economy by $1.5 trillion in five years."

Capgemini Research

Looking Ahead: Long-Term IIoT Success

New IIoT technologies are setting the market up for efficient, optimized, digital factories fueled by data-driven decision-making. After understanding how to overcome common challenges and which protocols to build an IIoT infrastructure on, take a look at the trends taking shape in 2024.

The resurgence of Generative AI (GenAI), an adaptable technology can recommend ways to make production lines more efficient and with less waste. GenAI can even design new parts or products to take a manufacturing business to the next level. By enhancing manufacturing processes, GenAI can reduce downtime, improve output, realize cost savings, and boost end-user satisfaction.

It's likely that **digital twins**, which refers to the digital replication or representation of physical machines and processes in cyberspace, will continue to be implemented at scale. Digital twins can be used for use cases like monitoring and analysis, remote control and optimization, simulation, and scenario planning.

Another trend that will surely be talked about next year is Unified Namespace. The concept of creating a single source of truth for manufacturing data has caught fire and organizations that base their infrastructure on a Unified Namespace plus MQTT are setting themselves up for long-term, future-proof success.

There is no denying the importance of implementing an IIoT system with a lens toward the future. Scalability, reliability, and security will continue to be the tenets of success for any IIoT deployment. Aligning the business to understand what can be accomplished with IIoT, bringing the right team together to steer the ship, and understanding how to achieve and amplify the ROI - all with security at the forefront - will keep IIoT initiatives central to business impact.

This report was written and sponsored by HiveMQ based on the data from an IIoT World Survey. HiveMQ markets an Enterprise MQTT Platform and to avoid influencing the survey results, was not identified as the sponsor of the survey.

About HiveMQ

HiveMQ empowers businesses to transform with the most trusted MQTT platform. Designed to connect, communicate, and control IoT data under real-world stress, the HiveMQ MQTT Platform is the proven enterprise standard for Industry 4.0. Leading brands like Audi, BMW, Liberty Global, Mercedes-Benz, Siemens, and ZF choose HiveMQ to build smarter IIoT projects, modernize factories, and create better customer experiences.

Visit **hivemq.com** to learn more.

HIVEMQ

www.hivemq.com