Remove five barriers to digital success

A guide to progressing IIoT

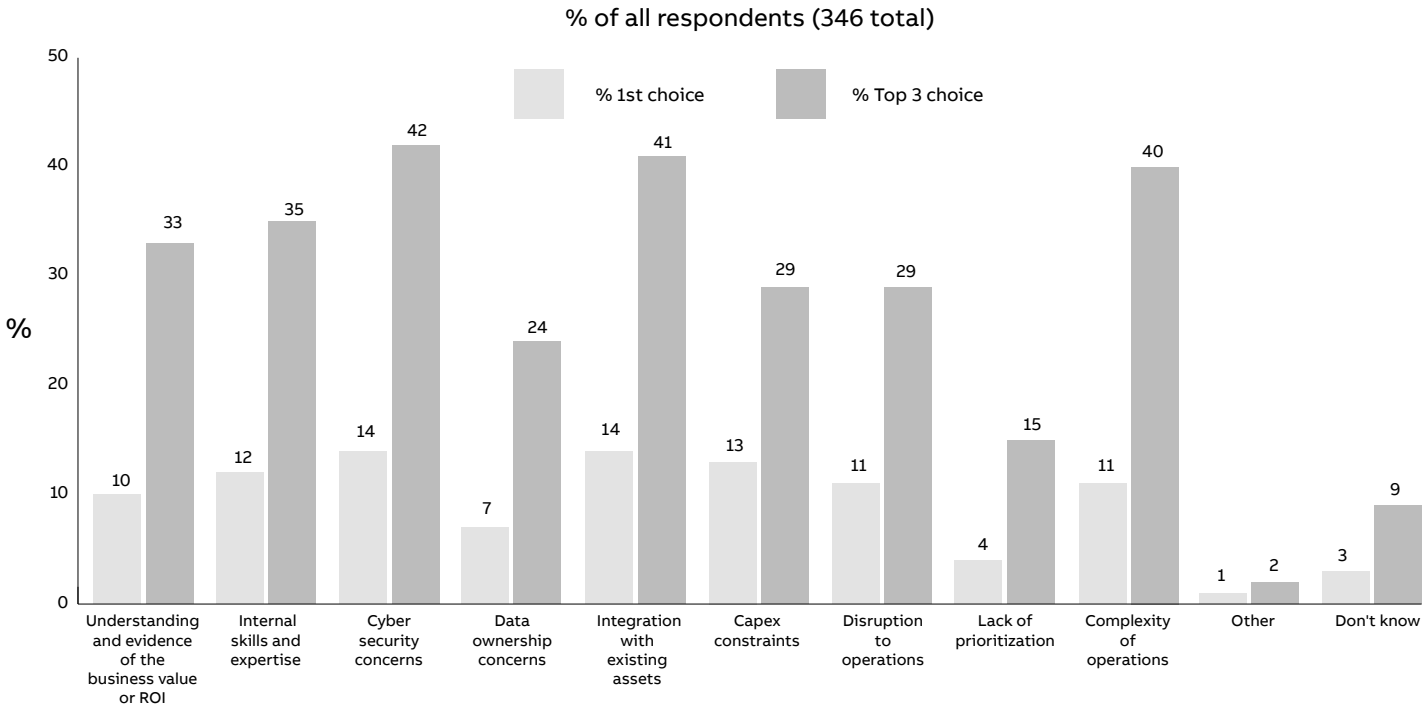
Contents

Introduction

For today's industrial businesses, digital transformation is too important to be held back by doubts, uncertainties or perceived technology challenges. While there are undoubtedly barriers to implementing Industrial Internet of Things (IIoT) technology, as this chart shows, they are far from being insurmountable.

This document will focus on five of the most significant barriers to digitalization, and how to overcome them in order to move forward with confidence in IIoT implementation. It includes facts from ABB research conducted between March and June 2023 with industrial decision makers across seven markets and nine industries, which you can also find in our whitepaper: **'See the full potential of digital, faster'.**

Barriers to Industrial IoT implementation for electrical systems



Barrier 1: Cyber security

"Attackers are getting smarter by the day. I can't afford to digitalize and then be compromised."

42% **say cyber security concerns are a barrier to IIoT implementation for electrical systems***

Safeguarding data across your IIoT infrastructure is essential in order to build future industrial systems based on the Internet of Things. However, benefiting from the data-driven insights IIoT offers, while protecting your operation, can seem confusing. That doesn't mean your organization should miss out on the benefits of IIoT simply because of a fear of connecting production systems to the company network and the internet. Applying cyber security to industrial systems isn't that complicated – or different to implementing security in a standard IT system – if certain steps are followed.

Your organization should employ a combination of firewalls, encryption, multi-factor authentication, and regular security audits to create a strong defense against cyber-attacks.

Human error remains one of the most significant vulnerabilities in data security. So ensuring that all employees are aware of data protection protocols and receive regular training on best practices will help minimize the risk of data breaches caused by inadvertent actions.

*Percentage of respondents who selected this option as a top 3 choice.

In addition there are four practical steps you can take to implement cyber security in your processes and operations, so you can be confident of taking advantage of the benefits big data offers.

01 Know your system

A candid assessment of your network system is necessary to understand the overall scope of your cyber security needs. This can be done by answering questions like: What are you protecting? How is the system architected? Does that architecture support strong cyber security? What assets do you have in the system? And what is the weakest link in the chain? If you don't know all these things, it is difficult to know where to start. Answering these questions in the form of an effective assessment should follow these three steps:

- List all cyber assets in your system. Cyber assets include any device connected to the industrial network which is used by the Digital Security Controls (DCS) system. Most commonly, devices are connected to a network using an Ethernet connection, but don't forget about other communication links between devices in the overall system since these can also be used in an attack. Creating this inventory list can be hard work, so look for tools and solutions that can be used to reduce the manual effort.

- Update system network drawings and add devices to a diagram. This is a critical step as it shows how devices are connected, and how they interact and communicate with each other.

- Perform a risk assessment. This will identify and prioritize the parts of the system that could cause the most harm, either financially or to health and safety, if they are attacked. The risk assessment process forces you to focus on each device and function to answer two critical questions: How likely is it that this device/function may be subject to a cyber incident? And, what is the impact of that incident as far as scale and consequences are concerned? These two elements, which you can call 'likelihood' and 'impact', equate to your total risk.

At this point you will have a good picture of which devices are in your system, how they are connected, where the risks are, and which risks are the most serious. Equipped with this knowledge, you can start implementing various cyber security controls, using the risk assessment as guidance on how to best prioritize your resources and budget. If you don't feel confident to perform all three steps, a service partner can provide the necessary support.

02 Configure a backup solution

Once you have assessed your system or systems, your next step must be to implement and configure a backup solution. A good backup is your last line of defense and ensures that the investment made in your Digital Security Controls (DSC) system is protected. In case of a hardware or software incident or failure, you can easily restore the full DCS system, or parts of it, and resume production as quickly as possible.

To determine backup setup, the backup rotation scheme and the cost of the system, you need to consider a business continuation plan. This defines how much data you can afford to lose (also known as RPO: Recovery Point Objective) and how quickly after a disaster you must be back in production (known as RTO: Recovery Time Objective). Once again, implementing these technicalities could be outsourced to a competent partner.

03 Put basic security controls in place

Security controls, such as protection and security updates, actively work to protect your system. The most common controls include:

- Ensuring all Windows computers are updated with the most recent, vendor-approved security updates to minimize vulnerabilities.
- Ensuring all Windows computers have malware protection that is frequently updated to keep the system secure by detecting and defending against the latest viruses.
- Ensuring that if things do go wrong, you have reliable backups to allow quick restoration of your system in order to resume production.

04 Provide training and control access

As mentioned, human error is an important vulnerability in data security, and will be targeted as such. Training and access control can significantly reduce the likelihood of being infected with ransomware, phishing or viruses, and should follow some key principles:

- Everyone who can come into contact with your system, or any part of it, should know what to do and what not to do. This limits the risk of malware entering the system, as well as accidental disruption due to carelessness.
- Access control should be understood by those who maintain and use it, and everyone responsible should know what to do in the event of an incident.
- Different access should be applied to different environments, such as multi-factor authentication (MFA) for cloud systems, password authentication and role-based access for OT networks, and physical access control where the OT network is housed.

Barrier 2: Integration

"Integrating all our data and solutions is hard enough when we do pilots, let alone when we scale."

41% named integration with existing assets as a barrier to IIoT implementation*

To benefit from IIoT, both your Information Technology (IT) and Operational Technology (OT) must be brought together. This requires horizontal integration (networking between machines to allow production data to be used) and vertical integration (connecting devices such as sensors to systems, to deliver business insights). In addition, IIoT vendors play an important role in helping to ensure effective integration in the wider ecosystem of solutions.

*Percentage of respondents who selected this option as a top 3 choice.

This means there are three essentials to consider before making any IIoT investment:

01 Integration on the IT side

- Integration on the IT side should focus on providing real-time communication with the enterprise's assets while retaining the ability to scale, maintain and secure the infrastructure.
- Organizations should ensure standard interfaces (such as open APIs) are used for data exchange, rather than incompatible protocols or proprietary ecosystems. Open APIs ensures standardized data exchange from cloud-to-cloud, or for data lake integration. They also allow multiple software companies to develop new solutions which will work with your IIoT investments.

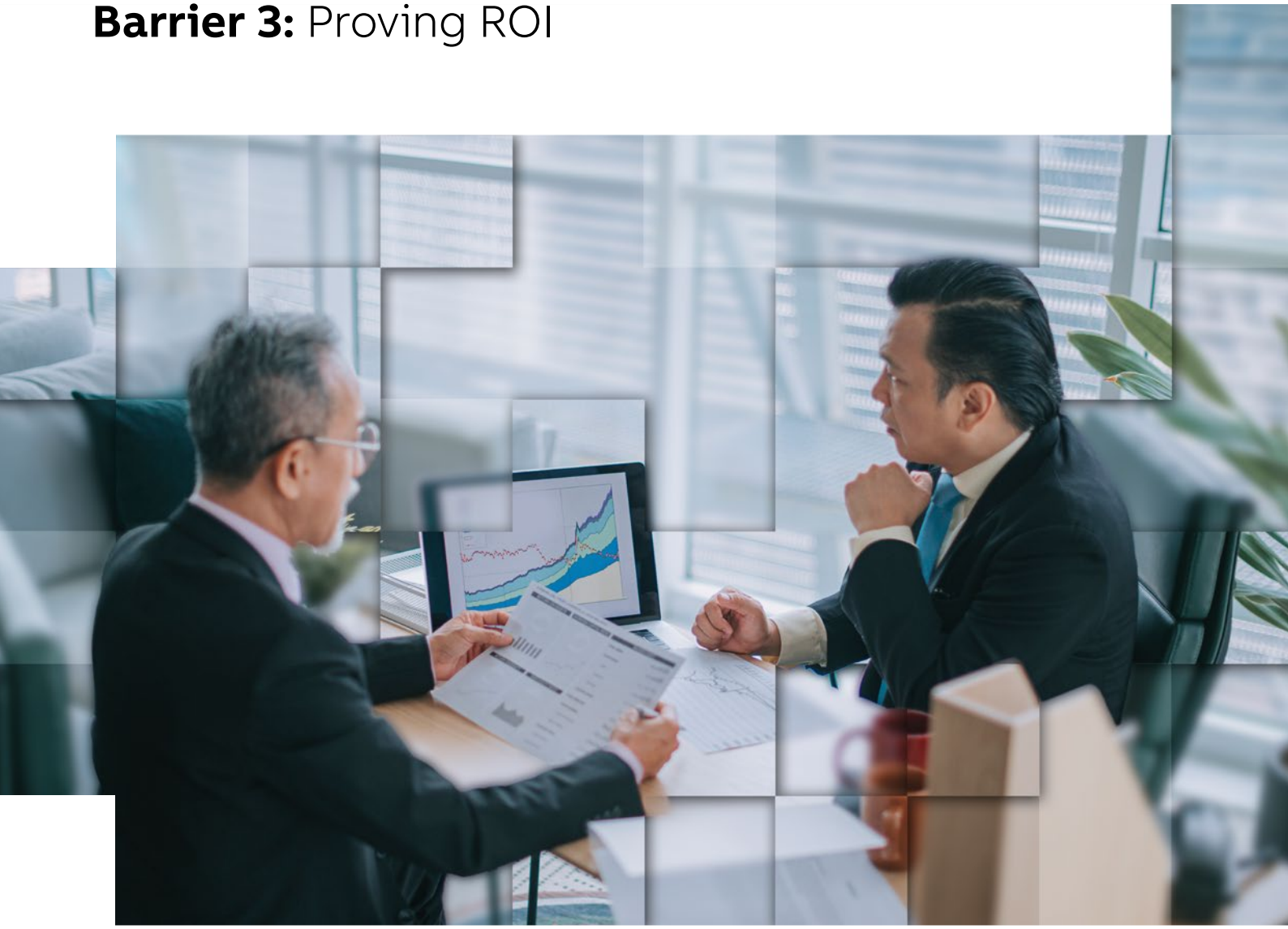
02 Integration on the OT side

- The use of international communication standards and industrial communication protocols – specifically International Data Transfer Agreement (IDTA) data container standards – will guarantee barrier-free data logistics between systems and devices.
- The integration hub should be robust and support the multiple protocols and file formats mentioned above and ensure extreme availability, since it is the foundation to drive better use of data.

03 Integration on the partner side

- Your IIoT vendors should be actively collaborating with a wide ecosystem of other experts to deliver ready-to-go, off-the-shelf solutions for highly complex and multi-layered industrial applications.
- Partners should recognize that the key to integrating existing IT and OT infrastructures is not necessarily to replace them but to establish connectors that allow data to be truly accessed, even if that is in parallel to existing solutions.
- Even if it is possible to exchange data between IT/OT systems, expert knowledge is required to interpret the data. Getting all involved parties around the table for comprehensive decision-making is crucial.
- Partners should share a vision with your organization of digital transformation that unites people, systems and equipment through secure OT/IT integration that ensures continued commercial success.

Barrier 3: Proving ROI



"I struggle to make the case for IIoT investment, because I can't prove ROI."

33% say evidence of business value or ROI is a barrier to IIoT implementation*

Like any business project, calculating Return on Investment (ROI) – the ratio between profit and the cost of the investment – for an IIoT project is essential. The costs incurred and the benefits gained from implementing an IIoT solution must balance in favor of the organization.

However, without clear data showing how the digital transformation process increases profits, it will be difficult for IIoT champions within the organization to secure funds since they will inevitably face resistance from the board. The benefits of IIoT such as increased efficiency, reduced maintenance costs, and lower unplanned labor costs must therefore be translated into a solid value proposition that demonstrates ROI. **There are three steps to achieving this:**

*Percentage of respondents who selected this option as a top 3 choice.

01

Identify all costs

These will include the direct investment costs for technology (e.g. sensor and device hardware, applications, software licenses, cloud subscriptions); costs associated with IIoT implementation (e.g. connectivity, installation, new tools and other expenses); plus ongoing costs such as cybersecurity, skills development, training, and costs related to managing organizational change.

02

Estimate the return from IIoT

Consider the cost savings that can be achieved from the project through the use of monitoring and diagnostic solutions integrated in electrical switchgear. The direct business cost of unplanned outages is typically $125,000 per hour*. You can calculate this figure for your own business by analyzing downtime, wasted production, purchase of spare parts and the wider implications of downtime for the operation. You can then contrast this figure with cost reductions in the future, based on the ability of an IIoT solution to improve uptime, reduce common causes of failure, lower the use of spare parts, and streamline maintenance time and frequency. In fact, predictive maintenance can decrease maintenance time and frequency by 30%, helping you to reduce total cost of ownership by 40% and giving a payback period of around 3 years.

03

Prepare your business case

Your business case should present the costs, benefits and risks associated with the investment. It should answer questions such as: What is our business need and how does IIoT fit strategically? What is the cost-benefit analysis and how does IIoT deliver value for money? Is there capacity and capability to implement IIoT within the organization? If not, how can we financially benefit from working with service partners?

Paint a picture of the end goal for stakeholders: a robust business case should provide decision-makers with assurance that IIoT project provides value for money, risks have been considered and mitigated, and that significant business value can be gained. In this it can start with the bigger picture: the full benefits you'd get from a fully mature solution. Then, step backwards to your proposed project.

*** ABB survey based on information provided by third parties in response to a questionnaire, rather than reviewing actual accounting records.**

Barrier 4: Skills

"We don't have the expertise needed to digitalize safely and confidently."

35% say internal skills expertise is a barrier to IIoT implementation*

To prepare for the jobs of tomorrow, companies must develop the digital skills necessary to support advanced technology. This means your organization may have to re-think its education and training processes, and in doing so, consider two important gaps:

*Percentage of respondents who selected this option as a top 3 choice.

The OT and IT gap

Spanning the gap between operational technology (OT) and information technology (IT) skills and capabilities is a key challenge. Historically, these two functions have run on different rails. IT has supported enterprise applications and office workers through an open architecture model (with systems such as ERP, CRM and Business Intelligence), while OT has supported industrial and environmental monitoring and control through a closed, proprietary architectural model (with systems such as MES and SCADA).

This means significant differences exist between OT and IT teams both in their approach and skillsets. To fill this gap and embrace all of the benefits of the industrial transformation, it's important to bring these two worlds together, which can only be done through an exchange of skills and by acquiring new skills.

The employee skills gap

Companies often feel that they do not have the required in-house skills to make use of digital technologies. This is due in part to the widening skills gap, caused by experienced personnel retiring and fewer professionals entering the field, particularly with new digital skills.

Redefining workers' roles and retaining human expertise digitally can be a challenge, but accessing both internal and external training expertise is a huge enabler for success.

It should be noted that as skills requirements change, many workers will be strongly motivated to acquire new skills and embrace the transition. This is an opportunity to not only train technical skills but also a range of soft skills such as problem solving, management, and analytical thinking.

Effective training

The easiest way to gain new IIoT skills and close the skills gap is through continuous learning and training across products and systems, service and maintenance.

To shorten the learning curve, training can be provided by a training specialist or by leveraging the skills and expertise of a supplier. Many manufacturers and technology providers offer specific training paths, webinars and programs to train end user and partners in digital technologies and how to improve the efficiency of a company's operations. E-learning tools are also valuable, since they give your employees access to a wide range of learning modules online so they can learn at their own pace, anytime and anywhere.

Typically, when you are dealing with a third party provider, you can also request specific training services for the commissioning phase of a new solution in order to train users on the new technologies.

To avoid a future skills shortage, training should also focus on passing on skills and knowledge to trainees outside of the learning environment, which is vitally important for both productivity and safety in the workplace.

What additional skills are needed?

Some core expertise is needed to maximize the use of IIoT, and where those skills are not available internally, hiring the following roles will help to ensure long-term digital success:

Data scientists and data architects

Solution architects and developers

UX designers and cyber security specialists

Artificial Intelligence experts

Depending where your organization is on the journey to digital transformation, outsourcing or forging strong technology partnerships to fulfil some, or all of these roles, can prove to be the most cost-effective option.

For example, if you lack expertise on analytics, you could consider outsourcing to a data science consultancy; if you are upgrading your digital switchgear capabilities, you can explore partnerships with companies specializing in electrical automation; or if IIoT involves significant organizational change, you can employ the services of a change management leader.

Barrier 5: Complexity

"We don't want to risk overcomplicating our crucial systems."

40% **say complexity of operation is a barrier to IIoT implementation***

Many operational experts think of digitalization as an added layer of technical complexity and risk that must be tackled, particularly when it comes to fundamental electrical systems. This can prevent companies moving quickly and proactively in IIoT.

To break down this barrier, it helps to examine what's meant by 'complexity' – since it can either be a perception of technical complexity (related to the company's digital landscape) or one of operational complexity (related to the use of new technology and IIoT solutions).

In the case of technical complexity, this scenario only arises if it is allowed to, typically as a result of businesses only digitalizing assets and components when they fail. While this can seem like 'buying time' and minimizing costs, industrial companies can end up with an overly complex system (and more downtime) further down the road – and also have trouble scaling, since it's now more difficult to plan and coordinate IIoT choices effectively. In short, concerns over complexity can actually lead to overly-complex systems.

In the case of operational complexity, companies must take a view that innovation in the organization is an essential requirement to remain competitive; and embrace a vision where deploying automation through AI and IIoT can effectively reduce complexity, not add to it.

*Percentage of respondents who selected this option as a top 3 choice.

How to reduce technical complexity

Proactive rather than reactive digitalization means replacing digital assets with carefully planned deployments, ahead of time, based on a multi-year roadmap which steers you towards digital transformation. Whether the deployments are modest or huge does not matter, so long as they are proactive.

This approach will not only minimize disruption, it will avoid a sprawl of different technologies and operational processes. Instead, you'll have a clear roadmap to guide purchasing decisions (without fear of complexity); a clear plan of how to harness analytics; and a more streamlined IIoT solution. In terms of allocating resources, you can also plan to have the right expertise on tap for implementations and scaling projects at the right time (especially if external experts are required to design the simplest possible digital ecosystem).

How to view operational complexity

Even if it feels like a complex technical challenge to implement digital systems, it's important to remember that once digitalization is in place it can dramatically reduce complexity in your operations. For example, digitalization enables predictive maintenance and smart field management. Prior to digitalization, you would have had to juggle the complexities of different assets, maintenance requirements and field-service schedules (plus diagnosing issues manually, with the associated labor costs). Post-digitalization, you can work out the best way forward automatically, which dramatically reduces operational complexity.

See the full potential of digital, faster

Want to find out more? Drawing on research from more than 300 industrial decision makers across the globe, our **whitepaper** reveals how IIoT investments are being made and the approaches companies are taking. It is designed to help you understand where you are today and guide you forward in implementing IIoT at scale.

You can also contact ABB for more insights and support on IIoT adoption and your journey to digitalization:

Visit global.abb for more information.