

# The Fourth Industrial Revolution: Technology Alliances Lead the Charge

Technology companies are coming together to enable the smart factory – and launching the Fourth Industrial Revolution



# Contents

## 3. The Fourth Industrial Revolution

Inside the smart factory

IIoT challenges and ecosystem solutions

## 7. Interoperability and Standardization

Customised solutions

Cognitive gateways

## 11. Security and Scalability

Distributed analytics

An eye on the future

Security considerations

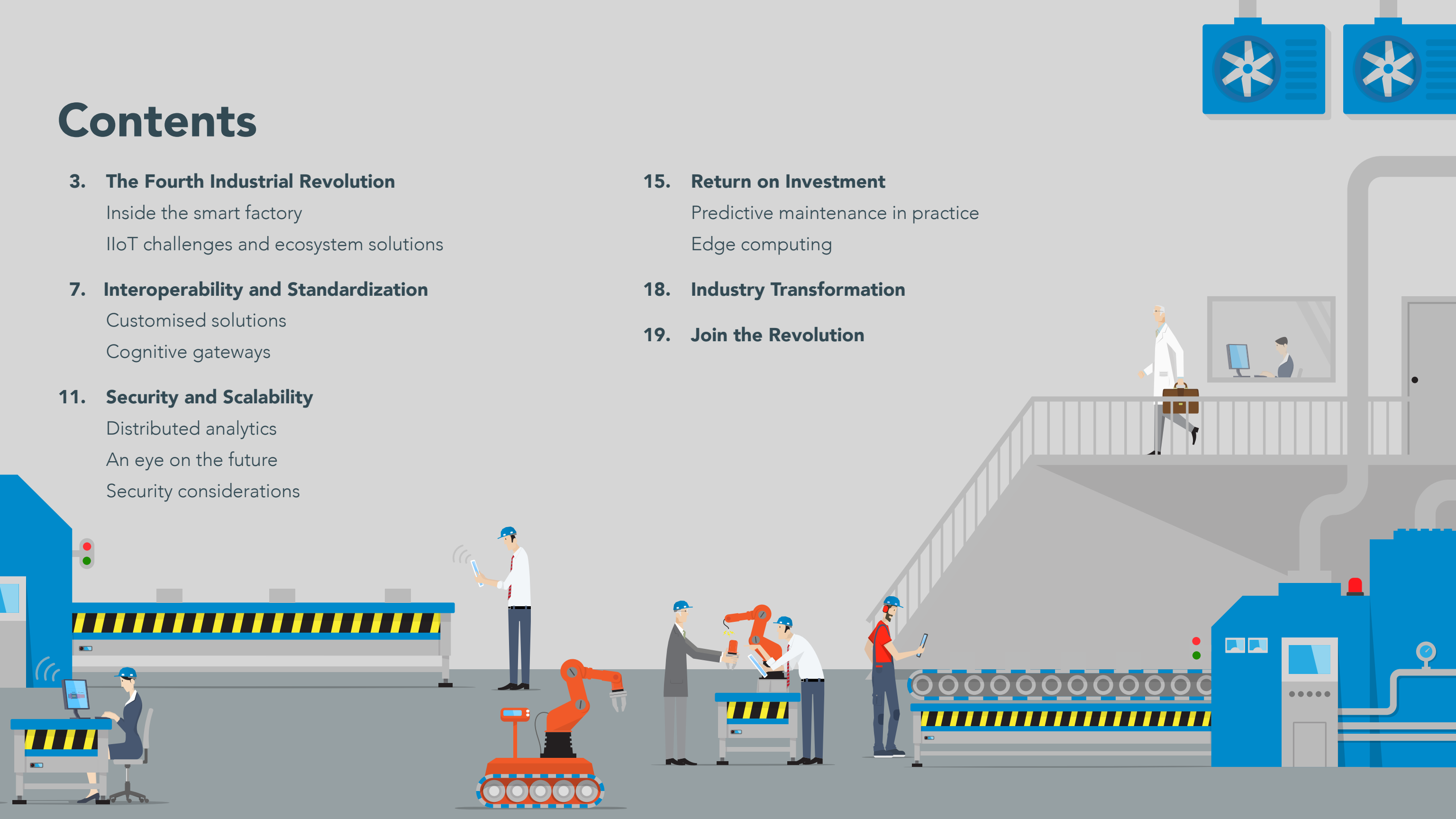
## 15. Return on Investment

Predictive maintenance in practice

Edge computing

## 18. Industry Transformation

## 19. Join the Revolution



# The Fourth Industrial Revolution

The Fourth Industrial Revolution is changing the very concept of manufacturing. Within the smart factory, software-defined automation allows manufacturers to link all stages of the value chain, rapidly adapt to changing markets, and create highly personalised products on a mass scale. These machines communicate their health and status in real time, increasing efficiency and throughput and minimizing downtime.

The opportunities presented by this revolution are incredible. According to McKinsey, the economic impact of smart factories could reach up to \$2.3 trillion per year by 2025.


At the heart of the Fourth Industrial Revolution is the Internet of Things (IoT), which uses digital technology to connect sensors, actuators, and machines to each other and to factory workers. The IoT enables a broad swath of transformational opportunities, including open-standards-based automation solutions, IT and operational technology (OT) convergence, and vastly enhanced business intelligence.

These opportunities flow from the IoT's ability to handle enormous variety, velocity and volumes of data. Many

manufacturers are already feeling the benefits of this access to industrial IoT (IIoT) data. In an Economist Intelligence Unit study of senior factory executives, 86% reported major increases in shop floor data collection over the past two years, and two-thirds said data insights have led to annual quality and efficiency savings of 10% or more.

But all of these advances are dependent upon collaboration – no single organisation can deliver the benefits of IIoT alone. That is why computing juggernaut Intel has partnered with technology leaders like ADLINK, Dell, IBM, PrismTech (an ADLINK company), and SAS. Together these companies are powering smart factories with solutions that generate value from industrial data.

This ebook examines the challenges manufacturers face as the Fourth Industrial Revolution comes to fruition. It looks at the huge business opportunities that smart factories present and the technologies that are enabling them. And it provides examples of how the collaborations between Intel, ADLINK, Dell, IBM, PrismTech, and SAS deliver transformational solutions manufacturers can use today to unlock the value of the IIoT.



**“The economic impact of smart factories could reach up to \$2.3 TRILLION per year by 2025”**

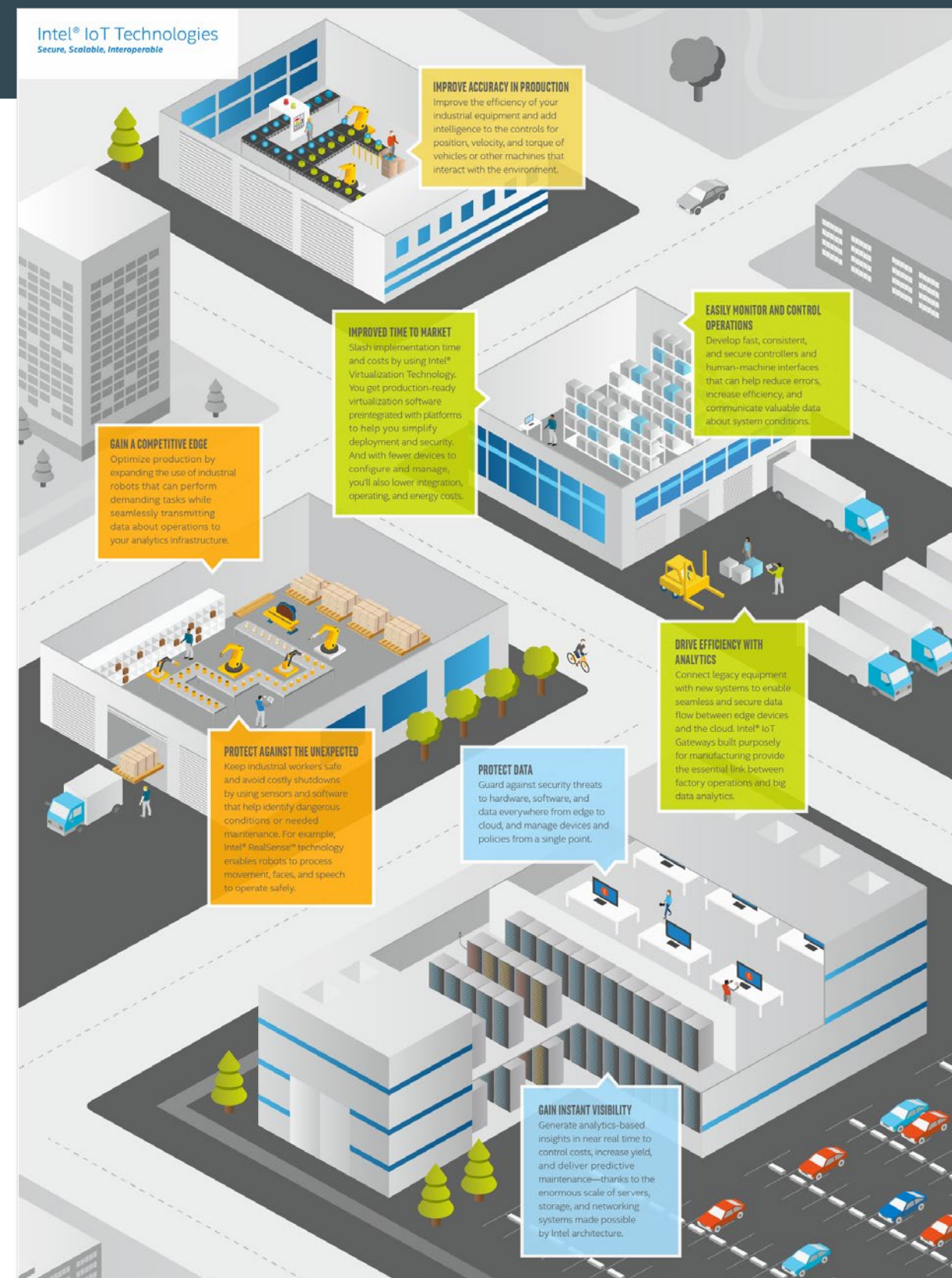


# Inside the Smart Factory

Every worker, tool, machine, and widget on a factory floor holds a wealth of information that could improve operations. With the IIoT, manufacturers can set that data free. They can transform these huge data sets into insights that reduce downtime, increase output, improve asset utilisation, and enable new revenue streams.

To support this transformation, the IIoT collects and analyses data at multiple levels. It all starts with edge devices, the IoT end points that sense and control their environment. Gateway devices then aggregate data from the edge devices and present it to the cloud, which provides elasticity as the means to store data and perform analytics.

In the graph to the right, at the top are management and monitoring solutions across all levels of the ecosystem. At the bottom are the technologies that enable development, test, and other critical capabilities, such as end-to-end security for the data and control planes.





# IIoT Challenges and Ecosystem Solutions

Manufacturers compete in a marketplace that has grown increasingly global, with fast-changing requirements and ever-greater demands for profitability. To keep pace, companies need to improve their processes through better visibility into their production status, equipment condition and other vital facets of operation.

The IIoT is already providing a compelling answer to this need. The market for the IIoT was valued at \$94 billion in 2014 and is expected to reach \$151 billion by 2020, a CAGR of 8.03% between 2015 and 2020, according to a research report by MarketsandMarkets.

This rapid growth represents huge opportunities for the industrial sector, but it is also triggering an unprecedented spike in data volumes. Manufacturers face numerous challenges in not only capitalising on the value of smart factories, but also dealing with issues such as interoperability, standardisation, scalability, and security.







On the standards front, many industrial devices are based on inflexible, fixed-function proprietary designs that use non-standard communications protocols. These industrial settings are held back by silos of data and islands of sensors and machines. Many companies have custom-built software that limits communication within the organisation, and complicates software updates and maintenance.

This is just one factor that makes it difficult to scale. Clear return on investment (ROI) on technology and solutions requires infrastructure and capabilities that can scale as manufacturing operations become increasingly complex. Given their attributes of scaling and elasticity, the cloud and standardized IoT gateways designed to connect sensors to the cloud are integral to the IIoT. As connected devices and data grows, the ability to scale with gateways and expand storage and networking assets, as well as compute resources, becomes a key enabler for the development of IIoT systems.

And of course security cannot be overlooked. Protecting industrial environments and critical infrastructure from the threat of cyber attacks is a challenge that keeps CIOs around the world up at night. While the IIoT presents a plethora of new opportunities for manufacturers, having more things connected to the internet and a diversity of equipment in smart factories amounts to a complex environment that requires a multi-layered security approach. Companies must reduce platform

vulnerabilities, protect data and incorporate device and network security intelligence.

Overcoming the challenges of smart factories will only be achieved through collaboration between industry leaders like the ones forged by Intel, ADLINK, Dell, IBM, PrismTech, and SAS where each provides best-in-class technologies and expertise. Such partnerships enable development of solutions that maximise smart factory benefits and investment, while minimising complexity and risk.

These partners are also participating in broader industry efforts around open-standards-based industrial solutions that promote easy connectivity and interoperability

---

**“IIoT was valued at \$94bn in 2014 and is expected to reach \$151bn by 2020”**

---

between devices. Efforts to make the IoT more open and cohesive have led to the creation of consortia such as the Industrial Internet Consortium (IIC) and Open Interconnect Consortium (OIC), promoting a standards-based and inclusive development environment. Manufacturers that leverage the public APIs and open standards from these groups will achieve greater success in the long run.

# Interoperability and Standardisation

## An ADLINK Perspective

While in some cases smart factories can be built new, for the most part manufacturers must retrofit existing facilities. Today's factories are full of legacy machines and sensors that are not connected, managed or secured. As a result, a lot of useful data remains inaccessible and locked away. To transform these facilities into smart factories, manufacturers must introduce connectivity into these older processes. This leads to a critical question: how can manufacturers connect their processes without the significant cost of replacing existing infrastructure?

---

### **“IoT gateways allow manufacturers to analyse real-time on the factory floor”**

---

Intel, ADLINK, PrismTech, and IBM have teamed up to solve these issues with standardized intelligent IoT gateways pre-integrated with business analytics software. These bolt-on devices enable companies to seamlessly interconnect industrial devices and secure data flow between equipment and the cloud without replacing existing infrastructure.

Designed with native intelligence, these gateways perform edge computing, allowing manufacturers to collect and analyse real-time and trended data on the factory floor to optimise factory equipment for power efficiency, performance and operational life. At the same time, these IoT gateways migrate collected edge data to the cloud, enabling higher-level analysis on IBM's leading big data analytics platform, PMQ.

Intelligent IoT gateways also perform a gatekeeper function, ensuring the transmission of data desired only for enterprise-class analytics to the cloud. This data is typically used for higher-level purposes such as monitoring performance over time or other insights, while day-to-day monitoring functions and intelligence-building can stay at the edge. Enabling such selectivity significantly reduces the cost of transporting, storing and processing data in the cloud, and ensures data security by only letting past the firewall what is necessary.

To ensure scalability and security, the ruggedized industrial gateways from companies like ADLINK use Intel's standards-based architecture and built-in security features. These features ensure the consistency and performance smart factories need.



### **5 benefits of intelligent IoT gateways**

- 1** Automated discovery and provisioning of edge devices to ease deployment
- 2** Protocol abstraction to increase interoperability
- 3** Fast, closed-loop response to improve operations
- 4** Decreased network traffic and cloud costs
- 5** World-class security to safeguard unprotected edge devices



# Customised Solutions

Predictive maintenance is one of the main use cases for the Intel-based solution. In this scenario, the solution collects equipment data and analyses it with sophisticated algorithms. Using historical performance as a guide, the software forecasts how monitored equipment and the production line as a whole will behave and offers insight into when to perform maintenance or replacement to reduce downtime and optimize yield and quality.

---

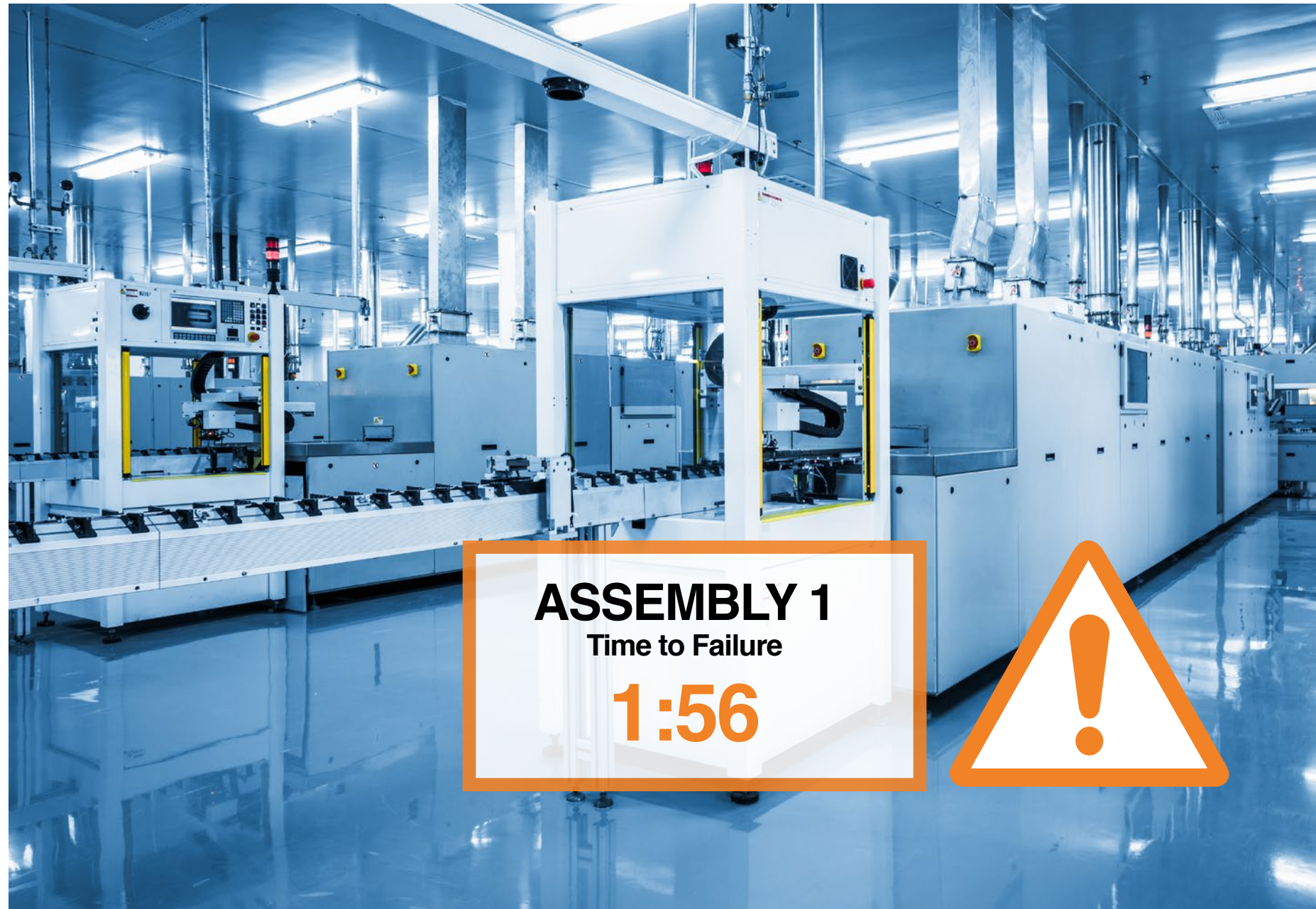
**“Not all IoT predictive analytics solutions are created equal”**

---

But with the many variables that make every factory different, the challenge is understanding how to implement the technology. Predictive maintenance must be customised for each facility, which involves a range of decisions about everything from how data should be gathered to where it should be analysed – in the cloud or at the edge of the network. Making these choices can be difficult because IoT solutions require expertise in both IT and shop-floor OT – and these two disciplines historically have had little in common.







To overcome these challenges, Intel, ADLINK, PrismTech, and IBM combined their respective expertise in number crunching, big data and industrial automation. The result is an all-in-one predictive maintenance solution that incorporates factory-optimised hardware, secure data distribution and advanced analytics. Manufacturers that deploy such a solution can expect improved product quality, increased yield and productivity, decreased downtime and costs, and faster, better-informed decision making.

Not all IoT predictive analytics solutions are created equal. Each must be customised in order to meet the exact needs of each individual facility, and this adds a layer of complexity that can make it difficult to select the right solution. Those that involve several market leaders working together are likely to be more rounded solutions.

The solution from Intel, ADLINK, PrismTech, and IBM is designed from the ground up for factory environments and is customisable to each application. Providing an excellent example of how predictive analytics is implemented, the solution can predict asset failure or quality issues. And organisations can integrate data into back-end systems for further analysis and business improvements.



# Cognitive Gateways

At the centre of the solution is ADLINK's cognitive gateway. Optimized for OT environments, these gateways gather data from sensors in the factory and perform on-the-spot analytics.

PrismTech's Vortex data distribution service makes it easy to connect and integrate these gateways and new devices into the solution. And IBM PMQ software provides the predictive model for analytics at the edge. On the server side, an ADLINK industrial appliance is preconfigured to support data capture, visualisation, scoring model updates, and results deployment. The scoring engine is developed using a software modeller, which is part of the IBM PMQ platform.

With its sophisticated machine learning capabilities, the complete Vortex Edge PMQ system provides stable, accurate, secure and fast analytics in the most extreme environments.



[click to view ADLINK case study video](#)



# Security and Scalability

## An SAS Perspective

Scalability is one of the key requirements for an IIoT solution. Data and computing requirements tend to expand over time, so manufacturers should look for an analytics architecture that can scale and can distribute the analytics load between the edge and the cloud. But setting up distributed analytics utilising edge and cloud resources often presents one of the biggest

---

**“Businesses need to assume  
all industrial systems are  
vulnerable to attack”**

---

hurdles for new IIoT efforts. For this reason, it's important to evaluate analytics technologies as much for their ease of deployment and ability to minimise project risk as for the sophistication of their insight tools.

Security and manageability are also essential to all connected systems. Many industrial control systems have

historically been perceived as secure because they were separate from IT networks and the internet – a division often referred to as an “air gap”. Businesses need to recognize this as the myth it is and assume that all industrial systems are vulnerable to attack.

The key is to be proactive in protecting all systems by implementing enterprise-class security across all the data gathering, communications, and analytics components.

At the same time, to avoid costly manual maintenance, IIoT implementations must provide a centralized environment to manage all IIoT devices.

Intel and SAS have taken all these requirements in mind and worked together to provide the highest levels of security and scalability, starting with the gateway and extending into the cloud. The resulting solution – SAS Analytics for IoT – combines SAS's analytics expertise with Intel's leadership in information architecture to create solutions that cover the full spectrum of IIoT requirements and turn raw data into valuable insights.



# Distributed Analytics

SAS Analytics for IoT delivers a full suite of analytics capabilities, end-to-end security, and integration with storage platforms like Hadoop. The result is a full-fledged IIoT solution designed for easy implementation.

Using Intel's scalable, secure processing architecture, SAS can deploy its best-in-class analytics expertise across a customer's infrastructure, from gateway devices at the edge all the way to powerful servers in the cloud. This distributed analytics capability enables manufacturers to find competitive advantages across their operations.

At the edge, SAS's streaming analytics allows factory equipment and worker to respond quickly to time-sensitive data. In the cloud, manufacturers can harness machine learning and deep analytics for big picture business insights. What's more, the unified architecture allows manufacturers to make continuous improvements across all domains.





# An Eye on the Future

Because IIoT continues to evolve, industrial organizations should regularly assess their use cases and analytics performance, and update these areas as new capabilities and opportunities arise. At the same time, they should reexamine existing deployments to ensure that analytics continues to achieve use-case goals.

---

**“Intel and SAS worked together to provide the highest levels of protection and manageability”**

---

Experience has shown that chasing the biggest, most impressive use case in the IIoT often results in failure. Many companies do better by taking advantage of the expertise of established leaders in the field, such as Intel and SAS, and starting with smaller steps, such as quickly deployed

use cases or dividing larger projects into multiple parts and then iterating toward larger goals over time.

Consider the Intel IoT Gateway architecture used by SAS Analytics for IoT. These gateways are available for a wide array of use cases, and designed for easy integration into existing IT and factory infrastructure. These gateways considerably simplify the task of exploring initial deployments, while also suiting long-term needs.

Organizations also need high-performance cloud servers and storage systems to efficiently process massive data volumes. SAS and Intel are working together to help these organizations select the best platforms for their applications, including high-performance solutions expressly designed to handle and store big data. With the guidance of these experts, manufacturers can create data centers that will meet their needs today and readily scale for the future.





# Security Considerations

The very connectedness of the IIoT elevates security considerations for all involved. Well-designed security solutions can provide end-to-end protection across a manufacturer's entire IoT platform, creating a chain of trust from thing to network to cloud.

In this arena, the merits of the Intel/SAS partnership are clear. Intel and SAS worked together closely to provide the highest levels of protection and manageability, starting with the gateway and extending into the cloud.

For example, Intel processors come with powerful security that establishes trusted execution environments (TEEs) for running critical high-integrity code and secure storage. Within these environments, key measurements for attestation and keys for end-to-end secure connections are protected. This ensures that only authorised code is allowed to run and only authorised changes are made.



[click to view SAS case study video](#) 



# Return on Investment

## A Dell Perspective

Like every business investment, return on investment (ROI) must be considered at all times when deploying a smart factory. The ability to prove ROI comes through intelligently connecting old machines and accessing trapped data – then utilising it with edge analytics and making the machines work autonomously. This is the key proposition of a smart factory and can unleash incredible value for manufacturers.

Consider the challenges surrounding equipment maintenance. Traditionally, manufacturers approached maintenance by either servicing equipment on a regular schedule, by replacing parts when performance decreased or signs of wear were observed, or by repairing or replacing equipment when it failed.

These approaches leave much to be desired. When maintenance is done on a schedule, equipment ends up being serviced when it is perfect working order. On the other hand, allowing equipment to degrade can impact product quality and lead to unplanned downtime. And all these approaches can incur unnecessarily high maintenance costs.

The IIoT and edge computing technology enables a brand new approach – predictive maintenance – that uses sensors to collect data about equipment performance. Software analyses the data and detects anomalies, so that staff can

take corrective actions long before they would ordinarily detect a problem. By allowing staff to service equipment at just the right time, predictive maintenance reduces downtime, improves equipment effectiveness, and lowers maintenance costs – all of which improves return on assets (RoA) by up to 24%.

The challenge is figuring out how to deploy this level of intelligence on the factory floor without rip-and-replace of existing assets. Intel and Dell tackled this challenge by combining Dell's expertise in rugged devices with Intel's leadership in high-performance computing. The result is an IoT Gateway durable enough to gather data where it's generated, and intelligent enough to support analytics software running locally. It offers benefits like standards-based architecture and ruggedized hardware. And importantly, it does not require rip-and-replace of existing assets.

Meanwhile, built-in security and easy integration with existing IT and OT infrastructure make for seamless deployment and operation. Analysing machine data locally also slashes the costs of data transmission to the cloud and enables faster responses to incoming data. Now manufacturers can run – and are already running – predictive maintenance models and factory optimisation solutions right where they're needed most.



# Predictive Maintenance in Practice

To understand how predictive maintenance works in a factory setting, consider a vibration sensor attached to the motor on a piece of factory equipment. As with any motor, the equipment experiences some vibration while it is in use, even if it is operating up to spec.

However, when the motor begins to fail, one of the first things that happens is that the vibration begins to increase. In the early stages, this vibration isn't enough for human workers to notice — it's not noticeably shaking, doesn't sound louder than usual, and isn't warm to the touch. But the electronic sensor can detect the change, and the predictive maintenance software can recognize the severity of the threat and provide personnel with the appropriate alerts and guidance on correcting the problem before the faulty motor affects production.

As this example shows, predictive maintenance offers four key benefits:

- Reduced unplanned downtime, because staffers are aware of equipment problems well before failure
- Improved equipment effectiveness, because staffers are alerted when equipment isn't operating efficiently
- Lower maintenance costs, because fixing problems early avoids big repair jobs
- Increased return on assets, because equipment stays within spec and runs more efficiently





### 4 stages of maintenance maturity

Most manufacturers take one of four approaches to equipment maintenance.	<b>1 Reactive.</b> Repair or replace equipment when it fails	<b>2 Preventive.</b> Repair or replace equipment based on a regular schedule	<b>3 Condition-monitoring.</b> Repair or replace equipment when performance decreases or signs of wear are detected	<b>4 Predictive.</b> Software detects anomalies that alert staff to take corrective actions before the problem is ordinarily detected or performance affected.
--	--	--	---	--

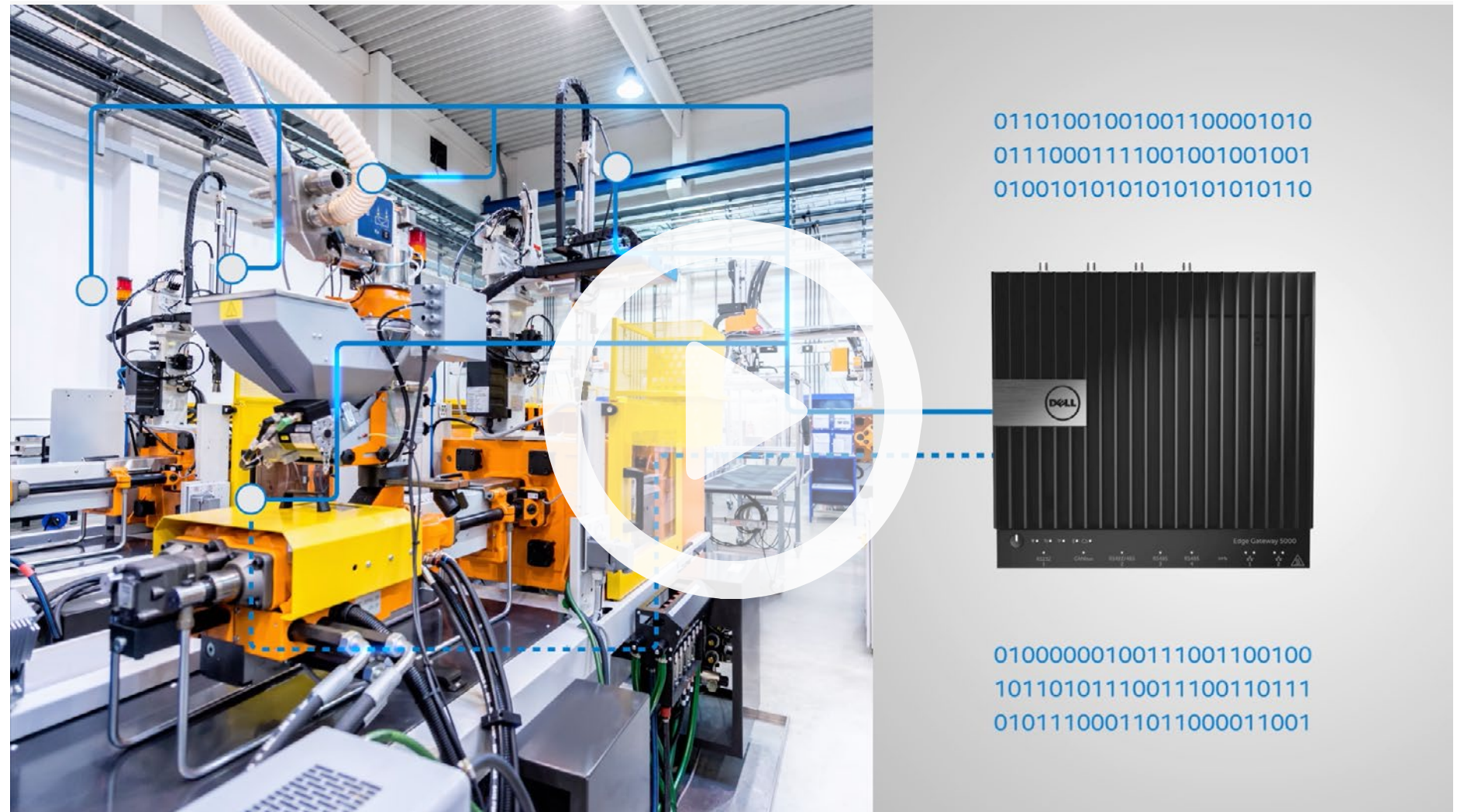


# Edge Computing

IIoT-based predictive maintenance is made possible in part because of edge computing, in which most data is analysed at the network edge and only necessary data is transmitted to the cloud or data centre. This approach uses network resources more efficiently, reduces cloud computing costs and provides continuity of service when connectivity isn't always available.

**“By allowing staff to service equipment at just the right time, predictive maintenance reduces downtime, improves equipment effectiveness, and lowers maintenance costs”**

Predictive maintenance is just the beginning. The IIoT solution that Dell and Intel created could be used for other purposes, such as real-time quality control or compliance initiatives. Organisations that take advantage of such collaborative solutions and invest in IIoT infrastructure will have a head start on the Fourth Industrial Revolution.



**click to view Dell case study video** 



# Industry Transformation

The Fourth Industrial Revolution represents a transformational time for the manufacturing industry. The innovation unlocked by collaboration between Intel and the partners in its IoT ecosystem is powering the major journey manufacturers need to make towards factory automation. Those who overcome the challenges and deploy the right technology to capitalise on smart factories and the IIoT will reap huge financial rewards and lead a lucrative generation of automated industrial processes.

No single organisation can deliver the benefits of IIoT alone. That is why Intel has partnered with technology leaders like ADLINK, Dell, IBM, PrismTech (an ADLINK company), and SAS. Together these companies are powering smart factories with solutions that generate value from industrial data.

---

**“No single organisation can deliver the benefits of IIoT alone.”**

---





# Join the Revolution

Intel's partnerships with IIoT leaders like ADLINK, Dell, IBM, PrismTech, and SAS are creating revolutionary solutions that are the foundation for smart factories. The interoperability, scalability, reliability, and security built into these solutions ensure that manufacturers can deploy IIoT technology with confidence.

To learn more, visit

[www.informationagehub.uk/fourth-industrial-revolution](http://www.informationagehub.uk/fourth-industrial-revolution)

