Life Is On | Schneider Electric

Industry 4.0: Minimizing Downtime Risk with Resilient Edge Computing

White Paper 287

Version 1

by Paul Lin and Steven Carlini

Executive summary

Industry 4.0 makes manufacturing “smart” through emerging technology innovations such as data analytics, autonomous robotics, and AI. These technologies drive increased productivity and performance throughout the value chain. These data-driven innovations require information technology (IT) systems deployed on-premise, often referred to as edge IT or edge computing. This edge IT can increase the risk of downtime for automation systems in some cases. Choosing IT enclosures designed for manufacturing environments and investing in proper power and cooling infrastructure can address the unique challenges of edge IT deployments in manufacturing environments. In this paper, we describe manufacturing environments, the cost of downtime, and the unique challenges in deploying industrial edge IT. We also provide best practices to ensure resilient edge computing by minimizing the risk of downtime.

RATE THIS PAPER ★★★★★

Introduction

With the advent of Industry 4.0, manufacturers can take advantage of technology innovations such as data analytics, digital twin, artificial intelligence, and autonomous robotics. These technologies drive increased productivity, reliability, reduced production cost, and better-informed decisions throughout the manufacturing process. New IT systems need to be introduced into production manufacturing environments to provide sufficient computing capacity to enable these technology innovations. As a result, there are often concerns over reliability, security, and continuity in manufacturing environments, which may hinder the adoption of the new IT systems.

There are a lot of manufacturing applications in industry such as logistics and food and beverage (F&B) process machines. The newly introduced IT systems could be logically "in parallel" or "in series" with these applications[1]. But this paper mainly focuses on the latter, where the IT systems can bring added value for automation systems. The IT systems are deployed as an on-premise data center (often called edge IT or edge computing). There are more and more applications introduced like this with Industry 4.0. The edge IT, however, may be perceived as an added risk of downtime on manufacturing automation systems, despite the benefits. So, it is important that manufacturers make the right edge IT investment to minimize the risks.

Meanwhile, unlike typical IT environments, manufacturing environments have unique challenges, such as harsh conditions and safety issues, which puts extra pressure on IT personnel who work in these environments. In this paper, we discuss the manufacturing environment, cost of downtime, and provide an overview of technology innovations used to achieve a "smart" factory in the era of Industry 4.0. We also compare availability for different degrees of resilient edge computing infrastructure solutions and provide best practices to minimize the risk of downtime.

Manufacturing environments and cost of downtime

As statistics of the past decade demonstrate, manufacturing downtime can cost organizations a significant amount of money per hour. Automation system downtime in manufacturing environments impacts productivity, profitability, customer experience, and even a manufacturer's brand reputation. Below are three statistics on the downtime costs for manufacturing environments in the past decade.

Automotive industry – In a survey commissioned by the Advanced Technology Services, Inc. (ATS) in 2005, 101 manufacturing executives from suppliers to engine makers to auto-makers were asked about cost of downtime. The survey found that downtime cost an average is $22,000 per minute with values as high as $50,000 per minute. On the high end, that equates to **$1.3 million per hour**[2].

All manufacturing business – In a survey conducted by IndustryWeek in 2013, covering hundreds of IT leaders, the survey showed downtime costs at an average of **$17,000 per incident**[3]. Another study conducted by Aberdeen Group in 2016 found that 82% of companies have experienced unplanned downtime over the past three years and the downtime could cost an average of **$260,000 per hour**, which was a 60% jump compared with $164,000 in 2014[4].

---

[1] In parallel means that there is a buffer for the IT systems to reboot or close for some time while the applications are still in operation such as logistics. In series, like links in a chain, means that applications like F&B process machines are dependent on the IT systems. If an IT system goes down, for even a second, you will experience immediate issues such as product quality, safety, assembly line stop, etc.

[2] https://news.thomasnet.com/companystory/downtime-costs-auto-industry-22k-minute-survey-481017

[3] https://www.industryweek.com/technology-and-iiot/information-technology/article/21960985/manufacturer-it-applications-study-finding-the-real-cost-of-downtime

[4] https://www.stratus.com/assets/aberdeen-maintaining-virtual-systems-uptime.pdf

We expect that the cost of downtime will be even higher in the era of Industry 4.0 as manufacturing processes are highly automated and integrated. Therefore, in order to prevent downtime, organizations need to make the right investments to ensure their critical processes are "always on".

Overview of Industry 4.0 technologies

There are several definitions of Industry 4.0 in the market. One definition from McKinsey is, "The next phase in the digitization of the manufacturing sector, driven by four disruptions: the astonishing rise in data volumes, computational power, and connectivity, especially new low-power wide-area networks; the emergence of analytics and business-intelligence capabilities; new forms of human-machine interaction such as touch interfaces and augmented-reality systems; and improvements in transferring digital instructions to the physical world, such as advanced robotics and 3-D printing." [5]

From this definition, we can say that Industry 4.0 is enabled by new technology innovations. **Figure 1** summarizes key emerging technology innovations which will enhance manufacturing operation efficiency, productivity, product quality, while reducing equipment failures, manufacturing costs, etc. in Industry 4.0.

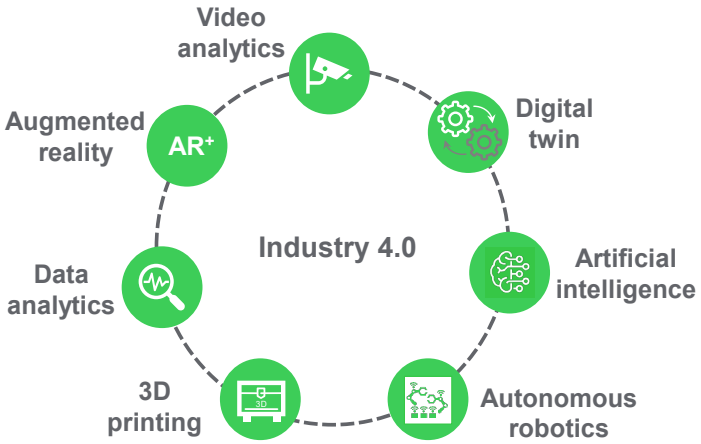

Figure 1
Key emerging technology innovations in Industry 4.0.

The following subsections describe each technology innovation and explain the benefits they provide to the industry.

Video analytics uses high-definition cameras for industrial quality vision inspection to detect defects. This technology can improve product quality and manufacturing productivity.

Digital twin[6] is defined, "fundamentally, as an evolving digital profile of the historical and current behavior of a physical object or process that helps optimize business performance. The digital twin can help predict outcomes and solve physical issues faster by detecting them sooner. It can achieve a complete digital footprint of the products from design and development through the end of the product lifecycle."

Artificial intelligence (AI)[7] is defined by Amazon as " the field of computer science dedicated to solving cognitive problems commonly associated with human intelligence, such as learning, problem solving, and pattern recognition." We often hear

[5] https://www.mckinsey.com/business-functions/operations/our-insights/manufacturings-next-act

[6] https://www2.deloitte.com/us/en/insights/focus/industry-4-0/digital-twin-technology-smart-factory.html

[7] https://aws.amazon.com/machine-learning/what-is-ai/

two phrases including machine learning (ML) and deep learning (DL) which are both computer science fields derived from the discipline of AI. AI can drive benefits throughout the value chain and also acts as the foundation of some other technology innovations such as autonomous robotics discussed below.

Autonomous robotics[8] are intelligent machines capable of performing tasks in the world by themselves, without explicit human control. In manufacturing environments, it means that the machine can communicate with other machines (M2M), the machine can interact with humans and the machine can maximize efficiency through intuitive collaboration with its users. Autonomous robotics can enhance manufacturing efficiency and productivity. Another perspective from Deloitte is that the autonomous robots will drive supply chain innovation[9].

3D printing, also known as additive manufacturing, is a technology to create a physical object from a digital design. It typically refers to making three-dimensional objects by layering materials on top of one another which makes it easy to produce spares, models, jigs, tools etc. to help manufacturers throughout R&D, production, and factory maintenance.

Data analytics is the science of analyzing raw data in order to make conclusions about that information. Manufacturers can leverage data analytics to increase productivity with quality assurance and defect tracking, minimize risk with conditional monitoring and predictive maintenance.

Augmented reality (AR) means "two different environments converging or blending in a way that boosts the effectiveness and efficiency of plant operators. One environment is "real" (what you see, unassisted, in front of your own eyes) and the other is "virtual" (not "real", but computer generated). Both of these environments can be understood in terms of a continuum, with real environments at one end and completely virtual environments at the other. What lies in between is augmented reality, which is, in essence, mixed reality." [10]

These technology innovations are data-driven and bring a new level of IIoT and computer capacity requirements to the manufacturing environment. IT personnel need to rethink their IT deployment strategies to support these technologies with more data collection, aggregation, processing, and analyzing, and deploy compute capacity closer to the users or "things". The following section explains how the addition of IT and OT enable these technologies.

How the addition of IT and OT enable these technologies

In order to achieve the benefits claimed above with these technology innovations, the industrial IT personnel need to **integrate IT and OT** and **deploy edge IT to the lower levels of the automation hierarchy** (such as control level, manufacturing execution system level, and ERP level) to support the technologies such as video analytics and autonomous robotics.

Integrate IT and OT

As electronics become smarter and lower-cost, we expect to see them embedded in the lower levels of the automation hierarchy including the control level, sensors, and actuators. This means that the OT systems will merge with the IT systems to

[8] https://mitpress.mit.edu/books/autonomous-robots

[9] https://www2.deloitte.com/us/en/pages/manufacturing/articles/autonomous-robots-supply-chain-innovation.html

[10] https://blog.se.com/machine-and-process-management/2018/01/16/driving-digital-transformation-augmented-reality/

achieve a more information-driven architecture. **Figure 2** illustrates the operational architecture enabled by the convergence of IT and OT based on the research spotlight from LNS[11]. Another proof of this trend is the latest Gartner research on IIoT in 2019, which shows the integration of IT and OT is becoming mature[12].

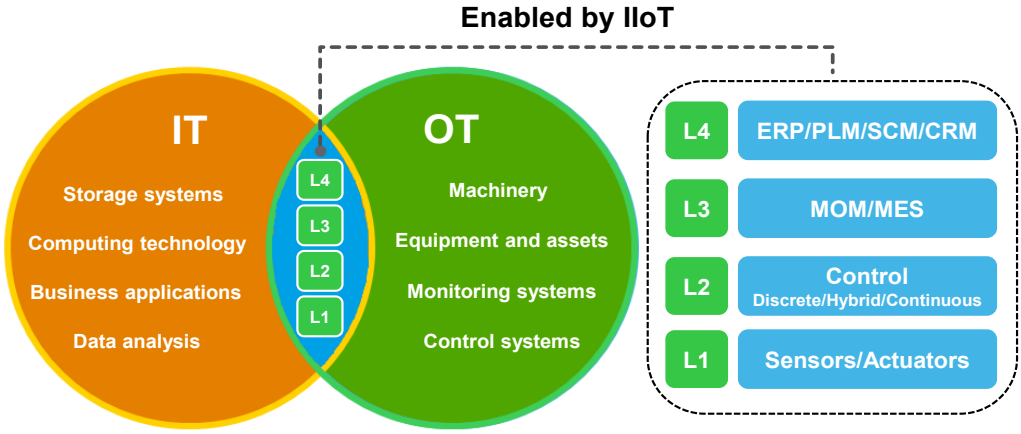

Figure 2
IT and OT are getting converged to enable smart enterprise control

Deploy edge IT to the lower levels of the automation hierarchy

The real-time controls of video analytics, augmented reality, and autonomous robotics will drive the computing capacity from cloud IT or enterprise IT[13] to the edge. The advantages of edge computing include low latency, real time response, mobility, and high security so as to achieve smart manufacturing. The OT devices such as sensors, actuators, and controllers are capable of interfacing transparently with the IT systems. For example, the control valves with embedded temperature, pressure, and acoustic sensors are able to operate autonomously using setpoints from the enterprise. Enterprise systems such as ERP, PLM, SCM, CRM, MOM, MES are supported by the enterprise IT or Cloud IT (as shown in **Figure 3**)[14]. Schneider Electric White Paper, *The Industrial Internet of Things: An Evolution to a Smart Manufacturing Enterprise*, discusses the information-driven automation architectures supported by the IIoT in detail.

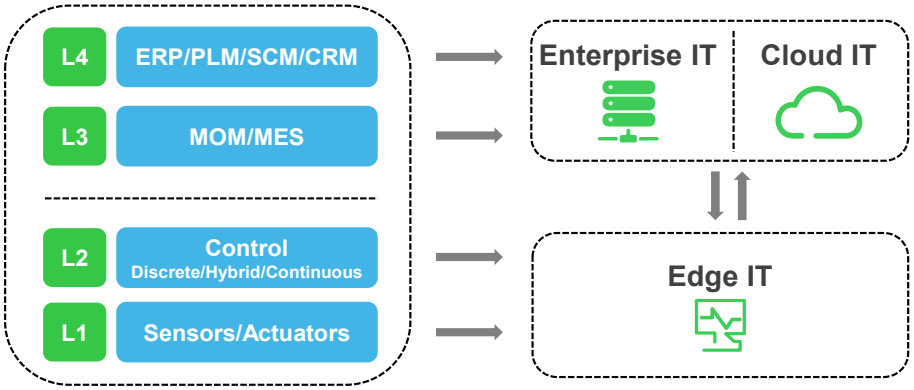

Figure 3
The information-driven automation architecture supported by hybrid IT

[11] "IIoT: Industrials Getting Results - Companies Reducing Risk & Improving Productivity in Operations"

[12] "Gartner Hype Cycle for the Internet of Things"

[13] Enterprise IT is normally a centralized IT system supported by enterprise owned data centers, while cloud IT is normally an IT service provided by third-party cloud service providers.

[14] ERP: Enterprise Resource Planning, PLM: Product Lifecycle Management, SCM: Supply Chain Management, CRM: Customer Relationship Management, MOM: Manufacturing Operation Management, MES: Manufacturing Execution System. For more information on explanation of industrial automation system level, see: https://www.electricaltechnology.org/2015/09/what-is-industrial-automation.html

An edge gateway, in an edge IT system, aggregates data from various sources and delivers real-time business information to the right people at the right time. This ensures a high level of performance and connectivity to address the critical needs of the applications. We will likely see more and more of these types of applications in Industry 4.0. The enterprise IT or cloud IT allows a company to analyze the whole plant, or multiple sites, or even the sites of suppliers. For example, logistics data, process data, and performance data can be compared at a higher level with advanced data analytics and AI. **Table 1** illustrates the technology innovations supported by different IT systems in manufacturing environments in Industry 4.0.

Table 1
Technology innovations are enabled by different IT systems in manufacturing environments in Industry 4.0.

Technology innovations	Edge IT	Enterprise IT	Cloud IT
Video analytics	√		
Digital twin		√	√
Artificial intelligence	√	√	√
Autonomous robotics	√		
3D printing	√		
Data analytics	√	√	√
Augmented reality	√		

As edge IT is introduced to manufacturing environments, IT personnel are facing added pressure to prevent failure of IT systems since they can lead to downtime of the automation systems. The more we depend on edge IT in automation processes in Industry 4.0, the more important it is to prevent failures or shutdowns of the IT systems. So, we need to ensure the edge IT systems are highly available and reliable, deployed and maintained properly, to avoid unexpected power outages and other forms of unscheduled downtime that would disrupt production. Moreover, deploying edge IT systems in industrial environments is also challenging, which is discussed in the following section.

Challenges of deploying edge IT in manufacturing environments

Unlike typical IT environments, there are many unique challenges and considerations to deploy edge IT as an on premise data center in manufacturing plant floors. The following sub-sections describe each in detail.

Availability – When edge IT is in series with manufacturing, the failure of an edge IT system can lead to downtime of the automation system, which will disrupt production. Using the automotive industry as an example, we now demonstrate how edge computing at different tier levels (i.e., differing levels of availability) impact the downtime cost of an organization. We assume the cost of downtime described previously of $1.3 million per hour. In one case, a tier-1[15] on-premise edge IT solution is deployed in series with manufacturing (availability is 99.67%, with 28.82 hours of downtime). In another case, a tier-3 edge IT solution results in an availability of 99.98%, with 1.58 hours of downtime. **Table 2** compares the results of automation system downtime and downtime cost when different tier-levels of edge IT are introduced. Note, this assumes the automation and manufacturing production is wholly dependent on the availability of IT. It shows that 95% of losses, or $35.3 million per year, can be eliminated by deploying tier-3 edge computing instead of tier-1 edge computing.

[15]Tiers are popular matrix measuring the availability of IT systems. For more information on this topic see: https://www.colocationamerica.com/data-center/tier-standards-overview.htm

Table 2

Comparisons on automation system downtime cost for different tier-level edge IT introduced

Edge IT Availability and Related Cost of Downtime					
Description	**IT availability**	**Downtime (hrs/year)**	**Losses ($M/hr)**	**Total Losses ($M)**	**% loss reduces**
Deploy Tier 1 edge IT	99.67%	28.82	1.3	38.7	Baseline
Deploy Tier 3 edge IT	99.98%	1.58	1.3	3.4	**95%**

Potential environmental risk – Manufacturing environments normally have less controlled ambient conditions. There is often a wide range of temperatures and humidity levels, a high degree of dust particles or other contaminants, and a higher potential of water leaks, vibration, collisions, and other nuisance events. These potential risks must be considered when deploying edge IT in an industrial environment. White Paper 278, *Three Types of Edge Computing Environments and their Impact on Physical Infrastructure Selection*, discusses the environmental types in detail.

Space constraints – There are often space constraints for deploying edge IT in manufacturing environments, especially for retrofits into existing plants. This means that space for a dedicated wiring closet may not be available. There is also the possibility that whatever open plant floor space might exist, is too valuable to occupy with edge IT.

Physical security – Compared with office and commercial environments, manufacturing environments will likely have unrestricted access to installed IT assets. People on the plant floor can access the IT equipment sitting out on the same floor. When the IT equipment is in an occupied "common" space, we lose the concentric circles of protection that we have when the IT equipment is in a dedicated secure room. People can now walk up to it and touch it, which might lead to malicious or accidental downtime.

Manageability – IT equipment is normally distributed throughout a manufacturing environment. Furthermore, there is typically little to no IT staff on the plant floor to monitor and manage the edge IT. This distributed layout combined with the limited presence of qualified IT staff, drives management challenges such as knowing where the edge IT cabinet is located, whether they are online or not, and being aware of risks to downtime.

Cyber security – The proliferation of IIoT represents more cyber security risks than before. We should consider both direct cyber-attacks via internet-connected devices, and vectors such as removable media devices. These cyber-attacks will threaten the uptime of IT and OT systems as well as data privacy (enterprise and customer data alike).

Best practices to achieve resilient edge computing

To address these challenges and minimize downtime risks, IT personnel need to introduce resilient edge computing solutions into manufacturing environments. Resilient solutions take advantage of existing best practices implemented in typical IT environments for the past several decades. These solutions also need to adopt unique best practices for deployment in manufacturing environments. This section summarizes some best practices to help IT personnel achieve resilient edge computing.

- Choose IT enclosures designed for manufacturing environments
- Use effective power protection and cooling approach
- Implement cyber security best practices
- Invest in monitoring and management software
- Leverage an ecosystem of partners to provide complete edge IT solutions

The following subsections describe each best practice in detail and also show some examples.

Choose IT enclosures designed for manufacturing environments

Purpose-built IT enclosures can address a lot of challenges discussed above such as environmental risks, space constraints, and physical security. The best practices for purpose-built IT enclosures are listed below.

- **Rugged enclosure design** – Durable enclosure material (i.e. stainless steel, aluminum), thermal insulation, coatings or paints, double-wall panels, and robust cable fittings (such as Roxtec) are designed to address the environmental risks including dust particles or other contaminants, water leaks, corrosion etc. Ruggedized enclosures should be deployed when manufacturing environments are harsh and uncontrolled. White Paper 278, *Three Types of Edge Computing Environments and their Impact on Physical Infrastructure Selection*, discusses harsh and uncontrolled environments in detail.
- **Flexible mounting enclosure design** – Wall-mounted enclosures can place the edge IT high on the wall, which addresses the floor space constraint in manufacturing environments and can also add a level of protection because a person with malicious intent would have to get on a stool or ladder to reach it.
- **Physical-security enclosure design** – With locks on IT cabinets, or setting alerts for doors propped open, or using biometric access locks, or using security cameras or combinations of these practices can help avoid malicious or unintended tampering.

Figure 4 shows two examples of IT enclosures purpose-built for manufacturing environments.

Figure 4

Examples of purpose-built IT enclosures

6U purpose-built IT enclosure

Ruggedized purpose-built IT enclosure

Use effective power protection and cooling approach

Proper power and cooling infrastructure systems like uninterruptible power supplies (UPSs) and air conditioners can minimize the risk of downtime.

- **UPSs,** typically integrated into the IT enclosures, provide uninterrupted, conditioned, clean and reliable power to edge IT loads.
- **Lithium-ion batteries** for UPSs are recommended. Compared with valve-regulated lead acid (VRLA) batteries, lithium-ion batteries have many benefits

such as longer life (normally over 10 years), much longer runtime for a given size, and embedded battery monitoring systems for safety. They can also better endure harsh manufacturing environments that experience a broad temperature range – over 40°C. Moreover, battery replacements are reduced thereby eliminating the risk of human error during replacements. White Paper 231, *FAQs for Using Lithium-ion Batteries with UPS*, discusses the common questions about lithium-ion batteries and their use in UPSs in detail. **Figure 5 (left)** shows an example of a purpose-built IT enclosure integrated with a li-ion UPS.

- **Dedicated air conditioners** such as a self-contained air conditioner can be mounted inside a ruggedized IT enclosure, which can avoid dust and keep the temperature and humidity regulated, even when the room environment is not. **Figure 6 (right)** shows an example of a ruggedized IT enclosure integrated with an air-cooled & self-contained air conditioner.
- **Redundant power and cooling systems** are recommended for critical edge IT applications to achieve concurrent maintainability.

Figure 5
Example of proper power and cooling protection for edge computing

Implement cyber security best practices

The complexity of IIoT means that cyber security must be designed into the components and their embedded networking systems that make up the automation system. The best practices for edge IT cyber security include:

- Adopt industrial security standards with certification to ensure the security of both IT and OT systems.
- Involve both IT and OT experts in the cyber security design.
- Choose an edge gateway with an embedded firewall to protect against network attacks.
- **Deploy a network intrusion detection systems (NIDS)**[16].
- **Use a defense-in-depth approach to cyber security**, where there are 6 key steps including security plan, network separation, perimeter protection, network segmentation, device hardening, and monitoring & update. White paper, *Cyber Security for Industrial Automation & Control Environments*, discusses these protection and prevention strategies in detail.

With these cyber security best practices, more and more industries can place their automation program/software in edge IT. Connected processes benefit from online updates of the latest antivirus intrusion software while a standalone process can be attacked by a USB thumb drive with no protection.

[16] Network Intrusion Detection Systems for Critical Infrastructure

Invest in monitoring and management software

A best practice used in typical IT environments is monitor and manage edge computing from a centralized location or remotely. Data center infrastructure management (DCIM) is a software management platform used for edge IT. DCIM supports IT staff by providing visibility into their infrastructure across hybrid environments, either on-site or remotely, while helping with their work/life balance. Next-generation DCIM provides big data analytics and AI, making maintenance more predictive by analyzing data in real time. For example, by analyzing the UPS age and efficiency, battery age, cooling performance, etc., DCIM can provide IT staff proactive recommendations, which ensures they have adequate backup in the event of an incident. White Paper 281, *Essential Guidance on DCIM for Edge Computing Infrastructure*, discusses essential DCIM functions for edge computing in detail. **Figure 6** shows an example "health" score card for a fleet of UPSs with next-generation DCIM.

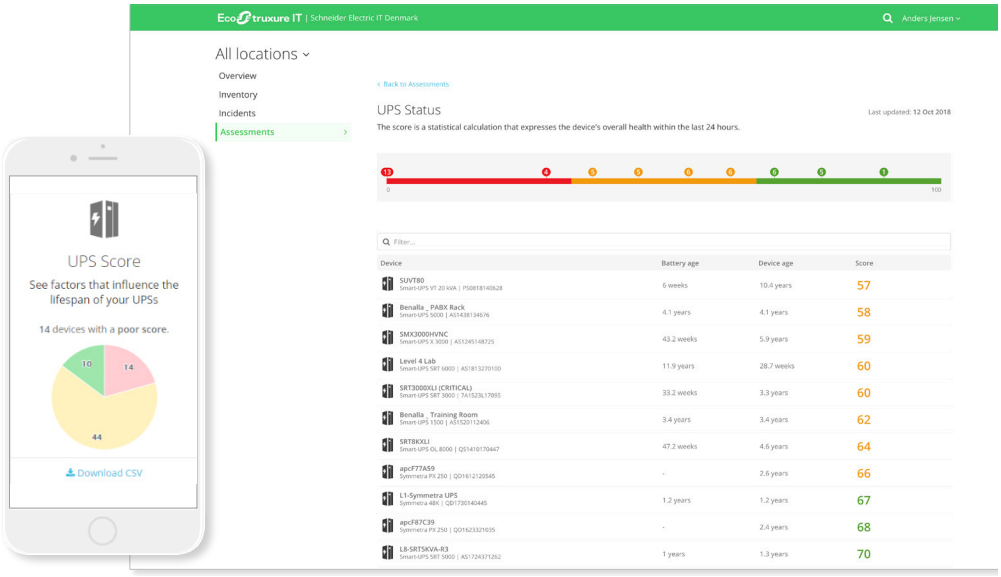

Figure 6
An example screenshot showing a health scorecard for a fleet of managed UPSs

Leverage an ecosystem of partners to provide complete edge IT solutions

Given the convergence of IT and OT, the complexity of the technology and solutions, the security requirements, and the services involved for the industrial edge computing, things can get complicated. For example, IT personnel need to work closely with different partners such as system integrators, industrial software providers, physical infrastructure vendors, etc., which can be very time-consuming and complicated. The best practice is to leverage an established ecosystem of partners using open technologies, which can deliver fully integrated micro data centers. For example, OT system integrators and IT solution providers are converging to provide better integrated solutions for industry end users. An example of IT and OT integrators working together is shown here: https://www.se.com/ww/en/partners/system-integrators/industry/.

This ecosystem promises faster, and easier deployment and lower defects compared to assembling your own solution from a disparate group of partners. White Paper 277, *Solving Edge Computing Infrastructure Challenges*, discusses this ecosystem in detail. **Figure 7** shows an integrated ecosystem of partners that work together to provide a total solution for industrial customers.

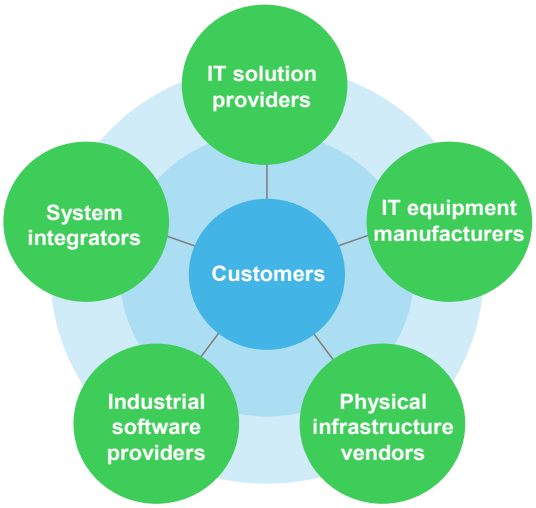

Figure 7
The integrated ecosystem of partners

Figure 8 shows an example of a fully integrated edge computing solution which leverages an ecosystem of partners such as IT solution providers, IT equipment manufacturers, and physical infrastructure vendors. According to World Wide Technology[17], this design can reduce field engineering costs by 25% to 40%, increase order processing speed by 20%, and reduce maintenance costs by 7%.

Figure 8
Example of a fully integrated edge computing solution

[17] https://www.wwt.com/wp-content/uploads/2015/03/WWT_Integration_Centers_Overview.pdf, Accessed on May 28, 2020

Conclusion

Manufacturing downtime represents a significant cost for industry stakeholders. Emerging technology innovations associated with Industry 4.0, such as video analytics, digital twin, AI, and autonomous robotics will lead to increased efficiency, productivity, product quality, and less equipment failures. These technology innovations are enabled by integrating IT and OT and deploying edge IT as an on-premise data center. But the introduction of edge IT to the lower levels of the automation hierarchy, such as sensors/actuators and control, will add downtime risks to manufacturing processes. The best practices provided in this paper can help industry IT personnel minimize the risk with resilient edge computing and address unique industrial challenges such as hash environment, cyber security, physical security, and manageability.

About the author

Paul Lin is the Research Director at Schneider Electric's Science Center. He is responsible for data center design and operation research and consults with clients on risk assessment and design practices to optimize the availability and efficiency of their data center environment. Before joining Schneider Electric, Paul worked as the R&D Project Leader in LG Electronics for several years. He is now designated as a “Data Center Certified Associate”, an internationally recognized validation of the knowledge and skills required for a data center professional. He is also a registered HVAC professional engineer. Paul holds a master’s degree in mechanical engineering from Jilin University with a background in HVAC and Thermodynamic Engineering.

Steven Carlini is the Vice President of Thought Leadership at Schneider Electric. He was behind some of the most innovative solutions that changed the data center landscape and architecture throughout his career. He holds a BSEE from the University of Oklahoma and an MBA in International Business from the University of Houston. He is a recognized expert in the field and a frequent speaker and panelist at data center industry events.

RATE THIS PAPER

Resources

FAQs for Using Lithium-ion Batteries with UPS
White Paper 231

Solving Edge Computing Infrastructure Challenges
White Paper 277

Three Types of Edge Computing Environments and their Impact on Physical Infrastructure Selection
White Paper 278

Essential Guidance on DCIM for Edge Computing Infrastructure
White Paper 281

The Industrial Internet of Things: An Evolution to a Smart Manufacturing Enterprise
White Paper

Cyber Security for Industrial Automation & Control Environments
White Paper

Browse all white papers
whitepapers.apc.com

Browse all TradeOff Tools™
tools.apc.com

Contact us

For feedback and comments about the content of this white paper:

Data Center Science Center
dcsc@schneider-electric.com

If you are a customer and have questions specific to your data center project:

Contact your Schneider Electric representative at
www.apc.com/support/contact/index.cfm