The key to any successful industrial digitalisation project

Posted on **7 Feb 2019** by **The Manufacturer**

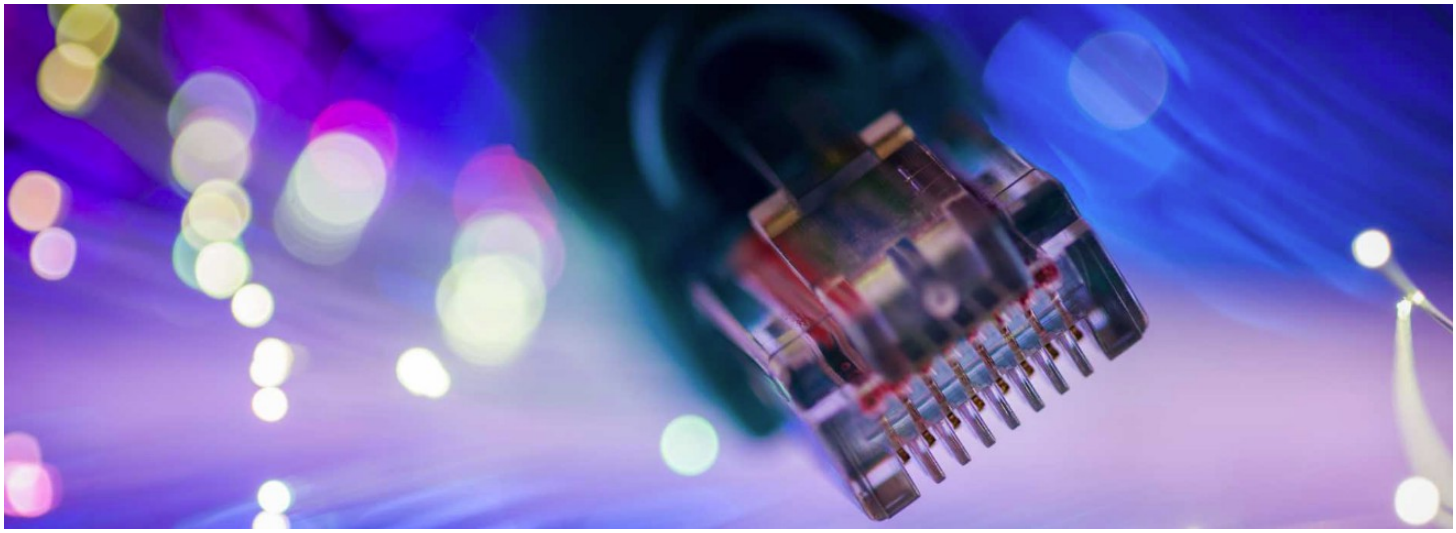
Intelligent use of real-time data is critical to successful industrial digitalisation. However, ensuring that data flows effectively is just as critical to success. Todd Gurela explains the importance of getting your manufacturing network right.

Industrial digitalisation, including the Industrial Internet of Things (IIoT), offers great promise for manufacturers looking to optimise business operations.

By bringing together the machines, processes, people and data on your plant floor through a secure Ethernet network, IIoT makes it possible to design, develop, and fabricate products faster, safer, and with less waste.

For example, one automotive parts supplier eliminated network downtime, saving around £750,000 in the process simply by deploying a new wireless network across the factory floor.

The time it took for the company to completely recoup their investment in the project? Just nine months.



The key to any successful industrial digitalisation project is factory data

Without data – extracted from multiple sources and delivered to the right application, at the right time – little optimisation can happen.

And there is a multitude of meaningful data held in factory equipment. Consider how real-time access to condition, performance, and quality data – across every machine on the floor – would help you make better business and production decisions.

Imagine the following. A machine sensor detects that volume is low for a particular part on your assembly line. Data analysis determines, based on real-time production speed and previous output totals, that the part needs to be re-stocked in one hour.

With this information, your team can arrange for replacement parts to arrive before you run out, and avoid a production stoppage.

This scenario may be a theoretical, but it illustrates a genuine truth. Manufacturers need reliable, scalable, secure factory networks so they can focus on their most important task: making whatever they make more efficiently, at higher quality levels, and at lower costs.

At the heart of this truth is the factory network. So, while the key to a successful Industry 4.0 project is data, the key to meaningful, accurate data is the network. And manufacturers need to plan carefully to ensure their network can deliver on their needs.

Five key network characteristics

There are five characteristics manufacturers should look for in a factory network before selecting a vendor.

In no particular order, they are:

Interoperability – this ability allows for the 'flattening' of the industrial network to improve data sharing, and usually includes Ethernet as a standard.

Automation – for 'plug and play' network deployment to streamline processes and drive productivity.

Simplicity – the network infrastructure should be simple, as should the management.

Security – your network should be secure and provide visibility into and control of your data to reduce risk, protect intellectual property, and ensure production integrity.

Intelligence – you need a network that makes it possible to analyse data, and take action quickly, even at the network edge.

Manufacturers need solutions with these features to help aggregate, visualise, and analyse data from connected machines and equipment, and to assure the reliable, rapid, and secure delivery of data. Anything less will leave them wanting, and with subpar results.

These five characteristics are explained in more detail below, along with a real-world case study of a British manufacturer who recently modernised its network and is now expanding globally.

1. Interoperability

Network interoperability allows manufacturers to seamlessly pull data from anywhere in their facility. An emerging standard in this area is Time Sensitive Networking (TSN).

Although not yet widely adopted, TSN provides a common communications pathway for your machines. With TSN, the future of industrial networks will be a single, open Ethernet network across the factory floor that enables manufacturers to access data with ease and efficiency.

Most important, TSN opens up critical control applications such as robot control, drive control, and vision systems to the Industrial Internet of Things (IIoT), making it possible for manufacturers to identify areas for optimisation and cost reduction.

Also, with the OPC-UA protocol now running over TSN, it also becomes possible to have standard and secure communication from sensor to cloud. In fact, TSN fills an important gap in standard networking by protecting critical traffic.

How so? Automation and control applications require consistent delivery of data from sensors, to controllers and actuators.

TSN ensures that critical traffic flows promptly, securing bandwidth and time in the network infrastructure for critical applications, while supporting all other forms of traffic.

And because TSN is delivered over standard Industrial Ethernet, control networks can take advantage of the security built into the technology.

TSN eliminates network silos that block reachability to critical plant areas, so that you can extract real-time data for analytics and business insights.

This is key to the future of factory networks, as TSN will drive the interoperability required for manufacturers to maximise the value from Industry 4.0 projects.

One leading manufacturer estimated that unscheduled downtime cost them more than £16,000/minute in lost profits and productivity. That's almost £1m per hour if production stops. Could your organisation survive a stoppage like that?

2. Automation

Network automation is critical for manufacturers who have growing network demands. This includes needing to add new machines, or integrate operational controls, to existing infrastructure as well as net-new deployments.

Network uptime becomes increasingly important as the network expands. Ask yourself whether your network and its supporting tools have the capability for 'plug and play' network deployments that greatly reduce downtime if – and when – failure occurs.

It's essential that factories leverage networks that automate certain tasks – to automatically set correct switch settings, for example – to meet Industry 4.0 objectives. The task is too overwhelming otherwise.

3. Simplicity

Like automation, network simplicity is an essential component of the factory network. Choosing a single network infrastructure, capable of handling TSN, Ethernet IP, Profinet, and CCLink traffic can significantly simplify installation, reduce maintenance expense, and reduce downtime.

It also makes it possible to get all your machine controls, from any of the top worldwide automation vendors, to talk through the same network hardware.

Consider also that you want a network that can be managed by operations and IT professionals. Avoid solutions that are too IT-centric and look for user-friendly tools that operations can use to troubleshoot network issues quickly.

Tools that visualise the network topology for operations professionals can be especially useful in this regard.

For example, knowing which PLC (including firmware data) is connected to which port, and which I/O is connected to the same switch, can help speed commissioning and troubleshooting.

Last, validated network designs are essential to factory success. These designs help manufacturers quickly roll out new network deployments and maintain the performance of automation equipment. Make sure this is part of the service your network vendor can provide.

4. Security

Cybersecurity is critically important on the factory floor. As manufacturing networks grow, so does the attack surface, or vectors, for malicious activity such as a ransomware attack.

According to the **Cisco *2017 Midyear Cybersecurity Report***, nearly 50% of manufacturers use six or more security vendors in their facilities. This mix and match of security products and vendors can be difficult to manage for even the most seasoned security expert.

No single product, technology or methodology can fully secure industrial operations. However, there are vendors that can provide comprehensive network security solutions in their plant network infrastructure that include simple protections for physical assets, such as blocking access to ports in unmanaged switches or using managed switches.

Protecting critical manufacturing assets requires a holistic defence-in-depth security approach that uses multiple layers of defence to address different types of threats. It also requires a network design that leverages industrial security best practices such as 'Demilitarized Zones' (DMZs) to provide pervasive security across the entire plant.

5. Intelligence

Consider for a moment how professional athletes react to their surroundings. They interpret what is happening in real-time, and make split-second decisions based on what is going on around them.

Part of what makes those decisions possible is how the players have been coached to react in certain situations. If players needed to ask their coach for advice before taking every shot, tackling the opposition, or sprinting for victory…well, the results wouldn't be very good.

Just as a team's performance improves when players can take in their surroundings and perform an appropriate action, the factory performs better when certain network data can be processed and actioned upon immediately – without needing to travel to the data centre first.

Processing data in this way is called 'edge', or 'fog', computing. It entails running applications right on your network hardware to make more intelligent, faster decisions.

Manufacturers need to access information quickly, filter it in real-time, then use that data to better understand processes and areas for improvement.

Processing data at the edge is key to unlocking networking intelligence, so it's important to ask yourself whether your factory network can support edge applications before beginning a project. And if it can't, it's time to consider a new network.

A final note on network intelligence. Once you deploy edge applications, make sure you have the tools to manage and implement them with confidence, at scale. Managing massive amounts of data can quickly

become a problem, so you'll need systems that can extract, compute, and move data to the right places at the right time.

The opportunity for manufacturers who invest in Industry 4.0 solutions is massive (and it's time that leaders from the top floor and shop floor realised it). But before any Industry 4.0 project can get off the ground, the right foundation needs to be in place.

The factory (or industrial) network is that foundation… and manufacturers owe it to themselves to select the best one available.

Case Study:

SAS International is a leading British manufacturer of quality metal ceilings and bespoke architectural metalwork. Installed in iconic, landmark buildings worldwide, SAS products lead through innovation, cutting-edge design and technical acoustic expertise.

Their success is built on continued investment in manufacturing and achieving value for clients through world-class engineered solutions.

In the UK, SAS operates factories in Bridgend, Birmingham and Maybole, with headquarters and warehouse facilities in Reading. The company has recently expanded its export markets and employs nearly 1,000 staff internationally.

However, the IT infrastructure was operating on ageing equipment with connectivity, visibility and security constraints.

The company's IT team recently modernised its network, upgrading from commercial-grade wireless to a new network solution with a unified dashboard that allows them to remotely manage distributed sites.

They now have instant visibility and control over the network devices, as well as the mobile devices used by employees daily.

Results

During the initial deployment, the IT team was able to identify cabling issues that previously they would not have been alerted to or been able to investigate.

With upcoming projects and continually working to optimise solutions, like cloud storage, the network is now robust enough and reliable enough to support future IT needs.

SAS is retrofitting numerous manufacturing machines with computers. This retrofit, partnered with the new network, allows remote communications between the machines and the designers without having to manually input data at the machines themselves.

The robust wireless infrastructure is changing the manual printing and checking of stock by enabling handheld scanners and creating a more efficient and cost-effective product flow.

Fault mitigation and anomaly detection have been huge benefits of the solution. For example, the IT team was able to quickly identify a bandwidth issue when a phenomenal amount of data was generated from an automated transfer to a shop machine.

They were able to spot the issue, identify the machine, and fix the problem. Before, they would merely have seen there was a network slowdown, but wouldn't have been able to identify or resolve the problem.

The SAS team will continue to benefit from the included firmware updates and new feature releases that are integrated into the solution, providing them with a future-proof solution as they expand to global sites in the future.

Todd Gurela *is CTO of Cisco's Manufacturing Industry Solutions Group and a global thought leader on digital manufacturing.*