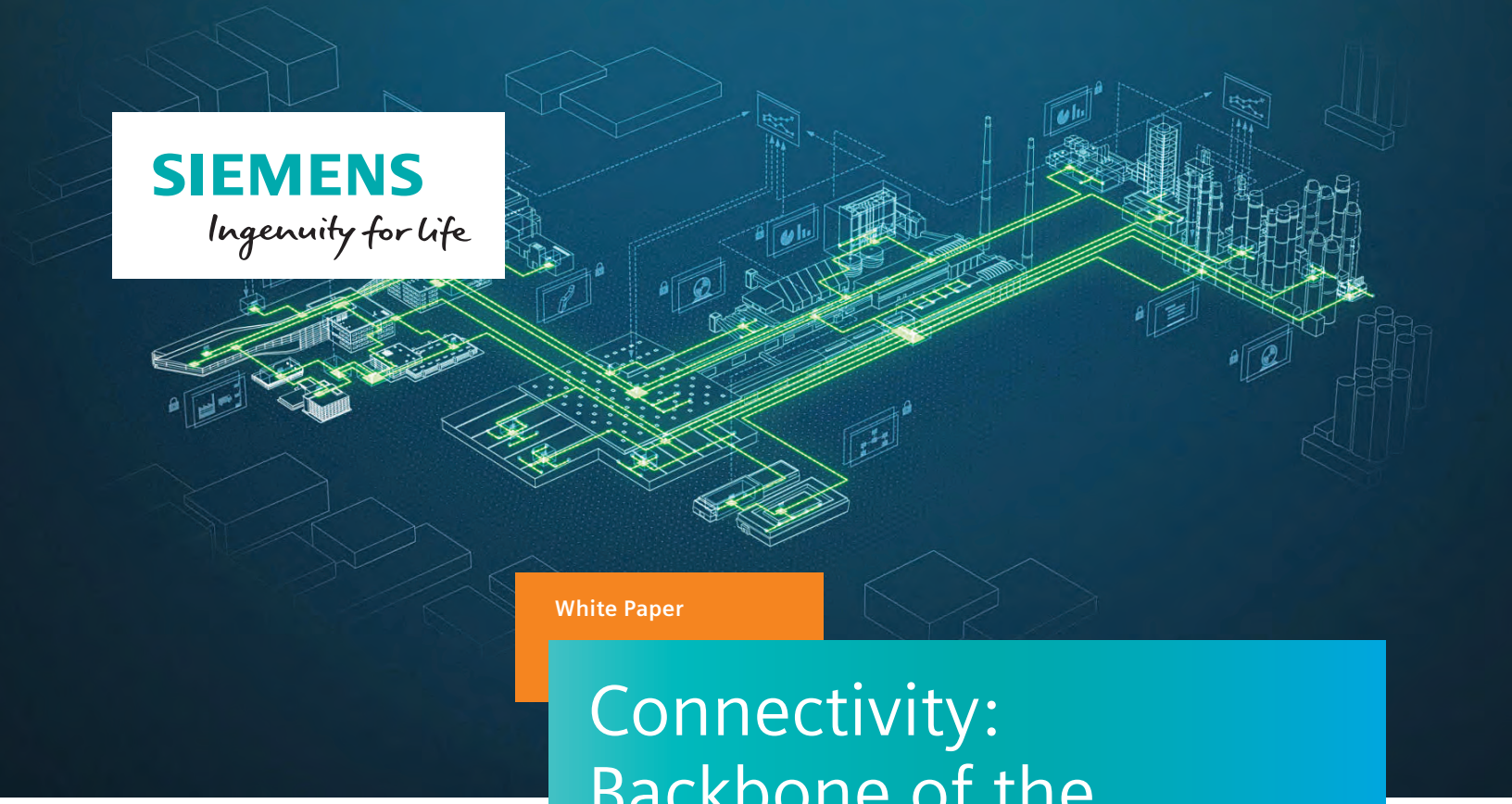


SIEMENS
Ingenuity for life

White Paper

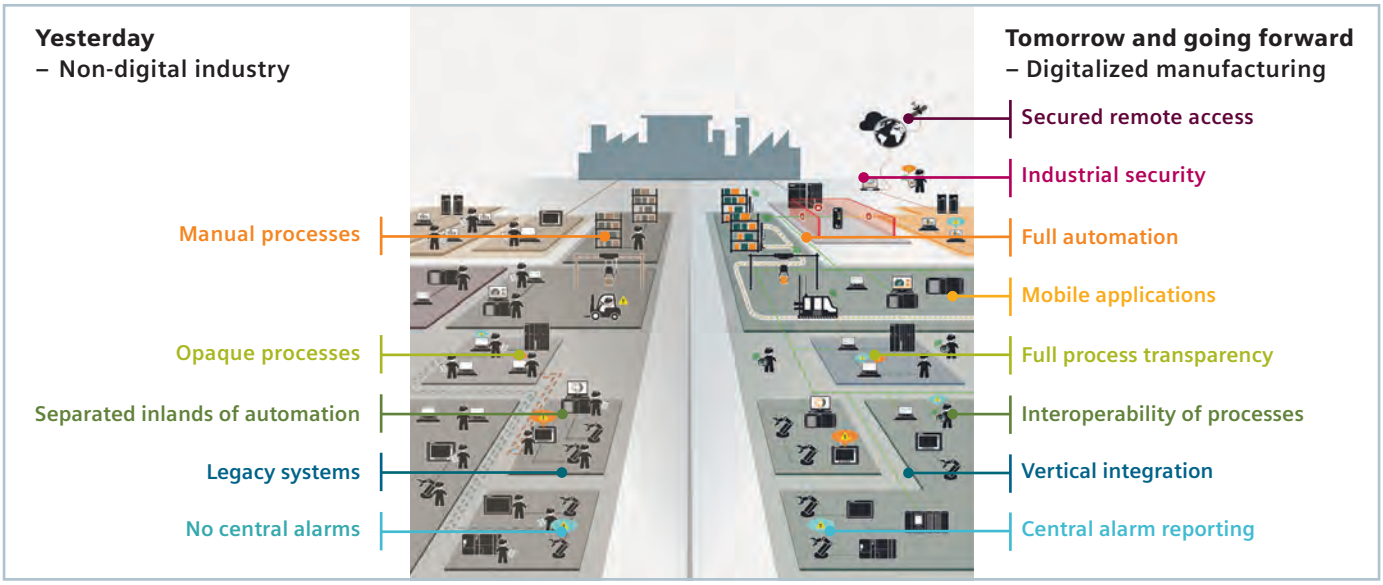
Connectivity: Backbone of the Digital Enterprise

After pioneering fast, reliable and secure industrial communications as the backbone of today's Digital Enterprise, Siemens is helping customers to bridge the divide between operational technology (OT) and enterprise information technology (IT) in ways to support collaboration and enhance overall production efficiency, reliability, visibility, flexibility and security much more.

For decades, the world's many industries have invested heavily in information technology (IT) to reduce costs, improve operational efficiency and visibility and, ultimately, to boost profits. In doing so, IT professionals have laid a big part of the foundation for what's called the Digital Enterprise. But for extractive, manufacturing and logistics industries, the Digital Enterprise also involves another form of IT on the "shop floor" side of an organization, which is commonly referred to as *Operational Technology (OT)*.

Over the same decades that gave rise to IT, companies have invested hundreds of billions in OT, much of it for increasingly smart machines and systems to automate discrete production tasks and continuous processes. This includes automation control and higher-level OT management platforms to efficiently operate, monitor and optimize OT performance and maximize the utilization of capital assets as much as possible. It also includes various industrial communication technologies that keep all these systems talking to each other and to their human operators.

The benefits have been many, including major reductions in costs, latencies and cycle times, as well as fewer data collection errors. Industrial communication – the so-called digital thread – has also helped interconnect what were once islands of activities and information, while also breaking down operational silos. Another benefit is full process transparency where, for example, it is possible to have instant access to quality data or stock levels, be more flexible and reduce reaction time to changing demand. In addition, companies can achieve vertical integration. This includes benefits such as instant access to service teams via internet, immediate response to product changes through automated download of new production data from R&D, implementation of the digital twin in Engineering and PLM processes and real-time, global data availability.



Benefits of a digitalized manufacturing environment.

Different perspectives. Connecting these two worlds – IT and OT – for a truly, end-to-end Digital Enterprise is ideally the role of modern industrial communications that are fast, reliable and secure. Unfortunately, for far too many organizations, sharing data between these two worlds can be a struggle because their network infrastructures could be more up-to-date and better connected.

Another important reason that makes connecting IT and OT a challenge is this: The perspectives of enterprise IT and OT professionals are typically very different. Although their jobs are inter-related in many ways, each tends to have dissimilar educational and on-the-job backgrounds than the other.

For example, IT staff often come from computer science backgrounds, while OT staff have industrial engineering backgrounds. IT professionals tend to focus on cost optimization and security, while OT professionals tend to concentrate on production throughput and machinery availability. Both share concerns for productivity and efficiency. These distinct pedigrees can result in sometimes suspicious and occasionally adversarial perspectives toward the work each other does.

It doesn't have to be that way and, indeed, shouldn't be if organizations are to realize the full promise of an end-to-end Digital Enterprise. That's because modern industrial communications can tie the IT and OT sides of the Digital Enterprise together, while also enabling major transformations in how raw materials are sourced and transported, products are made, and finished goods get to market.

Been there, done that. As one of the world's largest organizations and manufacturers, Siemens has experienced and bridged this IT/OT divide in its own global operations. We have deep insights into how to bridge this gap, which we want to share in this paper. The solution has both human and technology dimensions.

For example, we've learned that only through an active IT/OT collaboration based on the mutual understanding of each other's respective roles and backgrounds can data flows be optimized over a company's networks, the backbone of the Digital Enterprise. And we know that not all data spanning the Digital Enterprise is equal: some deserve special treatment, given the specific role particular data may play in a critical process or workflow.

Ultimately, by understanding the full potential of modern industrial communications, IT and OT can work together to ensure more operational efficiency, visibility, flexibility and security in production. This can help companies fully realize the promise of the Digital Enterprise to gain greater competitiveness and profitability both in the short-term today and the long-term tomorrow.

Marking the IT/OT divide: Different roles, perspectives and motivations

Classic corporate IT is a big job, although no more so than OT. Day-to-day, IT teams must be extremely tactical in support of end-user productivity, identity management, cybersecurity, office networks, and departmental file servers and printers, to name just some of their many day-to-day chores. Hours can be long and demands high.

At the same time, especially in large enterprises, their jobs can also involve the deployment and management of large strategic assets and capabilities – enterprise resource planning (ERP) systems, customer relationship management (CRM) systems, big data analytics and other core applications residing in either data centers or the cloud.

Mission-critical. Sophisticated IT often can be core to what many companies do and be the foundation of their customer value propositions, if not their competitive differentiators, as well.

Take FedEx, for example. Back in the 1990s, the company deployed technologies such as wireless handheld scanners for its courier and counter staff supported by giant back-end databases, pioneering self-service package tracking for customers via a web portal. For a time, this capability gave FedEx a big competitive edge, although it's now a standard in the logistics industry.

IT was so vital to FedEx that company founder and CEO Frederick W. Smith once described his firm as "an IT company that just happens to ship boxes to pay for it all." In fact, the public networks and FedEx's own private networks were critical enablers of that package-tracking functionality.

Hands-full. While IT teams keep their companies' front and back-office operations running, their OT counterparts have their hands plenty full keeping production running. Disruptions and downtime of components, instrumentation or systems can potentially have not only bottom-line consequences but also cascading downstream impacts on customer delivery commitments and satisfaction.

Life safety can be at stake, too. The Texas City refinery explosion in 2005, for example, killed 15 people and injured more than 100. The cause was found to be the failure of several level indicators, which led to the overfilling of a vapor-liquid separator. As a hydrocarbon geyser erupted, its flow was ignited by the engine of a pickup truck idling nearby.

Many OT professionals are always on call. That's because lots of industrial facilities – nuclear plants, oil platforms and public communications, to name just three – must operate around the clock, in real- or near-real time and with 99.999 percent uptime or better. Reliability, durability and availability are of utmost importance. In contrast, most enterprise IT networks must simply work during "business hours."

OT teams also need to ensure that a complex, often heterogeneous, technology landscape at the field level – including sensors, actuators, valves, instrumentation, and other devices, even conveyors – are all functioning properly, often in harsh operating conditions. At the same time, all these elements feed and draw operational data into and from a dynamic, vertical infrastructure consisting of a wide range of controllers, operator systems and manufacturing execution systems.

In-sync. In addition, OT solutions used in discrete manufacturing typically must be finely tuned across their operating network structures and constituent components (both hardware and software). Those always-on components must use fixed IP addressing, resulting in different bandwidth cost models compare to enterprise IT networks that typically use dynamically assigned IP addressing.

What's more, cycle timings, usually in milliseconds, and data communications need tight synchronization across all of those components. This is true regardless of the industry and is much more so in critical infrastructures such as power, communications and transportation.

OT networks differ from enterprise IT networks, too. Data packet routing between network nodes in the former must operate deterministically compared to the latter's "best-effort" routing. Deterministic means the routing of data packets must be pre-determined in advance of their transmission, so the packets and their information payloads get to where they need to go within the cycle times required by a machine or process.

Why? Cyclically executing process programs need constantly updated input data in order to issue the appropriate control commands to components. Those commands have to arrive when expected, within milliseconds. In other words, a network hiccup that might delay an outbound email by a couple seconds might not be noticed by a user, but a similar delay in a controller command arriving at its destination could disrupt an entire production line.

Bridging the IT/OT divide: Time to bring teams together

To be sure, more and more companies the world over are moving toward greater integration that will help make them truly end-to-end Digital Enterprises. They're bridging the divide separating IT and OT, in part by purposefully bringing both teams together to facilitate greater understanding and cooperation.

They're also facilitating a vibrant digital thread of data throughout their businesses by modernizing their network communications with advanced technologies, while incorporating OT's precision requirements for production networks and data functionality into a strategic plans for their overall enterprises.

Aligning perspectives. By aligning the different perspectives of IT and OT functions, these companies are helping to eliminate legacy information islands and silos that can slow down the speed of production and business, limit operational visibility and delay time to market.

They are leaving data synchronization and transcoding issues in the past, so they no longer experience time-consuming, error-ridden data handoffs and cycle-time latencies. Quality has risen; rework has dropped. Operational visibility has improved, too. And they have gained greater operational flexibility and new business agility that enables them to respond faster to dynamic customer demands and wholly new opportunities.

In short, they're gaining advantages over less innovative competitors, who might be overlooking or ignoring issues spawned by the IT/OT divide.

But for those latter companies taking a wait-and-see attitude toward end-to-end digitalization and modernizing their network communications, competitive disadvantage isn't their only risk of not doing so. They face a wide world of cyber threats – external and internal – just waiting to exploit the vulnerabilities inherent in a fragmented digital landscape.

Obscure vulnerabilities. While industrial networks may appear inside companies as a standalone, closed-loop systems, often they can be connected at some obscure point to the enterprise network. If so, the latter's external-facing cyber vulnerabilities can then extend to the industrial network.

Another set of security issues with industrial networks involves their evolution from early assortments of electrical relays or antiquated microprocessor controllers and manually monitored indicator lights, trips and breakers. Those legacy systems might work well enough to operate relatively simple processes even today, but they likely lack proper security controls.

For example, these systems may well be connected to modern distributed control systems (DCSs) that feature the latest programmable logic controllers (PLCs). The latter are essentially micro-computers using Windows or Linux and are connected over industrial Ethernet to human-machine interfaces (HMIs). In turn, these HMIs are often accessible anywhere in the world via PCs or touchscreen tablets and smartphones – by legitimate DCS operators or by hackers exploiting the vulnerabilities in the connections between old and new systems.

To make matters worse, the integration of the two kinds of networks can also introduce uncertainty within companies as to whether IT or OT owns responsibility for overall cybersecurity. As result, accountability issues can arise, manifesting themselves as cybersecurity gaps.

In contrast, for companies intent on building an end-to-end Digital Enterprise, the question of who owns cybersecurity will not be an issue. That's because IT and OT will have clearly defined roles and responsibilities, understood by both sides.

Advanced industrial communications: Ensuring the highest availability

Without fast, reliable and secure communications across all components and systems, the Digital Enterprise would remain a vision instead of the practical operating model it has become today. What follows is an overview of some of the key technologies and concepts that enable advanced industrial communications.

This overview can help provide both IT and OT professionals with some insight to why automation requires more deterministic data with greater network priority than that of office workers sending email. Redundancy is critical, too, to ensure high system availability. Also explained are some of the important protocols that help deliver priority data with sub-millisecond speeds. Industrial cybersecurity is also discussed.

Bottoms-up. To start, it helps to understand how automation in the Digital Enterprise works. Complex automated industrial systems used in discrete manufacturing and production processing require a DCS to operate. Organized as a hierarchy, a DCS starts by linking the various components – actuators, contactors, motors, sensors, switches and valves – that do the work at the field level (e.g., shop or production floor) to PLCs.

As mentioned previously, PLCs are micro-computers with software that monitors and controls the operations of these devices, such as turning motors on or off and opening or closing valves. PLCs can also control the motion of industrial robots, but require precise data timings to do so.

In turn, PLCs are connected to a HMI, typically a display of some kind that enables human operators to monitor overall system performance and component behaviors, then if necessary, adjust parameter set points. Many modern PLCs, such as Siemens SIMATIC S7 models, have built-in web servers. These enable the HMI to be securely displayed and the DCS accessible remotely in a web browser on a laptop, tablet or smartphone anywhere an Internet connection is available.

One or many DCSs can be vertically integrated to even higher-level systems, such a manufacturing execution system (MES) or a manufacturing operations management (MOM) system. These provide much wider, even enterprise-wide, views and controls.

Redundancy, key to availability. Asset utilization is tied to availability – the higher the availability of machinery, for example, the greater the asset utilization. The consequences of a system failure can be costly downtime, high restarting costs and the loss of valuable data or materials. That's why OT engineers have designed redundant control systems and redundantly configured networks.

In the event of a fault, a plant's high-availability industrial communication can take over automatically without any consequences for the facility. For example, to achieve the extremely fast response times industrial companies require, Siemens SCALANCE and RUGGEDCOM switches and other components have for many years used standardized network redundancy procedures. These support reconfiguration times of a few milliseconds in the event of a fault.

In general, there are two types of redundancy:

- **System redundancy:** A high-availability automation system is implemented by deploying backup systems and communication components that operate in parallel with failover to them if the primary system goes down;
- **Media redundancy:** Systems are only implemented individually, but should the network be interrupted, the plant will continue to operate along substitute communication paths.

While IT professionals are likely familiar with how system redundancy works, they may be interested in understanding more about media redundancy in an industrial context. There are a range of approaches to implement media redundancy, but two of the leading ones are PROFINET compliant MRP (Media Redundancy Protocol) and HRP (High-speed Redundancy Protocol). In fact, Siemens pioneered these protocols.

Based on IEC 62439-2, MRP enables rings of Ethernet switches to overcome any single point of failure with near instant recovery times. Operating at the MAC layer of the Ethernet switches, MRP uses redundant rings and ensures reconfiguration (relearning of the communication paths) times of 200 ms in rings of up to 50 switches. For smaller rings, the worst-case recovery time scales down.

To eliminate reconfiguration time, there is an extension to the MRP protocol – Media Redundancy for Planned Duplication (MRPD) – for sending message frames in duplicate within a ring structure, leveraging PROFINET IRT to do so. Standard recovery for MRPD is 0 ms.

The HSR (High availability Seamless Redundancy) protocol based on the IEC 62439-3 standard, utilizes double transmission of message frames over ring-topology networks in both directions. In the event of an error, the message frame will be transmitted without any delay. No reconfiguration time is necessary for the network, as is the case for most other redundancy protocols.

The PRP (Parallel Redundancy Protocol), again based on IEC 62439-3, also uses double transmission of message frames but it does so over two separate networks. Network access points connect up to two network segments or terminal devices without PRP functionality, without delay, over two parallel networks. This seamless data transmission offers extreme reliability and high availability in parallel networks and can be used for numerous applications, for example, in ships, energy switchgear or along pipelines.

Network segmentation. Virtual local area networks (VLANs) enable the partitioning of one physical LAN into a number of smaller, logical LANs. These help separate the networks connecting OT automation systems from IT systems, for better security and optimized real-time performance.

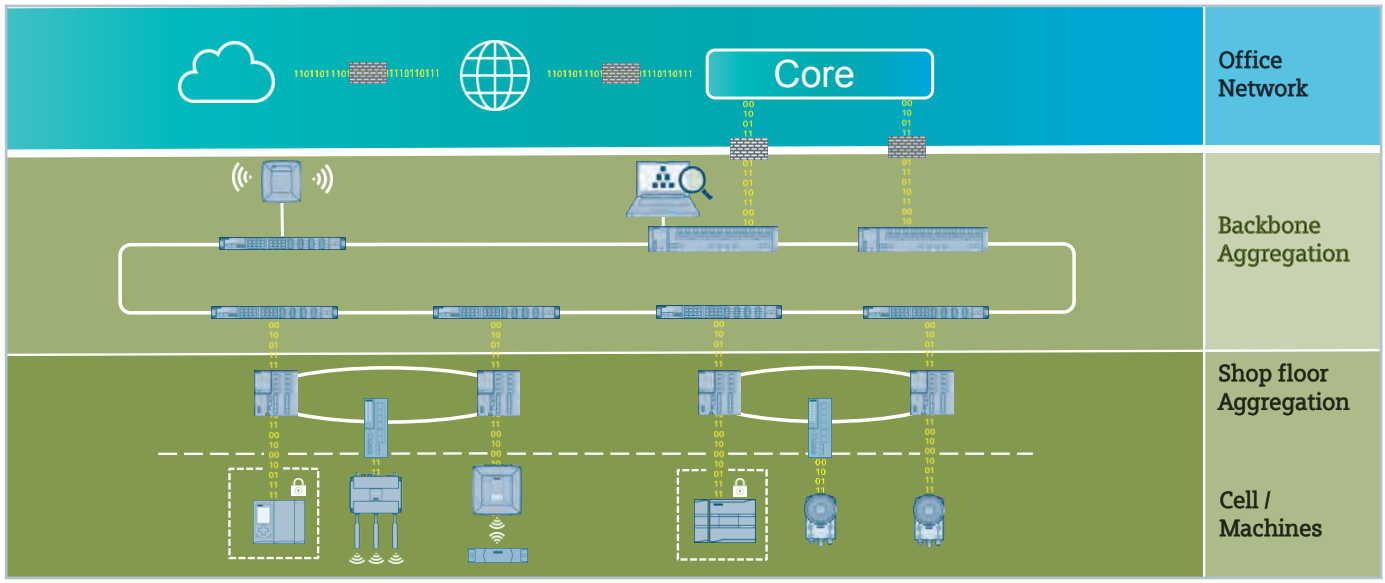
As enterprise LANs are usually maintained by a company's IT group, security concerns can override OT's concerns about maximizing uptime. But while a compromised endpoint on an enterprise LAN can generally be quickly isolated by disconnecting it from the LAN, "pulling the plug" on a compromised device that's tied into an OT automation LAN can be potentially disastrous to the system that component is part of.

With VLANs, the offending VLAN can be isolated from affecting its larger physical LAN domain, then OT can work with IT on the best way to remedy the security breach and minimize downtime and production impacts.

Another reason for using VLANs in OT environments is that the amount of real-time, broadcast and multicast data traffic OT systems typically generate using Ethernet can use most if not all available bandwidth. VLANs use OSI Layer-2 access switches to handle data traffic within a VLAN, while Layer-3 switches and routers direct data traffic across different VLANs.

Bridging IT and OT worlds. It's possible and highly desirable to interconnect the environments of IT and OT in practical, secure and accountable ways that respect the strengths and requirements of each. Following best practices, a robust network backbone should be established to create a structured and reliable interface that interconnects dedicated production and office networks.

The former will include production cell-to-machine and shop-floor-to-cell sub-networks, all with specific IP addressing for fully managed components and systems, plus the use of real-time, deterministic communication protocols. While this backbone will be an integral part of the OT production scope, especially in delivering the highest availability of product assets to the business, it will be aligned with IT in regard to user governance and security.



Connecting the IT and OT networks, with their different requirements, can be accomplished by starting with a defined backbone for the industrial side. The Cell/Machine and Shop-floor Aggregation levels are in production scope. The Backbone Aggregation level is still an integral part of the production scope but aligned with IT in regard to the interface.

A White Paper issued by: Siemens.

This way, for example, should a third-shift failure occur in off-hours, qualified and authorized production personnel can address the issue directly. And they can potentially do so much sooner than having to wait hours until an IT person arrives, according to the terms of an IT/OT service-level agreement. By minimizing the production disruption, such an approach can possibly avoid significant amounts of associated costs and risks to customer delivery commitments.

Facilitating data interchange. Highly automated production environments often have a wide variety of data communication interfaces, usually as a result of various field-level components being sourced from different manufacturers. These elements must communicate their data to – and, for many, get their instructions from – higher level control systems and HMIs. The former can include SCADA and manufacturing execution systems; the latter can include HMI panels, web interfaces, PCs, tablets and even smartphones.

So, how can data be exchanged effectively and efficiently across such heterogeneous communications landscapes? One approach is OPC Unified Architecture (UA) This a manufacturer-independent standard that allows field devices to communicate with each other. OPC UA can be used in all Ethernet networks thanks to its underlying TCP/IP communication protocol. In particular, OPC UA and PROFINET are fully compatible, enabling parallel operation.

Wireless, near and far. Wireless industrial communications, especially for wireless local area networks (WLANs), are fast becoming as ubiquitous in factories, warehouses and other production and logistics facilities as they are in non-industrial environments. Reasons include greater flexibility and speed in configuring (and re-configuring) floorplans and the elimination of long lengths of costly cabling.

Wireless industrial communications includes low-power, short-range Near Field Communication (NFC) technology used in Radio Frequency Identification (RFID) solutions for product authentication and asset tracking, among other NFC applications. Another NFC use is for machine diagnostics. Bluetooth can be used for relatively simple, close-range applications, usually in a symmetrical configuration by pairing two Bluetooth devices.

For longer range wireless communications of up to 300 feet between access points, IEEE 802.11 WiFi is most widely deployed. Compared to Bluetooth, WiFi has an asymmetrical client-server connection with data routed through a wireless access point. For specific directional applications, for applications that require a defined path, like monorails, cranes and automated guided vehicles, RCoax radiating cable emits a radial field along the axis of the cable, which can be laid in a floor or along overhead rails.

Beyond that are IEEE 802.16 WiMAX with a radius up to 30 miles; 3G and 4G LTE cellular, with coverage of up to depending on cell tower coverage over a specified geography. And, from the sky are geostationary satellite communications (also known as fixed satellite service, or FSS) used mostly for remote data telemetry; and, for more bandwidth, VSAT (very small aperture terminal) technology like what satellite TV uses, can provide wide-area coverage for maritime and land-based remote communications needs.

SCALANCE, RUGGEDCOM and Totally Integrated Automation

The Siemens SCALANCE industrial communications portfolio offers solutions for diverse industrial applications. It features:

- **SCALANCE X fast Ethernet switches**
- **SCALANCE W wireless LAN devices**
- **SCALANCE M modems and routers**
- **SCALANCE S security modules**

Most components are plug-and-play and most are self-configuring, with built-in diagnostics, all to ensure quick and easy network configuration and management.

As part of the Siemens Totally Integrated Automation (TIA) portfolio, SCALANCE products needing programming and configuration can have that done via the Siemens TIA Portal. This is a common engineering framework proven to save as much as 30 percent or more in project time.

Siemens RUGGEDCOM networking products are designed, engineered and built for even higher reliability levels required by harsh environments. Products include Ethernet Layer 2 and Layer 3 switches and routers, wireless devices and systems, media converters and more.

Ruggedization for reliable performance is the biggest differences in the components for industrial WLANs compared to non-industrial ones. They need to withstand temperature extremes, adverse weather and corrosive conditions that are typical of industrial environments. Within the Siemens SCALANCE and RUGGEDCOM portfolios are many examples of components with ruggedization designed, engineered and built into them, instead of being layered on.

Meet the digital thread. Of course, what ties together all these devices and systems is industrial data communications, the digital thread referenced earlier. These have come long way since early point-to-point, wired protocols such as analog 4-20mA current loop or analog/digital HART communications, both still widely used despite their limited communications capacity, including relatively slow data speeds.

In time, however, multipoint, digital fieldbus protocols emerged, such as PROFIBUS, one of eight fieldbus types described by the global IEC 61158 standard. These enabled local area network (LAN)-type connections to be used to link up to hundreds of devices. This tremendously simplified cabling and lowered its cost.

Today's industrial networks are quickly migrating to industrial Ethernet, which provides greater performance, higher speeds and more flexibility than fieldbus communications. It's based on the same Ethernet used in non-industrial IT networks, both wired (IEEE 802.3) and wireless (IEEE 802.11) protocols, but has been enhanced for the deterministic routing and real-time control that automation requires.

PROFINET, a top protocol. More than 20 different types of industrial Ethernet exist, each defined largely by how it implements determinism and real-time control capabilities. Siemens helped pioneer PROFINET, which is an open industrial Ethernet standard promoted by PROFIBUS and PROFINET International, with 1,400 member companies worldwide. PROFINET is considered the leading protocol that has two types depending on automation requirements:

- **PROFINET RT** (Real Time), the most popular industrial Ethernet automation network protocol available. This provides deterministic data speeds between 1 and 10 milliseconds (ms), by bypassing the TCP/IP layers in the Open Systems Interconnection (OSI) model.
- **PROFINET IRT** (Isochronous Real Time), for faster speeds to support specific machinery requirements, especially motion control. IRT permits cycle times of up to 250 microseconds (µs). These speeds are possible via an exclusive Siemens SCALANCE technology called iPCF (industrial Point Coordination Function) that is based on PROFINET.

Modernizing industrial communications: Making the digital thread real

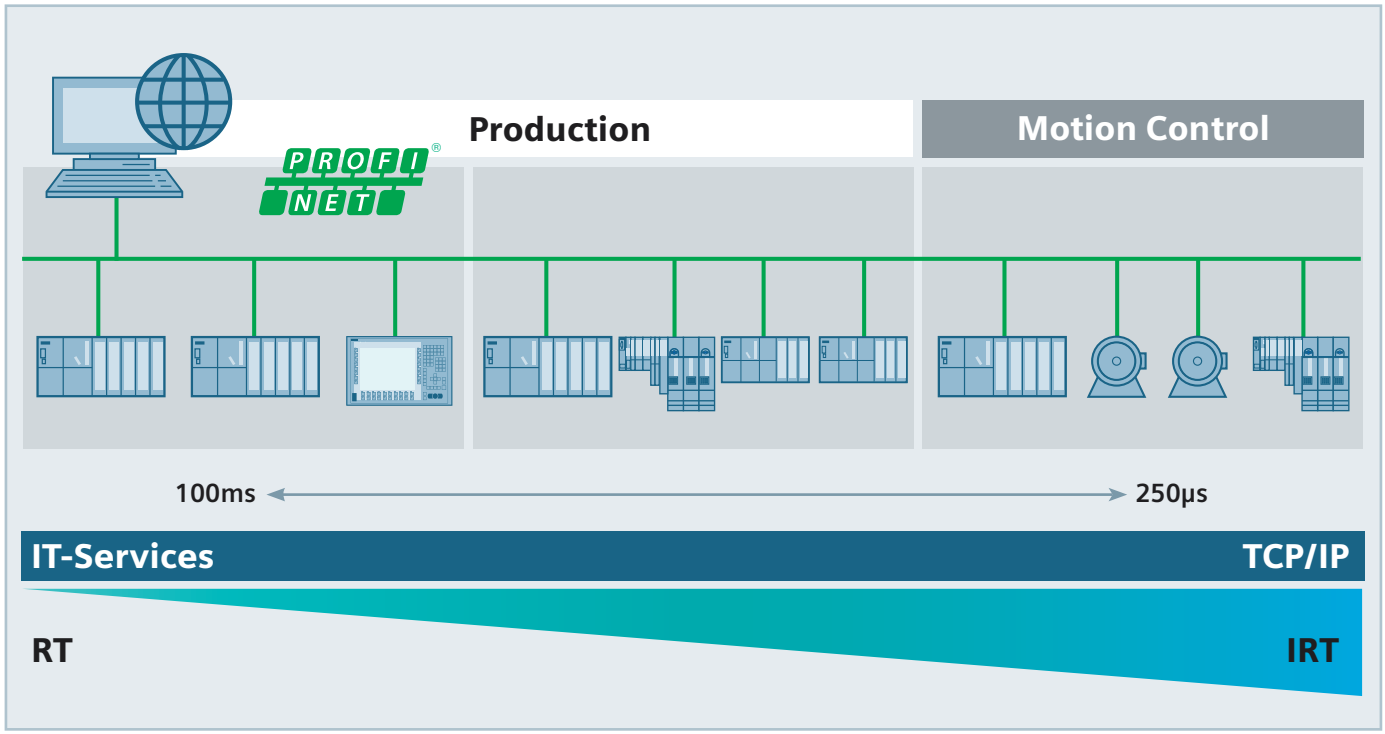
Today and in years to come, Digital Enterprises supported by advanced industrial communications and backed by fully aligned IT and OT teams will enjoy distinct competitive advantages over those without.

With a vibrant, coherent thread of data running end-to-end through their operations, companies can execute their business strategies faster, gain performance feedback and insights sooner, respond to market changes and opportunities more quickly, and improve their time to market with new products and services.

Another benefit of modernized industrial communications is simplification. This can help lower both capital costs and the management overhead and expenses required for operating highly integrated networks spanning both IT and OT environments. It can also vastly improve the reliability, visibility and security of dynamic OT landscapes to boost availability and, ultimately, asset utilization.

Siemens has strong legacy roots in both providing IT and OT solutions as well as bridging their differences to ensure our solutions offer customers the best of both worlds. A fully Digital Enterprise needs the expertise of both IT and OT teams to make it happen, enabled then with the connectivity that advanced industrial communication technologies can offer.

The sooner companies with such aspirations move forward to modernize their industrial data networks, the sooner they will realize the benefits of being a true Digital Enterprise.



The right industrial Ethernet can ensure reliable cycle times even across large networks.

A White Paper issued by: Siemens.

Published by
Siemens Industry, Inc. 2017.

Siemens Industry, Inc.
5300 Triangle Parkway
Norcross, GA 30092

For more information, please contact
our Customer Support Center.
Phone: 1-800-241-4453
E-mail: info.us@siemens.com

usa.siemens.com/industrial-communication

Order No.: NTWP-CNTVY-0917
Printed in U.S.A.

A White Paper issued by: Siemens.