TECHNICAL BRIEF

Advanced, Secure Networks: Strategic Backbones of Digitalization.

usa.siemens.com/industrial-networks

In recent years, rapid technology advancements have given rise to the industrial Internet of Things. Among them are cloud computing and storage, Big Data, and advanced analytics. But what makes it all work is secure, deterministic connectivity. That's why industrial enterprises wishing to pursue end-to-end digitalization of their operations must consider networks to be the strategic backbones of their operations.

Without these networks, modern industrial enterprises would come to a standstill. To support users in offices and remote locations, they need to connect large, strategic assets and capabilities consisting of sophisticated informa-tion technology (IT). Among them are enterprise resource planning (ERP) systems, customer relationship manage-ment (CRM) systems, big data analytics, and other core applications residing in either data centers or the cloud. Data and network security and access are paramount to prevent hacker intrusions and compromised data integrity and privacy.

And, to keep production running, they need to ensure the secure, interconnected operation of complex operational technology (OT) landscapes. These start at the field level, operating in real time and often in extreme environments. They include potentially thousands of sensors, actuators, valves, instrumentation, and other devices, usually from many different vendors. That's not to mention their constituent machinery and even conveyor systems, also from diverse sources. Meanwhile, all these components must feed and draw operational data into and from dynamic, vertical infrastructures consisting of a wide range of controllers, operator systems and manufacturing execution systems.

Unfortunately, many industrial enterprises have built their networks as components of their IT/OT infrastructure, adding networks or extending networks as needed.

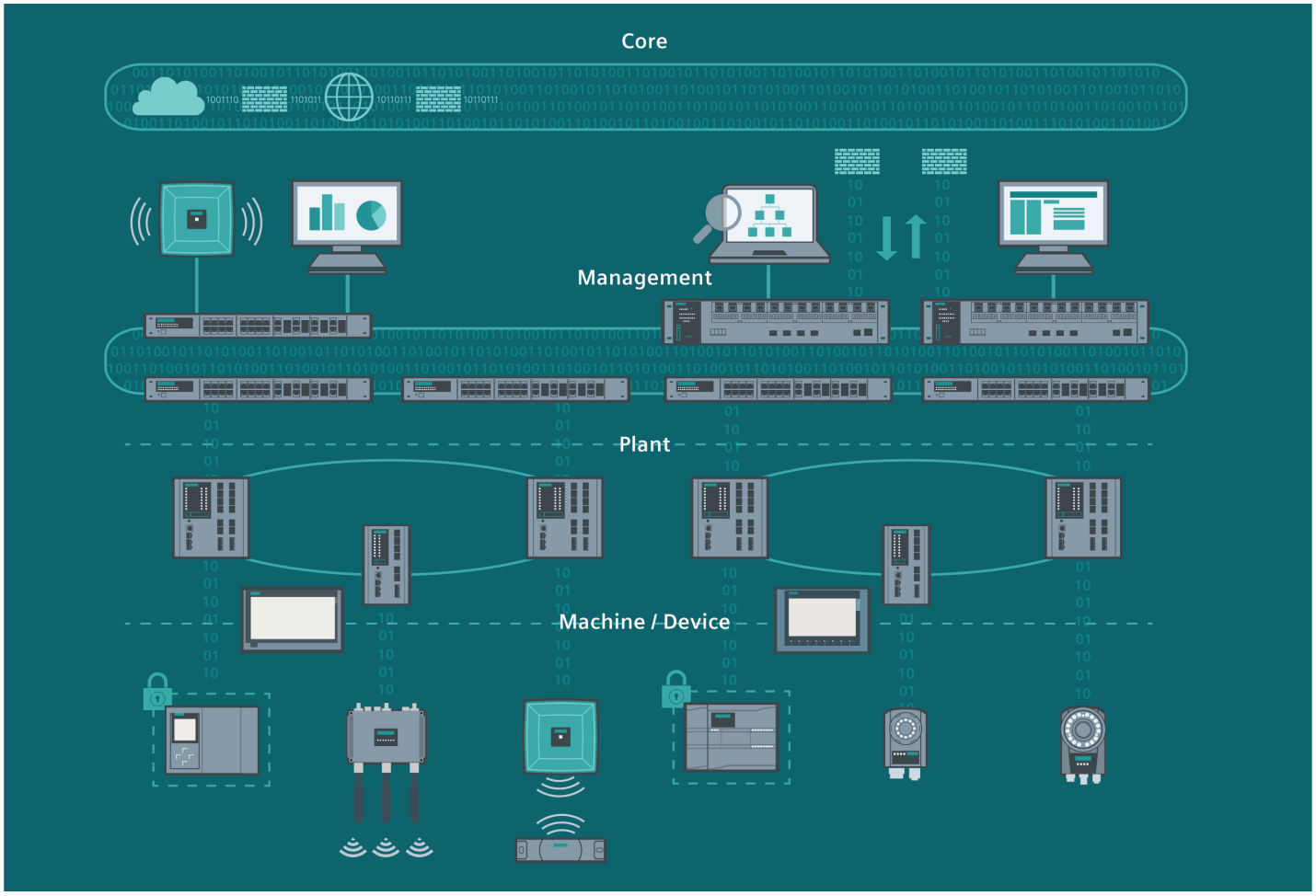
The result has been a patchwork of sub-optimal network segments, creating information islands that can prevent true, end-to-end digitalization. Worse, a fragmented network topology can expose operations to security vulnera-bilities that hackers can exploit to gain access to critical assets and data, both on or off the shop floor.

OT network requirements, far beyond IT demands But to build a network that is truly the strategic backbone that supports digital thread of data running seamlessly through an industrial enterprise, both IT and OT teams must collaborate to ensure office and production requirements are met. The latter will always be much more demanding, especially deterministic data prioritization.

That's when the data of a control command, for example, must get to its destination with precise, millisecond timing, to open or close a valve or to start or stop a motor.

SIEMENS

Designing an Industrial Network as the Strategic Backbone of the System



Connecting the IT and OT networks, with their different requirements, can be accomplished by starting with a defined backbone for the industrial side. The machine and plant-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.

At a macro level, many industrial facilities, such as utilities, public communications, and transportation systems, must operate 24/7/365, in real- or near-real time and with 99.999 percent uptime or better. Reliability, durability, and availability are critically important. Life safety can be at stake. Safety incidents and non-compliance with regulatory requirements can also incur costly fines.

In contrast, enterprise IT networks can operate on a best-effort basis, with data latencies many orders of magnitude higher than what OT networks can allow. Office users won't notice one or two second delays in sending an email or accessing a database, but such delays can cause costly production disruptions, possibly endangering personnel, the environment, or both.

Building networks as strategic backbones for digitalization

Complex, automated production systems require a distributed control system (DCS) to operate. Organized as a hierar-chy, a DCS starts by linking diverse small components and machines that do the work on the production floor to programmable logic controllers (PLCs). The PLCs, in turn, link to human-machine interfaces (HMIs), interactive displays through which human operators can monitor and adjust performance, as needed. One or many DCSs can be vertically integrated to even higher-level systems for overall production management and visibility.

To efficiently and securely move data deterministically, modern industrial communications use sophisticated data-prioritization and security techniques, such as:

Multicasting. The Internet Group Management Protocol (IGMP) enables devices, routers, and switches on an OT network to reliably transmit critical data on a one-to-many or many-to-many basis. Also, the global OPC UA communi-cations standard can link between machines from different vendors.

Redundancy. In general, two types of redundancy can support reconfiguration times of a few milliseconds or even microseconds in the event of a fault.

- **System redundancy:** Backup systems and communication components that operate in parallel with primary systems, which failover to them if the latter goes down.
- **Media redundancy:** Should the network be interrupted, the plant will continue to operate along substitute communication paths. Two leading protocols are PROFINET-compliant MRP (Media Redundancy Protocol) and HSR (High-availability Seamless Redundancy).

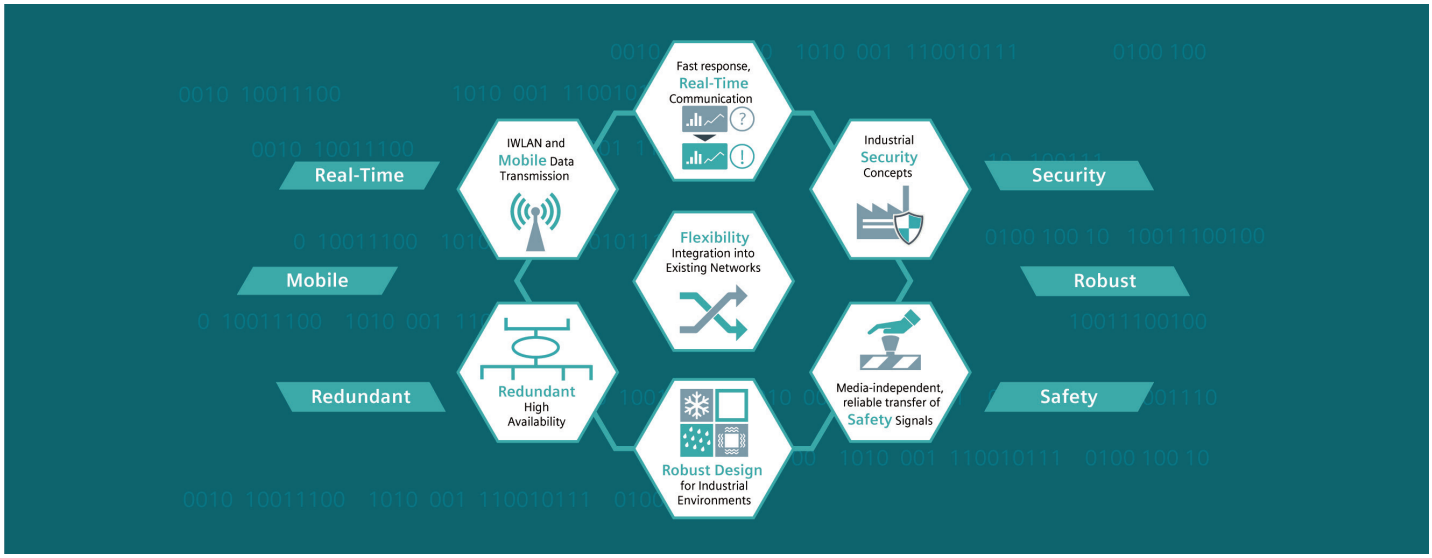
VLAN segmentation. Virtual local area networks (VLANs) can partition one physical LAN into a smaller, logical LANs. These separate networks connecting OT automation systems from IT systems, for better security and optimized real-time performance. OSI Layer-2 access switches handle data traffic within a VLAN, while Layer-3 switches and routers direct data traffic across different VLANs.

T/OT collaboration, the key to strategic backbone networks
Collaboration of IT and OT teams is the key to interconnecting each one's environment over a strategic backbone network in practical, secure and accountable ways that leverage their respective strengths and meet their requirements. This collaboration can provide the "best of both worlds" to facilitate end-to-end digitalization needed for quantum gains in operational efficiency, visibility, flexibility and security.

With expertise in providing IT/OT solutions and facilitating IT/OT collaboration, Siemens can help industrial enterprises of all sizes to design, deploy, and operate advanced networks spanning both environments. Ultimately, fully digitalized industrial enterprises, supported by well-aligned IT and OT teams, will benefit from dynamic threads of data running throughout their operations.

On the enterprise IT side, they'll be able to execute 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. On the OT production side, they'll improve the reliability, visibility and security to boost machine availability and utilization. Together, they will enjoy competitive advantages over companies that don't consider networks to be the strategic assets they are.

The Unique Requirements for Powerful, Flexible Industrial Networks



Industrial networks communication and data integration over the entire value chain have specific requirements that must be met in order to ensure a successful design and implementation.

Published by
Siemens Industry Inc.

Siemens Industry, Inc.
100 Technology Drive
Alpharetta, GA 30005
United States of America

www.usa.siemens.com/industrial-networks

Order No. NTAR-NTBKB-0422

SIEMENS