TECHNICAL BRIEF

# **Not all Data are Equal:** Understanding the types of data on your network and how to manage each of them

**usa.siemens.com/industrial-networks**

**As more and more industrial companies seek to become truly end-to-end Digital Enterprises spanning production, office, and remote working domains, a key fact should become clear: Networks are the backbones for their ambitions. In effect, the data running over their networks act as digital threads tying operations together across those domains. In these threads, however, not all data are equal.**

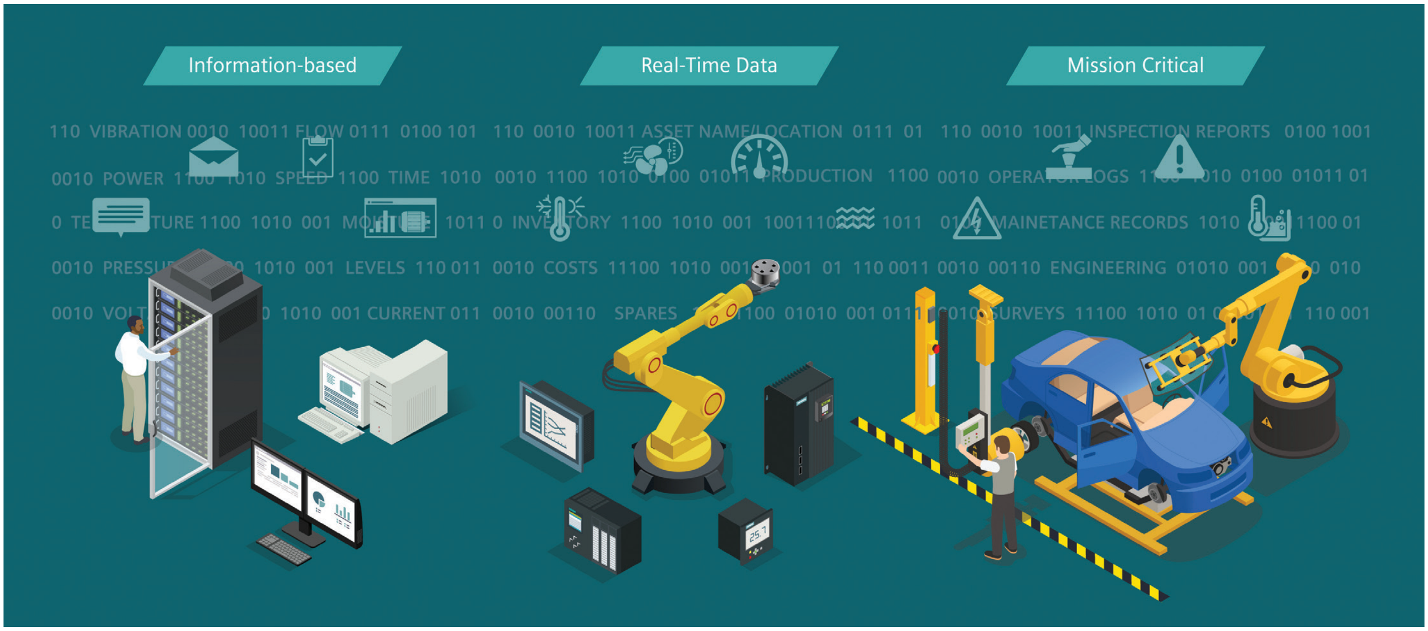
Some data, especially in industrial operations, must be prioritized over others. Otherwise, operational performance and asset availability can be compromised. Worse, costly and potentially life-threatening production disruptions can occur. These can lead to grave injuries, litigation, regulatory fines, missed commitments, and tarnished brand reputations.

Even more so, when considering infrastructure operations, such as bridges and tunnels or our energy grid, the repercussions of downtime extend beyond just a facility and can affect the masses with potential catastrophes like inaccurate messaging and signaling or wide-spread power outages.

This is why IT (Information Technology) and OT (Operational Technology) teams must collaborate more than ever to ensure their networks are designed both to prioritize certain data over others and to provide resiliency and availability to transmit data where it needs to go.

SIEMENS

# Turning Big Data into Actionable Data using a Network Prioritization Model




Industrial data sources can include all types of machines, equipment and devices that by themselves are not specific enough to take action on. It is the combination of connectivity, selective blending and advanced analytics that are key to understanding and gaining value from the data.

**While computer scientists and programmers distinguish data by whether packet payloads carry text, numbers, or some sort of multimedia, Siemens takes a practical view. We see three types of data, depending on their context and criticality, each requiring specific network prioritization:**

**1. Information-based.** *Does the data deliver information within user-acceptable latencies of 100 milliseconds (ms) or more? Is the data thread, from source to receiver, available 99.9 percent of the time or better, with no more than 8 hours of downtime during a year?*

This data type typically travels over enterprise IT networks and constitutes emails, file retrieval and sharing, database requests, application responses, and so forth. In most companies, voice-over-IP (VoIP) technology also uses informa-tion-based data to provide person-to-person communications and group conferencing.

In all these use cases, data packet routing can be "best effort" with packets re-sent as needed to meet quality of service (QoS) specifications. QoS, as defined by latency, jitter, and loss, is managed by network designs using settings and topolo-gies that have proven themselves over the years.

Typically, if network hiccups occur, users don't perceive delays in packet delivery. For example, if a file is sent to an office printer and gets held up for even a few seconds, most users won't know it. However, users of voice and conferencing applications will certainly know if VoIP QoS specs are not being met, which is why its data gets prioritized over other information-based data.

Enterprise IT networks are not only found in office environments, but also overlaying plant floors and warehouses. This way, plant personnel can securely communicate and access information just as their colleagues in offices or working remotely can.

In some cases, information-based data can be transmitted over external industrial networks set up for specific applications and operating in non-real-time over cellular, wide-area networks, and even satellite networks. One example is a remote lift station pumping wastewater to a municipal treatment plant. Because its data is not time-critical to operations, it can send data to a centralized control server in periodic batch modes at low baud rates that consume little bandwidth.

**2. Real-time.** *Does the data deliver operational information, such as counting, condition parameters, and control commands, with minimal latencies, usually less than 20 ms, on a consistent basis without jeopardizing operations? Is the data thread available 99.99 percent of the time, with no more than 48 minutes of downtime during a year?*

The real-time data distinction is that it supports time-sensitive, production operations. For example, cyclically executing process programs need input data constantly updated in real time to issue control commands to compo-nents. Robots and roaming automated guided vehicles (AGVs) must also have real-time data to do their jobs effectively and safely, as do all networked plant safety systems.

Real-time data requires a consistent and predictable, or deterministic, network for continued and uninterrupted production. Additionally, to support the latency needs of real-time data, sometimes in milliseconds, or even microsec-onds, this data must be prioritized over information based data.

OT networks serve as the backbones of complex, mixed-technology landscapes at the field leve cluding sensors, PLC's, relays, actuators, valves, instrumentation, and other devices. These components must function with precise, deterministic settings, often in harsh operating conditions. Plus, these elements feed and draw operational data into and from a dynamic, vertical infrastructure consisting of a wide range of data concentrators, signal controllers, edge computers, and system-wide control systems.

Packet delays can trigger equipment faults, which can lead to unplanned production downtime, sometimes of surprisingly long duration and cost. Plants involved in continuous processing, for example, can take hours to bring back up to speed and required temperatures. Feedstocks and work-in-progress may have to be scrapped. Cleaning of equipment and plumbing may be needed, too. Unplanned shutdowns can also damage sensitive equipment, requiring service, repairs, or replacements, any of which can add time to bringing production back online.

**3. Mission-critical.** *Does the data deliver information required in real time to operate equipment and systems without which potential catastrophes could occur? And is the redundancy supporting these digital threads sufficient to provide 24/7/365 availability with virtually no downtime at all?*

Mission-critical data supports key infrastructure, such as public communica-tion networks, the energy grid and its constituent utilities, nuclear plants, oil and gas operations, transportation systems, and military applications, to name a few. These must operate around the clock, in real- or near-real time and with 99.999 percent uptime or better.

Reliability, durability, and availability of this data type are of the highest importance, which is why its packets must be given highest priority of all data traveling over a shared network. In addition, these networks must be designed with immediate failover resiliency along with sufficient redundancy to ensure that resiliency. This way, chances of equipment faults can be minimized, if not eliminated. For example, protective relays in high-voltage, electric power substations, are one of the most crucial devices in the substation environment. Not only does a single relay need to be resilient to the environment around it, but multiple relays must be able to communicate to one another, process data, and operate in real-time. These real-time protection schemes are mission critical due to the requirement for protection of high-dollar assets, fault detection and recovery of the power grid, and other critical operations for the consistent and reliable delivery of electricity to consumers.

### The Importance of the Right Network

Of course, any of these data types are useless without reliable, secure network backbones to deliver their packet payloads within QoS specifications. Network availability starts with fail-safe network components that have industrial ruggedness engineered and built-in, such as what Siemens RUGGEDCOM devices offer.

Next comes data traffic shaping through intelligent network designs, especially segmentation via subnets, either physical or virtual ones. Flat networks typical of enterprise IT networks can make OT networks vulnerable to intruders, broadcast storms and other disruptions.

Finally, OT network performance can be further improved with enhanced capabilities like Siemens iCPF (industrial Point Coordination Function) for efficient polling available in the SCALANCE portfolio of wireless access points, as well as Siemens eRSTP (enhanced Rapid Spanning Tree Protocol) available in RUGGEDCOM switches for network redundancy.

If companies with sights set on becoming Digital Enterprises needed just one mission for their OT and IT teams to collaborate on, it would be this: To ensure proper data prioritization on their networks, whether the data is information-based, real-time, or mission-critical. Doing this together will make giant strides toward safeguarding the availability of production assets, while maximizing their availability and performance.

**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-NDATA-0422




SIEMENS