It's About Time: Evolving Network Standards for the Industrial IoT

The Industrial Internet of Things (IIoT) promises a world of smarter, hyper-connected devices and infrastructure where electrical grids, manufacturing machines, and transportation systems are outfitted with embedded sensing, processing, control, and analysis capabilities.

Once networked together, they'll create a smart system of systems that shares data between devices, across the enterprise, and in the cloud. These systems will generate incredible amounts of data, such as the condition monitoring solution for the Victoria Line of the London Underground rail system, which yields 32 TB of data every day. This Big Analog Data will be analyzed and processed to drive informed business decisions that will ultimately improve safety, uptime, and operational efficiency.

Though much of this raw, unprocessed data is not time critical and can be passed between network layers and subsystems with little regard for latency or synchronization, there is an entire class of mission-critical, time-sensitive data that must be transferred and shared within strict bounds of latency and reliability. This includes critical control and fault detection data that must be processed, shared, and acted upon immediately, regardless of other network traffic.

Much of today's network infrastructure is not equipped to handle such time-sensitive data. Many industrial systems and networks were designed according to the Purdue model for control hierarchy in which multiple, rigid bus layers are created and optimized to meet the requirements for specific tasks. Each layer has varying levels of latency, bandwidth, and Quality of Service, making interoperability challenging and the timely transfer of critical data virtually impossible. In addition, today's proprietary Ethernet derivatives have limited bandwidth and require modified hardware.

To support the new capabilities of IIoT-enabled infrastructure, designers and end users alike need reliable, remote, and secure access to smart edge devices. Network technologies must evolve to satisfy the requirements of these next-generation industrial systems and radically advance the way we operate our machines, electrical grids, and transportation systems.

TSN: The Time is Now

Existing IT networks are defined by IEEE 802 standards, which specify requirements for different Ethernet layers and functions and ensure interoperability between devices. Today, industrial suppliers, IT vendors, and silicon providers are collaborating within IEEE 802 and the recently formed AVnu Alliance to update standard Ethernet protocols and provide bounded, low-latency data transfer for time-critical data in IIoT applications.

> "Organizations like AVnu and the Industrial Internet Consortium are facilitating the expansion of Ethernet capabilities through standards. The broad market expansion of TSN will benefit numerous industries and applications and will be critical to achieving the vision of IoT with 50 billion connected devices."
>
> —**Paul Didier**, AVnu Alliance Board Member and IoT Solutions Architect, Cisco

This next-generation standard, called Time-Sensitive Networking or TSN, addresses existing network shortcomings. The AVnu Alliance, working with companies such as Broadcom, Cisco, Intel, and NI, will drive the creation of an interoperable ecosystem through certification, similar to how the Wi-Fi Alliance certifies products and devices to be compatible with the IEEE 802.11 standard. The new TSN standard will provide numerous benefits, including the following:

Bandwidth—Large data sets from advanced sensing applications such as machine vision, 3D scanning, and power analysis can put a strain on network bandwidth. Proprietary Ethernet derivatives commonly used for industrial control today are limited to 100 Mb of bandwidth and half-duplex communication. TSN will embrace standard Ethernet rates and support full-duplex communication.

Security—Most of the lower-level field buses used today achieve security through air gap and obscurity. They are influenced by the automotive industry, for which air-gapped and closed CAN networks carry all the control and operational data. But recent security breaches have exposed the need to fully extend security into the critical lower levels of control infrastructure. TSN protects critical control traffic and incorporates top-tier IT security provisions, while segmentation, performance protection, and temporal composability can add multiple levels of defense to the security framework.

Interoperability—By using standard Ethernet components, TSN can integrate with existing brownfield applications and standard IT traffic to improve ease of use. TSN inherits many features of existing Ethernet, such as HTTP interfaces and web services, which enable the remote diagnostics, visualization, and repair features common in IIoT systems. As an added benefit, leveraging standard Ethernet chipsets drives component cost down by virtue of high-volume, commercial silicon.

Latency and Synchronization—TSN prioritizes the low-latency communication required for fast system response and closed-loop control applications. It can achieve deterministic transfer times on the order of tens of microseconds and time synchronization between nodes down to tens of nanoseconds. To ensure reliable delivery of this time-critical traffic, TSN provides automated configurations for high-reliability data paths, where packets are duplicated and merged to provide lossless path redundancy.

The Future Will Arrive on Time

As IIoT adoption continues, increased amounts of data and widely distributed networks will require new standards for sharing and transferring critical information. Just as an ambulance or a fire engine receives priority among other traffic during an emergency, the TSN standard ensures that critical, time-sensitive data is delivered on time over standard network infrastructure. Welcome to life in the fast lane with the IIoT.

STANDARD IT AND TIME-SENSITIVE DATA CONVERGE TO CONNECT DEVICES AND THE ENTERPRISE