

Choosing the right plant-level Industrial Ethernet protocol

Ethernet dominates industrial automation communications, but users must choose the best industrial protocols for use at various architecture levels. Contextualization is key to transporting raw OT data. Object-orientation promotes consistency and efficiency, and compatibility with the latest programming languages.

INDUSTRIAL AUTOMATION APPLICATIONS RELY on connectivity from the lowest to the highest levels. The most basic field connections are hardwired I/O points, which over the years have been supplemented and even superseded by industrial fieldbuses. Other networks and protocols are more suitable for communications between higher level automation elements.

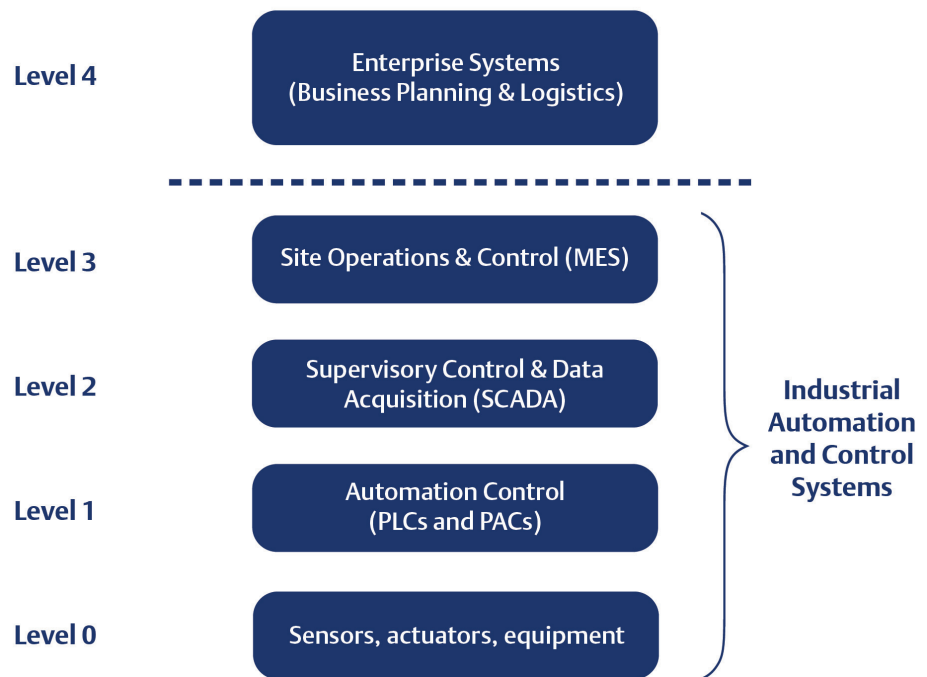
A significant advancement over the past decade has been the increasing use of Ethernet for industrial connectivity. Ethernet has emerged as a clear leader over many options, but even though this seems to simplify the issue, end users must still choose the right industrial Ethernet protocols.

Installations may require multiple protocols depending on the application and where each protocol is to be used within an automation systems architecture. Some industrial Ethernet protocols have deep roots and are mature, but many incorporate less than ideal legacy concepts. Other protocols are optimized for specific applications, such as high-speed motion. At the upper levels of industrial automation architectures, which is the plant-level networking above the controller network, there are specific requirements driving protocol selection, with a different emphasis than lower-level field device and I/O level networks.

Plant-level networks are where many different systems interact with each other, demanding a secure networking protocol which delivers rich contextual objects so the raw data is made available as useful information. This article discusses why OPC UA is an industrial protocol to consider for providing these features in a plant-level network. The OPC UA feature set makes it an effective protocol for supervisory connection to the industrial internet.

Building A Plant Network

Industrial automation systems are built from many devices and components connected or networked together. Field devices—such as sensors, actuators, and smart systems—are connected to controllers. These programmable logic controllers (PLCs) and programmable automation controllers (PACs) monitor and command the field devices, communicate with each other, and are networked to higher level



Industrial automation and control systems are architected with many levels of devices and networking.

systems for human-machine interface (HMI), supervisory control and data acquisition (SCADA), historizing, analysis, and other roles.

Industrial networking hierarchies are defined by many characteristics and are not always a precise definition because some network levels can be virtualized or collapsed together on one physical network. Here is one representation of relevant levels which must be networked within an industrial plant:

- **Level 4:** Business planning & logistics
- **Level 3:** MES, for site supervision
- **Level 2:** HMI and SCADA, supervisory control
- **Level 1:** Local PLC and PAC automation control
- **Level 0:** Field sensors, devices, and networks

Controllers can interact with field devices (and with each other) at Levels 0 and 1 using hardwired I/O, fieldbus networks, and industrial Ethernet. These connections are local to a site and are generally made up of small data packets which must be rapidly communicated because physical devices must be directly controlled in real time.

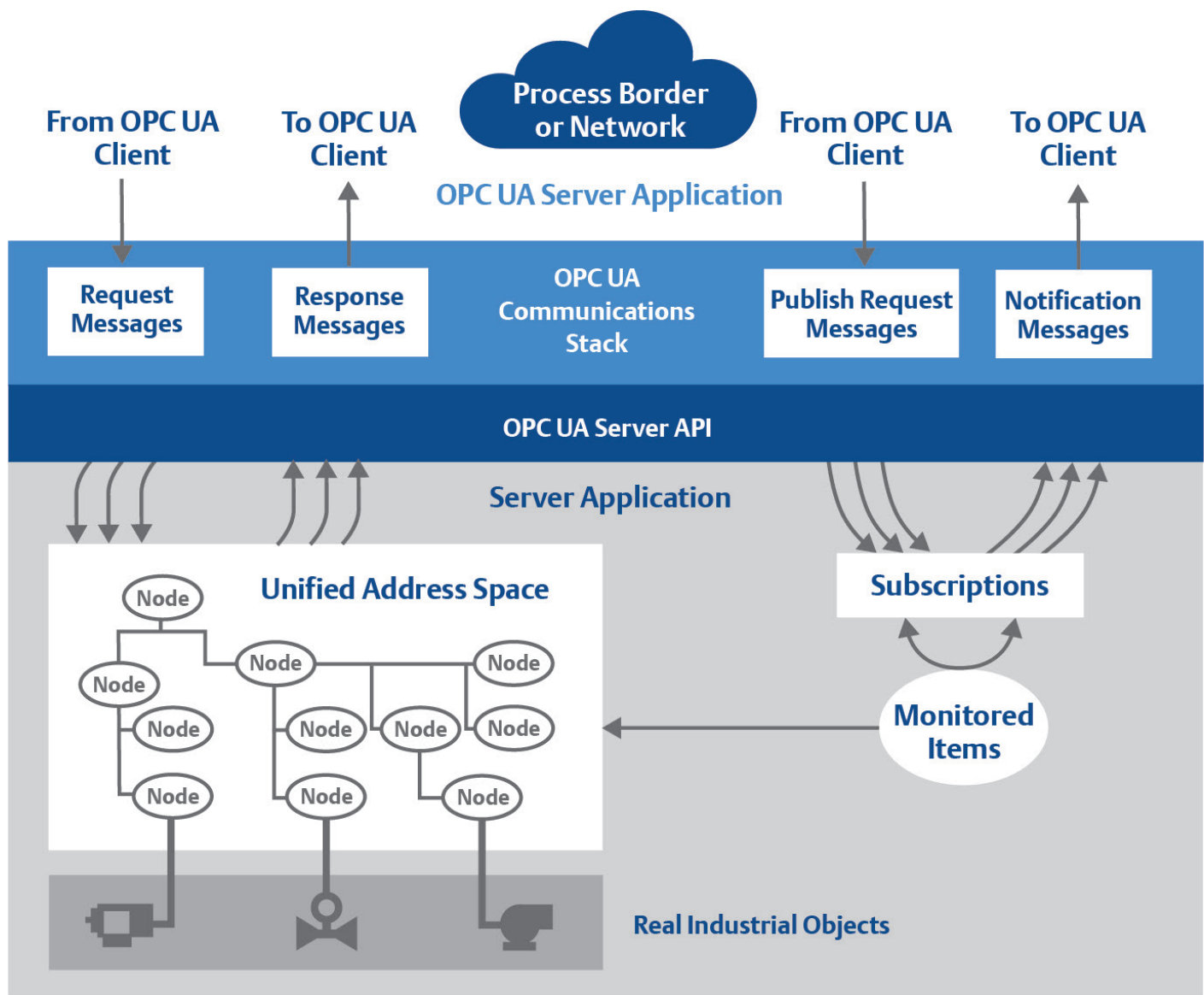
Communications above and among controllers have different needs. The industrial networks connecting Level 1 and above are sometimes collectively referred to as plant-level networks. Compared to lower level communications, plant-level data packets may have less stringent time requirements.

Plant-level networks interconnect widely varied systems compared to the more dedicated lower levels. This imposes new requirements for modern industrial plant-level network communications:

- **Secure:** Providing built-in security features
- **Contextualized and Object-Oriented:** Able to define and organize transported data
- **Platform Independent:** Enabling distributed applications to communicate seamlessly

As noted previously, Ethernet has become the physical network of choice. This is true for enterprise and business information technology (IT) applications as well as industrial operations technology (OT) systems. From a physical standpoint, Ethernet can operate using copper wires, fiber optics, and even wireless methods. What really

SOURCE: EMERSON



The OPC UA industrial communications protocol provides security and data contextualization using a platform independent architecture.

differentiates Ethernet for use in IT and OT settings is the different communications protocols that run over Ethernet.

Protocols

Adapting commercial IT Ethernet for industrial OT applications presents some challenges. Ethernet can rise to prominence for OT field networking based on the availability of good protocol choices such as ProfiNET, Ethernet/IP, and many others.

Field networking protocols are quite mission-specific for their OT roles, but the specialized nature and legacy roots of field networking protocols makes them less suitable for higher levels of the networking hierarchy. At these levels, users need protocols with greater flexibility and capability so they can interact with many system types. They prefer open solutions, but with the security provisions necessary for business and internet-facing connections.

Over the years, the OPC Foundation has

developed and maintained specifications for delivering secure and reliable interoperability. The most recent development, first released in 2008, is OPC Unified Architecture (UA).

At the Level 1 and above, OPC UA defines how information is modelled and communicated with specific security, contextualization, and object-oriented features—making it a good choice for most industrial applications. The comprehensive, modular, and scalable nature of OPC UA allows users to create a “system of systems”. That is, an integrated overall industrial automation system built from many subsystems of all sizes interacting seamlessly with each other. Clients and servers are defined as interacting partners.

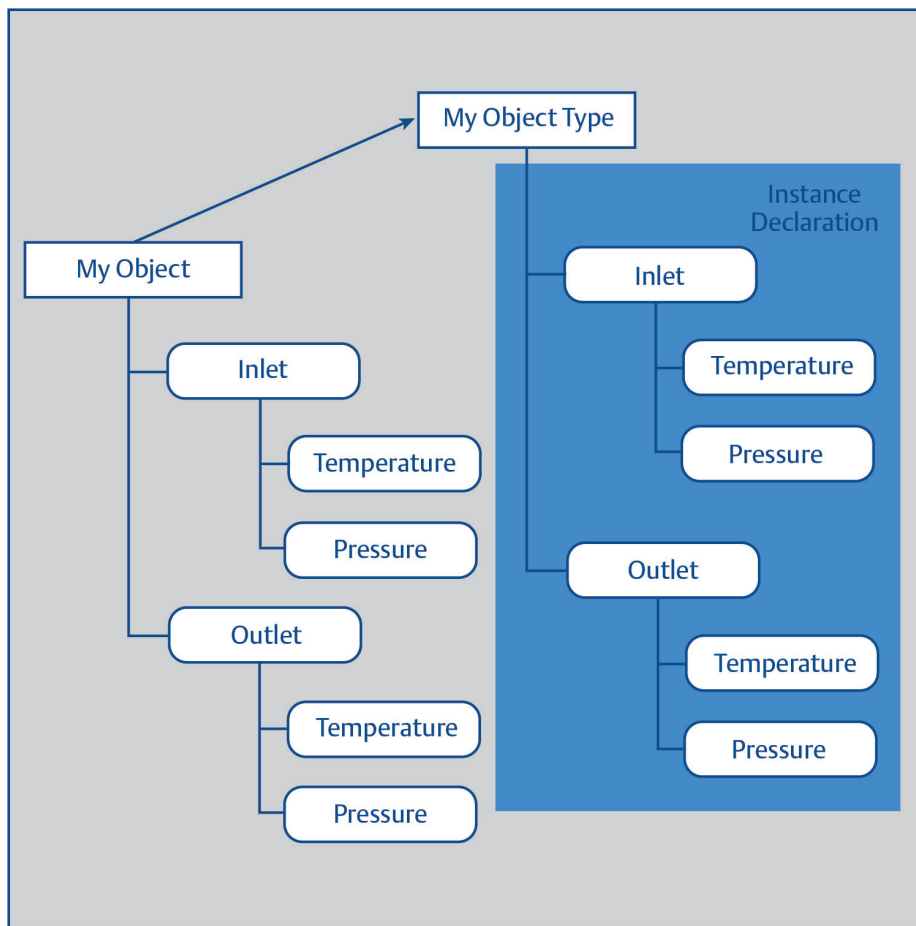
Security

As Ethernet and the internet have improved the ability for digital systems to communicate, they also have created security risks. Information security is defined by the triad of confidentiality, integrity, and availability

(CIA). Traditional fieldbus networks and earlier industrial Ethernet protocols focused on availability and integrity, with little or no consideration for confidentiality. Often this is referred to as the availability, Integrity and confidentiality (AIC) or reverse approach. Higher level networking demands a more balanced approach regardless of CIA or AIC.

Some protocols can be extended with the addition of security features like virtual private networks (VPNs) or transport layer security (TLS), although this is less than ideal. A better method is to design security constructs right into the protocol. OPC UA uses a built-in set of services for handling security certificates and establishing secure client/server sessions at the application level, channels at the communication level, and socket connections at the transport layer.

OPC UA provides native security mechanisms for clients to discover available servers, manage and distribute certificates and trust lists, and mediate with the certificate



Object-oriented techniques improve efficiency, enabling designers to create, re-use, and combine information models.

authority. OPC UA is well qualified for the role of a modern Ethernet protocol for secure industrial communications spanning Levels 0 through 4.

Context and object-orientation

Classic industrial protocols have emphasized reliable transmission of raw data. It was up to the designers to arrange the incoming data signals, and then to process these signals at the destination controllers to transform the raw data into useful information. Such processing included defining what the information was and scaling the values into engineering units, for instance.

This becomes burdensome if it must be performed at every step of a communications channel, such as from I/O signal to controller, from controller to HMI and SCADA, from SCADA to MES, and from SCADA or controller to historian.

A better method, called contextualization, calls for data to be transported with inherent semantics eliminating the need to program and configure PLCs and HMIs independently and carefully map the signals between them because the meaning of the data is understood by both collaborating applications. Contextualization lets users work using the same source data. The sophisticated self-discovery ability of OPC UA allows an

HMI configuration to navigate into a PLC configuration to obtain the desired data, with all scaling and properties inherently available in a standard format. OPC UA also supports the concept of hierarchy, which can be used by careful designers to keep the data organized in useful arrangements, much like a folder-based file system on a PC.

Contextualization enables an aggregation server to centralize the information for one or more areas of an industrial automation site. It can then serve this information to many clients for use by visualization, analytical, historian, and other applications.

Each client need only point to the node encapsulating all the needed information because the supplementary data is delivered in a structured format where data variables and properties are separated by references that define the relationship between them. This flattens the automation hierarchy to some extent and makes meaningful data available to each key stakeholder at their fingertips.

Object-oriented techniques are an organizational feature that can be used to formulate an information model and convey meaning in a standard format. For instance, a construct could represent the inlet and outlet temperatures and pressures of a pump.

Using object-oriented concepts, designers can develop best practice configurations that

can be reused. Not only that, the concept is expandable such that objects can also refer to and be assembled from other objects. Object-oriented design therefore improves efficiency and consistency.

Along with exposing information, an OPC UA server provides clients with a sophisticated set of services, including discovery services, subscription services, query services, and node management. It allows users to create object models that any client application can consume easily.

Platform Independence

OPC UA was created to remove the limitations imposed by OPC Classic, including dependence on Microsoft technology, and to address emerging requirements for security, communication across firewalls, and support of complex data structures. This allows distributed applications running on variety of platforms including real-time operating systems such as VxWorks or QNX prevalent in Level 1 real-time deterministic high-speed PLC/PACs to communicate with Level 2 systems in a seamless fashion

TSN is next level technology

Time Sensitive Networking (TSN) is a development supplementing standard Ethernet in the areas of Quality of Service (QoS), including bandwidth reservation, as well as synchronization. TSN enables determinism, security and the concept of guaranteed bandwidth crucial for demanding industrial applications while converging various standard and real time protocols into a single network. Using OPC-UA over TSN is an obvious evolution in industrial automation space to get the best of both worlds—contextualization, even more security, and guaranteed bandwidth.

OPC UA built for Industry

Designers are faced with many protocol choices when it comes to industrial automation connectivity, even though physical Ethernet is so prevalent. Sometimes they are constrained by the physical networks or digital protocols compatible with selected devices. However, modern architectures for plant-level networks demand that any communications be secure, contextualized, and object-oriented.

These exact features are built into OPC UA. The security provisions follow proven IT concepts. Contextualization is the key to transporting raw OT data to many different higher-level IT/OT systems with a framework of supporting information. Object-orientation promotes consistency and efficiency, and compatibility with the latest programming languages. Combined, these benefits make OPC UA the industrial automation communication protocol of choice.

Vibhoosh Gupta, *Emerson.*