ODVA

TECHNOLOGY OVERVIEW SERIES

Process Automation: EtherNet/IP at the Field Device Level

EtherNet/IP™
ODVA

The value of increased connectivity, including easier commissioning, troubleshooting, and asset tracking, driven by IIoT (Industrial Internet of Things) and Industry 4.0, have accelerated the transition from traditional fieldbus to industrial Ethernet. Digital transformation via Ethernet communication is now possible in process automation, including down to the field, via the introduction of the Ethernet-APL™ physical layer.

This paper presents the advantages of using the EtherNet/IP™ industrial control networking solution in process automation at the field device level. This approach enables end users to rely on a proven control technology that includes robust safety and security solutions while also being able to leverage edge and cloud analytics to gain insights into historical trends and to make predictions about future device and production status.

Introduction

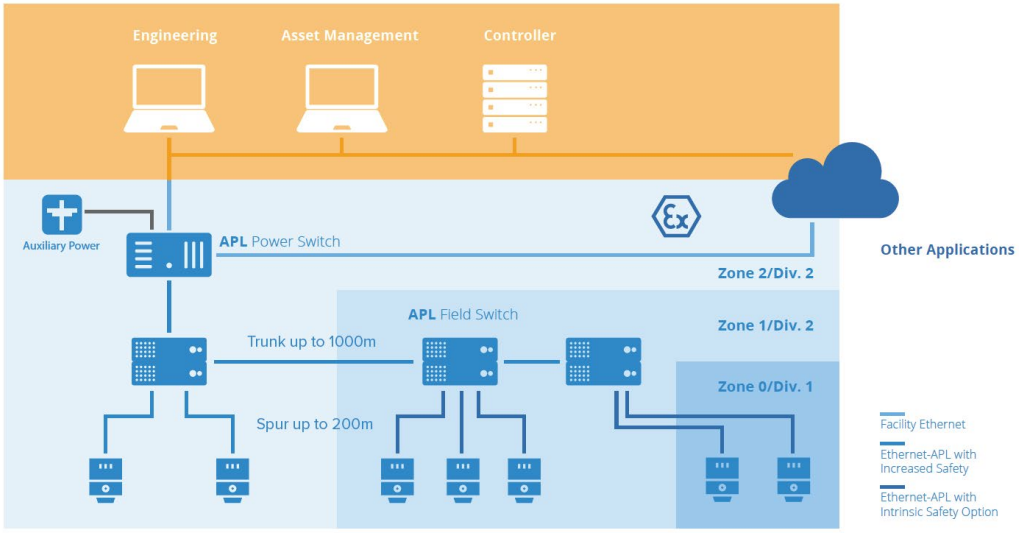
EtherNet/IP is a proven industrial control networking solution that can accommodate everything from a single controller, machine, or skid to entire facility installations across discrete, hybrid, and now process automation. Diverse industries such as automotive, semiconductor, packaging, food & beverage, pharmaceutical, water and wastewater, chemical, mining, oil & gas, and more rely on EtherNet/IP communication and control. EtherNet/IP utilizes ODVA's Common Industrial Protocol (CIP™) application layer and deploys it on standard networking technologies such as Ethernet, Wi-Fi, or 5G.

EtherNet/IP allows users to deliver the real-time, safe, secure and application specific functions that process automation practitioners require. For real-time data, users can gain unparalleled access to information from IIoT devices, allowing for visibility and insights into how operations are performing, which results in better business decisions. EtherNet/IP has become a leading industrial automation network solution in part by relying on commercial-off-the-shelf technology and standard, unmodified Internet Protocol and Ethernet made up of IEEE 802.3 combined with the TCP/IP Suite, and in turn this enables a more seamless, interconnected network for local, edge, and cloud applications. Reliable, real-time communication on the plant floor is made possible with EtherNet/IP through a properly planned network design that leverages segmentation via managed switches allowing for both efficient communication and greater security.

Although EtherNet/IP was introduced originally for discrete manufacturing, process automation specific enhancements such as Ethernet-APL (Advanced Physical Layer) and NAMUR NE 107 device status diagnostics have opened the door to the advantages of EtherNet/IP within process automation for network and device health monitoring, built in security and safety, and remote device configuration. In fact, EtherNet/IP has been named by NAMUR as one of the minimum binding requirements for the process industry.

EtherNet/IP communication networks can utilize the Ethernet-APL physical layer in process plants. Ethernet-APL is a combination of Single Pair Ethernet (SPE), engineered power, Intrinsic Safety, and Type A fieldbus cable. As a result, Ethernet-APL satisfies the process industry needs for long reach cabling of up to 1,000 meters per trunk length, powered infrastructure and intrinsic safety protection for all Class 1 hazardous Zones and Divisions. The use of 2-WISE (2-wire intrinsically safe Ethernet) to define intrinsic safety protection enables simple steps for verification without calculations, and 10BASE-T1L SPE enables dramatically increased speed at 10 Mbit/s compared to traditional process field networks. See Figure 3 for more details on SPE standards.

Figure 1: Ethernet-APL Topology and Distances



EtherNet/IP in Process Automation

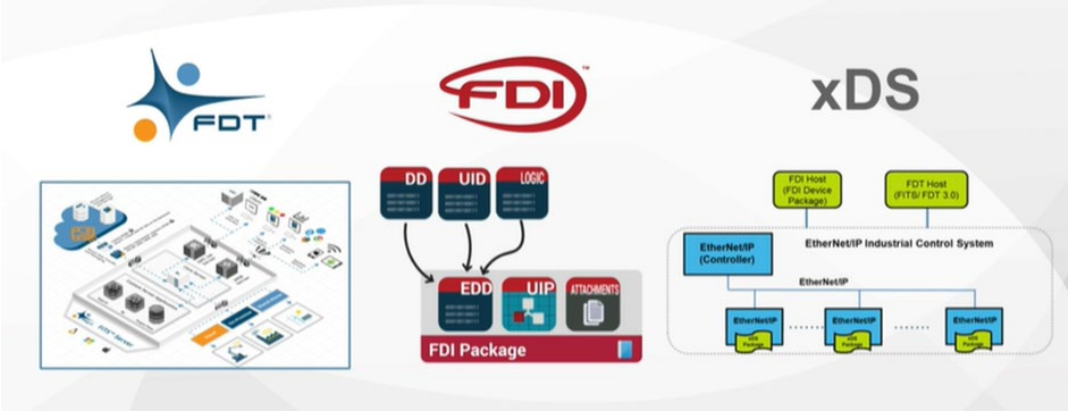
As companies digitalize in their journey to further optimize operations, EtherNet/IP is seeing sustained growth due to being a well-established automation solution that is continuously enhanced to address future advancements in industrial control and communication. With the availability of EtherNet/IP devices for the Ethernet-APL physical layer, users will be able to unlock the advantages of commercially based industrial control hardware, an IT friendly object-oriented foundation, and standard internet protocol compatibility including TCP/IP, HTTP, FTP, SNMP, and DHCP within the process industries.

It's clear that safety and security are chief concerns within process automation. These features, and more, are provided for via EtherNet/IP via network extensions for specialized applications that include safety, security, energy, and time synchronization. To address functional safety, EtherNet/IP provides support with CIP Safety™; for security, device defense is covered by CIP Security™; for sustainability and energy efficiency, CIP Energy™ is available; for time synchronization, CIP Sync™ is available. CIP Security offers the flexibility of different levels of device level security, and CIP Safety detects errors and allows devices to take appropriate action to prevent unintended harm.

EtherNet/IP also supports concurrent connections, allowing for failsafe controller redundancy for the most critical of process applications. Additionally, EtherNet/IP is able to deliver fault tolerant redundancy via the Parallel Redundancy Protocol and Device Level Ring. Furthermore, EtherNet/IP supports process automation through HART integration, and IO-Link integration. Broad usage of EtherNet/IP in process automation enables a more efficient and interconnected infrastructure along with seamless information sharing that improves on the communication that is now possible between HART and EtherNet/IP and between IO-Link and EtherNet/IP devices.

ODVA is continuing to expand the EtherNet/IP ecosystem with the next generation of digitized device description files, including FDT (Field Device Tool), FDI (Field Device Integration), and xDS, to simplify integration into process asset management tools. FDT technology standardizes the configuration interface between field devices and control systems, independent of communication protocol, allowing streamlined access to device parameters. The FDT Group developed the FDT IIoT Server (FITS) to enable mobility, cloud and fog enterprise applications, as well as sensor-to-cloud and enterprise-wide connectivity. An FDI device package includes the device definitions, user interface plug-ins, certificates, and useful documentation to simplify integration with field devices and FDI host-enabled plant, enterprise, and cloud-based systems. xDS is an information model for EtherNet/IP devices that will describe how to represent the associated device to the overall system. The end goals of the device description efforts are to provide a standard, robust and detailed description of device information, implement secure device description artifacts, and prepare for a future driven by Industry 4.0 and IIoT.

Figure 2: FDT FITS, FDI Device Package, and EtherNet/IP xDS



Finally, ODVA supports the PA-DIM process automation device information model specification that can be integrated across communication protocols, meets the requirements of the NAMUR Open Architecture (NOA), and enables end users to better use device data from across the plant. A partnership between ODVA, OPC Foundation, PI, and VDMA to develop a new interface standard for the acquisition of energy consumption data in industrial manufacturing to improve power consumption management is also underway. Additionally, EtherNet/IP plans to continue to evolve for future requirements by enabling reliable, secure communications between CIP-enabled industrial control system devices and the cloud as well as to enable common cloud gateway and device management tasks. One of the ways this will be accomplished is via a joint working group with the OPC Foundation to develop an OPC UA companion specification for CIP.

Single Pair Ethernet

As a media independent network, EtherNet/IP is well positioned to take advantage of the benefits of Single Pair Ethernet (SPE) since SPE is just another physical layer. SPE allows for cost and size reductions in Ethernet PHYs (physical layer data transceivers), cables and connectors that enable cost effective connectivity for smaller devices as well as more efficient long cable runs. This opens up the possibility to connect simple devices to Ethernet that were previously only hardwired or controlled via fieldbus technology. One of the most clear and important benefits of SPE is the lower cost of the overall installation relative to standard Ethernet since only a single twisted-pair cable is required. While this may seem small, the difference can add up quickly with factories and plants that have cable runs of hundreds of meters and thousands of communication nodes.

Additional device connectivity opens up possibilities for diagnostics along with development of prognostics. Incentives to utilizing SPE to add devices to Ethernet networks include remote commissioning, digital troubleshooting, and failure prediction via edge and/or cloud-enabled analytics. The cost savings from being able to quickly and easily add a new device to the network and to identify a malfunctioning device without having to physically test for failures adds up quickly between labor savings and downtime reduction. Industrial Ethernet networks, such as EtherNet/IP, over SPE can help convert previously untapped data into insights that can transform operations to increase Overall Equipment Effectiveness (OEE)/production output, flexibility and quality while also driving down cost.

Single Pair Ethernet (SPE) is a crucial enabler of adding the Things in IIoT to digital Operational Technology (OT) networks. These things include contactors, push buttons, and motor starters located in cabinets, along with temperature, level, and flow sensors in process plants. Many of these devices are currently analog with little to no diagnostic or parametrization capabilities. Some of these devices are already on digital fieldbus networks today; however, their status and commissioning abilities are oftentimes under-utilized, leading to a substantial amount of stranded data and untapped operational improvement potential.

It's important to note that SPE encompasses 10BASE-T1L General Purpose SPE applications, 10BASE-T1S in-cabinet applications, and 10BASE-T1L Ethernet-APL applications. Furthermore, there are multiple IEEE SPE standards in addition to those mentioned here, such as 100BASE-T1 for automotive applications.

Figure 3: SPE Standards

SPE Standard	SPE Identifier	Main Industry	Max Speed	Max Length
IEEE 802.3 ch	10GBASE-T1	Automotive	2.5/5/10 Gbit/s	15
IEEE 802.3 bw	100BASE-T1	Automotive	100 Mbit/s	15
IEEE 802.3 bp	1000BASE-T1	Automotive	1 Gbit/s	15-40
IEEE 802.3 cg	10BASE-T1S	Industrial Automation	10 Mbit/s	25
IEEE 802.3 cg	10BASE-T1L	Process Automation	10 Mbit/s	1000+

SPE will help enable IT/OT convergence by allowing OT devices to leverage the same underlying Ethernet technologies making it easier to ensure data makes its way up from the field level through switches/routers/firewalls and onto SCADA, MES, ERP, and cloud systems. CIP Security helps enable this convergence by utilizing robust and ubiquitous security technologies to achieve protection of EtherNet/IP control system devices. CIP Security can be used as a major part of an IEC 62443-4-2 security certification, and also can apply to the system level through IEC 62443-3-3. The adoption of SPE by both device manufacturers and end users alike is a critical step in unlocking the full potential of IIoT to transform business through more efficient operations.

SPE can also reduce the labor and time needed for panel installations with easier to use connectors and fewer cables. ODVA's in-cabinet resource-constrained device solution is an example as it enables contactors and push buttons to be connected to EtherNet/IP via a 10BASE-T1S SPE multidrop flat cable.

SPE for Process Automation: Ethernet-APL

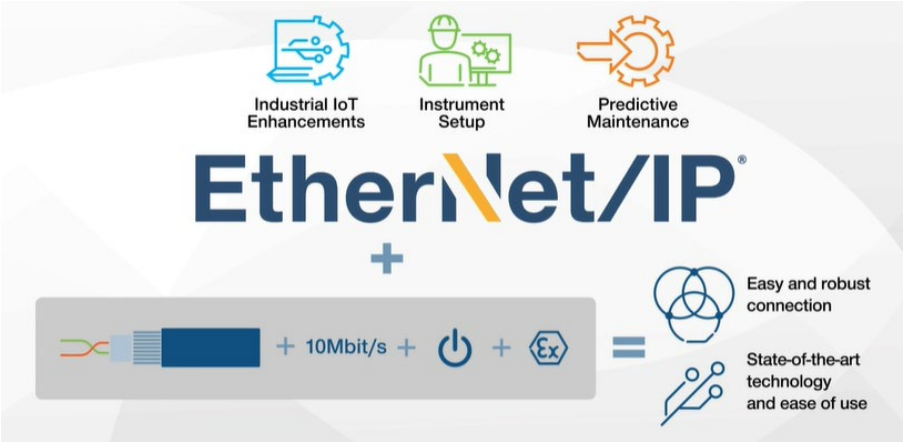
Ethernet-APL is a specialized version of SPE for process automation that includes hazardous area protection, power to field instrumentation, and support for long cable runs of up to 1,000 meters. According to ARC's Valentijn de Leeuw, "Felix Hanisch, president of the NAMUR board, mentioned that an Ethernet-APL information highway to the OT systems is critical, and maybe the industry's last chance to enable "top-to-bottom" digital transformation."

Ethernet-APL meets the ruggedness and simplicity expected by the process industries for a control network. The Trunk and Spur topologies are familiar to end users and Ethernet-APL allows up to 1,000-meter trunk lengths and 200-meter spur lengths.

ethernet-apl™
advanced physical layer

The long cable lengths of up to 1,000 meters, potential reuse of type A fieldbus cable (IEC 61158-2), and up to 10 Mbit/s communication speeds of Ethernet-APL can enable the benefits of Ethernet to be realized at the field level in process plants. One of these advantages is that process instrumentation can easily communicate multiple variables such as temperature, level, and flow from one instrument via the increased bandwidth of Ethernet-APL.

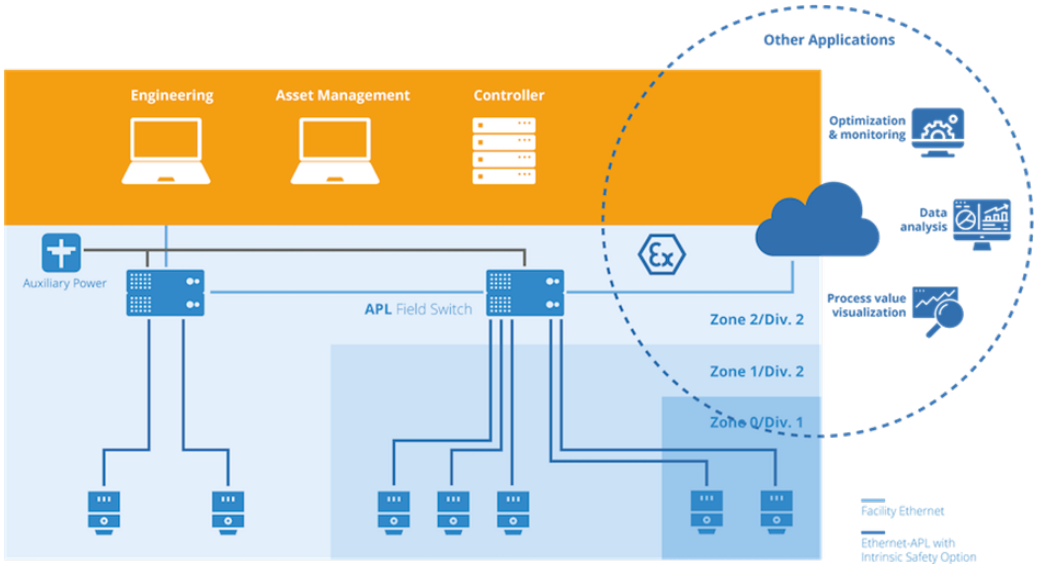
Figure 4: EtherNet/IP + Ethernet-APL Advantages



Ethernet-APL leverages the same Type A fieldbus cable that is currently installed in process plants today. In fact, existing Type A cable may be reused if the cable integrity is verified and impedance standards of 100 ohms with +/- 20 ohms tolerances are met.

Since it is just a physical layer, Ethernet-APL allows end users to access standard safety and security services built on IEC 61508 and ISA/IEC 62443 from the leading industrial automation standards bodies. This includes CIP Safety and CIP Security capabilities for EtherNet/IP. EtherNet/IP is able to expand precise, efficient Ethernet-based control and commissioning across process field instrumentation via the Ethernet-APL physical layer. The full use of EtherNet/IP in process automation enables concurrent seamless connectivity from the field devices to the controllers, to Industrial IoT applications, as well as the edge and cloud for prognostic analysis.

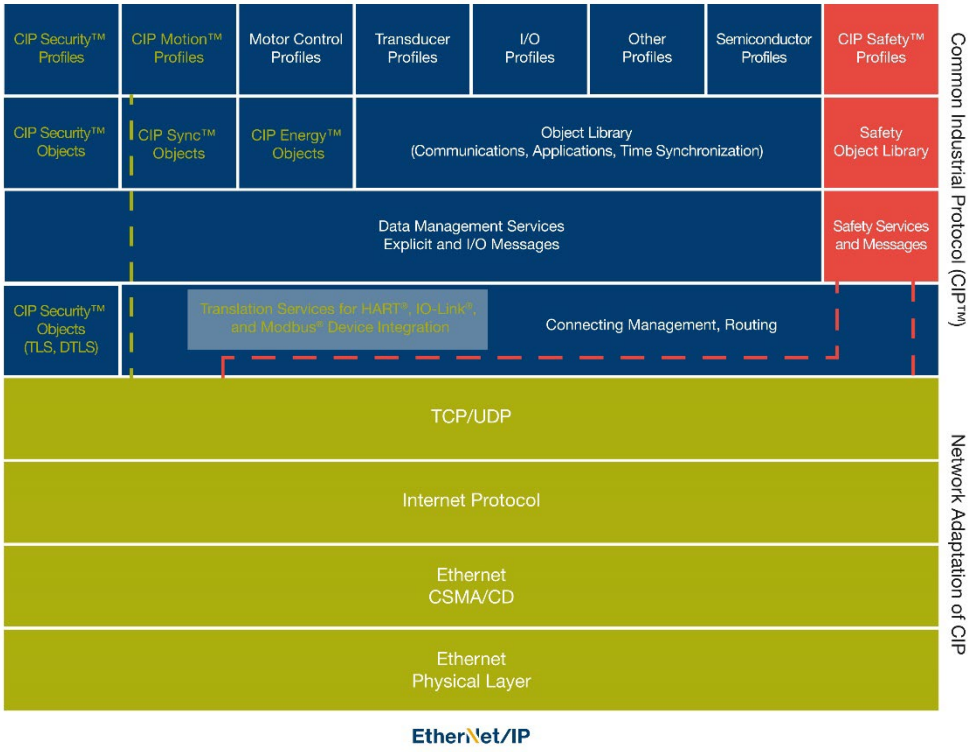
Figure 5: Ethernet-APL Application Enablement



Wireless

The newest application areas that EtherNet/IP solutions are targeting include wireless communication for hard-to-reach devices over 5G. Wireless support for Private 5G has recently been proven in a joint test bed with Rockwell Automation, Ericsson, Qualcomm, and Verizon. Additionally, CIP Safety can be run over wireless due to relying on the black channel principle that leverages data validation techniques built into the network extension.

Figure 6: CIP and EtherNet/IP OSI Model



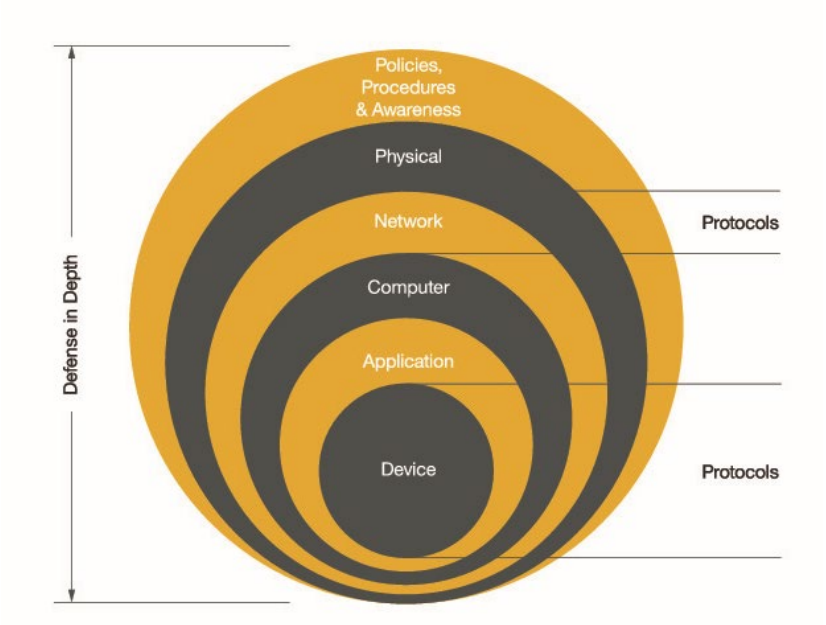
Security

Utilizing Ethernet networks at the field device level in process automation requires the ability to secure communications and devices to help prevent intrusions from bad actors. EtherNet/IP offers the CIP Security cybersecurity network extension that provides the last mile of security-related requirements and capabilities for devices. CIP Security is just one part of a defense-in-depth architecture that is recommended by ODVA.

A defense-in-depth architecture is one of the most important ways to reduce your attack profile. A bad actor can be a singular, highly skilled person, a cooperative group, or even a nation state. With that in mind, it's necessary to create a defense that includes many layers of deterrence. Physical security is a valuable consideration given that wireless networks can be potentially reached outside of company property, open USB ports invite spyware, and lost electronic entrance security keys allow uninvited access that can significantly increase the attack vector of a facility.

Contractors and supply chain partners cannot be forgotten about either as they can have access into critical operational technology systems or be the weak link in the supply chain if they present a soft or easy-to-beat target due to limited security measures. Traditional security within switches including firewalls, approved listing, deep packet inspection, etc. is also a must have.

Figure 7: Defense-in-Depth Security Approach



Another method to minimize the abilities for attackers to be successful is to conduct regular threat modelling using the STRIDE, DREAD, or Attack Tree approaches. The STRIDE approach covers spoofing, tampering, repudiation, information disclosure (privacy breach or data leak), denial of service, and elevation of privilege. The DREAD threat model includes damage, reproducibility, exploitability, affected users, and discoverability. Attack Trees or Threat Trees are a logical approach to better understand how an intrusion could happen in a detailed, logical, and step by step manner.

Regardless of the threat model employed, it's important to conduct these analyses on a regular basis to take into account changes in manufacturing footprints and newly discovered threats. Another valuable approach is to think of security as a state of mind within an organization. The best policies, procedures, and systems can be overcome, but a host of vigilant employees can be much harder to defeat. In summary, security should be treated with the same care as safety when designing, updating, and operating an industrial facility. Security is an invaluable investment in the future of your enterprise.

For field level device security, CIP Security for EtherNet/IP devices makes use of the IETF-standard Transportation Layer Security (RFC 5246) and Datagram Transport Layer Security (RFC 6347) protocols in order to provide a secure transport for EtherNet/IP traffic. TLS is used for the TCP-based communications such as diagnostics and commissioning, and DTLS for the UDP-based transport communications such as I/O data.

Secure EtherNet/IP transport via CIP Security provides the following security attributes:

- Authentication of the endpoints — ensuring that the target and originator are both trusted entities. End point authentication is accomplished using X.509 certificates or pre-shared keys.
- Message integrity and authentication — ensuring that the message was sent by the trusted endpoint and was not modified in transit. Message integrity and authentication is accomplished via TLS message authentication code (HMAC).
- Message encryption — optional capability to encrypt the communications, provided by the encryption algorithm that is negotiated via the TLS handshake.

CIP Security provides user and device authentication, a trust domain, device identity, device integrity, data confidentiality, and policy enforcement (authorization). Policy-based authentication and authorization help support zero trust. CIP Security provides these security properties via five separate security profiles that provide flexibility for vendors in adding security features to their device depending on the intended application(s) and use case(s). A security profile is a set of well-defined capabilities to facilitate device interoperability and end-user selection of devices with the appropriate security capability. The first security profile is the EtherNet/IP Confidentiality Profile, which provides secure communications between EtherNet/IP endpoints to assure data confidentiality. The second profile is the CIP User Authentication Profile, which provides Authentication at a user level for CIP communications. This is used as a basis for Authorization and Role Based Access Control. The third profile is the Resource-Constrained CIP Security Profile, which provides a lightweight version of the protections afforded by the first two CIP Security profiles specifically for highly resource-constrained devices.

The fourth security profile is the Pull Model Profile that enables ease of use for device replacement and commissioning, using EST and DNS-SD technologies. Certificates involve a private key that is stored on a device. When a device fails, it needs a brand-new certificate. The Pull Model allows a device to automatically discover and request a certificate using DNS-SD for discovery and EST for certificate request. The automatic discovery and request/grant of a certificate allows automatic device replacement to proceed even when security is being used. The fifth security profile is the Device-Based Firewall Profile, which provides a simple mechanism to filter traffic based on IP Address/port/protocol. The Device-Based Firewall works much like the “IP Tables” program that has been present in Linux/Unix for many years, and is implemented via a new object (called the Ingress Egress Object).

Figure 8: CIP Security Profiles

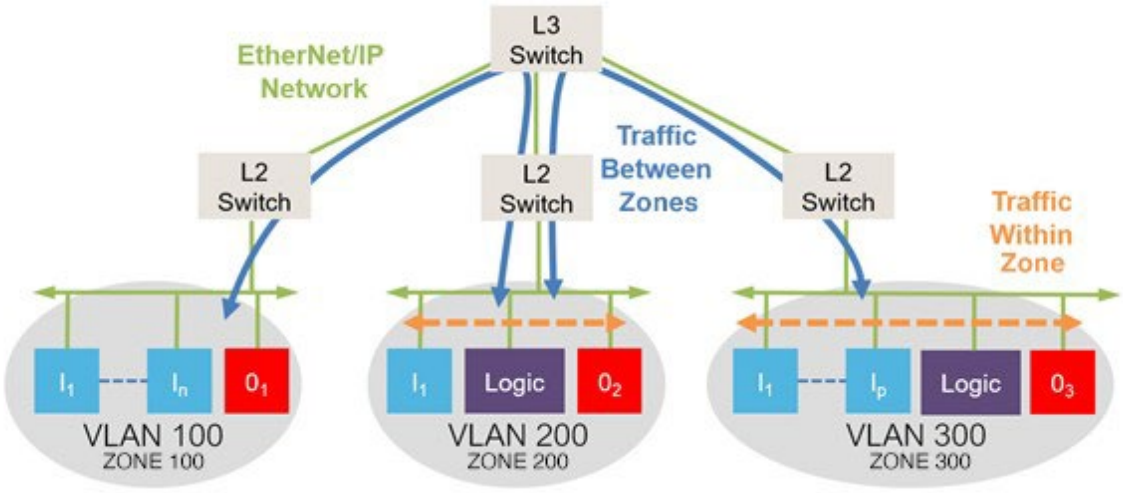
Security Properties	EtherNet/IP Confidentiality Profile	CIP User Authentication Profile	Resource-Constrained CIP Security Profile	Pull Model Profile	Device-Based Firewall
Device Authentication	X		X		X
Trust Domain	Broad – group of devices	Narrow – Users/Roles	Broad; option to be narrow via gateway or proxy		
Device Identity	X	X (Identity of User)	X (via PSK)	X	
Data Integrity	X		X		
Data	X		X		
User Authentication		X	Via gateway or proxy		
Change Detection					
Policy Enforcement		Fixed	Via gateway or proxy		

Additionally, a key component of proper EtherNet/IP network design and planning for optimal operation and enhanced defense in depth security is utilizing segmented networks with vertically layered switches. In the same way that ships have compartments that can be sealed in case of a hull breach, having a network with zones can help to contain a security or operational issue from impacting too much of the larger system. This design ensures that a failure in one zone or within one switch doesn't affect the entire operation.

A secure conduit is the interlinking of the different security zones. It's critical to ensure that the communication paths between zones are access controlled, are resistant to denial-of-service attacks, and don't allow issue from a compromised zone to spread to the broader network. VLANs (Virtual Local Area Networks) are a way to improve security and contain broadcast messaging as a part of implementing secure zones and conduits.

A fully switched network eliminates collisions and improves deterministic behavior of networks such as EtherNet/IP. The addition of secure zones and conduits per the ISA/IEC 62443 security standards provides a way to segment and zone sub-systems in a control network. Zones can be defined by groups of nodes that have similar functional and security requirements. Examples of a similar requirements include devices that are all in the same functional area, contain intellectual property, enable motion, or control environmentally sensitive materials.

Figure 9: EtherNet/IP Switched Architecture with Zones and Conduits



As the inevitable march toward seamless device to enterprise connectivity moves forward, driven by Industry 4.0 and Industrial IoT, the reality is that automation devices that control the motion of motors, drives, pneumatic cylinders, etc. will be opened up to both the business benefits as well as the potential for unwanted intrusion as a result of internet connectivity. Today, many skids are already connected via cellular data to allow OEMs to provide end users with remote operations support.

Even the best designed second communication channel for diagnostics can still potentially expose valuable intellectual property and trade secrets. Avoiding all external exposure of automation devices is of course possible, but then the user will not be able to take advantage of the diagnostic and prognostic benefits afforded by increased connectivity. In the absence of this extreme measure, adding device level security is a low-cost protection that provides a last level of defense for your critical motion control devices. ODVA is committed to providing users with the most secure automation network solutions via CIP Security, which will continue to be enhanced to add new capabilities and protections as technology and threats evolve.

Safety

Just as security is required for process automation field level devices, safety is just as important to ensure that loss of life and/or limb, environmental accidents, and operational disruptions are minimized to the extent possible. ODVA offers the CIP Safety network extension for EtherNet/IP to enable Ethernet network level safety.

Communication networks are very complex, from the device to the switch, router, through all the network media, and to another device. It would be a massive undertaking to try to make an entire communication network meet the principles of functional safety, and any change to any part of the network could require revalidation. While this idea is a theoretical possibility, functional safety over communication networks instead follows a concept called the “gray channel” principle, which is laid out in IEC 61508.

The gray channel principle stipulates that two safety devices must have enough intelligence in themselves, and enough diagnostics in their communications, that the entire communication network has zero impact on the ability of the device to detect communication errors. Even though Ethernet communication networks have considerable error detection built into them, none of that may be used to satisfy any part of the safety function.

CIP Safety devices create a logical connection to each other, independent of the network technologies being used. In the devices, common errors are mitigated with various techniques, as described in IEC 61784-3-2. Time stamps are used with time expectation to detect if packets are lost, delayed, repeated or transmitted out of order. Unique device identifiers are used to authenticate the communication between two safety devices. Additional diagnostics and checks are included to validate that the messages are not corrupted in transit and all these features are separate from standard communication methods.

When these mitigations are put together as CIP Safety, a single connection between two devices, wired or wireless, can be used for communications certified up to SIL 3 per IEC 61508 and up to Category 4/PLe per ISO 13849-1.

Safety application coverage in CIP provides the ability to mix safety devices and standard devices on the same network or wire for seamless integration and increased flexibility. CIP Safety provides fail-safe communication between nodes such as safety I/O blocks, safety interlock switches, and safety controllers. CIP Safety is made up of high integrity safety services and diagnostics in the application layer and doesn't require special communications hardware. CIP Safety can also coexist with other application layer standards like CIP Security.

CIP Safety does not prevent communication errors from occurring, but instead it ensures transmission integrity by detecting errors and allowing devices to take appropriate actions as follows:

- All CIP Safety data is produced with a timestamp which allows safety consumers to determine the age of the produced data.
- A production Identifier is encoded in each data production to ensure that each received message arrives at the correct consumer.
- All safety transfers on CIP Safety use Safety CRCs or checksums to ensure the integrity of the transfer of information.
- Data and CRC or checksum redundancy with cross checking provides an additional measure of protection by detecting possible corruption of transmitted data.
- The CIP Safety protocol is present only in safety devices; this prevents standard devices from masquerading as safety devices.

CIP Safety packets are made up of the following four sections (note that no packet has all four): data, timestamp, time correction and time coordination. When configuring a CIP Safety device over the network, there are measures to ensure integrity of the configuration, such as:

- Safety Network Number which identifies each network path in the system individually, allowing each device to be uniquely identified.
- Configuration Ownership can be enforced to ensure that safety configurations cannot be changed by other devices in the network.

Figure 10: CIP Safety Functionality and Benefits

CIP Safety IEC 61784-3-2:2016 Page 29	Time Stamp	Time Expectation	Connection Authentication	Data Integrity Assurance	Redundancy with Cross Checking	Diff. Data Integrity Assurance Systems
Corruption				✓	✓	
Unintended repetition	✓			✓		
Incorrect sequence	✓			✓		
Loss		✓		✓		
Unacceptable delay		✓				
Insertion	✓		✓	✓		
Masquerade	✓		✓	✓	✓	✓
Addressing			✓	✓		

CIP Safety has been certified by TÜV Rheinland as a gray channel protocol, which means that the safety integrity is not dependent on the physical media. As a gray channel protocol, CIP Safety can be communicated with over different wired Ethernet platforms (10, 100 Mbps and 1 Gbps), fiber optics, and wireless systems such as existing WiFi (802.11a/b/g/n/ac). CIP Safety is expected to be forward compatible to new standards like WiFi 6 (802.11ax) and 5G.

Summary

EtherNet/IP now provides users a complete industrial communication network for all of their potential automation applications, regardless of whether they are in discrete, hybrid, or process markets. EtherNet/IP is able to meet the full set of requirements of the process industries to help end users operate plants with superior yields, minimal downtime, and reduced costs. EtherNet/IP offers process automation practitioners an easy to use, lightweight, proven, secure, and safe control communication network that also enables valuable diagnostics and process variables to be available in both the control room and in the cloud for enhanced insights and timely operational optimization measures. EtherNet/IP offers the robust network solutions that process users demand including Ethernet-APL, PA-DIM, NE 107, and fail-safe redundancy. To learn more contact ODVA or visit www.odva.org.

Ethernet-APL is a trademark of FieldComm Group, ODVA Inc., OPC Foundation, and PROFIBUS Nutzerorganisation e.V.
CIP, CIP Energy, CIP Safety, CIP Security, CIP Sync, and EtherNet/IP are trademarks of ODVA, Inc.
Trademarks not belonging to ODVA, Inc. are property of their respective companies