Ethernet I/O – Technical Considerations

Ethernet I/O is popular for a number of reasons, among them:

- Ability to take advantage of existing network infrastructure and lower cost network components
- Distributed remote I/O configurations at lower cost than proprietary or custom cabling systems
- Multi-vendor availability of I/O using standardized industrial protocols like ModbusTCP
- Widespread use, understanding, and availability of Ethernet cabling, switches, network administration, etc.

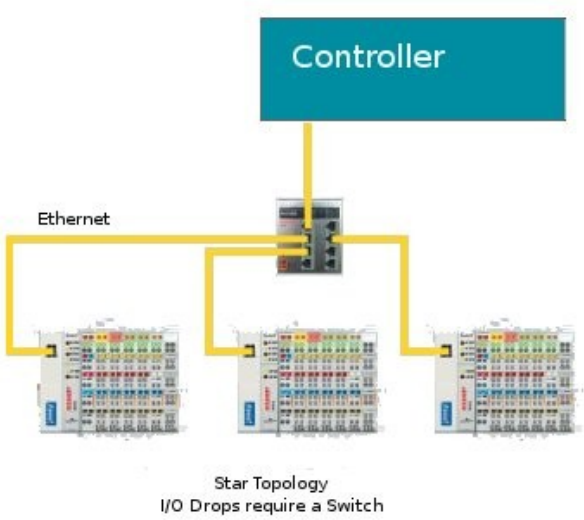
The number of vendors offering Ethernet I/O products is continually growing. However, not all products are designed for all applications. Robustness, throughput, capacity and security are some of the factors which differentiate Ethernet I/O products, beyond the bus protocol(s) implemented. This paper will discuss some of the important considerations when selecting Ethernet I/O products.

Network Topologies

I/O vendors implement Ethernet I/O in 2 primary form factors:

(a) each I/O module is a unique TCP address allowing for cost effective distributed I/O when a small number of points are required at each location

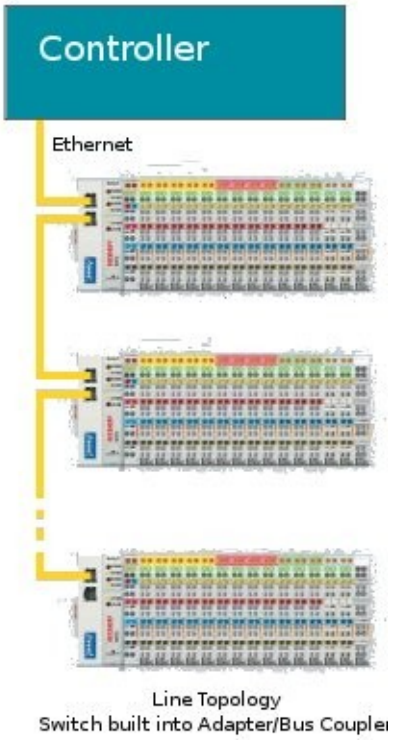
(b) an Ethernet I/O adapter (sometimes called a bus coupler) is a unique TCP address for an entire I/O cluster (or "drop"), allowing for a larger number of I/O points at each location, without the cost of the Ethernet interface in each module. This strategy also allows the same I/O modules to be used for multiple configurations, such as local bus, or on other distributed bus network protocol installations (eg: different Ethernet protocols, Profibus, DeviceNet, or proprietary networks).



Star Topology
I/O Drops require a Switch

The network topology in both the above cases has been typically implemented as a "star", where the I/O drops connect via switches or hubs.

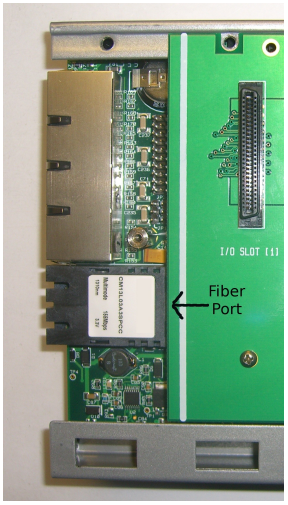
Some vendors now include an embedded switch in the I/O modules and adapters, allowing the I/O stations to be configured in a line topology, which can significantly reduce the wiring effort and the cabling costs in many applications.



Line Topology
Switch built into Adapter/Bus Coupler

Fiber

Many industrial and utility Ethernet users prefer a fiber optic backbone which allows for longer, noise-immune runs between drops. Most I/O modules and adapters have an RJ-45 style Ethernet connector, which means that external media converters or a switch which has fiber ports is required, which can add cost and potential failure points due to increasing the number of connection junctions.



Some vendors, such as SoftPLC Corporation in their Smart™ Adapter, incorporate a fiber optic Ethernet connection port directly into the module or adapter, which can save wiring and cabling costs, particularly if the adapter also has a built in switch.

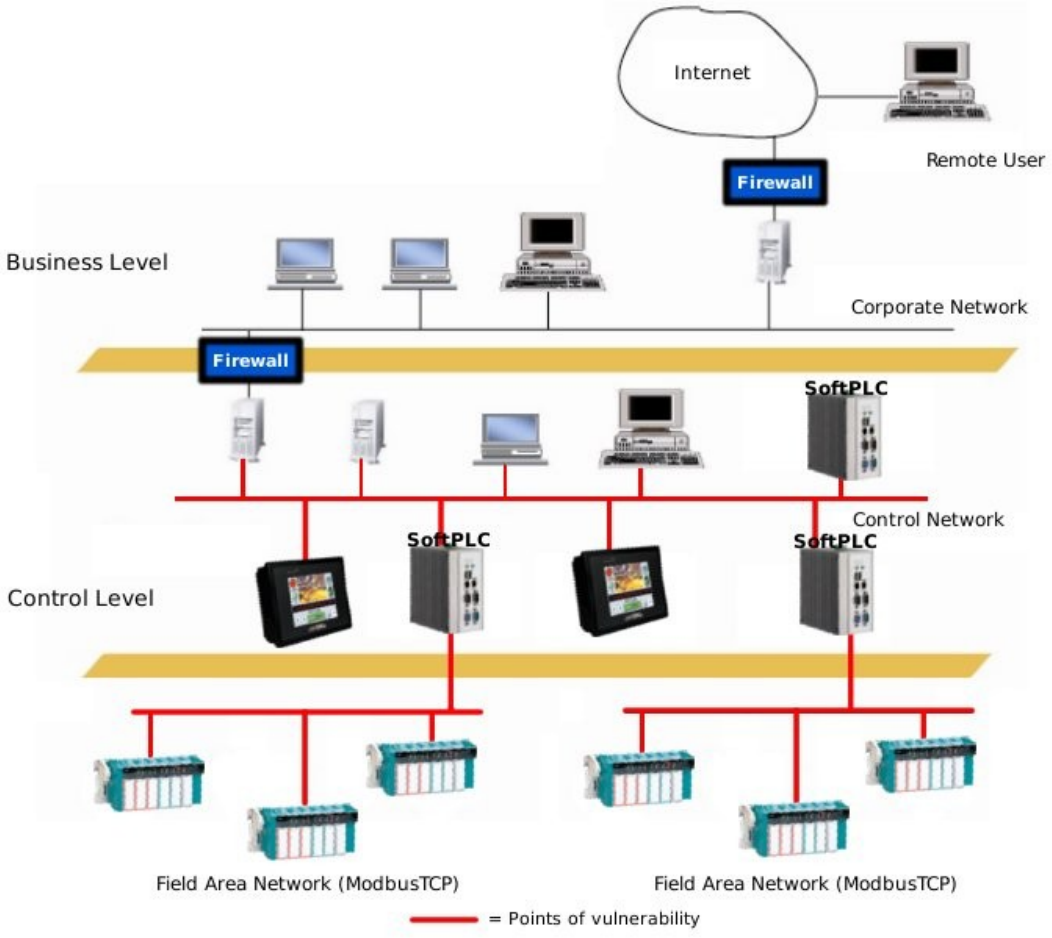
Security

Typical network security schemes are designed to protect the file server, with the thought that if a workstation is compromised the danger is minimal. For industrial networks, the end devices (eg: PLC's, RTU's and remote I/O) can be just as important, or more crucial, than the file server and securing them should be considered in the overall security design. Enterprise-class firewalls provide access security against Internet attacks, but the most harmful programs – those that can paralyze automation systems are often introduced internally.

For example, application software (eg: SCADA) usually provides password protection and/or some type of access control, and these systems are further protected by the plant network security infrastructure. However, end-devices can be targets for a network security attack, and because they contain sensitive data and can allow an attacker to get control of the process, these end-devices need protection as well.

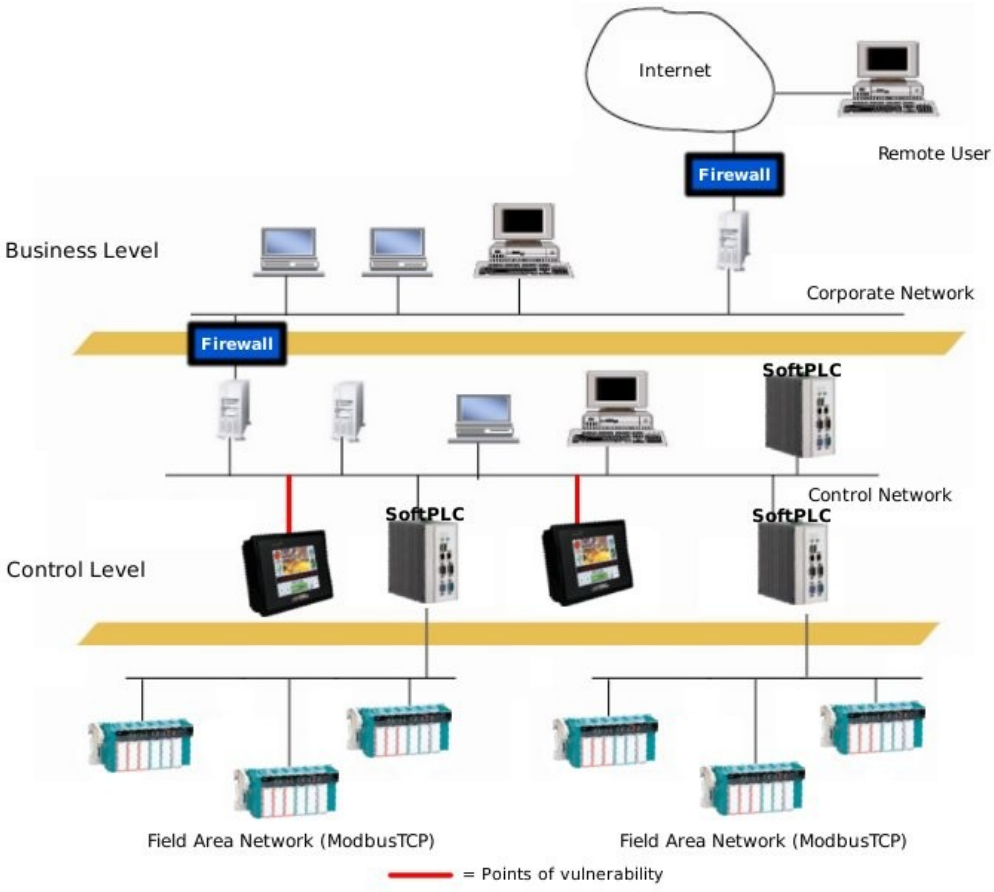
Most industrial Ethernet protocols from the application software level to the plant-floor devices merely encapsulate existing protocols over TCP/IP (eg: Modbus, Profibus), so they provide less security than even many “insecure” internet protocols (eg: Telnet, http) which at least provide some weak authentication. There is no means for authenticating devices or users, nor for encrypting messages in transit.

Additionally, the end-devices on these networks normally do not implement any filtering to block unauthorized access and are vulnerable to attack both from outside the facility as well as internally. The diagram below shows a typical configuration with standard security as applied by an IT department. The entire control level of the plant is vulnerable to attack from any access below the Firewall, such as modems on equipment, authorized users on any of the computers at the control level, or internal connections (eg: a laptop used for maintenance of a controller or field device).



Some protection for end-devices can be achieved with intelligent switches, which have the ability to permit or deny network traffic based on IP address or TCP/UDP port number. However, setting these up and maintaining them can become a chore. Some end-device vendors, such as HMI's, SCADA or PLC programming software, provide security features directly in their products.

For example, SoftPLC Corporation provides a secure solution for end-devices by embedding a high-end firewall into their PLC's and Smart™ Ethernet I/O adapters. Each Smart device also includes a switch, so security protections can be done at all devices on the network, as shown in the following diagram. Access and authentication protection can be provided at every control node in the network I/O, whether a controller or remote I/O drop!



Additionally, with the intelligence built into the Smart products, authentication prevention can check for authorization before applying an operation, such as whether or not to connect, shut down/startup, etc.

Local Intelligence

Most Ethernet I/O modules and bus couplers are relatively “dumb” devices. They act as the interface from the I/O states to the Ethernet and provide some communication error reporting. These devices also provide a configuration method to assign the IP address, and define a failure state for the connected I/O.

In contrast, an intelligent Ethernet I/O adapter, like the SoftPLC Smart Adapter, with local logic control can provide segmented operations. For example, if the master dies, the failure states of each I/O point can be based on process or programmed conditions rather than a limited choice of on/off/last state for the entire I/O drop. Another example would be logic to determine whether or not to trip a circuit breaker in the event of a fault.

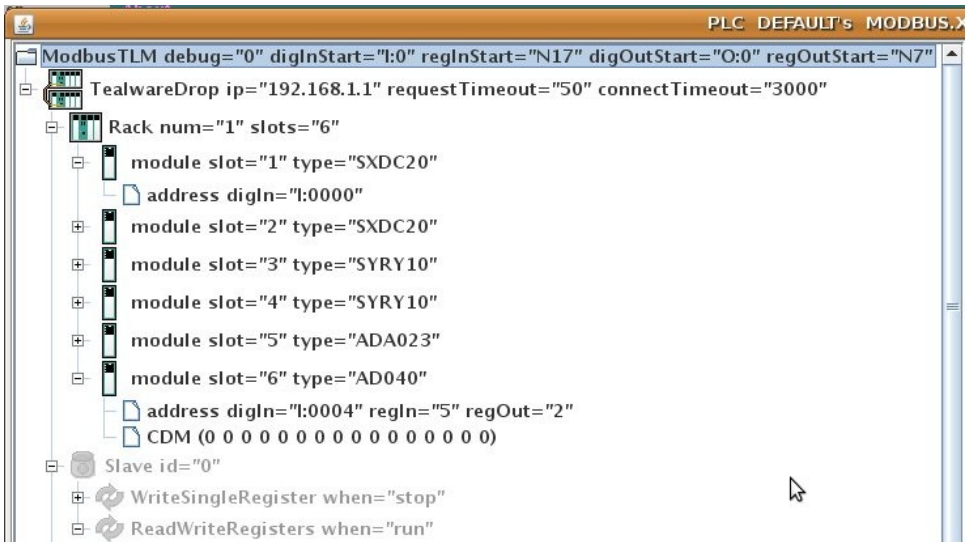
With the SoftPLC Smart Adapter, for example, advanced features can be embedded, such as Sequence of Events recording (SOE). The SOE provides a log of I/O states accurate to +/-1 msec, with the timing coordinated across the entire network via the IEEE1588 standard. Cost savings over using a stand-alone SOE are tremendous, eliminating the duplicate wiring of the I/O points and the cost/installation/space requirements of the stand-alone SOE.

Configuration

While multi-vendor installations do provide users with the opportunity to pick and choose products that best match their application requirements, such as using Vendor A for the controller (PLC/RTU) and Vendor B for the I/O, there can be some disadvantages with this approach as well. Configuring and troubleshooting multi-vendor systems without cooperation between the vendors can be more difficult than products from the same vendor. By its nature, a generic configuration routine must be general enough to support many vendor products and implementations of a standard interface, such as a ModbusTCP communications driver. Therefore, details about vendor specific enhancements or specialty functions cannot be supported easily.

For example, SoftPLC controllers can be used with any ModbusTCP I/O product using a driver configuration process built into the configuration software. This process requires knowledge from the user regarding how the I/O modules map to Modbus addresses and the commands needed to control them.

However, when a SoftPLC controller is used with SoftPLC Corp's Tealware™ I/O there are some nice advantages. I/O Configuration is easily accomplished with an editor that includes an “auto-Configuration” option, which can not only detect modules in use, but also has knowledge of each I/O module's capabilities and requirements.



Even in manual configuration mode, users can select modules by Catalog Number, and the editor will automatically determine the proper Modbus commands and addresses. Additionally, an “outputs when stopped” command allows users to determine the state of Tealware outputs when the SoftPLC controller is stopped, such as changing to Program mode.

Bus Protocol

Most Ethernet I/O vendors support ModbusIP (TCP and/or UDP), which is fast becoming the worldwide standard, due to the number of installed nodes and widespread support within the vendor community. ModbusIP is a truly open standard and has proven to be suitable for most industrial applications. Other protocols (such as Ethernet/IP, Profinet, and others) have less widespread support, due to their semi-proprietary nature and promotion by single vendors. Comparisons of the available bus protocols is beyond the scope of this paper.

Summary

There are a wide variety of Ethernet I/O product options. The factors discussed in this paper will affect not only cost and ease of implementation, but the long term success of the installation. For installations which require a number of I/O points at a location, an adapter based system can lower cost and simplify network configuration. Adapters with built-in switches and fiber connections do even more to lower costs and make the system more robust.

Adapters with built-in intelligence can provide users with tremendous control over system operations, performance, and reliability. Intelligent adapters can also eliminate the need for additional hardware/software to perform auxiliary functions. Further, adapters with built-in security features can make industrial networks secure from attacks both outside the facility and within the facility.

Complete products, like SoftPLC Corporation's Smart Adapter, combine the functions of distributed Ethernet I/O control, secure Ethernet routing and switch functions, fiber optic interface, advanced localized intelligence capabilities, and (when used with SoftPLC controllers) ease of maintenance and troubleshooting.

This paper was written by Cindy Hollenbeck, VP of SoftPLC Corporation (http://softplc.com), a supplier of industrial control equipment and software.