BELDEN
SENDING ALL THE RIGHT SIGNALS

White Paper

How to make a good Automation Data Network?

Achieving Successful IT/ OT Network Convergence

Experience-Based Best Practices

Mike Smith
IT/OT Industry Expert

Table of Contents

Executive Summary

For years, office Information Technology (IT) networks and plant floor Operational Technology (OT) networks were wholly separate. On top of that, IT and OT personnel often had little to do with one another. With the advent of industrial Ethernet replacing fieldbus protocols on the plant floor, they now share a common network, creating valuable opportunities to combine resources and collaborate on goals for overall organizational success.

However, this network convergence also sets the stage for interactions - some might say showdowns - between IT and OT network personnel with very different training, experiences and cultures. The extent to which these necessary collaborations become adversarial or collaborative is dependent upon the approach taken by the organizations and individuals involved.

There is a great deal of misunderstanding about what convergence is and what it entails—for example, one group within the organization might be working toward the creation of one single, flat network while the other is attempting to segregate through technologies such as VLANs. The chances of success in this environment are low due to the steep learning curve and the opportunity for costly missteps when combining these different perspectives.

Fortunately, these challenges have become less necessary to endure. As more and more organizations converge their networks, there is a growing body of resources and best practices being published. Assistance is available through third-party consultants, manufacturer representatives and resources such as this white paper. This is a collection of experiences from Belden and partners who have helped many organizations successfully establish their own converged network. These insights can help you reduce your learning curve and benefit from a converged IT/OT network quickly and efficiently at your location.

Be certain.
Belden.

What "One Network" Means

With Ethernet now commonly running on both the office/enterprise/IT side and the industrial/Operational Technology (OT) plant floor, isolated networks are no longer advisable. Converged networks give us the ability to selectively share data. Thus, we are seeing the emergence of what has become known as the convergence of IT and OT—or the creation of a single network.

The properly converged IT/OT network is not one big flat network, but one network strategically protected, so only appropriate data flows. Selective sharing controls device connectivity and data access to ensure only authorized information and resources are accessed. Specific data might flow one way, from plant to office or office to plant; back and forth both ways; or not at all. This selective sharing is a key to an effective and secure network.

The Benefits of a Converged Network

1. **Economies of Scale**
   Moving to Ethernet in the Industrial/OT environment is both practical and cost-effective. Since Ethernet is prevalent and standards-based, it can be found in consumer appliances, IIoT devices and ruggedized industrial devices. By leveraging the availability of Ethernet products and associated standards, you can now choose the best solutions from different manufacturers and they should communicate with each other with little effort.
2. **Interoperability**
   The flexibility of implementing Ethernet on a converged network provides exponential benefits to the individuals in both IT and OT. Historically, industrial devices communicated through fieldbus protocols. However, implementing a fieldbus protocol, such as PROFIBUS, limits device options to only those which speak PROFIBUS. Alternatively, Ethernet supports multiple protocols. For example, think of Ethernet as a highway. All different types and brands of vehicles can travel on a highway. Fieldbus, on the other hand, is like a train track, where only trains can travel.
3. **Information**
   All machines are gathering data. However, data without context is useless. With the speed and immediacy of Ethernet communications, operators can, for the first time, collect highly detailed, real-time production data that can be strategically deployed to make smarter, cheaper, more efficient business decisions. By converging your network, IT and OT can leverage the skillsets of both teams to interpret and analyze the information.

The Value of Data

The primary interest of many manufacturers is often data capture and analysis due to its powerful and quick rewards. They can raise the bar on production goals, then gather the appropriate data and determine how to get there.

Value is locked in OT production data nearly everywhere. For example, a past client who produces consumer goods lacked insight on the speed or functionality of their machines. When machine issues occurred, operators had difficulty communicating with maintenance staff. To combat this, an OT network was built that allowed their existing HMI to connect to a communication server and contact the appropriate maintenance personnel.

Through that data, they are able to monitor machines more effectively, measure response times and use real-time production data to proactively contact the appropriate person when a machine reaches certain milestones.

Many companies like these are also finding that having production and sourcing information down to each individual component is extremely valuable. They can use this information to track and trace issues with specific units and ensure that such issues are minimized. Further, many industrial companies are finding that collecting data and storing it is valuable, even if you don't have the right questions to ask yet. Manufacturers might want to investigate something later and having production data to analyze from previous months and years is very valuable in the pursuit of such knowledge.

In the pre-Ethernet days, if this type of information was collected at all, it might be hand captured on clipboards and all but lost. Even if it was later looked at, it was subject to illegibility, transposed digits, decimals in the wrong place and any other type of human error. Using Ethernet to capture and analyze information makes it potentially useful intelligence as opposed to pen scribbles. Nearly every industrial company can benefit from these possibilities, and with the technology so readily available, more and more are moving forward to put it to work.

How to Design a Converged Network

Avoid quick fixes and short-sighted solutions, such as connecting existing IT and existing OT networks. A converged network should not be formed from two existing networks. The methodology "just plug them in" seldom works.

1. **Network Audit**

   The first step in designing this new network is identifying what is on the network currently. This process is known as a network audit and gives insight into what devices are where, and what each is currently talking to. This is also a good time to develop accurate documentation as to the network structure.

   Odds are, if you've never audited and inventoried the network, you may be in for some surprises. Things tend to be added over the years without concern for the holistic nature of the network. This is your opportunity to start with a clean, streamlined, efficient slate. The concept of a handful of OT devices being joined with an IT network is not unusual and it is usually only discovered—and expensively so—when there is an IT-side incident or shut down.

   Through a network audit, one factory discovered their capping machine was built with an unmonitored and unprotected cellular connection to the Internet. This device was unknown to the buyer of the equipment and they had no idea who had access to it or how it was connected. This is just one example of how network audits are essential to designing a converged network.

2. **Assessment**

   Once you've inventoried everything, your next step is to assess the status of your current network. At this snapshot in time, what is the quality of your network? You will identify the purpose of each device and decide what should be talking to what. Then you can create the optimal data flows for each case. It's a very individual and technical discussion for the organization, and strategic planning should be done.

   As a few general examples, production data might flow up to analysis software that may reside in the enterprise where it may be selectively reported to salespeople and non-technical managers. Other OT-generated data, such as real-time status reports or maintenance schedules, would likely stay in OT. By the same manner, IT data, such as personnel records and salary data, should not be accessible by the plant floor.

3. **Structuring IT and OT**

   The inventory/audit will help you keep all OT machine functions out of the IT world and vice versa, ensuring that nothing is inappropriately tied to the wrong network, so the proper security protections, resources and connections can be applied. The often cited Purdue Architecture Model is a good, simplified illustration of a basic network architecture.

   There are certainly some gray areas. Remember, it's not **where** the device is located, it's **what** it does. For example, there might be a device used to access e-mail on the plant floor and these would be connected to the IT network, not the OT network. Purposes should NOT be mixed; mixing

   capacity opens up serious vulnerabilities. The PC on the plant floor with browser and e-mail function should NOT also be used for production data. Each device should be strictly determined as an IT or OT device (think: what it does, not where it is located) and attached to the network accordingly.

4. **Consider a DMZ**

   In between the IT and OT domains is what is known as the DMZ. This shared territory is where both worlds come together and what is shared with whom is determined. Physically, this area is a collection of servers and PCs, with information flowing up from OT and down from IT, directionally protected by firewalls. Here it is appropriately processed and then directed back to the pre-determined location. The information flowing in and out is carefully controlled - selectively shared one way or two as appropriate.

   One important function of the DMZ is to keep a wide buffer zone between the outside world accessed by IT—with its threat of hackers and viruses—and the bread and butter world of OT. Threats from the business side need to be isolated from the OT world and can be accomplished through compartmentalization such as ISA99 / IEC62443. This protects the manufacturing side from being impacted by IT threats and allows production to continue. Further, the DMZ helps ensure that production equipment would not be subject to IT necessities, such as virus scans or firmware updates.

Don't Make Security an Afterthought

A plan needs to exist and be integrated as to how you will share data. Begin with determining security needs that should be built into your network. The National Institute of Standards and Technology (NIST) has made recommendations on cybersecurity for reference.

Don't wait for the perfect solution to solve every scenario. As part of this plan, document what simple actions you can take to increase your security and implement them immediately.

A New Organizational Agreement

Even in an organization where IT and OT people work well together, inevitably, it will come up: Who is in charge in situation x? Does IT or OT have the final word on equipment and operations in the DMZ? Who specs network-wide Ethernet equipment?

When the converged organization is built, the purpose is to share information and support both the OT mission and the IT mission. Decisions need to be thoughtfully made to ensure there is not a "winner" and a "loser" and subsequent disgruntlement. A better way may be to create a new dotted line organization, frontloading universal buy-in from both IT and OT, at all levels.

In most organizations, this starts with immediate and demonstrated support from the top. It's good practice to see leaders from both the business and production teams join together and express their support for all IT/OT convergence activities. It is vitally important that IT and OT collaborate and communicate, establishing clear responsibilities. Whether that is two individuals serving as representatives, a committee or a newly created role such as an Automation and Data Exchange Engineer (ADX).

The Automation & Data Exchange (ADX) Engineer

We suggest the addition of a new individual, a professional who understands first-hand the functions and priorities of both the IT and the OT worlds and is capable of communicating with and relating to both departments. We call this individual the Automation & Data Exchange (ADX) Engineer. It is imperative that this person is cross-trained substantially in both OT and IT practices with their background of what discipline they came from originally being less important. They could, for example, be a networking engineer who has spent time working or training on the plant floor learning about automation operations, needs, and challenges. Or, they could be an automation engineer who has completed networking classes and earned certifications from educational organizations or vendors.

Led by the ADX Engineer, there should be governance responsibilities for all things related to the converged network, answering directly to upper management. One of their early duties might be to develop proper procedures for management and operation of the converged network. They can create a Standard Operating Procedures (SOP) guide for everyone to be aware of the new road ahead. The valid concerns of both IT and OT disciplines will be accounted for, with potential SOPs including directives such as "Patches will always be tested in an isolated sandbox before being applied to any OT equipment," or "Internet-connected devices shall not be placed directly on the OT network."

The committee or ADX Engineer should also lead all convergence establishment and maintenance activities. If it is a multi-location organization, they can start with a "pilot project" at a smaller location and take key learnings on to additional locations. After assessing the extent of the convergence challenge at each location, they can also decide, case by case, whether internal resources possess the expertise—and the extra time—to tackle each project. They can work together to identify and select a turnkey third-party expert, identify local resources to handle the job, or some combination of both as the team sees fit.

Often, an outside third-party is beneficial as they can provide insight from a different perspective, share best-practices and provide instant, on-demand man power.

Encouraging Cooperation

In the drive for successful IT/OT convergence, we have seen situations where one group or the other, resisting change, stuck their head in the sand and refused to cooperate, causing very difficult roadblocks. We have seen situations where one group or the other called in outside help and, literally, said "don't let the (other department) know that you're here." Fortunately, this is not the norm; most organizations are made up of professionals who will work together for the common good and it is assumed that your organization will not experience anything like this. But, theoretically, what if it does?

The visible involvement of C-Level executives will help in this regard. If it's holding up progress, they will hash it out. Petty squabbles like "I'm not working with that guy, he messed up (fill in the blank) last year" will presumably dissolve if cooperation is expected.

Another effective strategy is to involve a third party, at least at first. It's often amazing, humbly speaking, how an idea repeatedly expressed by an insider is ignored, but that same idea expressed by an outside expert is considered genius. That's reality and it's helpful to understand. Of course, a well-chosen IT/OT consultant who has "been there/done that" provides both technological and psychological mediator-type assistance and will deliver much more than inside people ever could, drawing upon the experience of driving convergence in other organizations and helping to flatten the learning curve.

It is important that the consultant understands, has experience in and speaks the language of both IT and OT. They should be without loyalty to one side and have knowledge of both so they are not seen as "the IT consultant" or "the OT consultant" but as the "Convergence Consultant." Otherwise, the internal disconnect can be worsened and frustrations compounded. Bringing in someone with a proven track record of understanding the needs of both IT and OT immediately bridges the gap, and sets the organization up for IT/OT convergence success.

Conclusion

The march towards the convergence of IT and OT functions on a single Ethernet network is inevitable for companies that wish to maximize the benefits of Ethernet connectivity while also optimizing the efficiency of the network. This will not come without challenges and growing pains which vary from costly, multi-year processes, to being accomplished by a smooth, mutually beneficial effort. Using information in resources such as this white paper can help move your organization decisively into the latter.