BELDEN
SENDING ALL THE RIGHT SIGNALS®

White Paper

Substation Communications Design Legacy to IEC 61850 Best Practices

Eric Byres, P. Eng., ISA Fellow
CTO and VP Engineering
Tofino Security, a Belden Brand
eric.byres@belden.com

Tim Wallaert, BSEE, MBA
Director – Vertical Markets, Energy
Belden
tim.wallaert@belden.com

Table of Contents

Executive Summary

Over the past decade, two trends have converged that have caused many utilities to re-evaluate their substation communications infrastructure. One trend is the migration of the electrical grid from a reliable, but inflexible system to the "Smart Grid," which promises adaptability and efficiency. It also requires the two-way communication of data, something that is not possible with traditional electrical grids.

The other trend is the increasing adoption by industry of Ethernet networking technologies for their communications. The ARC Advisory Group estimates that the adoption of industrial Ethernet networks is growing at a >12 percent plus CAGR (Compound Annual Growth Rate).

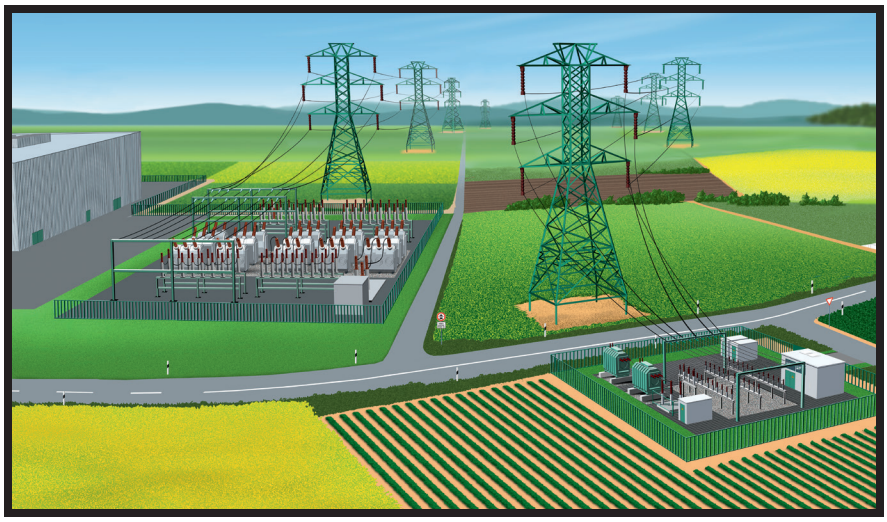
As a result of these trends, many utilities are faced with having to design and implement communications infrastructures that are unlike anything they have been involved with before.

If you are an engineer, field technician, manager or IT professional involved with such a project, you may be wondering where to begin. Alternatively, if you are working with an automation vendor or system integrator, you may want to become better informed to contribute to the project's success.

To help you, we have consolidated our learning and experience from helping hundreds of customers around the world design robust substation communications networks. The result is an easy-to-follow process that will assist you when designing new or upgraded communications systems. Here are the ten best practices discussed in this white paper:

1 – Segment Operational Networks
2 – Add Serial Communications Devices to Ethernet Infrastructure
3 – The Importance of Power over Ethernet
4 - Time Synchronization
5 – Selecting Appropriate Switches and Routers for the Environment
6 – Building Multiple Layers of Security
7 – Adding Communications Infrastructure between Master, Backup and Substations
8 – Choosing the Correct Cables, Jackets and Connectors
9 - Vendor Selection
10 – Good Project Management

This white paper will walk you through each of the best practices, explaining the importance of each one and providing guidance on how to apply it to your needs.



The Foundation of the Smart Grid: Modern Two-Way Communications Networks

Electric utilities are constantly searching for the most efficient, reliable and cost-effective ways to deliver electricity to customers. A vision for doing just that and more is provided with the smart grid model.

One definition of the smart grid, based on work from the U.S. Department of Energy, is:

"A modernized electrical grid that uses information and communications technology to gather and act on information in an automated fashion … to improve the efficiency, reliability, economics, and sustainability of the production and distribution of electricity."

The promises of the smart grid are exciting on many fronts. It pledges to:

- Integrate renewable energy sources into the grid, thus reducing dependency on traditional sources that may be harmful to the environment.
- Save electricity in its own operations, thus improving the efficiency of the system.
- Improve reliability by monitoring equipment and fixing problems before they cause an outage.
- Improve recovery time by being able to smartly switch power around downed areas.
- Meet peak demand without requiring the build-out of additional traditional generating facilities.

To accomplish all of this, the elements of the electrical grid have to be able to communicate and share data quickly. Utilities, consumers and the system must be communicating with each other all the time, a capability that requires a colossal modernization. A new two-way communications infrastructure is being built to do this, and at its heart is the substation.

Reliable Substation Communications is Vital

Today, the majority of utilities are still using technologies ranging from modem connectivity to serial bus technology to 'talk' to their substations to gather important, needed information. In order to integrate with the smart grid, substations need to be upgraded to modern Ethernet and IP-based systems.

The magnitude of this effort is huge. For example, in the U.S., there are roughly 14,000 transmission substations and 48,000 distribution substations. Upgrading these stations to communicate within a smart grid will not happen overnight and will require a significant capital outlay.

According to research completed by Pike Research in 2012, the global market for substation automation will continue to grow, increasing from $2.7 billion in 2012 to $4.3 billion in 2020. Substation automation equipment includes communications devices, protective relays, supervisory control and data acquisition (SCADA) devices, and other related sensors.

The Pike Research data shows that new transmission substations account for the largest segment of the substation automaton revenue, followed by retrofits of existing transmission substations (7.1 percent CAGR) and automation of distribution substations (7.0 percent CAGR).

The large investments in substations being undertaken today will only pay off if the resulting communications infrastructure is high performing, reliable and secure.

Through years of experience in automating substations around the world, we have developed 10 best practices for reliable substation communications. These practices are part of our **Substation Communications Legacy to IEC 61850 Design Checkup**, a process we use with utilities to ensure that network upgrades benefit from proven techniques.

Here are the 10 best practices:

1. Segment Operational Networks

The first best practice we recommend is to segment all networks into operational zones or areas. Networks tend to grow incrementally, resulting in large, flat networks. Too often we find networks that have become vast, sprawling systems that are difficult to manage or secure.

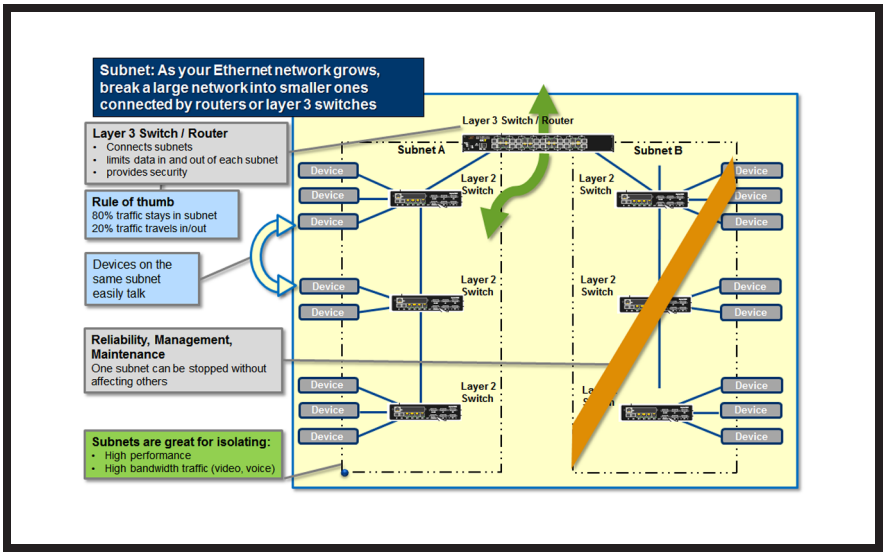


Figure 1. Subnets divide up devices into physical groups and make the network more manageable.

By dividing up large networks into smaller ones, you can improve the manageability, reliability and security of your system. This is a key requirement in many standards, including the ISA IEC 62443 standard for industrial security. It also makes isolating network issues much easier and improves overall system reliability.

There are a number of options for technologies to divide your networks into zones. These include:

Subnets

This technique divides up devices into physical groupings based on function or location for ease of maintenance and security. Each subnet has a specified range of IP addresses and is connected to other subnets using a Layer 3 switch or router.[1]

Subnets prevent "broadcast" messages from being sent between areas, reducing the chances of traffic storms impacting substation operations. Subnets are also good for isolating high performance and high bandwidth traffic on separate networks, giving you easier ways to manage the network and increase performance.

Many of these switch and router devices can also act as packet-filters, offering limited protection against cyberattacks.

Virtual Local Area Networks (VLANs)

VLANs create logical groups of Ethernet devices that cannot be physically grouped. They work by having Ethernet switches insert a "tag" (basically a 4-byte field) into each Ethernet message. Other switches on the network can read this tag and make decisions on whether a message should be forwarded or not.

VLANs are great traffic management tools as they allow devices to see only the data they need. They are frequently used to isolate high bandwidth traffic, such as video and voice, when subnetting is not possible due to the physical separation of equipment.

Similar to subnetting, Layer 3 switches and routers are used to configure and enforce the VLANs, limiting the data in and out of the VLAN.

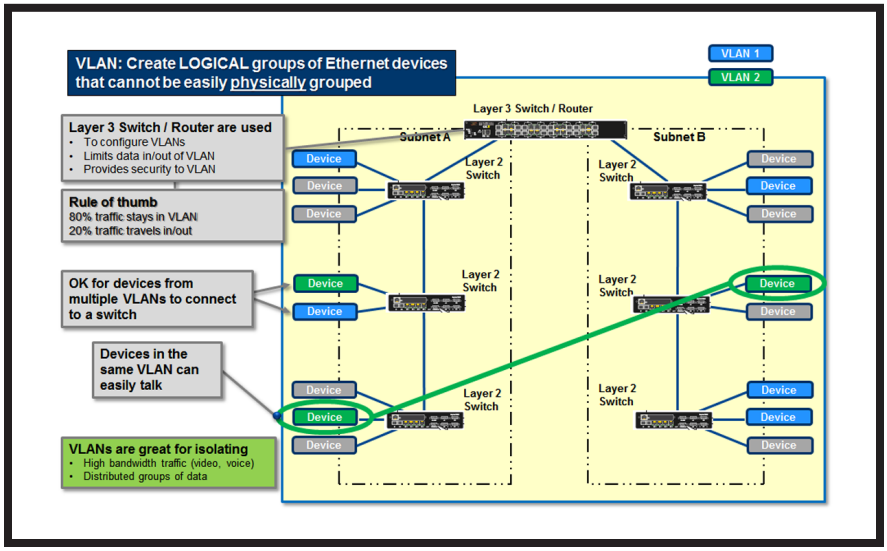


Figure 2. VLANs divide up devices into virtual groups and also help make the network more manageable.

Devices from multiple VLANS may connect to a switch, and devices in the same VLAN can easily communicate between one another.

When Segmentation Is Not Possible

If you are unable to segment your network using one of the above technologies, possibly because it involves a process or protocols that cannot be maintained across a subnetted system, then you need to take extra care to secure your network. One way to do so is with the use of transparent firewalls, which are discussed further in section 6.

2. Add Serial Communications Devices to Ethernet Infrastructure

This best practice helps utilities connect legacy Intelligent Electronic Devices (IEDs) and other serial communications devices to an Ethernet network. This extends the useful life of the equipment and it can significantly reduce the cost of upgrading to a communications system that is "smart grid ready."

You may be wondering if Ethernet is suitable for real-time control and information. The answer is a resounding "yes."

In the past, Ethernet technology was 10 Mbps, half-duplex and hubs. Today's Ethernet is 100 Mbps and higher, full-duplex and switches. The switches eliminate collisions and the other improvements make it an even better choice technically than many of the fieldbuses it replaces.

3. The Importance of Power over Ethernet

What is Power over Ethernet (PoE)? It's the practice of using a single industrial Ethernet cable to provide power and Ethernet communications to devices.

This best practice is vital when implementing physical security surveillance systems. It is not a simple process to wire and connect security cameras, card readers, routers, keypads and telephones, for example, together for substation security. Note that remote monitoring of substation security is an important element of an overall defense in depth protection strategy (more on this later).

Instead of using multiple cords or cables (one for power, one for pan/tilt/zoom control, and one for video), PoE gives you the ability to simplify your security installation and commissioning processes by replacing these with a single connection. This lowers costs as fewer components are needed and the replacement process is simplified.

Planning for PoE involves:

- Determining all the pieces to be used (cameras, telephones etc.).
- Identifying the power consumption (in watts) of each device.
- Totaling the power requirements of all PoE devices that will be wired to one PoE switch.

Note that most devices are "standard" PoE, requiring up to 13 watts, but some may be classified as "PoE+", ranging from 13 to 25.5 watts.

4. Time Synchronization (Fault Event Replay)

As a utility operator, you need to know when events, such as faults, occurred, what happened throughout the event, and what pieces of equipment and substations were involved. This requires time synchronization, also known as fault event replay.

Examples of the equipment that must have accurate time stamping are IEDs, merging units (MUs), control units, Ethernet switches and any other system that requires synchronization within the substation automation system. Factors such as the protocols used, traffic load, communications media and cable distance of the network can affect the timing accuracy.

To ensure precision, we recommend using gear that supports the IEEE-1588 protocol for devices on Ethernet requiring extremely high timing accuracy, that is, to less than one microsecond. IRIG-B is a similar, but older technology.

To implement time synchronization:

- Determine the timing needs of your application which can range from sub-microseconds to milliseconds.
- Make sure that all switches, routers and terminal servers in the path between devices needing to be synchronized support the timing technology being used.
- Connect all devices to a synchronized global positioning system or master clock.

5. Selecting Appropriate Switches and Routers for the Environment

Similar to power plants, substations contain valuable pieces of equipment typically housed in unconditioned control sheds inside the fence. While this provides some level of protection against the elements, temperature swings can be extreme, rodents and other pests can invade the shed, and dirt and grime can accumulate on the equipment. Other stresses can include humidity, corrosion and electromechanical noise.

It is therefore important to select only switches and routers that have the protection against the environmental and other hazards that exist in your substations.

IEEE 1613 and IEC-61850 Part 3 describe the device standards that need to be met for environmental protection. As a utility operator you must ensure that network products meet or exceed all relevant industry standards.

Taking the time to select equipment with appropriate environmental and electrical ratings at the beginning of a project eliminates trouble in the future. You'll save yourself costly repairs and downtime.

6. Building Multiple Layers of Security

Industrial infrastructure, especially critical infrastructure such as the electrical grid, is an increasing target for both sophisticated cyberattacks and for activists. Protecting substations is therefore vital. This best practice looks at how to design security measures that contribute to an overall security strategy.

Most engineers are aware that NERC CIP specifies the minimum requirements for security in the power industry. Unfortunately, NERC CIP uses an electronic security perimeter (ESP) philosophy based on hiding all critical assets behind a monolithic boundary. For example, a single firewall could be installed on the boundary between all critical control assets and the business network, with the hope that it will prevent all unauthorized access to the critical assets.

Industry experience has shown that monolithic designs present a single point of failure in a complex system. Few systems are so simple as to have single points of entry. For example, this is what the U.S. Department of Homeland Security has found:

"In ….hundreds of vulnerability assessments in the private sector, in no case have we ever found the operations network, the SCADA system or energy management system separated from the enterprise network. On average, we see 11 direct connections between those networks. In some extreme cases, we have identified up to 250 connections … ."

With the help of Murphy's Law, eventually all single-point solutions are either bypassed or experience some sort of malfunction, leaving the system open to attack.

A more realistic strategy is based on "Defense in Depth" (DiD) – multiple layers of defense distributed throughout the control network – as a strategy for securing operations.

DiD maintains an ESP firewall between the business and control networks, but adds security solutions inside the control system that protect the substations if the main firewall is bypassed. The solutions work in parallel, with one technology often overlapping with others, to form a significant safeguard against either attack or human error.

There are two primary options for implementing network security technologies for a substation:

- Industrial firewalls that control and monitor traffic; comparing the traffic passing through to a predefined security policy, and discarding messages that do not meet the policy's requirements. Firewalls can be installed both at the ESP boundary and between internal zones.
- VPNs (Virtual Private Networks) are networks that are layered onto a more general network using specific protocols or methods to ensure "private" transmission of data. VPN sessions tunnel across the transport network in an encrypted format, making them "invisible" for all practical purposes.

A network protected using a DiD strategy responds to threats, such as a traffic storm (caused by device failures) or a USB-based virus, by limiting the impact to the zone where the problem started. Alarm messages from the firewalls would pinpoint the zone and even the source of the problem.

Routing Firewalls Guarding the Substation Perimeter

To create a security perimeter for the substation, a security control point needs to be established to restrict and monitor traffic flowing into and out of the substation. Typically, this will be a dedicated firewall, but in some cases a router or terminal server can be used. These need to be able to filter large amounts of traffic and interface transparently to IT systems using security protocols, such as RADIUS and TACACS+. It is critical that this device is both security hardened and monitored for indication of attacks.

Transparent Firewalls to Protect Core Processes

Transparent firewalls[2] are security devices with special features for industrial use. At first glance they appear on the network like a traditional Ethernet switch, but they actually inspect network messages in great detail.

The "transparent" feature allows them to be dropped into existing systems without requiring readdressing of the station devices. This means that organizations can retrofit security zones into live environments without a shutdown. They also allow the installation of security controls within a single subnetwork; for example within a large process bus.

The "firewall" feature provides detailed "stateful"[3] inspection of all network protocols so inappropriate traffic can be blocked. For example, rate limits can be set to prevent "traffic storms" while deep packet inspection rules can be set to prevent inappropriate commands from being sent to IEDs or controllers.

Defense in Depth is Critical

This overall best practice depends on using a multi-layer defense model, which involves not just networking, computer and device protection technology, but things like physical security and policies and procedures. The techniques used should be based on doing a risk assessment for critical assets and processes.

Security is covered in the Design Checkup, but you may require even more assistance in this area. If so, choose a partner who has experience in cyber security for substations and, in particular, securing industrial protocols.

7. Adding Communications Infrastructure between Master, Backup and Substations

As the design of the substation begins to come together, utilities must think about how all of the pieces will communicate with each other. How can we move the data from the substation to other locations? After all, this is what is needed to realize the promise of the smart grid.

Substations can communicate with the master control station and the backup control station using a variety of networking technologies. These include Ethernet WAN, Cellular 3G or MPLS-PPP WAN. Whichever technology is chosen, consider making it redundant, such as adding yet another cellular backup. Robust communication keeps small issues small and ensures high availability of systems.

To evaluate your utility's need for redundancy use our simple, quick equation known as the **Unplanned Downtime Calculator –** *see* **table 1, below**. It can help make the case for investing in redundancy.

Unplanned Downtime Calculator					
$	X	product value	per	Y	unit of time, e.g. hour
	times				
	V	average Meant Time to Repair - MTTR (in same time units as above)			
	times				
	W	# of downtime events per year			
	equals				
$	Z	per year of downtime expense			

Table 1. Unplanned Downtime Calculator

While there have been numerous redundancy schemes developed over the years, there are three that are particularly useful for master to substation redundancy. They are Rapid Spanning Tree Protocol (RSTP), Cellular Redundancy and Parallel Redundancy Protocol (PRP) - *see* table 2.

RSTP uses a physical ring, but logically disables one link to prevent messages from being forwarded on and causing message looping. If a break is detected on the network, the disabled link is re-enabled and messages then flow through the network using the new path. The main advantage of RSTP technique is that it can be used on any network topology. Its main drawback however is that recovery times may be as long as 5-20ms per switch.

When it is not possible or practical to add a separate physical hardwired Ethernet line, cellular redundancy can be used to provide a means of backing up communication. The

Protocol	Works Best On	Pros	Cons
Rapid Spanning Tree Protocol (RSTP) (IEEE 802.1D-2004)	Any Ethernet WAN	Can implement on any topology or mesh	Potentially long recovery. 5-20ms per switch
Cellular Redundancy	When a second hard-wired Ethernet line is not available	Provides alternative to running a physical line for redundancy	Potentially long recovery. Dependent upon wireless internet
Parallel Redundancy Protocol (IEC 62439-3:2012-07)	Any Ethernet WAN	Zero packet loss. "0ms" recovery. Can be added to any existing network.	Requires separate redundancy boxes.

Table 2. Three Redundancy Schemes Particularly Useful for Master to Substation Redundancy.

cellular link remains in a standby mode until communications via the primary hardwired Ethernet line is lost. Communication is then transferred to the cellular link (figure 3). The drawback of this approach is that recovery times will be dependent upon establishing the wireless internet connection.

Lastly, new redundant protocols have emerged that allow for zero packet loss and "0ms recovery." These protocols are defined by IEC 62439-3:2012-07. Parallel Redundancy Protocol (PRP) is one of these protocols and is particularly useful for master to substation communications (figure 4).

PRP requires the addition of a switch that has dual attached nodes. This device is sometimes referred to as a "redundant box" or "red box" for short. As traffic comes into the red box, it duplicates the message packet. One packet is sent over one network, the second is sent over the other. The red box on the other end forwards the first message it receives to its destination and discards the duplicate when it arrives.

In the event of a network failure on one of the links, the message continues to be sent over the link that is still up. Thus, no packets are ever lost in the event of a communication failure on one of the links. Devices on either end see no delay in receiving packets. For the price of the additional hardware for the two red boxes, this provides the best method of implementing redundancy with no impact to operations.

Finally, while on the topic of keeping systems available, consider providing redundant power supplies to critical communication devices such as routers.

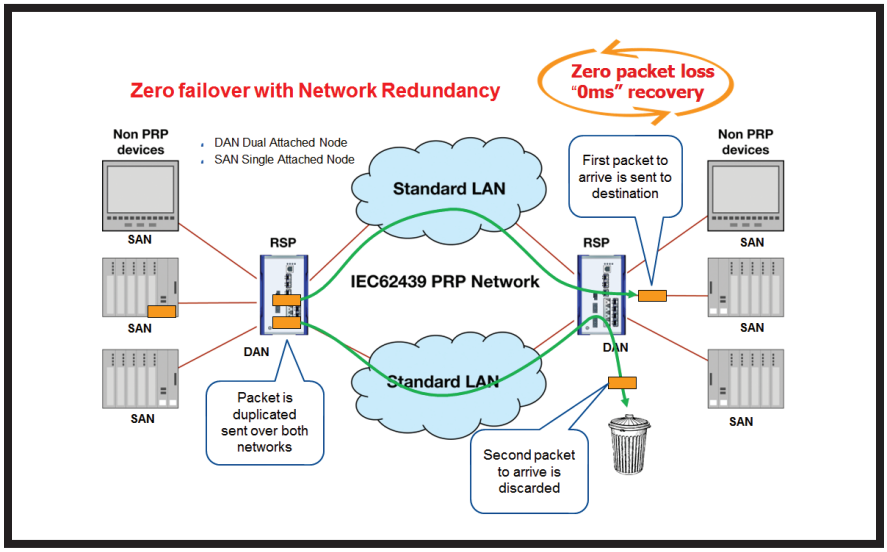


Figure 4. Parallel Redundancy Protocol (PRP)

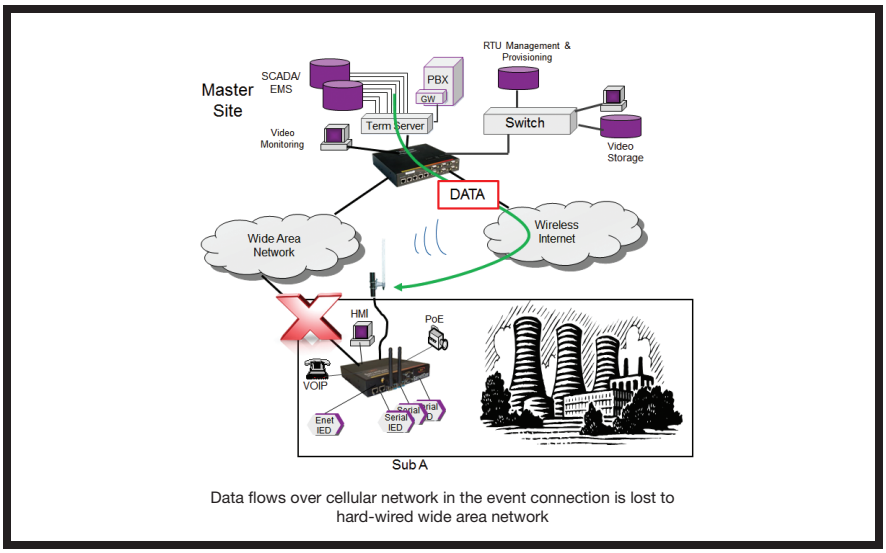


Figure 3. Cellular Backup

8. Choosing the Correct Cables, Jackets and Connectors

Often overlooked in complete communications infrastructure design are the physical cables themselves. More communication problems have been caused by improper cables or shoddy installation than one can imagine. Don't leave this critical portion of the design up to the whims of the installing contractor!

It is vital to determine the proper cabling infrastructure that fully supports the system requirements.

These are specific steps to take to ensure successful implementation:

a. Determine Copper and Fiber Media Requirements

Plan the physical layout carefully considering distances and the data rate requirements to determine the need for copper and fiber media. Fiber is required for distances of greater than 100 meters and signal transmission rates of 10Gbps or higher.

Failures in the physical layer account for the largest problem area and are among the most difficult to troubleshoot and correct. In fact, according to Datacom's Network

Management Special, 72 percent of all communication errors are introduced at the physical layers, such as cables and connectors.

b. Use Industrial Grade Cabling

After all of your planning, you want to be sure that your substation infrastructure will perform as designed in its harsh environment. Commercial grade cable is not designed nor intended to be used in industrial environments.

c. The Right Jacketing for the Location

The proper jacket material will provide the needed protection against the variety of environmental and physical challenges for both copper and fiber cables. Consult with the cable manufacturer about the jacket that would be most appropriate for the specific installation needs.

d. Choose High Performance Cable Designs

Copper cables with Bonded-Twisted-Pair technology are designed for high-balance performance for optimal signal transmission integrity. Proper fiber cable selection of multi-mode or single mode designs is critical to attaining system performance.

e. Consider Electrical Noise

EMI and RFI noise levels must be evaluated to determine if shielded or unshielded constructions need to be used. Highly balanced, bonded-pair cables in shielded or unshielded configurations provide the most robust noise immunity performance. Fiber cable provides the ultimate level of noise immunity.

Finally, make sure that the IEC 525 Substation cabling installation guidelines are followed. This will ensure that the cables are installed properly and will work properly for years to come.

9. Vendor Selection

Here are some factors to consider when selecting a vendor of substation networking equipment:

- Using a vendor that offers everything from cables, connectors to switches, routers, and security devices eliminates the need for multiple project managers from several different organizations.
- Experienced application engineers at the vendor organization should review your application. Most utility process control and industrial applications don't include enough data to come anywhere near Ethernet's capacity. However, you want to be sure that you will have capacity to spare and that areas of risk have been dealt with in the network design.
- Work with an organization that has the ability to provide training to employees. Also, look for a company that uses tools designed to operate the way controls engineers and maintenance workers both work and think.
- A vendor with experience specifically securing substations and industrial protocols will provide the best payback on investments in security technologies.
- A vendor that offers network certification with extended warranties will greatly contribute to substation future-proofing.

10. Good Project Management – A Key to Success

Project management is the key to the successful implementation of substation design and automation. Without managing the project properly, important steps could be overlooked causing much bigger issues in the future.

We recommend using the Industrial Networking Project Checklist provided in Appendix 1. Following this will help ensure that the project has the highest probability of success.

Conclusion

While the smart grid promises vast improvements for the reliability, efficiency and economics of utilities, it will not meet the goal power producers envision without a robust communications infrastructure in place at transmission and distribution substations.

Belden's **Substation Communications Legacy to IEC 61850 Design Checkup** helps utilities compare their designs to industry best-practices and provides options for improving established communications systems.

Investments in good network design and communications infrastructure will improve reliability and contribute to an economical energy delivery system.

References

- Energy.gov "Smart Grid".
  http://energy.gov/oe/technology-development/smart-grid
- Navigant Research "Smart Grid Technologies", Q1, 2013.
  http://www.navigantresearch.com/research/smart-grid-technologies
- Navigant Research "Driven by Smart Grid Integration, the Electric Utility Substation Automation Market Will Reach $4.3 Billion by 2020", Aug 7, 2012.
  http://www.navigantresearch.com/newsroom/driven-by-smart-grid-integration-the-electric-utility-substation-automation-market-will-reach-4-3-billion-by-2020
- EIA: U.S. Energy Information Administration "Market Trends — Electricity Growth in electricity use slows but still increases by 28 percent from 2011 to 2040".
  http://www.eia.gov/forecasts/aeo/MT_electric.cfm#cap_addition
- International Energy Agency "WORLD ENERGY OUTLOOK 2013 FACTSHEET" Nov 12, 2013.
  http://www.worldenergyoutlook.org/media/weowebsite/factsheets/WEO2013_Factsheets.pdf

Additional Resources

1. Obtain further Substation Communication resources, including network diagrams and other tools, at:
   - www.belden.com/power-td
2. Find out about the Belden Certified Industrial Network Program, which provides expert network design services, outstanding warranties and flexibility for the future, at:
   - www.belden.com/certified-industrial-network
3. Contact a Belden representative for assistance:
   - Call **510-438-9071** if you are in the U.S. or Canada.
   - Alternatively, complete the form at www.belden.com/contact.

About Belden

Belden Inc., a global leader in high-quality, end-to-end signal transmission solutions, delivers a comprehensive product portfolio designed to meet the mission-critical network infrastructure needs of industrial, enterprise and broadcast markets.

With innovative solutions targeted at reliable and secure transmission of rapidly growing amounts of data, audio and video needed for today's applications, Belden is at the center of the global transformation to a connected world.

Founded in 1902, the company is headquartered in St. Louis and has manufacturing capabilities in North and South America, Europe and Asia. For more information go to www.belden.com or @BeldenInc.

©Copyright 2014, Belden Inc.