

Getting Ready for IP Convergence

By Hans Scharler



Convergence is a buzzword. The concept may mean different things to different people. The promise with convergence is that we will save money, while we combine and open up new services. Sometimes buzzwords lose their meaning when they're over used. Convergence, convergence, and convergence.

You might be a manager deciding on how to progress toward IP, or you might be a SCADA technician wondering how reliable your systems will be with IP at the helm. The goal here is to introduce convergence concepts such as the internet protocol, quality of service, security, and testing; to cover some of the challenges; and to discover how to get ready for IP convergence through effective training solutions.

Utilities are facing the convergence of services onto one network to support SCADA, voice, surveillance video, and data acquisition services from neighborhoods, the grid, and substations. Combining discrete networks is possible because equipment is shifting to a common protocol, namely the internet protocol (IP).

Meeting Challenges, Reaping Rewards

All of this is a scary proposition. Questions of security, reliability, and quality are probably the first thoughts that come to mind. All the challenges created by converged networks are bridged through proper training, planning, phased-rollouts, compliant security policies, technical expertise, and realistic expectations.

The silver lining is that when properly implemented, we set the stage for new functionality, have a platform that scales up, and provide seamless collaboration among systems, agencies, and resources. Other industries have been faced with IP convergence challenges when they tried to combine voice and data on the same network. They learned a lot in the process, and we can take advantage of their struggles and implement training in advance. In the end, you will be confident that you have a practical approach to implementing and maintaining converged networks.

Let's take a moment to look at what IP is all about.

IP is a suite of protocols that defines methods to transport data inside of a network and between networks to ultimately connect devices together.

Continued on page 36

IP Convergence

Continued from page 35

Although IP has the word internet in the name, the protocol does not require “the internet.” This means our very secure systems do not have to involve the public internet, but rather very secure and closed-off networks. IP uses packets that contain our data with sender and receiver information added to allow them to properly route, switch, block, or check as necessary. Services, such as data acquisition and SCADA control applications, will be packetized and placed on the network.

The Future of Internet Protocol

The future of the internet protocol is IPv6. The new suite of protocols is being deployed in networks systematically as we speak. IPv6 allows for expanded addressing to accommodate the growing demand and limited supply of addresses offered by IP. We also gain other ways to handle QoS, and IPv6 features mandatory internet protocol security (IPsec). Expect IPv6 to become a reality over time as you follow a convergence path. Incorporating IPv6 into a plan now will help minimize the negative impact and help maximize the benefits of the

next generation protocols. The timing is perfect for relevant training.

Real-time SCADA and non-real-time services will be on the same network.

A real-time service is a service where the transactions mean something in the moment in which they were created, like a phone call. A phone call works really well when the listener hears what you are saying as you talk. In fact, the time it takes over an IP network is somewhere around 150ms or less. This is measurable, and we can help assess the quality of a real-time service using this benchmark of time. Types of SCADA will be considered a real-time service.

Non-real-time services do not have to adhere to immediate time constraints. For example, when you download a file, all the pieces that make up the file may be sent in pieces that must be fit back together. If a piece is missing, a file transfer service can resend data that is missing because it has the luxury of time. However, many retransmissions cause transfers to be slow and hinder other services on the network. Excessive retransmissions are also a sign that devices along the path are not keeping



up or the links themselves have high error rates.

One way to look at convergence is that it is the combination of real-time services and non-real-time services. These classes of service will compete against each other. One has a low latency requirement, and the other takes up bandwidth to process large quantities of acknowledged data. A network connecting centralized databases and HMIs to substations will have a mixture of data services on a converged system. Potentially, real-time services for SCADA, voice, and video will exist on the network as well as non-real-time data acquisition services like metering and status and alarm monitoring. A balanced policy is needed to ensure quality of service (QoS) for both categories of service.

Going IP requires knowledge of IP to troubleshoot and install IP equipment such as IP RTUs and terminal servers for serial data. Once you go to a class on setting up a network, not only will you be able to keep your neighbors out of your wireless network, but you will also be able to confidently work around IP.

Security: Another Area to Tackle

Security is a legitimate concern for any type of network. With SCADA being critical to our infrastructure, it is important to be thinking and learning all you can about security during every step of the process.

The devices that support the network, such as IP-based RTUs, server-based HMI interfaces, firewalls, switches, routers, terminals, and servers, will need compliant authorization control policies. Deploying such a policy requires quite a bit of logistical work and deep planning. Technologies like WiMAX are being discussed in the grid to collect meter data. One way to secure

wireless is to limit wireless systems to one-way traffic. Wireless nodes in the neighborhood would be able to collect data only from metering devices, which completely prevents the remote control of unauthorized devices and systems. Beyond wireless, there are vulnerabilities to wired networks,

Continued on page 38



Reliable

Always Ready

Smart Meter Access



SkyTerra Communications

10802 Parkridge Boulevard, Reston, VA 20191-4334

Tel: +1 703 390 2700

www.skyterra.com

IP Convergence

Continued from page 37

including security holes in common operating systems, the ability to introduce system-wide changes, user access control, and the human factor. Educating users of all security levels will be required to ensure the integrity of the services.

The Network Should Work as You Expect

Stability and reliability come into question with IP-based networks. How often have you heard these comments around the office, "The network is down" or "My email is taking forever to download"? The good news is that we have to pick and choose what the converged network will support. We can limit bulk traffic, compress voice, selectively transmit video, and dedicate bandwidth and prioritize holding queues for SCADA and mission-critical applications on network devices such as routers and switches.


The network will be made up of a mixture of existing circuits, leased telecom lines, wireless links, and updated fiber optics. Technicians will have to properly test and maintain low error rates to sup-

port the highest throughputs possible for IP packet, traffic. A single error may cause a packet to be retransmitted causing a cascade of issues including lower quality of service and reliability.

With training on how to use or reuse test tools like transport testers and laptops, techs will be able to maintain IP-based networks, while organizations will be able to get a return on investment on previously purchased test equipment. Fiber optics introduces the need for new skills like splicing, cleaning, and connectorization and requires splicers, power meters, and regular maintenance supplies. When new equipment and test sets are needed, look for precise recommendations that fit into your organization and impact the reliability of the network.

A Total Training Plan

The benefits from IP convergence take time to realize and require a phased plan to avoid premature convergence, headaches, and resistance. Training bridges the gap during the transition. Everyone, including managers, planners, engineers, and techni-

cians, require proper training—a total training plan—to make the best decisions and to design stable and secure networks. Training will enable technicians to effectively troubleshoot and maintain next-generation networks and services. The perfect time for establishing a training program is *now*. Other enterprise industries have dealt with convergence, and we can learn from their mistakes and tactics. Key decisions are being made today, so making training a part of the process now will have an impact from the top down. Managers and planners can rest assured that they are making the best decisions possible, while engineers and technicians are enabled to design and support the converged infrastructure. 

Hans Scharler is a security consultant and senior technical trainer with TESSCO Technologies. For more information, visit www.tessco.com/go/utilities for products and training services customized for the needs of utilities.

EXPERIENCED · INDEPENDENT · CONSULTANTS

PROFESSIONAL

MITIGATE RISK

Strategic Communication Planning

Technology Assessments: Private vs. Commercial

QUALIFIED

Land Mobile Radio Design

Radio Path & Propagation Studies

Cross Departmental Requirements Gathering

Business Cases & Economic Analysis

Microwave & Fixed Data Design and Procurement

MAXIMIZE INVESTMENTS

RESPECTED

the power to help you succeed.



Power System
Engineering, Inc.

Phone: 608-268-3520

www.powersystem.org

Madison, WI · Minneapolis, MN · Marietta, OH · Indianapolis, IN