Unified Field Area Network Architecture for Distribution Automation

Internet of Things Field Infrastructure

Last update: January 21, 2014

1. Executive Summary

In recent years, the utility industry has seen a major push toward enhanced monitoring, control, automation, and management of the medium-voltage (MV) and low-voltage (LV) grids, from the distribution substation to the meters, through the deployment of distribution automation (DA) solutions. These DA solutions provide five key benefits:

- Increase in operational reliability through self-healing grids
- Higher operational efficiency through reduction in feeder losses
- Incorporation of distributed generation while maintaining grid stability
- Improvement in system performance using power quality monitoring and distribution level sensing
- Increase in customer engagement through demand response and advanced metering infrastructure (AMI) deployments

These applications hold the potential to provide significant benefits to utilities and their customers (Table 1) and quickly realize a positive return on investment (ROI). However, to make these DA applications successful and to achieve the vision of ubiquitous access to near-real-time information, a transformation of the last-mile data communications network is required.

Table 1. DA Opportunity

U.S. Utility Macro Efficiency and Reliability	
Cost of power interruptions	$79-$160 billion/year
Voltage conservation potential	90,107 GWh[2*]
U.S. technical and nontechnical losses	6.35%[3]
Cost of truck rolls	$40+[4]

[*] - Annual energy consumption reduction if 40% penetration of CVR

[1] - Energy Information Administration

[2] - Cost of a truck roll for meter reading (Talquin Electric)

(**Source:** GTM Research)

Last-mile data communications networks have gained considerable momentum over the past few years because of their prominent role in the smart-grid infrastructure. These networks, referred as Field Area Networks (FANs), support a variety of applications, including DA, remote asset management, smart metering, and remote workforce automation. FANs also serve as a foundation for future applications which comprise distributed power generation and energy storage, electric vehicle (EV) charging, and microgrids.

Unified FAN architecture is an open-standards- and IP-based communications architecture that provides network connectivity between field devices in the distribution grid to the control centers. The goal of this white paper is to provide utilities with a framework for a unified FAN architecture that makes the communications network for DA and other applications easier to deploy and manage.

The unified FAN architecture provides utilities with many benefits, as compared with proprietary and non-IP-based technologies:

- Helps utilities to make optimal choices of communication technology based on specific application and deployment requirements, as well as to deploy a single converged IP-based architecture
- Provides utilities with a graceful migration roadmap for grid modernization and eliminates millions of dollars of capital expenditures (CapEx) associated with a complete equipment upgrade of deployed legacy assets
- Reduces project schedule risks and cost over-runs by recommending mature and robust networking technologies
- Eliminates additional costs, time, and risks associated with design, deployment, and operation of proprietary procedures for security, high availability, quality of service (QoS), and other functions, plus new IT and security architectures and software applications
- Reduces overhead and maintenance (O&M) costs and streamlines network operations based on IT best practices and eliminates the need for proprietary architectures
- Enables quick and cost-effective deployment of future applications based on integrated multiservice capabilities
- Reduces costs and facilitates a more efficient procurement process by providing utilities with a rich and broad ecosystem of vendors and eliminating vendor exclusivity

The white paper is organized as follows. In section 2, read about DA applications. Section 3 describes the challenges and trade-offs associated with FAN deployments and introduces the concept of unified FAN architecture as a solution to these challenges. Section 4 outlines more details about the unified FAN architecture and associated benefits. In subsequent sections, read about considerations associated with different communications and networking protocols as well as the benefits to utilities associated with each of these choices.

Note: Because this is an architecture framework, this paper focuses on defining networking functionality and relevant standards, without calling out specific products and services from any vendors.

2. Overview of Distribution Automation

Distribution Automation (DA) solutions integrate distribution grid control and protection solutions (devices and head-end software applications) within data communications infrastructures. These applications include the remote monitoring and control of components in the substation (substation automation), all components on feeders (feeder automation), and of components at customer sites (meter automation). They enable grid operators to collect and analyze data about power distribution and consumption in near real time, and provide predictive information and recommendations to utilities, their suppliers, and their customers on how best to manage power.

The remainder of this section examines DA applications in detail.

2.1 Self-Healing Grid and Outage Management

Traditionally, outage management systems have comprised the response systems put in place to react to telephone calls from customers reporting outages. Incorporating automated fault location, isolation, and service restoration (FLISR) mechanisms to identify, diagnose, locate, and resolve electrical outages can significantly enhance outage management.

Monitored circuit breakers, faulted circuit indicators, smart meters with outage detection, and solid state breakers and switches for fast fault clearing, system reconfiguration, and transient-free switching can all be part of advanced outage management systems.

For more details about self-healing grids and other reliability improvement applications, refer to the U.S. Department of Energy's (DOE's) report on Reliability Improvements from the Application of Distribution Automation Technologies [1].

The benefits of enhanced outage management performance as enabled by DA applications can readily lead to a positive return on investment (ROI) and justify the investment, including:

- Reduced outage durations because of faster restoration and associated reductions in Customer Average Interruption Duration Index (CAIDI) and Sustained Average Interruption Duration Index (SAIDI)
- Higher levels of productivity and financial performance for businesses
- Greater convenience, savings from less food spoilage, and avoidance of medical and safety problems for consumers
- Prioritized restoration of emergency facilities and other critical customers
- Improved customer satisfaction by providing up-to-date and accurate outage and restoration information

Table 2. Summary of Changes in Distribution Reliability

Indices	Description	Range of Percent Changes
SAIFI	System Average Interruption Frequency Index (outages)	-11% to - 49%
MAIFI	Momentary Average Interruption Frequency Index (interruptions)	-13% to - 35%
SAIDI	System Average Interruption Duration Index (minutes)	+4% to - 56%

(**Source:** U.S. DOE report [1])

U.S. DOE in its report on Reliability Improvements from the Application of Distribution Automation Technologies [1] provide a summary of the results based on four projects across a total of 1250 distribution feeders. The results (Table 2) show significant improvement in reducing sustained interruptions, momentary interruptions, and average system interruption duration as calculated by changes in SAIFI, MAIFI, and SAIDI, respectively. In particular, utilities demonstrated up to 50 percent in these indices for the feeder groups with the worst baseline reliability levels.

2.2 Volt/VAR Monitoring and Control

Utilities have deployed volt/volt-ampere reactive (VAR) systems to the substations for many years to achieve one or more of the following objectives:

- Lowering voltage levels during peak periods to achieve peak demand reductions
- Lowering voltage levels for longer periods to achieve electricity conservation
- Reducing energy losses over feeders

In general, utilities applying these technologies expect to see 1-percent reductions in electricity consumption for every 1-percent reduction in voltage levels.

However, the capabilities of these systems are limited for three reasons:

- Lack of communications outside the substations
- Limited voltage monitoring and control points
- Coarse control increments for the voltage regulators and capacitors

Advanced volt VAR optimization (VVO) has been made possible through recent improvements in sensors, deployment of pervasive communications, control algorithms, and information processing technologies that monitor voltage levels throughout the distribution system. This information is sent to devices that can adjust voltage-regulating equipment and capacitor banks on distribution feeders in near real time, facilitating quick adjustments in response to constantly changing load and voltage conditions. Adjustments to individual devices and systems can also be coordinated so that voltage levels can be optimized along feeder lines. In addition, these solutions are crucial to energy operations as renewable energy and distributed generation are integrated into the LV and MV grid in order to keep power outputs balanced.

For more details on volt/VAR monitoring and control, refer to the U.S. DOE's Report on Application of Automated Controls for Voltage and Reactive Power Management [2]. In the same report, the U.S. DOE provides the following observations:

- For the 31 feeders for which projects have reported hourly load data, one-half are witnessing line-loss reductions in the range of 0 to 5 percent, and five feeders experienced loss reductions greater than 5 percent. These results are in the range of other industry estimates which indicate that line-loss reductions of 5 to 10 percent are possible.
- In general, feeders with the worst baseline power factors (that is, those with the highest amount of inductive loads) showed the greatest reductions in line losses.
- The initial results for conservation voltage reductions indicate a potential for peak demand reductions of approximately 1 to 2.5 percent.

Examples of other DA applications are:

- Integration of distributed energy resources (DER)
- Remote asset monitoring and distribution grid (MV/LV) sensing applications
- Distribution and feeder planning and load-forecasting applications

The European Commission (EC) Joint Research Centre (JRC) provides a summary of results based on a total of 281 smart-grid projects across 30 countries (EU-27, Croatia, Switzerland, and Norway) in its report, “Smart Grid projects in Europe: Lessons learned and current developments.” [3]

3. Communication Networks for DA: Requirements and Challenges

Utilities require a pervasive communication infrastructure across their service territories to implement these DA applications. As they embark on these deployments, they face the unique challenges of performance, coverage, cost, and lifetime and innovation:

- **Performance:** Utilities need to deploy multiple applications, with different network performance (bandwidth and latency) requirements. For example, substation automation Generic Object-Oriented Substation Events (GOOSE) applications require low-latency communications with latency budgets in order of milliseconds, while a conservation voltage reduction (CVR) application has latency expectation of seconds. Each application also has a unique data requirement, payload, and frequency of communications, hence bandwidth requirements.

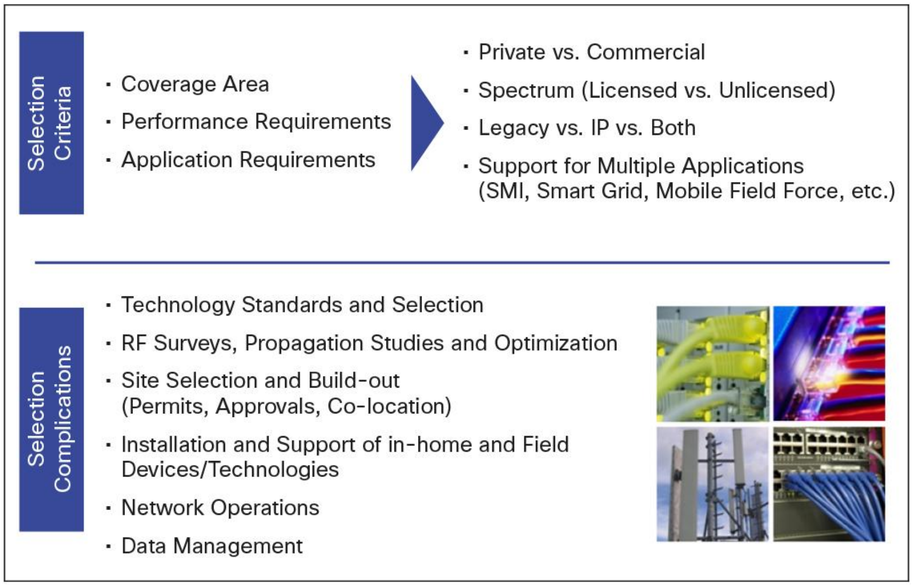
- **Coverage:** Utilities typically have thousands of square miles (or kilometers) of service territory, with a combination of urban, suburban, and rural areas. For each area, selecting one or more communication technologies must be done after thorough analysis of its characteristics, cost, and other associated operational challenges. For example, rural areas may have poor cellular coverage, requiring private network deployments or satellite-based networks for backhaul. In contrast, most metropolitan areas are now deploying high-speed mobile 4G/(Long-Term Evolution (LTE) and wired broadband technologies and can provide a nice fit for certain applications.
- **Cost:** While utilities have the choice of deploying different communication technologies, each technology has a different cost structure. Private communication networks are CapEx-intensive with low OpEx, while a service-provider-based public solution such as cellular or satellite requires higher OpEx with lower upfront CapEx. Similarly, the ROI on a high-throughput and low-latency private network is substantially higher in dense customer areas, as compared with a sparse customer density area. Finally, different utilities have different preferences based on their ability to finance capital: IOUs traditionally have preferred capital-intensive deployments as compared with municipal utilities that may gravitate more toward O&M-based deployments. In some cases, the same utility may even have requirements that vary over larger time frames or geographies because of changes in financing models or different technological guidance from different regulatory jurisdictions. A converged IP-based approach means these multiple technology approaches can coexist without potentially stranding the investment.
- **Lifetime and Innovation:** Field infrastructures are deployed with an average lifetime of 15 to 20 years, which may appear incompatible with the pace of evolution in data communications and innovation in DA and other utility applications. A layered networking architecture ensures integration of these innovations over the expected lifetime of the deployment. For example, most utilities today have significant deployments of legacy, serial-based distribution assets. Over the next few years newer protocols such as International Electrochemical Commission (IEC) 61850 [19] and beyond are expected to be prevalent. The capability to integrate existing remote terminal units (RTUs) running proprietary or serial protocols and intelligent electronic devices (IEDs) running standard IPv4-based protocols over an IP-based network is a clear benefit of a layered architecture.

To meet all the performance, coverage, cost, and lifecycle requirements of the network, utilities require a combination of multiple communication technologies, because no single communications technology can meet all of their requirements. The dynamic nature and wide range of communication technologies available today provide utilities with numerous options. However, this also creates the multiple challenges of choosing the appropriate technology and networking architecture:

- Matching the business and technical requirements to the technology that can support it
- Understanding the maturity, interoperability, and cost-effective deployment of the technology
- Learning the operational procedures for each communications technology, because it may be necessary to deploy, operate, and troubleshoot the network and implement network services for security, high availability, QoS, and other functions differently by communication technology
- Qualifying and learning a new set of headend software and IT infrastructure for each application whose headend software and IT infrastructure differs from the utility’s existing design

These choices can have a significant impact as they may add time, cost, and risk to the project. Figure 1 demonstrates the key considerations for determining network infrastructure.

Figure 1. Technology Selection



Selection Criteria

- Coverage Area
- Performance Requirements
- Application Requirements

- Private vs. Commercial
- Spectrum (Licensed vs. Unlicensed)
- Legacy vs. IP vs. Both
- Support for Multiple Applications (SMI, Smart Grid, Mobile Field Force, etc.)

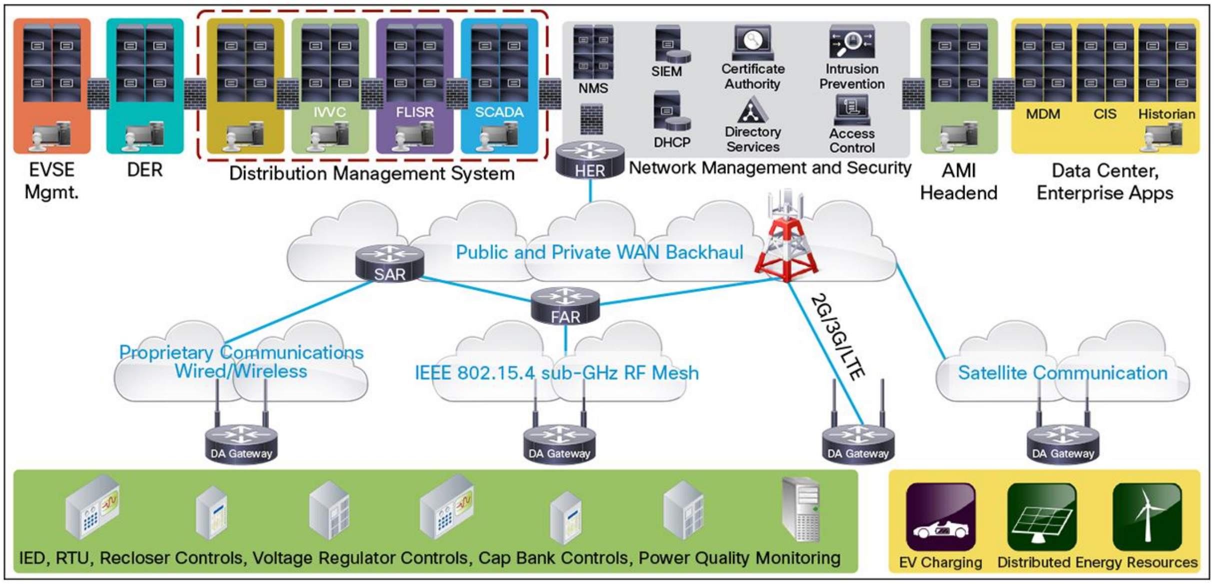
Selection Complications

- Technology Standards and Selection
- RF Surveys, Propagation Studies and Optimization
- Site Selection and Build-out (Permits, Approvals, Co-location)
- Installation and Support of in-home and Field Devices/Technologies
- Network Operations
- Data Management

(**Source:** Accenture)

4. Unified Field Area Network Architecture

Figure 2. Unified Field Area Network Architecture


EVSE Mgmt.
DER
IVVC
FLISR
SCADA
Distribution Management System
NMS
HER
SIEM
DHCP
Certificate Authority
Directory Services
Intrusion Prevention
Access Control
Network Management and Security
AMI Headend
MDM
CIS
Historian
Data Center, Enterprise Apps
Public and Private WAN Backhaul
SAR
FAR
2G/3G/LTE
Proprietary Communications Wired/Wireless
IEEE 802.15.4 sub-GHz RF Mesh
Satellite Communication
DA Gateway
DA Gateway
DA Gateway
DA Gateway
IED, RTU, Recloser Controls, Voltage Regulator Controls, Cap Bank Controls, Power Quality Monitoring
EV Charging
Distributed Energy Resources

(**Source:** Cisco)

Unified FAN architecture is defined as an open-standards- and IP-based communications architecture that provides network connectivity between field devices in the distribution grid to the control centers. The unified FAN architecture (Figure 2) consists of three distinct components:

- **Field devices:** Utilities use a variety of distribution and control equipment, such as distribution switchgear, automated switches, reclosers, and fault interrupters for overhead, pad-mounted, and subsurface installations. The associated control equipment provides local intelligence capabilities to sense grid conditions, select operations based on grid conditions, and coordinate the timing of these operations. In addition, utilities also use MV/LV sensors for power quality (PQ) and voltage monitoring and outage detection. This equipment can connect to a FAN through communication interfaces such as serial (RS-232/RS-485), IEEE 802.3 Ethernet [27], IEEE 802.15.4g/e [34] & [28] RF, IEEE 1901.2 narrowband PLC (NB-PLC) [33], Cellular: 2G, 3G & 4G/LTE or IEEE 802.11 Wi-Fi [26].
- **Control center:** Utilities deploy DA applications, such as Supervisory Control and Data Acquisition (SCADA) protocol-based headend, in a central location, such as the control center. These applications enable continuous monitoring and automatic control of distribution field devices. As utilities roll out more automation on their distribution grids, they deploy more sophisticated applications for FLISR, VVO, and remote asset management. In addition to the DA applications, the control center applications may also need to work with other applications such as the AMI headend or enterprise applications (these applications are typically not colocated in the same control center).
- **Communication network:** Communications networks enable network connectivity between the control center applications and field devices. In most cases, the communication network will be a combination of multiple technologies, as discussed in the previous section. Well-designed communications networks ensure reliable and real-time data delivery. In addition to providing highly reliable data connectivity, applications require homogenous network services with consistent implementations across different technologies. Typical examples of IP-based **network services** are security services, such as data integrity, confidentiality and privacy; network segmentation; high availability and disaster recovery through dynamic routing services; multiservice traffic prioritization through QoS; time distribution; and network management services. Table 3 provides a list of IP network services.

Components of the communication network (“places in the network”), as shown in Figure 2, are:

- **DA gateway:** Provides network (FAN) connectivity and a rich set of network services to field devices. This can be either a standalone device connecting to field devices through a serial (RS-232/RS-485) or IEEE 802.3 Ethernet port, or it can be an integrated communication interface providing wireless connectivity such as IEEE 802.15.4g/e RF, IEEE 1901.2 NB-PLC, Cellular: 2G, 3G & 4G/LTE or IEEE 802.11 Wi-Fi.
- **Field-area router (FAR):** Aggregates traffic from multiple RF and PLC mesh-based field devices and provides network connectivity with a rich set of IP network services.
- **Substation automation router (SAR):** Aggregates traffic from multiple substation devices and provides network connectivity with a rich set of IP network services.
- **Headend router (HER):** Aggregates traffic from all the field and substation devices, provides IP network services, and forwards traffic to different control center applications.

The key features of the unified FAN architecture are:

- Communications technology-agnostic and layered network services based on IP architectures (section 5)
- Standards-based integration of legacy assets (section 6)
- Network security and compliance (section 7)
- High-availability and disaster-recovery architecture (section 8)
- Total cost of ownership (TCO) reduction (section 9)
- Scalability and interoperability between the control center and the end devices (section 10)

The unified FAN architecture provides utilities with many benefits as compared with proprietary and non-IP-based technologies:

- Enables utilities to make optimal choices of communication technology based on specific application requirements and deployment regions as well as to deploy a single, converged, IP-based architecture. An optimum choice would not be possible by a single communication technology or proprietary communication network architecture.
- Provides utilities with a graceful migration roadmap for grid modernization, hence eliminating millions of dollars of CapEx associated with a complete equipment upgrade of deployed legacy distribution assets by enabling integration of legacy assets taking advantage of a rich set of standards-based IP technologies for transport of serial and non-IP traffic.
- Eliminates additional cost, time, and risks of defining operational procedures for multiple, new, proprietary communication technologies for the DA deployment and associated training programs by adopting IP-based architecture with communications technology-agnostic network services. Adopting IP networking architectures ensures the different IP-based communications technologies have consistent network services (detailed discussion in section 5) implementations for providing security, high availability, QoS, and other functions.
- Reduces O&M costs, streamlines network operations, and eliminates the need for training and defining operating procedures based on proprietary architectures. The unified FAN architecture facilitates consistent deployment, operations, and troubleshooting methodologies across different IP-based communications technologies and works well with existing network operations best practices (detailed discussion in section 9).
- Eliminates deployment of new control center and IT architectures and software applications. The unified FAN architecture works well with existing IT and network security best practices architectures. This eliminates the need for qualification, integration, training, and defining operating procedures of new network services software applications, which could add millions of dollars and many months of effort as well as increase risk to the DA deployment (detailed discussion in section 10).
- Enables quick and cost-effective deployment of future applications. Multiservice capabilities, such as QoS and network segmentation, are core to the unified FAN architecture and enable utilities to extend other applications on the same communication architecture. This, in turn, reduces the cost, time, and risks associated with deploying new FAN applications.
- Reduces costs and facilitates a more efficient procurement process by providing utilities with a rich and broad ecosystem of vendors and eliminating vendor exclusivity. All the technologies and networking capabilities recommended in the unified FAN architecture are open-standards-based.

- Reduces project schedule risks and cost over-runs by recommending mature and robust networking technologies that have been validated successfully in large-scale Internet of Things (IoT) and other networking field deployments and developed through a robust standards process.

Note on distributed application architectures: IP-based networks provide bidirectional communications with flexible communications paths and enable hierarchical and distributed application architectures. Examples include:

- **Hierarchical substation-based application architectures:** In a substation-based hierarchical architecture, the utility's private network core infrastructure can be used for field device connectivity. In this case, the SAR provides network services and security capabilities to the DA gateways and field devices. While dependent on the security and protocol requirements and network design, the HER aggregates traffic from groups of SARs or FARs. In addition, this architecture provides bidirectional communication between headend applications and field devices for specific data flows such as supervisory monitoring.
- **Peer-to-peer application architectures:** In this case the utility's network infrastructures must be configured with network services that enable bidirectional communications and data-plane[1] functions between field devices. Network architects should consider application requirements, such as disaster recovery, latency, segmentation, prioritization, and dependence on sublayer technologies. In addition, direct communications stay a key requirement between headend applications and field devices for specific data flow such as supervisory monitoring.

Depending on the choice of network design (for both of the examples discussed above), the HER, SAR, or FAR can provide control plane[2] network services and utility headend applications (such as network management system [NMS]) provide management plane[3] network services.

The key benefits of distributed application architectures are:

- Higher resiliency to the architecture by reducing dependency on WAN connectivity
- Improved latency profile for latency-sensitive applications in cases where the utility has low bandwidth and unreliable WAN connectivity
- Reduced WAN bandwidth requirements through local processing of data
- Improved scalability through distributed data processing

As utilities choose distributed application architectures, consistency of network and security services across the multiple tiers is important. Choosing an IP-based architecture between HER and SAR and a proprietary, non-IP architecture between SAR and DA gateways or between DA gateways adds complexity and risks to the deployment and significantly reduces the benefits of the unified FAN architecture to the utility. For example, the utility may have to provide custom integration software between the IP-based and non-IP proprietary technologies.

While the discussion in this paper takes the example of a control center-based architecture, all the architectural principles and technologies proposed in the unified FAN architecture and mentioned in this document can be applied to and are consistent with these distributed application architectures.

One of the key considerations in distributed application architectures is defining groups of (potentially overlapping) field devices and substations that communicate with each other. Considerations based on these groups generate

[1] The data plane forwards data sent from the device connected to a network device.

[2] The control plane of a network device processes the traffic that is paramount to maintaining the functionality of the network infrastructure. The control plane consists of applications and protocols between network devices, such as routing protocols (for example, Border Gateway Protocol [BGP]) and security protocols (for example, Internet Key Exchange version 2 [IKEv2]).

[3] The management plane manages traffic that is sent to the network communications device and is made up of protocols such as Secure Shell (SSH) Protocol and Simple Network Management Protocol (SNMP).

additional requirements and challenges, and require supplementary design, network features, and application capabilities. One example is defining the behavior of groups in case of fault (link and device) scenarios and associated networking and application requirements for high availability and disaster recovery. Another example is of additional security requirements for group-based encryption and traffic segmentation. While, examples of considerations for distributed application architectures have been included in the subsequent sections, a comprehensive discussion of network requirements for distributed architectures is outside the scope of this white paper.

5. Communications Technology-Agnostic and Layered Network Services Based on IP Architectures

There have been significant advancements in physical- and data-link-layer technologies, such as Ethernet (IEEE 802.1), Wi-Fi (IEEE 802.11), wireless personal-area network (WPAN) (IEEE 802.15.4g/e), PLC (IEEE 1901 B-PLC and 1901.2 NB-PLC) and cellular (2G, 3G, 4G/LTE), giving utilities numerous options. The layered capabilities of an IP-based architecture help utilities make an optimal choice of communication technology based on specific application and deployment requirements (as discussed in section 3). This optimum choice would not be possible in a non-layered architecture, where the application layer is tied to the underlying communication.

IP-based network architectures provide a set of well-defined network services for security, high availability, QoS, and other functions. Table 3 provides a list of IP-based network services. Adopting IP networking architectures ensures the different IP-based communications technologies have consistent network services implementations and capabilities.

The following example highlights the benefits of adopting communications technology-agnostic and layered network services based on IP architectures and protocols, such as those listed in Internet Protocols for the Smart Grid-RFC 6272 [18].

Example: Quality of service (QoS) capability prioritizes traffic and ensures service-level agreements for different classes of traffic. IP networks define scalable end-to-end QoS based on Differentiated Services Code Point (DSCP) marking, as defined in RFC 2474 [37], 2475 [38], and 3260 [39].

Benefits: IP-based networks provide consistent QoS behavior independent of the underlying communication technology. In addition, communication technologies provide predefined mapping between IP DSCP marking and QoS identifiers for the communications technology. This eliminates additional cost, time, and risks associated with designing QoS architectures, defining operational procedures, validating QoS behavior, and implementing associated training for every new and proprietary communication technologies.

Table 3. Taking Advantage of IP-Based Network Services

Network Services	Layers and Services	Benefits
Unique device addressing (network layer)	From IPv4 (32-bit address space, now deprecated at Internet Assigned Numbers Authority [IANA]) to IPv6 (128-bit address space), including multiple scopes (global, private, and link)	Large address space able to cope with the IoT evolution Private or public infrastructure
Address autoconfiguration (network layer)	Manual (IPv4/IPv6), stateless (IPv6), stateful (Dynamic Host Configuration Protocol [DHCP] for IPv4 and IPv6), and prefix delegation (DHCPv6 PD)	Centralized or distributed address management; additional DHCP options Zero-touch provisioning

Network Services	Layers and Services	Benefits
Media independency (PHY and MAC layers)	IEEE 802.3 Ethernet, IEEE 802.11 Wi-Fi, IEEE 802.16 WiMAX, IEEE 802.15.4g/e RF IPv6 over low-power wireless personal-area networks (6LoWPAN), and IEEE 1901.2 NB-PLC 6LoWPAN Serial, ATM, Frame Relay, and SONET/SDH	Media diversity for local and backhaul communications Smooth evolution over long lifetime period **Note:** IPv6/6LoWPAN is the only IP protocol version defined for IEEE 802.15.4g/e and 1901.2
Routing (network layer)	Static, Routing Information Protocol (RIP), OSPF, Enhanced Interior Gateway Routing Protocol (EIGRP), Intermediate System-to-Intermediate System (IS-IS), Multiprotocol Border Gateway Protocol (MP-BGP), and Routing Protocol for Low-Power and Lossy Networks (RPL) (IPv6 only)	Dynamic reactivity to communication and network device failures Scalability of deployment
Data integrity, confidentiality, and privacy (all layers)	Layer 2 (MAC specific), Layer 3 (IP Security [IPsec] IPv4/IPv6), Layer 4 (TCP/TLS, User Datagram Protocol [UDP]/Datagram Transport Layer Security [DTLS]), and Layer 7 (application-dependent authentication and encryption Packet filtering, deep packet inspection (DPI), intrusion detection system (IDS), and flow monitoring	Multilayered, highly secure networking
Multicast (network layer)	IPv4/IPv6 multicast protocols: Interior Group Management Protocol (IGMP)/Multicast Listener Discovery (MLD), Protocol Independent Multicast (PIM), and MP-BGP	Scalable software upgrade; group commands
QoS	Specific MAC-layer Class of Service (CoS), such as Ethernet and WiMAX IPv4/IPv6 QoS Differentiated Services (DiffServ) architecture	Multiservice FANs Prioritization of data traffic Service-level agreements
Network segmentation and isolation	Virtual private networks (VPNs) (Layer 3), such as IPsec VPN, Virtual Routing and Forwarding (VRF) Lite	Shared infrastructures but dedicated and isolated traffic paths for critical applications
Time distribution	Layer 3, such as Network Time Protocol version 4 (NTPv4)	Secure NTP4 for both IPv4 and IPv6
Management	Domain Name System (DNS), IP Flow Information Export (IPFIX), Simple Network Management Protocol (SNMP), Constrained Application Protocol (CoAP), SSH, telnet, XML/Netconf, etc.	Push and pull management models Scalable endpoint management

(**Source:** Cisco)

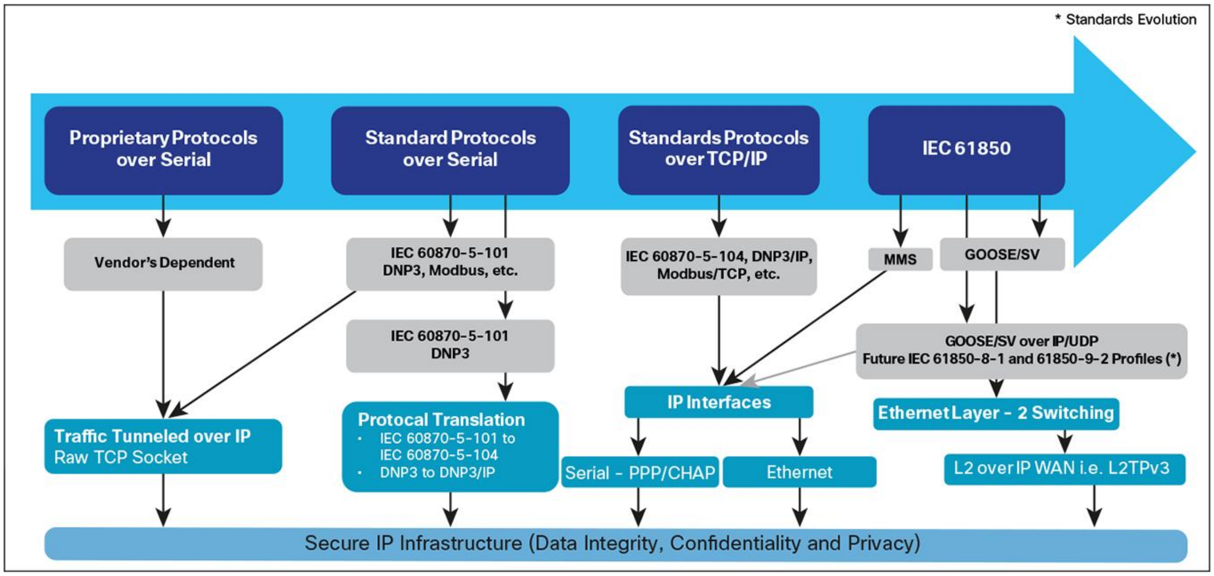
6. Standards-Based Integration of Legacy Assets

Over the expected lifetime of a DA solution deployment, it is expected that the SCADA system will be updated in association with use cases and protocol evolutions. Today, utilities have a mix of multiple different SCADA protocols and associated network interfaces across their service territories. As utilities evaluate DA communications solutions, one key consideration is standards-based integration of legacy SCADA protocols for graceful migrations. This section evaluates how different categories of SCADA protocols may be transported over an IP infrastructure. SCADA protocols can be classified into four broad categories and associated solutions for integrating and transporting them over IP networks (Figure 3):

- **SCADA protocols with native IP support** such as Distributed Network Protocol (DNP3) IP, IEC 60870-5-104, and IEC 61850 Manufacturing Message Specification (MMS) can natively attach to an IP-based network. IEC 61850-90-5 aims to create an IP-based routable profile (for GOOSE and sampled values). The routable profile, combined with multicast technologies, facilitates a scalable use of GOOSE and sampled values over the WAN and avoids issues such as the spreading of fault domains between substations (one of the limitations of Ethernet Layer 2-based profile). It also facilitates new and extended use cases of protection schemes in DA, and the integration of distributed energy resources (DER) and distributed generation.

- **Tunneling** is a generic feature that can be applied to any standards-based (for example, DNP, IEC 60870-5-101) or proprietary serial protocols. In this case, when frames are received over a source serial (RS232 or RS-485) port on a DA gateway configured for tunneling, it encapsulated the data in TCP/IP or UDP/IP header, hence creating an IP packet. Similar steps are implemented on the destination end.
- **Serial protocol translation** is implemented on the IP source's DA gateway connected to a serial-based DA device. When frames are received over a source serial port, it converts the packet from Application Service Data Unit (ASDU) over frame to ASDU over TCP/IP, and then forwards it to the destination node, hence creating an IP packet. Similar steps are implemented on the destination end. In many cases, serial protocols have evolved and have a new corresponding specification for their TCP/IP implementation (for example IEC 60870-5-101 and IEC 60870-5-104).
- **Tunneling Ethernet-based (non-IP) protocols** such as GOOSE/IEC 61850 can be achieved using IP technologies such as Layer 2 Tunneling Protocol version 3 (L2TPv3). When Ethernet (non-IP) frames are received over a source Ethernet port, they are encapsulated in IP packets, and then forwarded to the destination node.

Figure 3. Evolution of DA Protocols


* Standards Evolution
Proprietary Protocols over Serial
Standard Protocols over Serial
Standards Protocols over TCP/IP
IEC 61850
Vendor's Dependent
IEC 60870-5-101
DNP3, Modbus, etc.
IEC 60870-5-104, DNP3/IP,
Modbus/TCP, etc.
MMS
GOOSE/SV
IEC 60870-5-101
DNP3
GOOSE/SV over IP/UDP
Future IEC 61850-8-1 and 61850-9-2 Profiles (*)
IP Interfaces
Ethernet Layer - 2 Switching
Traffic Tunneled over IP
Raw TCP Socket
Protocal Translation
• IEC 60870-5-101 to IEC 60870-5-104
• DNP3 to DNP3/IP
Serial - PPP/CHAP
Ethernet
L2 over IP WAN i.e. L2TPv3
Secure IP Infrastructure (Data Integrity, Confidentiality and Privacy)

(**Source:** Cisco)

It must be noted that all SCADA protocols supporting IP have been defined for IPv4 in their original specifications. With the growth of popularity in native IPv6 networks (for example, IEEE 802.15.4 and IEEE 1091.2) comes a requirement to transport IPv4 traffic over IPv6 network. The unified FAN architecture meets this requirement by using the Mapping of Address and Port using Translation (MAP-T) protocol, which is being developed as part of the IETF Soft Wire working group.

Benefits: The unified FAN architecture facilitates standards-based integration of legacy assets with the following benefits:

- Provides a graceful migration roadmap for grid modernization, and eliminates millions of dollars of CapEx associated with a complete equipment upgrade of deployed legacy distribution assets.
- Helps utilities use a rich set of network security, disaster recovery, QoS, and other capabilities based on a consistent network services implementation independent of whether the DA asset is legacy serial-based or IP-enabled. This, in turn, eliminates additional cost, time, and risks associated with creating custom architectures for each serial protocol implementation.

7. Network Security and Compliance

Adding networking capabilities to the smart-grid last mile requires considering it as a critical infrastructure, which must integrate network security mechanisms to control access to critical utility assets, monitor the network, mitigate threats, and protect grid facilities. Security is a very broad topic and can be further divided into four areas, as discussed in more details in the following sections.

Benefits: Implementing network security based on a unified FAN architecture provides utilities with the following benefits:

- Functions, such as access control and data integrity, are independent of the choice of underlying communications technology. This means utilities can unify their security operational procedures and streamline network operations, thus reducing O&M costs.
- Easy integration with existing legacy DA devices: These capabilities provide utilities with a graceful migration roadmap for grid modernization and eliminates millions of dollars of CapEx associated with a complete equipment upgrade of deployed legacy distribution assets.
- Adopting these solutions based on standard IT security solutions provides utilities with a rich and broad ecosystem of vendors and eliminates vendor exclusivity. This allows utilities to benefit from a rich set of security capabilities and innovations in this rich ecosystem of vendors, which would not have been possible with a proprietary technology, and to reduce costs and implement a more efficient procurement process.

7.1 Access Control

Access control solutions are based on two fundamental elements: first, strong identity management mechanisms for all grid elements including users, devices, and applications; and second, mutual authentication of nodes involved in communications.

For identity and certificate management, utilities should use standards-based mechanisms such as X.509-based digital certificate [8], IETF Simple Certificate Enrolment Protocol (SCEP) [5] for installing new certificates in a highly secure way, and Online Certificate Status Protocol (OCSP) [9] and Certificate Revocation Lists (CRL) [10] for revoking compromised certificates in a highly secure way. This highly secure identity also forms the basis of authentication, authorization, and accounting (AAA) services performed between the different entities in the network FAN, HERs, NMS, and authentication servers. Similarly, for AAA services, we recommend utilities use standards-based mechanisms such as IEEE 802.1x [31], Extensible Authentication Protocol (EAP) [32], and Remote Authentication Dial-In User Service (RADIUS) [30], in conjunction with the X.509 certificate-based identity.

Benefits: The access control solution allows utilities to integrate their DA assets into their existing public key infrastructure (PKI)[4]; scalable, remote, certificate management solution; and access control solutions, hence, eliminating the need for deploying, qualifying, integrating, training, and defining operating procedures for a new custom solution. This, in turn, cuts millions of dollars of cost and many months of effort, and reduces risk to the DA deployment.

7.2 Data Integrity, Confidentiality, and Privacy

Data encryption technologies ensure data integrity and confidentiality for data from DA devices when flowing across public or private networks. Data encryption solutions are based on two fundamental capabilities: **encryption technology** and **key management**.

Utilities can choose from a variety of encryption mechanisms available at various layers (link layer, network layer, transport layer, and application layer) of the communication stack to provide data confidentiality. This choice is based on application requirements, node constraints in terms of processing power, the network architecture, and scalability of deployment. To balance the need for encryption with the processing capabilities and scalability requirements, particularly on low-end sensors with scarce computing resources, utilities should select the appropriate layer encryption, for example: link-layer encryption takes advantage of hardware assistance on PHY and MAC layers such as IEEE 802.15.4g/e, and IEEE 1901.2 NB-PLC for more advanced devices with hardware-based crypto engine implementations.

Because utilities deploy tens of thousands of DA devices, **key management**[5] **(generation and exchange)** can become a significantly challenging task. Utilities should consider solutions based on X.509 certificates and Internet Key Exchange version 2 (IKEv2- RFC 4306) [6] for scalable key management, mutual authentication, and establishment and maintenance of security associations (SAs). Group-based key management for link-layer encryption is provided by IEEE 802.11i [23] and group-based key management for network-layer encryption is provided by Group Domain of Interpretation (GDOI- RFC6407) [7].

Benefits: Implementing these data integrity, confidentiality, and privacy solutions provides utilities with the following benefits:

- These encryption capabilities can easily work with existing legacy DA devices that may not have any encryption support. This provides utilities with a graceful migration roadmap for grid modernization, and eliminates millions of dollars of CapEx associated with a complete equipment upgrade of deployed legacy distribution assets.
- They provide enhanced security based on certificates, standards-based key management procedures, and other network services rather than on preshared keys.
- This network-based design choice is fully compatible with all IP network services, including multicast, network segmentation, and QoS, while preserving network visibility into the traffic at the FAR and headend aggregation router. Some of these capabilities might be lost in higher-layer encryption methods.

[4] PKI-based model is consistent with and can be extended to meet the requirements of distributed application architecture. Mutual trust between multiple DA gateways can be achieved based on membership in the utility's (common) PKI.

[5] Group-based encryption mechanisms can provide scalable encryption and key management architecture for distributed application architectures.

Note regarding IEC 62351: The IEC 62351 [17] set of security standards extends the security capabilities of the underlying network in order to establish end-to-end security. As an example, IEC 61850 GOOSE messages define methods to protect data packets as defined in IEC 62351-6 [16]. Furthermore, the IEC 62351-8 [21] and IEC62351-9 [22] provide the basis for interoperability of key and certificate management functions. These standards also embrace the same principles and standards mentioned above for providing these capabilities, hence allowing utilities to unify their certificate and key management solutions.

Note regarding application-layer security: Application-layer security specific to a given application and application protocol, complements network-layer security and can be used or be supplemented by use of application-layer techniques that verify message integrity and proof of origin (digitally signed firmware images or digitally signed commands). Implementing application-layer encryption, while providing higher levels of security, may conflict with distributed application architectures[6].

7.3 Threat Detection and Mitigation

Threat detection solutions identify any anomalies in traffic patterns by monitoring application-specific traffic at different places (for example, DA gateway, FAR, HER) in the network using packet filtering and inspection capabilities, such as access lists, firewalling, intrusion detection, deep packet inspection, and IPFIX, and also network management features, such as syslog and IPFIX information. Event logs from most if not all communicating devices can be collected and passed on to a security incident and event manager (SIEM) tool. IPFIX applications can collect these records from routers, enabling traffic profiling, capacity planning, and denial of service (DoS) detection. Such applications can correlate events occurring in different parts of the grid to identify security incidents, facilitating a quicker and more coordinated response.

Threat mitigation solutions[7] provide mechanisms to segment and isolate the network to limit the impact of and protect the utility's network, in case a single device, or a single set of devices, gets compromised. Standards-based networking features such as Layer 2 Ethernet virtual LANs (VLANs), Layer VRF-Lite, or IPsec Generic Routing Encapsulation (GRE) tunnels can be set up.

Based on the security and application requirements, the segmentation of traffic can start at different places in the network. For example, FAR interfaces place traffic from different sets of devices in an isolated domain, headend aggregation routers and firewalls isolate and filter traffic dedicated to headend application servers, and different applications in the control center tier are part of a layered design based on stricter restrictions with increasing security levels.

Benefits: Adopting a threat detection and mitigation solution based on standard IT solutions provides utilities with a rich and broad ecosystem of vendors and eliminates vendor exclusivity. It also:

- Helps utilities benefit from a rich set of capabilities and innovations in this rich ecosystem of vendors, which would not have been possible with a proprietary technology
- Reduces costs and facilitates a more efficient procurement process

[6] Distributed application architectures require data visibility at the field devices, substation devices, and control center applications and should consider network layer encryption.

[7] Threat detection solutions are consistent with and can be extended to meet the requirements of distributed application architectures. Additional group-based rules for allowing and restricting traffic flows must be configured using standard features such as Layer 2 VLANs and Layer 3 VRFs.

7.4 Device and Platform Integrity and Vulnerability Management

A basic tenet of security design is to ensure that devices, platforms, endpoints, and applications cannot be compromised easily and are resistant to both physical and Internet attacks. Field devices such as FARs and DA gateways are typically deployed in physically non-secure locations. As part of the network design process, we recommend utilities consider hardware-based capabilities such as motion detectors, tamper-resistant mechanical design, hardware signature of equipment (for example, IEEE 802.1AR standards-based highly secure unique device identifier), and tamper-proof, highly secure storage based on security co-processors. To protect against Internet attacks, we recommend capabilities such as digitally signed software image for authentication and integrity validation.

Vulnerability management is another key aspect. The massive adoption of IP standards by the Industry has driven cooperation on security, helping global teams to identify, inform, and fix security issues, and making "security through obscurity" clearly inappropriate. Utilities deploying unified FAN architecture should strongly consider how to mandate or adopt the following security processes. Software development processes, known as Secure Software Development Lifecycle principles, provide more robust and highly secure software and firmware solutions from vendors adopting them. Security officers, often already managing security for the utility's IT enterprise solutions, should review endorsement by vendors of official processes to publish security advisories, such as Common Vulnerability Scoring System (CVSS), combined with collaboration with organizations such as national or regional Computer Emergency Response Team (CERT), Computer Security Incident Response Team (CSIRT), and vendors (for example, Cisco PSIRT). In addition, we recommend internal and third-party vulnerability assessments and penetration tests to validate product-level and solution-level robustness against network attacks.

Benefits: The above solution helps utilities use their existing IT risk management processes for grid deployments, thus, eliminating the need for defining operating procedures for a new custom solution. This, in turn, cuts millions of dollars of cost and many months of effort, and reduces risk to the DA deployment.

8. Disaster Recovery (DR) and High Availability (HA) Architecture

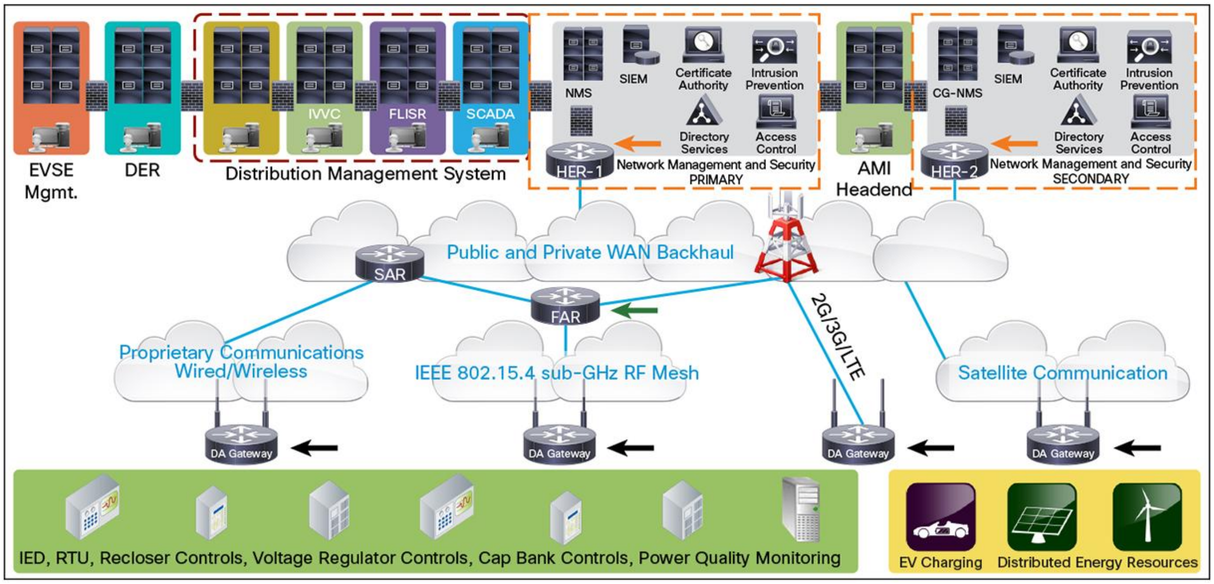
As utilities look at rolling out high-value DA applications, end-to-end network reliability and availability can be critical. The level of the solution availability is dependent on products, links, and network design considerations, as well as the criticality of a given asset based on place in the network. We will segment our analysis into two sections: **product- and link-level reliability and end-to-end network-level reliability**.

Product and link level reliability: As utilities deploy FAN architectures, they should consider the impact of device failures (full or partial), specific interface failures, or failures in the link between devices. The degree of impact can then be weighed in relation to cost and expectations to define the level of reliability and appropriate reliability mechanisms. Figure 4 shows some examples.

Discussion for the example shown in Figure 4: All traffic coming from all DA devices flows through the HERs), increasing the chance of device failure. We recommend utilities either deploy multiple control centers providing geo-redundancy or chassis-level redundancy with transparent failover capabilities using routing protocols. Further down in the architecture, each SAR and FAR typically aggregates traffic from tens of DA devices. We recommend utilities consider characteristics such as power redundancy with the ability to connect multiple power inputs or battery backup support, dual backhaul communication interfaces to protect against link failure, and hardened hardware that is compliant with industrial-grade standards (for example, IE61850-3/IEEE1613) for harsh deployments. Redundancy characteristics of the FAR chassis may be reviewed in an overall cost constraint.

Finally, DA gateways connect a single DA device. We recommend redundancy mechanisms, such as power redundancy, as well as hardened hardware that is compliant with industrial-grade standards (for example, IE61850-3/IEEE1613) for harsh deployments.

Figure 4. Hardware Reliability


EVSE Mgmt.
DER
IVVC
FLISR
SCADA
Distribution Management System
NMS
SIEM
Certificate Authority
Intrusion Prevention
Directory Services
Access Control
HER-1
Network Management and Security PRIMARY
AMI Headend
CG-NMS
SIEM
Certificate Authority
Intrusion Prevention
Directory Services
Access Control
HER-2
Network Management and Security SECONDARY
Public and Private WAN Backhaul
SAR
FAR
2G/3G/LTE
Proprietary Communications Wired/Wireless
IEEE 802.15.4 sub-GHz RF Mesh
Satellite Communication
DA Gateway
DA Gateway
DA Gateway
DA Gateway
IED, RTU, Recloser Controls, Voltage Regulator Controls, Cap Bank Controls, Power Quality Monitoring
EV Charging
Distributed Energy Resources

End-to-end network reliability[8]**:** Network- or solution-level reliability capabilities enhance network robustness and disaster recovery capabilities by creating redundancy across different components in the network. In case of failure, the stand-by components will automatically take over without impacting the DA application. Figure 5 shows some examples.

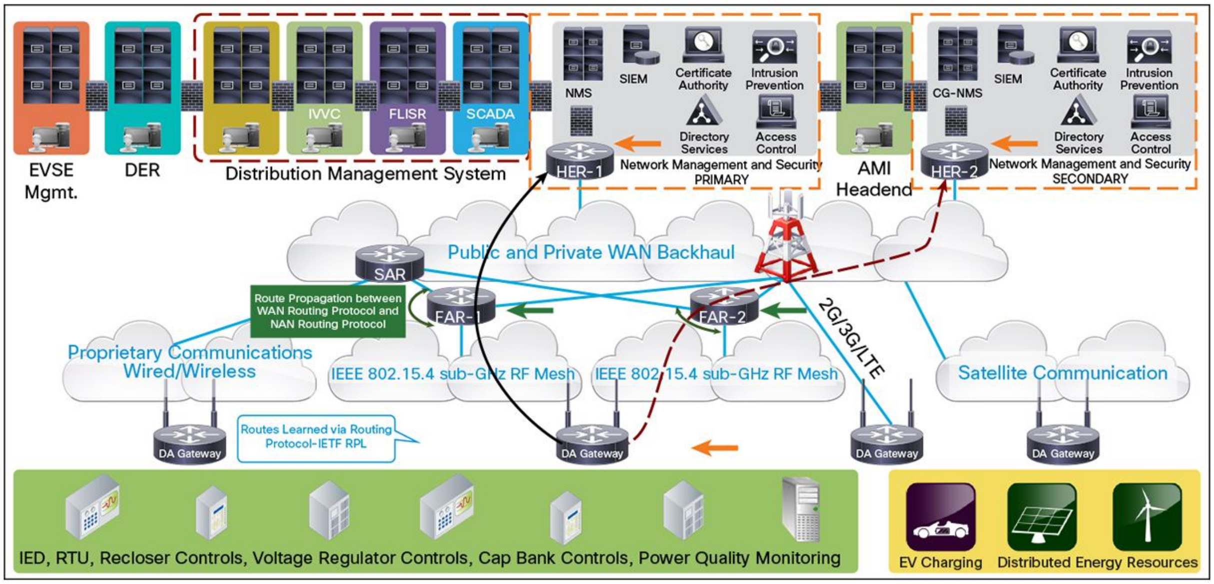
In this case, the utility is running redundant control center architecture using dynamic routing standards such as OSPFv2 [36] or OSPFv3 [35] MP-BGP ([13] and [14]) in the WAN, and RPL ([11] and [12]) as the neighborhood-area network (NAN) protocol for an IEEE 802.15.4g/e RF or IEEE 1901.2 NB-PLC mesh subnet with standards-based route redistribution, a mechanism used for years by Internet service providers (ISPs) and enterprises.

Discussion for the example shown in Figure 5: The benefit of dynamic IP routing (or Layer 3) protocol becomes crucial for network redundancy as illustrated by the following failover scenarios. In this example, a DA gateway uses FAR-1, attached to HER-1, as the primary path (as depicted by the black arrow) for connecting to the headend. In case of failure on FAR-1, the DA gateway can automatically reconnect to an adjacent FAR (FAR-2) through the mesh network via the WPAN migration mechanism, and gets its reachability updated through FAR-2, which will reflect the change in its RPL database, redistributing the information to HER-2 into BGP that will also update HER-1, without any manual intervention. Communications between the DA gateway's devices and SCADA server(s) will transparently use the backup path (as depicted by the dark red arrow) without the need to update any IP addresses, or perform any manual reregistration.

[8] In addition to the DR and HA architecture discussed, distributed application architectures are new. Architects must define the expected behavior of groups in case of fault scenarios (link and device). Additional network connectivity and routing protocol requirements, as well as additional application capabilities such as data replication, should be considered and included in the final solution design.

Note: While an end-to-end Layer 3 routing approach simplifies the dynamicity of endpoint reachability, whatever the PHY and MAC layers, it should be highlighted that in case of Layer 2 domain and technology implementing non-standards-based Layer 2 meshing protocol, the mapping of Layer 2 and Layer 3 reachability between technology domains is outside the scope of any standard and requires a proprietary and custom-built Layer 2-to-Layer 3 translator.

Figure 5. High Availability and Disaster Recovery Architecture



EVSE Mgmt.
DER
IVVC
FLISR
SCADA
Distribution Management System
NMS
SIEM
Certificate Authority
Intrusion Prevention
Directory Services
Access Control
HER-1
Network Management and Security PRIMARY
AMI Headend
CG-NMS
SIEM
Certificate Authority
Intrusion Prevention
Directory Services
Access Control
HER-2
Network Management and Security SECONDARY
Public and Private WAN Backhaul
SAR
Route Propagation between WAN Routing Protocol and NAN Routing Protocol
FAR-1
FAR-2
2G/3G/LTE
Proprietary Communications Wired/Wireless
IEEE 802.15.4 sub-GHz RF Mesh
IEEE 802.15.4 sub-GHz RF Mesh
Satellite Communication
Routes Learned via Routing Protocol-IETF RPL
DA Gateway
DA Gateway
DA Gateway
DA Gateway
IED, RTU, Recloser Controls, Voltage Regulator Controls, Cap Bank Controls, Power Quality Monitoring
EV Charging
Distributed Energy Resources

Benefits: Implementing disaster recovery and high availability based on unified FAN architecture provides utilities with the following benefits:

- These DR and HA capabilities can easily work with existing legacy DA devices and applications, providing utilities with a graceful migration roadmap for grid modernization and eliminating millions of dollars of CapEx associated with a complete equipment upgrade of legacy assets.
- Adopting hardware-reliability standards such as IEC61850-3/IEEE1613 lowers failure rates associated with field devices and thus reduces O&M costs associated with truck rolls.
- These DR and HA capabilities are independent of the choice of underlying communications technology and applications. This means utilities can unify their operational procedures and streamline network operations for disaster recovery, which reduces O&M costs as compared with defining DR and HA capabilities for each and every application and proprietary communications technology.
- These DR and HA capabilities enable advanced DR and HA capabilities with higher levels of service availability. The link-independent nature allows utilities to implement high availability across multiple communications technologies (such as cellular and RF mesh connectivity to a single endpoint).
- Utilities today have a well-defined architecture for high availability and disaster recovery at their WAN edge. The unified FAN architecture works well with this existing architecture and eliminates the need for qualification, integration, training, and defining operating procedures of new HA/DR platforms, which could add millions of dollars and many months of effort, and increase risk to the DA deployment.

- Adopting these standard, IT-based, DR and HA solutions provides utilities with a rich and broad ecosystem of vendors. This allows utilities to benefit from a rich set of capabilities and innovations in this rich ecosystem of vendors, which would not have been possible with a proprietary technology. It also reduces costs and facilitates a more efficient procurement process.

9. Ease of Use to Reduce Total Cost of Ownership (TCO)

Because utilities deploy communications to tens of thousands of DA devices, having a comprehensive communications NMS is critical to reduce the TCO of the network. When considering TCO, there are two key components: **cost of deployment** and **cost of managing the network over its lifetime**.

Zero-touch deployment[9]: Field technicians should be provided with a highly secure and automated zero-touch deployment (ZTD) process. As part of the ZTD process, the DA gateway should automatically authenticate with the headend based on device credentials. This device should then authenticate automatically with the utility's authentication and authorization solution. After that, the DA gateway should enroll in a highly secure way with the utility's PKI and also establish encryption mechanisms without manual intervention. (Security mechanisms are discussed in sections 7.1 and 7.2). Finally, the DA gateway and NMS should follow an automated process to complete IP address allocation, device discovery, and registration without any manual intervention requirements.

Network monitoring and troubleshooting[10]: Operating large communication networks, with thousands of devices spanning over tens of thousands of miles of distribution feeders, imposes significant challenges for the utility. Utilities can optimize their operational expenses associated with managing this communication network by deploying a robust and feature-rich NMS with the following capabilities:

- Complete fault, configuration, accounting, performance, and security (FCAPS) network management capabilities as provided by a traditional NMS solution
- Alignment with the utility business process requirements from DA device lifecycle management for operations, with emphasis on highly secure network commissioning and monitoring
- Network management function visualization on a geographic information system (GIS) map view for operator ease of use
- Integration with utility operations and enterprise bus through a northbound API to allow various SCADA applications to pull service-specific network communications data
- Emphasis on wireless-specific network management and troubleshooting procedures

Note: Distribution grid and FAN deployments necessitate certain purpose-built features, as discussed above, in addition to traditional FCAPS capabilities.

[9] The ZTD architecture discussed here is applicable to distributed application architectures. Architects must define the expected ZTD behavior for different groups. Additional network deployment and application installation requirements should be considered and included in the final solution design.

[10] The NMS architecture discussed here is applicable to distributed application architectures and provides centralized monitoring of the network conditions, alarms, and events to a network operator, which is critical to ensure proper operations of the DA applications.

Benefits: Implementing network management based on unified FAN architecture helps utilities reduce:

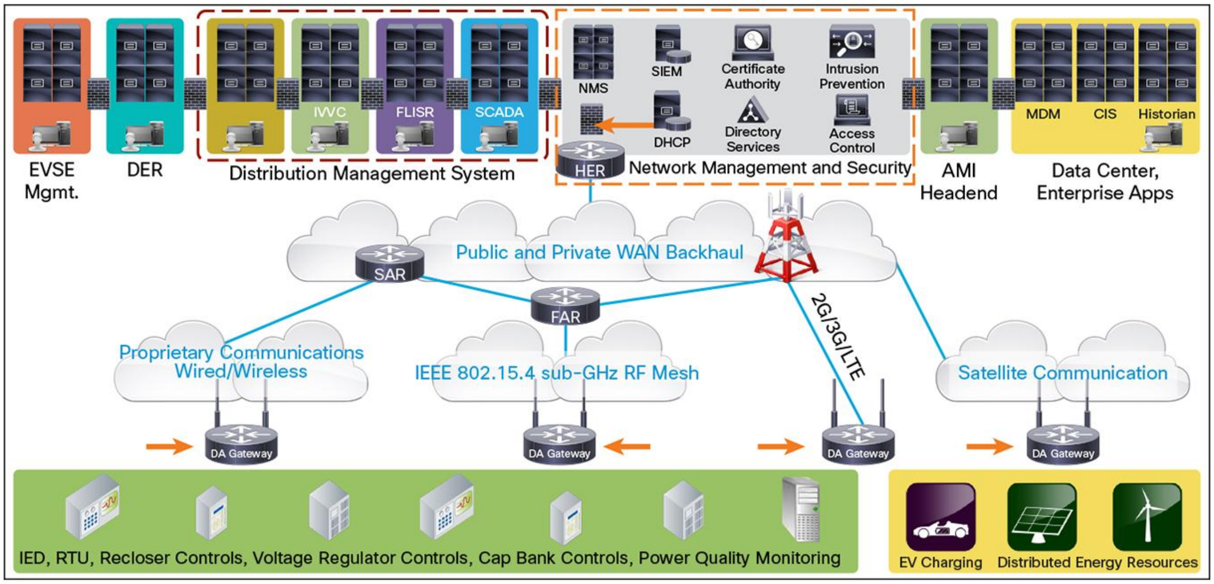
- O&M costs by providing a strong set of GIS-based and wireless-centric network monitoring and troubleshooting tools
- Deployment costs because, with ZTD processes, the utility does not need to send network experts to configure networked devices on every deployment site
- Time to deployment because a DA gateway automatically completes the authentication, configuration, and registration steps in a few minutes
- Risk of configuration errors, such as typing an incorrect IP address or server address, because all the setup is completed without any manual inputs from any field technician

10. Interoperability and Scalability between Control Center and End Devices

Endpoints and communication devices, such as DA gateways, deployed in the field interact with the utility headend infrastructure for network services using various standards-based protocols as discussed in the sections above. Typically, utilities have well-defined and robust IT standards for network connectivity with devices deployed outside their control centers, for example, in distribution centers and service centers. As utilities look at deploying communication networks for field devices, they should plan for ease of integration into existing IT solutions and applications. Figure 6 shows an example.

Discussion of the example shown in Figure 6: Utilities typically have an IP address management (IPAM) solution deployed for their enterprise networks. Field devices not only need to get an IP address, but often also require additional information, such as SCADA, NMS, or time server address. Field devices and DA gateways implemented with standards-based DHCP clients can easily be connected and receive their parameters from an existing solution.

Figure 6. Interoperability and Scalability between Control-Center and End Devices


EVSE Mgmt.
DER
IVVC
FLISR
SCADA
Distribution Management System
NMS
SIEM
Certificate Authority
Intrusion Prevention
DHCP
Directory Services
Access Control
HER
Network Management and Security
AMI Headend
MDM
CIS
Historian
Data Center, Enterprise Apps
Public and Private WAN Backhaul
SAR
FAR
2G/3G/LTE
Proprietary Communications Wired/Wireless
IEEE 802.15.4 sub-GHz RF Mesh
Satellite Communication
DA Gateway
DA Gateway
DA Gateway
DA Gateway
IED, RTU, Recloser Controls, Voltage Regulator Controls, Cap Bank Controls, Power Quality Monitoring
EV Charging
Distributed Energy Resources

Another consideration is the overall scalability related to the interaction between the field devices and the headend. Because utilities roll out thousands of devices, consideration should be made to the required scalability of network services, such as encryption, identity management, etc., and this should be designed into the network services headend.

Example: Utilities typically have a well-defined and robust encryption solution for performing network-layer encryption (IPsec). IPsec is a key requirement for any DA deployment running over public infrastructures, such as cellular, and this entails running IPsec-based encryption between the headend aggregation routers and the FARs acting as DA gateways. While basic IPsec tunnel setup can work well for small pilots, production deployment with thousands of DA gateways will represent a significant operational challenge in headend aggregation router scalability and management. We recommend utilities adopt IKEv2-based solutions. IKEv2 is a next-generation key management protocol based on RFC 5996 used for performing mutual authentication and also establishing and maintaining security associations (SAs).

Benefits: Implementing interoperability and scalability based on unified FAN architecture provides utilities with the following benefits:

- Performing detailed scalability design up front for all headend components and applications reduces the risk of finding scalability limitations further in the project and reduces the risk of project over-runs and schedule slips.
- Using an advanced IKEv2-based solution, as discussed in the example above, provides utilities with a more scalable solution and allows them to reduce the number of headend components. This, in turn, reduces up-front CapEx of headend equipment, and reduce OpEx because of reduced power and space costs, plus easier operations and maintenance.
- Using existing IT and security solutions and processes, as shown in the IPAM example, eliminates the need for additional qualification and integration of a new IPAM application into the utility's control center. This also eliminates the need for new training on how to manage, troubleshoot, and define operating procedures of new IPAM solutions. The same savings and benefits can apply to any existing IT and security solution, beyond the example of IPAM. This, in turn, could save millions of dollars and many months of effort, and reduce risks to the DA deployment.
- Providing a broad ecosystem of IT vendors to choose from reduces costs and facilitates a more efficient procurement process.

11. Conclusion

Distribution automation encompasses a wide range of possible applications, each with its own specific communications requirements. Specific DA application requirements, objectives, and the planned implementation will ultimately determine overall communications needs. This white paper defines a unified FAN architecture and provides a framework for the communications requirements imposed by DA applications in terms of performance, cost, and coverage, support of standards, security, manageability, scalability, and reliability.

To summarize, the key features and considerations of the unified FAN architecture are:

- Communications technology-agnostic and layered network services based on IP architectures
- Standards-based integration of legacy assets
- Network security and compliance
- Disaster recovery and high availability architecture

- Ease of use to reduce total cost of ownership
- Scalability and interoperability between the control center to the end devices

The unified FAN architecture provides utilities with many benefits, as compared with proprietary and non-IP-based technologies:

- Facilities optimal choices of communication technology based on specific application and deployment requirements, as well as deployment of a single, converged, IP-based architecture
- Provides a graceful migration roadmap for grid modernization, and eliminates millions of dollars of CapEx associated with a complete equipment upgrade of deployed legacy assets
- Reduces project schedule risks and cost over-runs by recommending mature and robust networking technologies
- Eliminates additional cost, time, and risks associated with design, deployment, and operation of proprietary procedures for security, high availability, QoS, and other functions, and also new IT and security architectures and software applications
- Reduces O&M costs and streamlines network operations based on IT best practices and eliminates the need for proprietary architectures
- Enables quick and cost-effective deployment of future applications based on integrated multiservice capabilities
- Reduces costs and facilitates a more efficient procurement process by providing utilities with a rich and broad ecosystem of vendors and eliminating vendor exclusivity

12. References

[1] U.S. Department of Energy (DOE). Smart Grid Investment Grant (SGIG) program under the American Recovery and Reinvestment Act of 2009**. (December 2012).** Reliability Improvements from the Application of Distribution Automation Technologies - Initial Results

[2] U.S. Department of Energy (DOE). Smart Grid Investment Grant (SGIG) program under the American Recovery and Reinvestment Act of 2009. **(December 2012).** Application of Automated Controls for Voltage and Reactive Power Management - Initial Results

[3] European Commission Joint Research Centre (JRC) (2013). Smart Grid projects in Europe: Lessons learned and current developments - 2012 Update

[4] IETF, Mapping of Address and Port using Translation (MAP-T) - Draft-ietf-softwire-map-t-04

[5] IETF, Simple Certificate Enrollment Protocol (SCEP) - Draft-nourse-scep-23

[6] IETF, Internet Key Exchange (IKEv2) Protocol - RFC 5996

[7] IETF, The Group Domain of Interpretation - RFC 6407

[8] IETF, Internet X.509 Public Key Infrastructure - RFC 2528

[9] IETF, X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol (OCSP) - RFC 2560

[10] IETF, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile - RFC 5280

[11] IETF, Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile - RFC 6818

[12] IETF, IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) - RFC 6550

[13] IETF, A Border Gateway Protocol 4 (BGP-4) - RFC 4271

[14] IETF, Multiprotocol Extensions for BGP-4 - RFC 4760

[15] Maik Seewald, Cisco, CIGRE, Lisbon 2013, IP Multicast Technologies for Power System Networks

[16] IEC, Power systems management and associated information exchange - Data and communications security, IEC 62351- Part 6: Security for IEC 61850

[17] IEC, Power systems management and associated information exchange - Data and communications security, IEC 62351

[18] IETF, Internet Protocols for the Smart Grid - RFC 6272

[19] IEC, Communication networks and systems for power utility automation, IEC 61850 - Part 90-5

[20] Dr.sc. Goran Leci, dipl.ing.el. Koncar, CIGRE, Paris 2014, Automatic Voltage Control of OLTC Power Transformers between Substations

[21] IEC, Power systems management and associated information exchange - Data and communications security, IEC 62351 - Part 8: Role-based access control **(work in progress)**

[22] IEC, Power systems management and associated information exchange - Data and communications security, IEC 62351-Part 9 (work in progress)

[23] Nancy Cam-Winget, Cisco, Tim Moore, Microsoft, Dorothy Stanley, Agere Systems, Jesse Walker, Intel Corporation, IEEE 802.11i Overview

[24] IETF, Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information - RFC 7011

[25] IEEE 802.11i, IEEE 802.11i-2004: Amendment 6: Medium Access Control (MAC) Security Enhancements

[26] IEEE, IEEE 802.11: Wireless LAN

[27] IEEE, IEEE 802.3: Ethernet

[28] IEEE, 802.15.4e-2012 - IEEE Standard for Local and metropolitan area networks-Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 1: MAC sublayer

[29] IETF, Behavior of and Requirements for Internet Firewalls - RFC 2979

[30] IETF, Remote Authentication Dial In User Service (RADIUS) - RFC 2865

[31] IETF, IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines - RFC 3580

[32] IETF, Extensible Authentication Protocol (EAP) - RFC 3748

[33] IEEE, 1901-2 - IEEE Standard for Low-Frequency (less than 500 kHz) Narrowband Power Line Communications for Smart Grid Applications

[34] IEEE, 802.15.4g-2012 - IEEE Standard for Local and metropolitan area networks-Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 3: Physical Layer (PHY) Specifications for Low-Data-Rate, Wireless, Smart Metering Utility Networks

[35] IETF, OSPF for IPv6 - RFC 7011

[36] IETF, OSPF Version 2 - RFC 2328

[37] IETF, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers - RFC 2474

[38] IETF, An Architecture for Differentiated Services- RFC 2475

[39] IETF, New Terminology and Clarifications for Diffserv - RFC 3260

13. Contributors

Adam Gauci, Cyber Security Marketing Manager, Schneider Electric, adam.gauci@schneider-electric.com

Al Vazquez, Enterprise Wireless Network Architect, Southern California Edison, al.vazquez@sce.com

Ben Kellison, Senior Analyst, Green Tech Media, kellison@gtmresearch.com

Borre Jensen, Manager Network Department, BKK, Borre.Jensen@bkk.no

Buddy Marshall, Ph.D., P.E., Principal Consultant, Power System Applications, OSI Inc., buddy.marshall@osii.com

Camillo Ascione, Network & System Integration Product Unit Co-Head, Italtel SpA, camillo.ascione@italtel.com

Carlos Mota Pinto, Associate Director, Smart Systems Development, EDP, carlos.motapinto@edp.pt

Craig Watson, Network Services Manager, Black & Veatch, watsonc@bv.com

Dale Robinson, Networks, Senior Manager, Accenture Technology Consulting, dale.e.robinson@accenture.com

Dr. Dominik Engel, Director, Josef Ressel Center for User-Centric Smart Grid Privacy, Security and Control, Salzburg University of Applied Sciences, dominik.engel@en-trust.at

Evan Kaverman, Networks, Consultant, Accenture Technology Consulting, evan.g.kaverman@accenture.com

Fabio Mostarda, Network and Security Architect, Selene SpA, A2A Group, fabio.mostarda@selenebs.it

Frank Bodewes, Telecommunication consultant, Asset Management, Enexis B.V., frank.bodewes@enexis.nl

Goran Leci, PhD, Deputy Director BU, Končar–Power Plant and Electric Traction Engineering Inc., goran.leci@koncar-ket.hr

James Formea, Senior Communications Engineer, Eaton’s Cooper Power Systems Business, JamesDFormea@Eaton.com

Dr. Jayant Kumar, Global Smart Grid Program Director, Alstom Grid, jayant.s.kumar@alstom.com

John-Paul Knauss, Principal Distribution Automation Engineer, National Grid, John-Paul.Knauss@nationalgrid.com

Lance Irwin, Business Development Manager, Schneider Electric, lance.irwin@schneider-electric.com

Lucio Cremaschini, PowerGrid Operations Manager, A2A Reti Elettriche SpA, A2A Group, lucio.cremaschini@a2a.eu

Melanie Miller, Manager New Technology Evaluation and Grant Strategy, Duke Energy, Melanie.Miller@duke-energy.com

Maik Seewald, Technical Business Development Manager, Energy, Cisco, maseewal@cisco.com

Dr. Mathias Uslar, R&D Division Energy, OFFIS, uslar@offis.de

Michael Dulaney, Director Business Development, Energy, Cisco, midulane@cisco.com

Nelson Freire, ECIL Energia, Executive Director, nlfreire@ecilenergia.com.br

Nick Orndorff, DMS Product Manager, OSI Inc., nick.orndorff@osii.com

Nitin Nayar, Product Manager, Cisco, nnayar@cisco.com

Patrick Grossetete, Distinguished Technical Marketing Engineer, Cisco, pgrosset@cisco.com

Paul Found, Systems Automation & Protection Team Lead, BC Hydro, paul.found@bchydro.com

Paul J. Zawada, P.E., Principal, Syntonous LLC, zawada@syntonous.com

Philippe Tordjman, Substation Automation Solutions, Business Development Director, Alstom Grid, philippe.tordjman@alstom.com

Roger Hey, Future Networks Manager, Western Power Distribution, rhey@westernpower.co.uk

Ross Hendrix, Networks, Manager, Accenture Technology Consulting, ross.a.hendrix@accenture.com

Sara Bavarian, Distribution Automation Engineer, Powertech Labs Inc., sara.bavarian@powertechlabs.com

Sol Lancashire, Telecom Architect, BC Hydro, sol.lancashire@bchydro.com

Tom Berry, Communications Solutions Architect, Schneider Electric, tom.berry@schneider-electric.com

Tom Johnson, Automation Market Manager, Smart Grid Solutions Marketing, Itron, tom.johnson@itron.com

Vaibhav Parmar, Networks, Managing Director, Accenture Technology Consulting, vaibhav.j.parmar@accenture.com

Yves Chollot, MV Solutions, Schneider Electric, yves.chollot@schneider-electric.com