PNNL-28720

Assessment of CReST-VCT Deployment in Real-Time Environments

Communication Systems Examination

May 2019

J Ogle
MD Touhiduzzaman
P Thekkumparambath Mana

U.S. DEPARTMENT OF ENERGY

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from the
Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062;
ph: (865) 576-8401
fax: (865) 576-5728
email: reports@adonis.osti.gov

Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
email: orders@ntis.gov <https://www.ntis.gov/about>
Online ordering: http://www.ntis.gov

1.0 Introduction

Incorporation of decentralized generation or distributed energy resources (DERs) such as solar and wind, is transforming the electricity grid. Developers, consumers, and energy providers are turning to renewable DER sources to supplement or supplant traditional sources. These resources can provide greater overall value when they are grid connected (EPRI 2014). While utilizing DERs as virtual power plants (VPPs) to provide grid support services offers a wide range of potential benefits, new levels of coordination between transmission and distribution systems must be realized to maintain overall grid stability (North American Electric Reliability Corporation 2017). To address this gap, Ke et al. have proposed the Coordinated Real-time Sub-Transmission Volt-Var Control Tool (CReST-VCT) (Ke, Samaan and Holzer 2018). This solution co-optimizes transmission and distribution control systems. The transmission control system requests grid services, such as reactive power support, from the distribution control system. The distribution control system evaluates its resources, including potential DERs, and determines the extent to which it can meet the request of the transmission system controller. It then reports back the limits of its operations to the transmission control system for consideration at the next coordination interval. A high level view of the CReST-VCT system model is depicted in **Figure 1**.

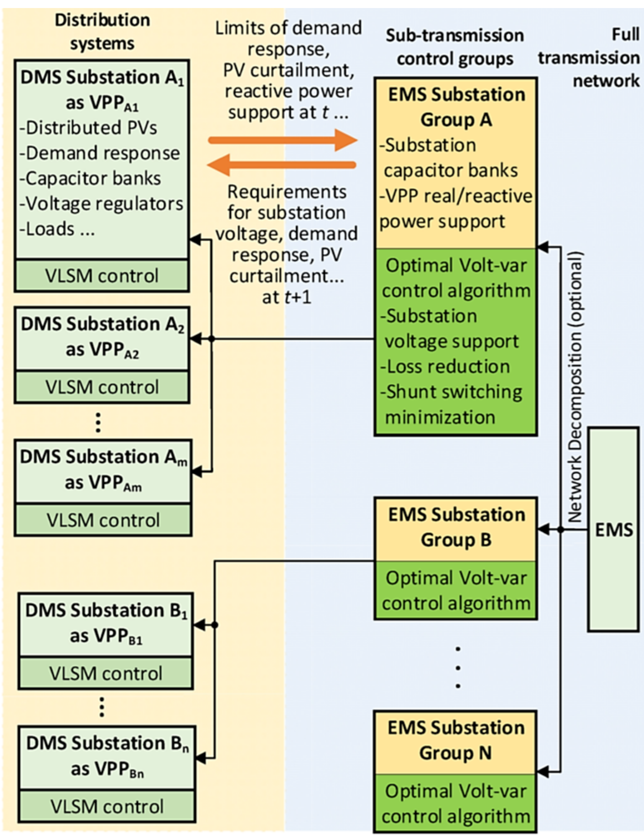

Figure 1. Crest-VCT Operation

Operation of systems such as CReST-VCT depends on the communication network between the various elements. Successful real-time operation will depend on the ability of the algorithm to complete necessary analysis and the ability of the communication system to transfer data reliably and within necessary time constraints.

In this paper, we examine the communication systems that are necessary to support the integration of the CReST-VCT optimization mechanism in a real-time operational environment. The required communication interfaces will be identified based on the operation model of CReST-VCT. The characteristics of the communication systems at these interfaces will be described to establish the context within which CReST-VCT will operate. The related protocols and cybersecurity domain will be reviewed. Potential issues and concerns will be identified to guide subsequent integration efforts.

2.0 CReST-VCT Operational Model Summary

Real-time execution of the CReST-VCT system must support interaction between transmission and distribution control center systems—that is, between the energy management system (EMS) and distribution management system (DMS), and between the DMS, substation, and field devices. CReST-VCT may be extended to consider the use of many different types of flexible resources for optimization. This could include communication between the utility's control systems and multiple third parties, as in the case of DERs not owned by the operating utility. However, for this initial examination of the dependencies between CReST-VCT and communication systems, only utility-owned DERs are considered.

The CReST-VCT algorithm runs on a repeating interval of nominally five minutes. Figure 2 depicts a simplified view of the process. Information exchange between systems that traverses communication networks occurs during each operational interval at points highlighted with a red vertical line. These exchanges are the focus of this paper. They span different networks within a utility communication system that may use varying technologies. Figure 2 represents the operation at the EMS, DMS, and DER and the data flow. From preliminary tests, the CReST-VCT algorithm takes about 45 seconds to solve at the EMS. About 15 seconds is available for sending a reactive power demand request, photovoltaic (PV) curtailment, etc. from the EMS to the DMS. Because an EMS might communicate with multiple DMSs, the communication may be staggered within those 15 seconds. At the DMS, solving the voltage-load sensitivity matrix (VLSM)–based volt-var control (VVC) algorithm takes about 30 seconds, using the operating points from the EMS, to set real and reactive power dispatch set points for DERs and flexible resources. The DMS will also obtain the reactive power capacity from the DERs and aggregate the information. The messaging to and from the DERs, and aggregation at the DMS, may take up to 120 seconds, over various elements of communication infrastructure. An additional ~30 seconds will be required if reoptimization is required at the DMS. Dispatch of new set points, reaggregation of limits, if required, and sending the DER flexibility limits to the EMS may take about 60 seconds. The cycle is repeated every five minutes.

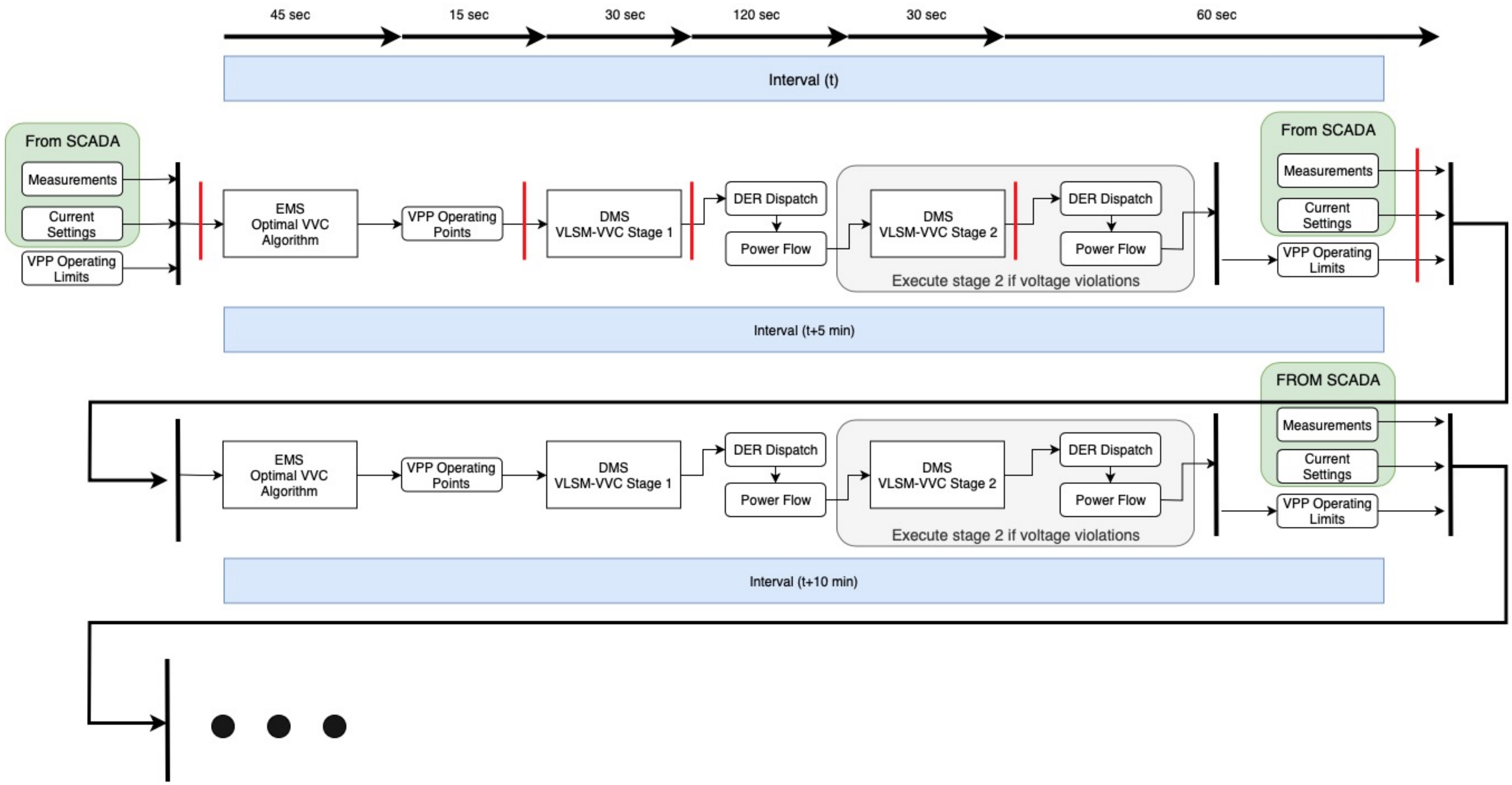

Figure 2. Operational Flow of CReST-VCT

3.0 CReST-VCT Communication Network Context

This section describes the communication network infrastructure that will be employed by the CReST-VCT tool. The physical, logical, and performance characteristics are discussed to establish the high level communication network context for coordination across the various systems involved.

Communication networks define protocols that establish rules that the systems that use the network must follow to transfer information across the network. There are many different standard protocols that cover different aspects of the communication system. The Open Systems Interconnection (OSI) Reference Model was established as a standard conceptual model that characterizes the structure and functions of a communication protocol. Figure 3 presents the seven-layer OSI model with an overview of the various functions at each layer. In general, most smart grid domain devices, including DERs, use a defined application layer protocol to communicate with each other. Those application layer protocols run over a standard Transport Control Protocol (TCP)/Internet Protocol (IP) connection. These IP connections may run over a variety of different physical layer protocols and media. Different protocols can be used in different layers on the devices that employ the CReST-VCT communication network. Specific protocols related to these systems are presented later in this document.

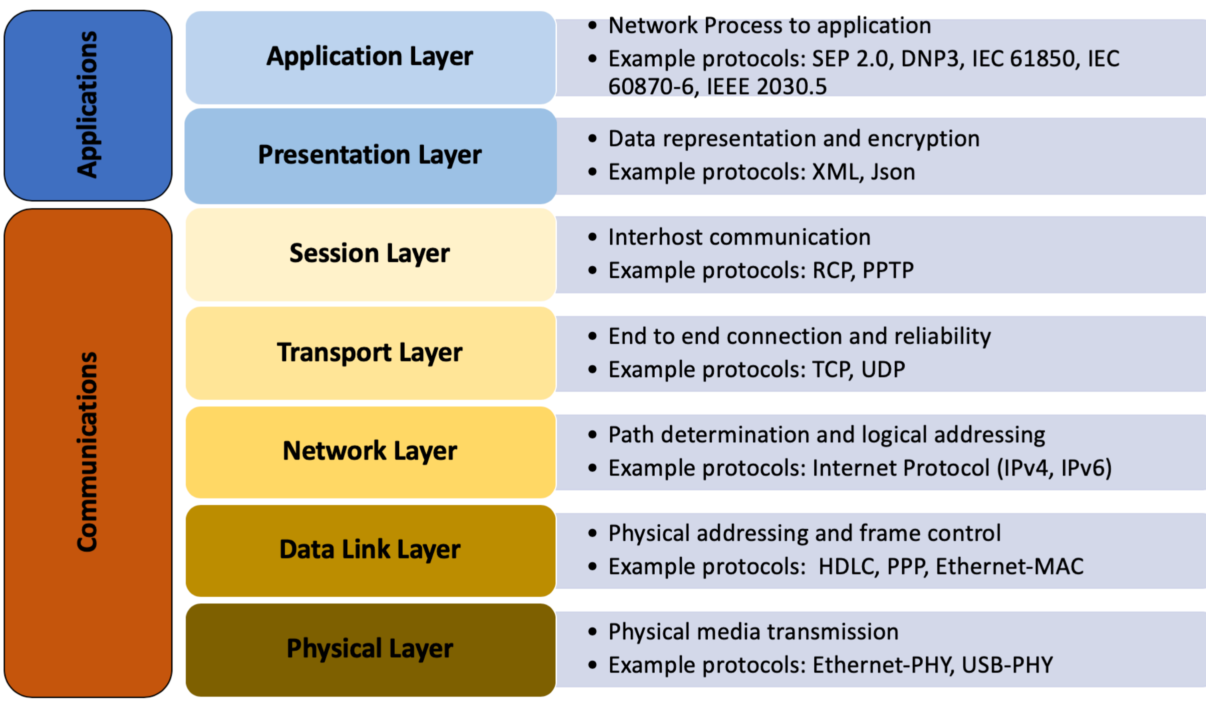

Figure 3. Hierarchal OSI Model Along with Their Functionalities and Protocols

3.1 Communication Network Characteristics

Many attributes in communication networks can influence the performance that is experienced by the users of the utility network structure. For examining dependence on communications systems for CReST-VCT, the following characteristics will be referenced.

Bandwidth can have multiple meanings in communication networks. In the context of this paper, bandwidth refers to the amount of data that can be transferred from one point to another over a communication system in a certain time. Bandwidth is measured in units of bits per second (bps, kbps, Mbps, Gbps). Throughput and goodput are additional metrics that are used to reflect the data transfer capacity of a network link that take into account retransmissions of bits and protocol overhead. For the purposes of this paper, where network structure is being identified, bandwidth will be used to compare the fundamental capacities of the physical network technologies.

Latency can also have different meanings in communication networks. In the context of this paper, latency refers to the time it takes to transfer data from one point to another over a communication system. It depends on the bandwidth of the system, the reliability of the system, network topology, and the efficiencies of the equipment and protocols used. A low-latency system has a short delay from when data is transmitted from one end of a link to when it is received at the other end.

Jitter in communication networks refers to variations in the latency of the transfer of packets from one point to another. Jitter can result from network congestion, packet route changes, and timing drift. In general, jitter is a consideration for real-time systems, including video and telephony. In power systems, jitter is an important consideration in some protection schemes. For the purpose of this paper, the data transfers associated with the CReST-VCT algorithm are not expected to require real-time performance, and jitter will not be a key consideration.

Availability in communication networks refers to the uptime of a network over a given period. Uptime refers to the amount of time a network is functional. It is expressed as a percentage. For example, a yearly availability metric of 99.999% (often referred to as five-nines) would indicate that the network experienced approximately 5 minutes of downtime over the course of the 525,600 total minutes in the year. Availability is related to the reliability of the components of the communication network system.

Reliability has multiple meanings in communication networks. In some contexts, reliability refers to the likelihood of failure of a network component, or the aggregation of the likelihoods of failures of components, to the network system level. Depending on the requirements of the users of a communication network, different design techniques, such as redundant equipment or paths, may be applied to maintain network availability even with component failures. Reliability is also used to characterize the behavior of communication protocols. A reliable communication protocol operates such that the sender of a message is notified by the receiver that the message was indeed received. This feature of a protocol enables automatic retransmissions should a message fail to be received. In this context, reliability is synonymous with assurance. The IP stack includes TCP, which is a reliable protocol, and User Datagram Protocol, which is an unreliable protocol.

3.2 Utility Communication Network Infrastructure

Due to the complexity of the electricity industry and the electricity grid, utilities rely on a complex set of communication networks to support their operations. These networks support interactions between systems within the utility as well as with external entities. Cisco Systems describes an industry reference model for the electric utility that defined 11 tiers of networks (Cisco Systems 2012). With prevalent use of supervisory control and data acquisition (SCADA), growing phasor measurement unit data collection at the transmission level, and increasing situational awareness and automation needs at the distribution level, grid operators are more dependent upon communications than ever (PNNL 2015).

The CReST-VCT tool provides an optimization that helps manage the increasing complexity of the grid by coordinating the transmission and distribution systems to better utilize DERs for grid services. As such, it relies on communications networks to support its operation. Figure 4 provides a simplified view of the various communication networks that are traversed to support real-time operation of CReST-VCT. This is a subset of the 11-tier model referenced above.

Utilities' communication networks are multi-tiered and use a variety of technologies. Utilities commonly maintain an operational network domain to support critical electricity grid communications and a separate enterprise network domain to support corporate business processes. With advances in networking technologies in recent years, it is becoming increasingly common to share physical infrastructure across these different logical network domains while maintaining appropriate performance and security requirements for each function. As the energy industry evolves with increasing levels of DERs, non-utility owners of DERs may participate in markets and grid services in coordination with the utility or distribution system operator. This coordination will make use of the internet and cloud services rather than the utility's private control network (Taft, De Martini and Kristov n.d.).

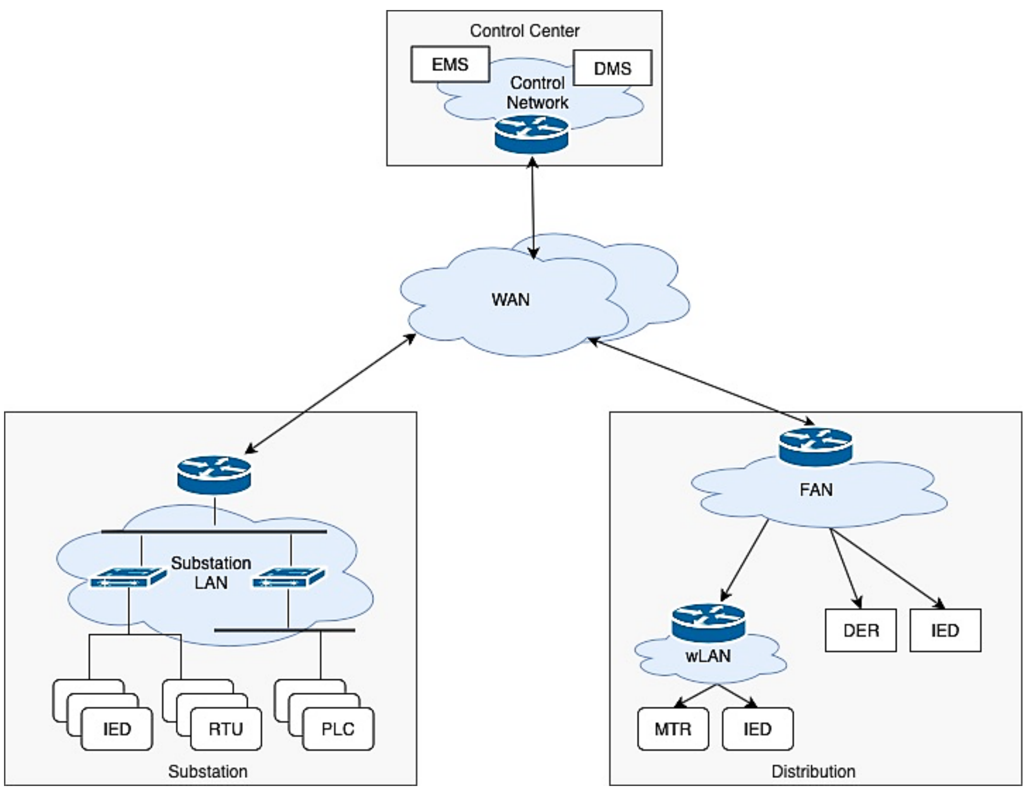

Figure 4. Communication Networks Supporting CReST-VCT

Operation of the CReST-VCT tool would involve communications across multiple network domains:

- Control center network (CCN) – Connects system applications in the utility control center.
- Wide area network (WAN) – An intermediate network to transport communications between systems at the control center to locations distributed across the utility service territory, such as substations.
- Substation local area network (LAN) – Connects devices within a substation, such as a switch and a relay. Devices on the substation LAN are connected to the control center applications through the WAN.
- Field area network (FAN) – Connects grid devices located outside the substation on the distribution feeders to applications in the control center (through the WAN). Devices include capacitor banks, regulators, or utility-owned DERs. The FAN may be configured to support peer-to-peer communication between grid devices for distributed control.
- Neighborhood area network (NAN) – Connects devices located on the distribution feeder, the meter, or behind-the-meter devices to applications in the control center. The NAN can be considered a subnetwork of the FAN.

Each of the network systems identified above represents a complex system of infrastructure and components that work together to provide data transfer services. Physical media (cables, fiber, wireless) connect networking equipment, such as switches and routers, that manage the flow of data across the network. Other equipment, such as firewalls, intrusion protection systems, and load balancers are interconnected within these network devices to maintain security and maximize efficiency. These individual network systems are connected together to form the utility network structure hierarchy depicted in Figure 4.

3.3 Communication Network Structures

3.3.1 Control Center Communications

A utility's control center and data center host critical operation and business applications and data. These systems increasingly share data to support their specific business needs. Applications in the control center and data center are maintained in carefully managed, environmentally controlled, secure locations. High-speed links are used between application servers and network equipment. Redundant equipment, redundant network feeds, and seamless failover are among the best practices used in designs of data center networks.

It is common practice to have a back-up control center that is capable of operating the grid should the primary control center have a significant failure or in case of a disaster. Best practice suggests that the back-up center be geographically separated from the primary center. The centers are often run in an active–active manner such that data flows in parallel to both primary and secondary so that no restoration activity is required to switch to the back-up location.

The control applications may use business data that is maintained in the corporate network. An example is geographic information systems data. The enterprise data center is also designed with high availability and reliability in mind. Disaster recovery sites similar to the control center are set up, but may not be active–active for all systems. Designs for disaster recovery vary depending on the recovery time objectives, but enable recovery of critical systems in the required time.

3.3.2 WAN

The WAN extends utility communications networks over a wide geographic area. In the electric utility context, the WAN connects substations, generation stations, and other energy delivery sites and equipment to the operations control center. In the past, the utility would utilize separate WAN infrastructure to support different business needs that had different network requirements. Control networks to support SCADA and teleprotection were separate from enterprise networks that transferred corporate data. Control networks achieved necessary latency, reliability, and predictability with time division multiplexing (TDM) technology and synchronous optical network (SONET) rings, which have inherent fixed latency. The current trend is moving away from this purpose-built network infrastructure at the WAN level.

For operational efficiency, and to scale to the increasing demands for deep situational awareness, utilities have been migrating toward a converged packet-based WAN network shared between corporate services and control services. IP-based networks with packet routing do not inherently have fixed, predictable latency such as is provided by legacy TDM networks. However, network technologies such as multiprotocol label service (MPLS) are used to manage network flows to make sure the utility control communication requirements are met (Fujikawa, et al. 2004). A detailed description of MPLS is beyond the scope of this paper. In short, it enables traffic engineering to establish virtual network segments that can follow a predefined path so that each segment can be have appropriate deterministic traffic, prioritization of flows, and flexible allocation of bandwidth over a single physical network (Hunt 2011). Assuming tools like MPLS are used, this paper will consider that the control system traffic related to CReST-VCT is not affected by corporate or other potential uses of a common WAN.

The WAN is made up of multiple physical communication network technologies and may be segmented into multiple subnetworks. Construction of physical networks across a wide geographic area can be a complicated, costly, and lengthy process. Hence, utilities often use a mix of utility-owned private network infrastructure and leased network infrastructure or services from telecommunication service providers. Through the use of MPLS, service providers can create a virtual private network (VPN) connection for utility customers to offer guaranteed service level agreements. This allows utilities to maintain the communication network operations the same as if the infrastructure was private.

Private infrastructure typically consists of fiber optic and wireless media. Fiber may be installed underground or overhead on towers and poles. Microwave radios are often used to transport traffic across long distances or to and from distant locations where fiber construction would be cost prohibitive. The radio frequencies used for this wireless transport vary, but both licensed and unlicensed frequencies are available.

Because broad business processes and critical infrastructure rely on the WAN network, there is an emphasis on reliability and resilience. In many cases, the WAN may be built with redundant links, equipment, and communication rings to support high availability. A common design methodology is to establish a high-speed core WAN network ring to connect control centers and critical substations. A second tier of WAN rings may extend the range to secondary substations. Radial extension out from the rings are the third tier of connection used to reach more remote areas.

The core network tier will have the highest bandwidth to support aggregation from lower tiers. As communication links extend toward the edge of coverage, bandwidth and data rates will decrease in general. Data rates in the 1 Gbps to 100 Gbps may be realized as part of the core

WAN. For lower-tier aggregation down to a radial access link, data rates down to 1 Mbps or lower could be used. Specific bandwidth, data rates, and implementations will be dictated by the demand and the geographic and business constraints of a given utility.

3.3.3 Substation LAN – sLAN

The substation LAN facilitates communication between devices within the substation to support station operations as well as communication between substation equipment and the control center. The substation connects to the WAN to support communication between substation infrastructure and the control center. To maintain security regardless of whether the WAN is private or uses leased services, all network traffic in and out of the substation must pass through a firewall at the substation edge demilitarized zone (DMZ). IEC 61850 provides a reference model for a substation communications network that uses three different networks or zones:

- The electronic security protection (ESP) zone contains all grid-related infrastructure and is the highest security zone.
- The multiservice zone contains physical security components such as ethernet-connected badge readers, local authentication, authorization, accounting, and logging applications.
- The corporate zone is an extension of the corporate network in a substation. It provides employees with access to corporate services like email, internet, and IP phones through ethernet or WiFi interfaces. It is the lowest security zone.

As CReST-VCT is concerned with operation of grid-related infrastructure, the ESP zone is of primary interest for this paper. The ESP zone contains a station bus and a process bus. The station bus connects grid devices across the different bays of equipment. It also connects the devices to the gateway router to enable connection to the control center. The process bus connects measurement and control equipment to intelligent electronic devices (IEDs). It carries power measurements and equipment status data from the switchyard source devices, such as current and potential transformers, to the IEDs and to relays that process the data into measurements and control and protection decisions. The process bus carries sampled measurement values from primary equipment in the switchyard to the protection equipment in the station control structure. These measurements are sampled at a continuous high rate resulting in high communication network bandwidth. Whereas the station bus supports control signaling that is not data intensive with lower bandwidth. Connected devices within a station bus are in close proximity with each other inside a control building in the station. The process bus connects equipment outside the control building, spread across the switchyard, making efficient cabling designs an important consideration. Separating these functions into two different network structures allows optimization of design and construction of each structure resulting in an overall more optimal substation communication network.

Within the ESP zone, devices such as IEDs, remote telemetry units (RTUs), and programmable logic controllers (PLCs) are connected to network switches in a variety of topologies such as hub-and-spoke, rings, and tree. Physical and logical redundancy techniques are employed to support high availability and reliability of critical substation communications (Liu, Panteli and Crossley 2014).

Similar to the WAN, the substation supports safe and reliable operation of the grid. As such, there is an emphasis on reliability, security, and resilience in the design of substation LANs. Latency and jitter are also important considerations, because protection services are located within the substation. Equipment within the substation control zone is connected primarily through wired connections. Connection to equipment in the switchyard may be wired or wireless, depending on the criticality of the function.

3.3.4 FAN and NAN

FANs provide communication connectivity to grid sensors and control devices on the distribution system such as meters, regulators, and capacitor banks. The FAN can be the gateway to customer-owned DERs and controllable loads behind the meter. The FAN may be segmented into multiple tiers to address varying requirements of different grid applications in a way that optimizes operational costs. The top level connects to the WAN and provides higher-bandwidth, lower-latency communication services. This layer is referred to as the FAN. The next level, sometimes called the NAN, provides lower bandwidth with higher-latency communication services. Grid devices that support distribution automation use cases such as fault location, isolation, and service restoration (FLISR), where fast coordinated response is required, would be connected to the top tier. Advanced metering infrastructure (AMI) and other less time-critical use cases would be connected to the NAN tier. The FAN tier may serve as the backhaul to the WAN for the NAN tier.

The FAN may be implemented with either private or public infrastructure. Wireless networks are the most common form of connectivity due to the large scale and the wide area that must be covered. For private infrastructure at the top tier of a FAN, a number of different technologies have been used, including WiFi, WiMAX, and recently, private LTE, in early trials. For the NAN tier, mesh and point-to-multipoint wireless networks are often deployed. IEEE 802.15.4 low power network standards are offered by a variety of vendors. Automated metering infrastructure is an example of a NAN wireless network. Both unlicensed and licensed radio frequency solutions are available and deployed.

Public cellular is an option in the FAN. It may be used as a backhaul for a wireless network in the field as part of a FAN. It may also be used to directly connect devices in the field or at the NAN tier.

Historically, communication networks at the FAN/NAN level were not associated with grid operations. Automated metering was one of the earliest large-scale communication needs at this level. This application did not require low latency or high availability for network connections. This led to the deployment of low power, low bandwidth, lossy networks. Data from meters could be collected over hours or even daily, and mechanisms could be put in place to mitigate individual packet loss, such as redundant data transmissions.

With the rise of the smart grid, the requirements for communication networks in the FAN/NAN have become more demanding. Distribution automation use cases dictate much higher performance in bandwidth, latency, and reliability. New technologies are being deployed to meet these requirements. However, a significant amount of AMI network infrastructure has already been deployed, so the existing infrastructure base may not meet the necessary increasing performance demands of new use cases. Since the CReST-VCT tool relies on timely control and situational awareness of distributed grid resources, these legacy AMI networks are likely too constrained to provide the reliability and latency required for the desired five-minute optimization interval.

3.4 Utility Communication Network Characteristics

The communication network structures discussed above must support a wide variety of applications or use cases. Each network layer may involve multiple technologies to support the overall needs within the specific geographic and business constraints of the utility. Prior studies have summarized required network performance of smart grid use cases and characterized various network technologies that are used in the network structures described above (M. P. Kuzlu 2014) (Kuzlu and Pipattanasomporn 2013) (Cisco 2019). Table 1 provides an aggregation of these characteristics.

Table 1. Typical Required Network Characteristics for Smart Grid Applications

Network Tier	Bandwidth	Latency	Availability
WAN	> 1 Gbps	< 50 ms	Very High
sLAN	> 10 Mbps	< 10 ms	Very High
FAN	> 1.2 Mbps	< 1 s	High
NAN	> 100 kbps	< 30 s	Medium

The CReST-VCT tool, when integrated into a real-time operation system, will primarily rely on the existing utility network structures to communicate with the necessary systems and devices. The characteristics presented here are representative of those that CReST-VCT would experience. When non-utility DER resources are incorporated into the operation of a CReST-VCT tool, an analysis of the various types of communication systems used by the non-utility third party will need to be conducted and Table 1 extended.

4.0 Protocol Landscape

The CReST-VCT tool is protocol independent. The tool itself does not introduce any new requirements for existing protocols used to communicate between EMS/DSM, grid devices, or DER systems, such as ModBus, DNP3, IEC 61850, and IEEE 2030.5. The system designers will need to evaluate protocol choices to determine which is most suitable. These existing protocols may introduce timing dependencies, given their specific data models or interaction patterns. Some commonly used smart grid standards that are compatible with CReST-VCT tool are summarized below.

IEC 60870-6 (IEC 60870-6-503 2014): This protocol is defined as an inter-control center protocol (ICCP), and is used in communicating information between a control center and EMS/DMS that it operates and also between a control center and a subtransmission substation. This protocol maintains client-server applications and provides a complete set of management tools and interfaces for SCADA. The CReST-VCT tool will leverage this ICCP protocol for data exchange between the EMS and DMS.

IEC 61850 (IEC 61850 2019): This protocol applies to communication networks in substation automation systems, and to protection, monitoring, and control of all devices, as well as interoperability within different devices (e.g., RTUs, IEDs) located in a modernized substation. IEC 61850 supports the Sampled Value (SV), Generic Object Oriented System-wide Events (GOOSE), Generic Substation State Event (GSSE), Simple Network Time Protocol (SNTP), and Manufacturing Message Specification (MMS) protocols. The timestamp resolution for an IED is <4 µs. GOOSE response time requirements from application to application, according to IEC 61850, are <10 ms for tripping and <100 ms for other operations.

DNP3: DNP3, Distributed Network Protocol version 3, is used for communication between a SCADA master station and RTUs/IEDs. This protocol supports time synchronization with RTUs. With DNP3, enables sending of relatively small amounts of data can be sent reliably with deterministic sequences.

Modbus: Modbus is an open serial communication protocol that has been used for various applications in substations such as energy management and substation automation. Usually, ModBus is connected between a SCADA master and RTU station and maintains client-service communication between those devices. The ModBus protocol is implemented by using different transmission protocols such as asynchronous serial transmission, ModBus plus, or TCP/IP over ethernet.

IEEE 2030.5 (IEEE 2030.5 2018): DER operators, manufacturers, and DER aggregators use the IEEE 2030.5 standard for DER integration into the grid. This standard incorporated technologies already in use for communication between utilities and aggregators, along with smart inverters, and aligned with IEC 61850, SunSpec specifications, and IEEE 1547. IEEE 2030.5 supports DER functions such as anti-islanding, ramp rate setting, and dynamic volt-var, and those functions are initiated through a control event called *DERControl.* The application layer with TCP/IP providing function supports different physical layers such as IEEE 802.15.4 (IEEE 802.15.4 2006), IEEE 802.11 (IEEE 802.11 2016), IEEE 1901 (IEEE 1901 2010), IEEE 1901.2 (IEEE 1901.2 2013).

IEEE 1547 (IEEE 1547 2018): This standard is used for interconnecting DER with electric power systems. This standard covers distributed generators and distributed energy storage technologies, but does not cover controllable loads used for demand response and those DERs that transfer switch at <100 ms. This standard applies to systems that are capable of frequency response and regulating voltage. Though IEEE 1547 standards do not specify protocol requirements, the functions and responses expected from DERs are outlined.

IEEE C37.118 (IEEE C37.118.1 2011): Phasor measurement units enable wide area visibility and allow distributed coordinated control at the subtransmission level. This standard is used for synchrophasors in power systems, and defines a relevant communication protocol for phasor data exchange. This protocol is based on ethernet, IP, or Fieldbus, and supports the capability to receive time from the global positioning system to maintain sufficient accuracy to keep steady-state error within required limits.

Table 2 lists protocols that will be most suitable for the CReST-VCT tool.

Table 2. Suitable Standards for CReST-VCT

Area	Standard	Description
Control Center	ICCP	Allow monitoring and control over a WAN among control centers or among EMSs and DMSs
Substation	DNP3	Specifies protocols for communication among different items of substation equipment
	IEC 61850	Specifies protocol for communication among IEDs (GOOSE, SMV, MMS)
	Modbus	Used to connect a SCADA master station with RTUs
	IEEE C37.118	Use for synchrophasors in power systems
Distributed generation	IEEE 2030.5	Smart inverter protocol (PV systems communicate to utilities through smart inverters)
	IEEE 1547	Standard for interconnecting distributed resources

5.0 Cyber Security

A cyber security failure scenario is a realistic event that damages confidentiality, integrity, and availability of cyber assets that reside within control center and substation. Diverse threat agents can cause cyber security failure to occur in EMS, DMS, and DER domains. The different failure scenarios must be understood in order to apply proper mitigation strategies. The National Electric Sector Cybersecurity Organization Resource (NESCOR) has introduced 111 unique cyber event failure scenarios that cover the smart grid domains (e.g., AMI, DER, and distribution grid management) (EPRI 2013). Some of the failure scenarios in the DER domain are related to distributed energy resource management systems (DERMS) and field DER energy management systems, and some of the failure scenarios in the wide area monitoring, protection, and control (WAMPAC) domain are related to EMSs and DMSs. Below are some of the NESCOR cyber threats to DERs and WAMPAC:

- DER.14: DER Systems Shut Down by Spoofed SCADA Control Commands
- DER.15: Threat Agent Spoofs DER Data Monitored by DER SCADA Systems
- DER.17: Utility DERMS Miscalculates DER Energy/Service Requests
- DER.26: Spoofed Microgrid Status Messages Cause Disconnect from Grid
- WAMPAC.11: Compromised Communications between Substations

CReST-VCT uses the interface between the EMS and the DMS. The system design and implementation must ensure this interface is properly secured. Note that the EMS and DMS may reside in different security zones within the utility IT infrastructure. Some of the EMSs reside in a North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) jurisdiction. For example, a control center or a generation control center that provides critical operating functions is identified in NERC CIP-002-5.1 (North American Electric Reliability Corporation 2016). To secure the EMSs that fall under NERC CIP standards, a system is designed following the NERC guidance for secure remote interactive access (North American Electric Reliability Corporation 2011). Security is achieved by configuring the VPN to prevent split tunneling, providing two-factor authentication, disabling all ports that are not required, and limiting allowable protocols, by keeping patches current, and maintaining the firewall.

The other operational functions of the tool use existing network interfaces, such as SCADA, that should already use appropriate security measures for control of critical infrastructure. The algorithm will not be a stand-alone tool, but part of the EMS suite, using communication capabilities that already exist between an EMS and DMS, and from DMS to field devices, and for the SCADA measurements.

6.0 Communication Integration for Devices

Communication capability in inverters connected to PV systems is necessary to obtain maximum value from implementation of the CReST-VCT algorithm. This discussion on communication integration would assume that the inverters already have advanced functionalities that enable them to set active power limits and reactive power compensation. Though advanced inverters with such functionalities have been rolled out by utilities, communication capabilities have not been fully used yet. For urban and suburban areas that have already benefited from AMI or distribution automation, residential and commercial PV may use the communication infrastructure already in place to support these other applications. Depending on the bandwidth and latency requirements, these devices may connect at either the NAN or FAN tier. Existing residential and commercial inverters can be retrofitted with devices that provide a communication card. However, these can incur additional costs (Reiter, et al. 2015), and thus many smart inverter deployments have yet to roll out the communication capabilities or have limited them to certain areas. In an interview with GreenTech Media, the vice-president of the Medium Power Solutions group of SMA America mentioned that oftentimes adding the advanced functionalities is a matter of firmware upgrade, and may not incur any additional costs (GreenTech Media 2019). Setting up communication infrastructure in inverters can cost about $150, depending on the customer's existing communication channels (GreenTech Media 2019). As noted in this article, a white paper from Western Electric Industry Leaders working group estimated that adding advanced features and communications in inverters can add about 10% to manufacturing cost of inverters and 5 to 10% to total installation costs (GreenTech Media 2019).

Communication capability in home appliances already follow standards set by the Consumer Technology Association (CTA) or Consumer Electronics Association (CEA). Some of these may be used by inverter manufacturers as well (Brian 2016). The ANSI/CEA-2045 (now CTA-2045) Modular Communication Interface Standard that is used for energy management through thermostats may be used for smart inverters (ANSI/CTA 2018, ANSI/CTA 2018) (SunSpec 2019). Communication card manufacturers like Tigo are already providing communication-enabled monitoring facilities for residential PV (Tigo Energy 2019).

As utilities in the United States are introducing smart inverters with communication capabilities, lessons from large-scale inverter retrofitting, such as that done in Germany, can be useful (Appen, et al. 2013). For about 315,000 inverters installed prior to 2012 in Germany, retrofitting was required to enable features like frequency ride-through (Appen, et al. 2013). This resulted in higher net expenditure than the inverter price at the time by about $703/inverter (Reiter, et al. 2015).

IEEE 1547-2018 standards allow participation of smart inverters to provide grid support. In addition, rules like California's Rule 21 and Hawaii's Rule 14H require inverters to have advanced functionalities such as anti-islanding, soft start, and voltage ride-through.

With these rules and standards in place, and the ongoing work in developing regulations and standards, utilities in the United States may choose to install smart inverters already equipped with communications, rather than trying to retrofit. The president and COO of San Diego Gas & Electric, Mike Niggil, stated that they would prefer to add $150 worth of features to a $1500 residential home inverter than to try to retrofit later (GreenTech Media 2019). If the inverters installed throughout a utility have means to communicate with the utility, the implementation costs of the CReST-VCT algorithm would be greatly reduced. The same holds for other communicable devices in substations, voltage regulators, etc.

7.0 CREST-VCT Communication System Considerations

The CREST-VCT algorithm requires coordination across the EMS, DMS, substation, and DER field devices. As described in the sections above, this coordination depends on messages that traverse multiple tiers of a typical utility's communication network infrastructure. This messaging can use a number of different application and network layer standard protocols. The communication networks use various physical technologies with different characteristics. Similarly, the technology to integrate communications capabilities in DER equipment may vary.

To support the integration of the CReST-VCT tool into a real-time operation environment, a system design model must be produced, to perform simulations and analysis that help determine the overall effect of the different permutations of the communication system variables described herein. The following system considerations should be examined in this model to determine the optimal configurations for an operations system:

- timing
- scalability
- resiliency
- interoperability.

These elements are discussed in more detail below.

7.1 System Timing

CReST-VCT operation spans multiple tiers of a typical utility's communication network. Different communication system technologies may be used each, with its own performance and reliability characteristics, as outlined in Table 1.

The design of CReST-VCT is such that its data requirements are low, because coordination is based at a summary VPP level. However, the majority of the communication traffic will be from DER dispatch signals and field measurements. The DER dispatch signals may be based on different protocol standards described in Section 4.0. This will create variability in the timing that the system design model should analyze.

Tests of the algorithm have observed execution times of less than 1 minute. This leaves multiple minutes to support communication to field devices for DER dispatch. Examination of the communication network latency figures in Table 1 indicates that that each network tier supports the required latency when operating in an overall operating time budget of minutes. The system design model would need to validate this with the modeled data and protocol overheads and variability of communications.

The latency of communication will depend on which layer of the network a DER resource is connected to. A DER connected at the NAN layer will have significantly more latency than a device connected at the substation LAN. This will create variability in the timing that the system design model can analyze.

Feeder devices such as regulators, capacitor banks, or DERs connected at the FAN or the NAN layer are subject to the widest range of possible communication network performance. The specific geographic location with reference to network infrastructure, the surrounding topology, and network utilization introduces variations in performance in wireless networks. Studies have shown wide variation in cellular latency and bandwidth, for example (Gember, et al. 2012). Congestion in cellular networks introduced significant variations over the course of the day with business hours being the time with the highest latencies. AMI networks represent one of the more constrained wireless networks in use at utilities. Nominal data rates range from 10 kbps to 1.2 Mbps, and again, the specific location in the wireless network will introduce variability. The system model should analyze these different configurations.

Given the variability in performance of wireless networks due to technology or due to specific constraints of a location, it is feasible that certain network connections could introduce enough latency or unreliability to render the connected asset a poor candidate for use in CReST-VCT–based operation. For example, the constraints of AMI networks at the NAN level need to considered. Through the system model analysis, the minimum network characteristics can be studied and methods devised to classify the quality of a device's network connection to determine whether it can be used with the tool.

7.2 System Scalability

The CReST-VCT tool provides a mechanism to parallelize the algorithm computation by dividing the system into substation groups. However, each of these groups is expected to be synchronized to the same five-minute operational interval to make sure the DER dispatch and supporting field measurements are coordinated across the grid. This means that the DER dispatch and field measurements will be executed in parallel. This could pose scalability issues for the communication network infrastructure.

SCADA systems at the substation level operate at the typical poll cycle of one to several seconds for all points. Because these points are maintained continuously, it is assumed that communication networks will be scaled appropriately for normal operations independently of CReST-VCT. Connection to devices outside the substation to take advantage of CReST-VCT optimization capabilities may drive new connections to the SCADA system. Further, CReST-VCT increases the potential hosting capacity of DERs that might otherwise be curtailed, increasing the possible number of DERs a given feeder can support. The potential optimizations with a five-minute interval could again provide incentive to connect more devices and interact with those devices more often.

The system design model will need to analyze the communication load based on the number of controlled devices to assess the capacity. This analysis will need to be conducted across the target protocol and communication technologies that may be used to determine the overall scalability of the tool.

7.3 System Resilience

The utility employs various network designs and technologies to provide the required availability for its control networks. Redundancy of network equipment and redundant network paths are employed to support reliability, for example. However, given the wide-area nature of the utility network, it is not always feasible to provide full redundancy. The utility is forced to prioritize its investments based on the criticality of the links. Just as is the case with the electricity grid network, communication networks will sometimes fail.

It will be important for CReST-VCT to be able to respond appropriately to a communication network failure. A resilient implementation would let the system react to the specific failure scenario and adjust, to continue performing, but with reduced function or benefit. The effect of a communication network performance issue or disruption in service would depend on the location of the failure. Any disruption in service at the CCN would have a significant effect on the CReST-VCT tool, since algorithms run and coordination is initiated at this level. If a specific FAN segment is disrupted, though, the CReST-VCT tool could disable consideration of that area's assets and run the optimization for the remaining connected system. The system design model should include a mechanism to notify CReST-VCT of a dependent communication system failure so that it can adjust its operation.

7.4 System Interoperability

The CReST-VCT tool itself introduces a potential new interface between the EMS and the DMS. The application layer protocol for that interface will need to be determined in the system design phase. Outside of that interface, CReST-VCT operation would be based on the existing communication protocols that are already in use by EMS and DMS systems.

However, for connected DER, the protocol standard landscape is very mixed. While standards such as IEEE 1547-2018 are specifying the potential choices for communication protocols that inverters must support, there are still choices. Further, the standards are focused on the application layer with a trend toward convergence on the IP network layer. The physical networks are not specified. Thus, from a communication network perspective, interoperability may be challenged.

Utilities have often had to face interoperability challenges for communication networks. Each utility standardizes internally, adopting a standard that they prefer, and uses it to dictate procurement decisions. This places a burden on software and device providers that must support multiple standards to serve multiple utilities.

In the next phase, the system design model will evaluate various standards to assess any limitations that a given choice or combination of choices may present. This may identify more optimal configurations that can inform regulators, utilities, and the industry.

8.0 Conclusion

CReST-VCT coordinates between transmission and distribution controllers to use DER devices to provide voltage support at the subtransmission level while maintaining operational requirements at the distribution level. The optimization algorithms depend on the communication between the transmission and substation control systems. They also depend on communication between the control center and the substation and feeder DER resources. This paper includes discussion of the communication networks on which CReST-VCT will be dependent.

Initial examination suggests it is feasible for modern utility communication networks to support the CReST-VCT tool operation in a real-time production environment. Maximizing the benefit and performance will depend on the system design and on integration of the tool into the utility production control systems. Several system considerations including timing, scalability, resilience, and interoperability were discussed.

In future work, the overall system design will be modeled, defining detailed information exchange profiles including the interface between the EMS and DMS and any controlled devices. Specific protocols will be assessed, and communication system requirements formalized. The variations in communication technologies discussed in this paper will be analyzed and characterized with reference to the system operational requirements. This analysis can then be used to provide guidance for integration into utility environments. It can also be used to inform appropriate behavior for the CReST-VCT tool when faced with communication system failures.

9.0 Bibliography

ANSI/CTA. 2018. "Modular Communication Interface for Energy Management." *Modular Communication Interface for Energy Management.* https://standards.cta.tech/kwspub/published_docs/ANSI-CTA-2045-A-Preview.pdf.

Appen, Jan von, Martin Braun, Thomas Stetz, Konrad Diwold, and Dominik Geibel. 2013. "Time in the Sun: The Challenge of High PV Penetration in the German Electric Grid." *IEEE Power and Energy Magazine*, March-April.

Brian, Steel. 2016. "Standard Communication Interface and Certification Test programs for Smart inverters." *Distributech .* EPRI, February 9th.

Cisco Systems. 2012. "Cisco GridBlocks Architecture: A Reference for Utility Network Design." April. Accessed May 13, 2019. https://www.cisco.com/c/dam/en_us/solutions/industries/docs/energy/gridblocks_ref_model.pdf.

Cisco Systems. 2019. "Distribution Automation - Feeder Automation." *Distribution Automation Feeder Automation Design Guide.* https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/Distributed-Automation/Feeder-Automation/DG/DA-FA-DG.html.

EPRI. 2013. "Electric Sector Failure Scenarios and Impact Analyses." Palo Alto, CA, USA.

EPRI. 2014. "The Integrated Grid." https://www.energy.gov/sites/prod/files/2015/03/f20/EPRI%20Integrated%20Grid021014.pdf.

Fujikawa, F, K Kuwabara, Y Koda, and M Kiuchi. 2004. "Examination of Electric Power Utility Network Applying IP Router/MPLS Router/Wide-Area Ethernet." *IEEE Power Engineering Society General Meeting.* Denver.

Gember, A, A Akella, J Pang, A Varshavsky, and R Caceres. 2012. "Obtaining In-Context Measurements of Cellular Network Performance." *Proceedings of the 2012 Internet Measurement Conference.* Boston.

GreenTech Media. 2019. *SMA:PV Inverters Can Be Made Grid-Smart for Little Addtional Cost.* April 27. https://www.greentechmedia.com/articles/read/SMA-Sees-Little-Costs-to-Make-Inverter-Grid-Smart#gs.8m9x7r.

GreenTech Media. 2019. *Western Utilities Call for Smart Solar Inverters.* April 27. https://www.greentechmedia.com/articles/read/western-utilities-call-for-smart-solar-inverters#gs.8mb02b.

Hunt, L. 2011. "Drivers for packet-based utility communications networks-teleprotection." *2011 International Conference on Advanced Power System Automation and Protection.* Beijing.

IEC 60870-6-503. 2014. *Telecontrol Equipment and Systems - Part 6-503: Telecontrol Protocols Compatible With ISO Standards And ITU-T Recomendations - TASE.2 Services And Protocol.* Available at https://webstore.ansi.org/Standards/IEC/IEC60870503Ed2014. Also referred to as Inter-Control Center Communications Protocol (ICCP).

IEC 61850. 2019. *Communication networks and systems for power utility automation.* Available at https://webstore.iec.ch/publication/6028.

IEEE 1547. 2018. *IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces.* Available at https://standards.ieee.org/standard/1547-2018.html.

IEEE 1901. 2010. *IEEE Standard for Broadband over Power Line Networks: Medium Access Control and Physical Layer Specifications.* Available at https://standards.ieee.org/standard/1901-2010.html.

IEEE 1901.2. 2013. *IEEE Standard for Low-Frequency (less than 500 kHz) Narrowband Power Line Communications for Smart Grid Applications.* Available at https://standards.ieee.org/standard/1901_2-2013.html.

IEEE 2030.5. 2018. *IEEE Standard for Smart Energy Profile Application Protocol.* Available at https://standards.ieee.org/standard/2030_5-2018.html.

IEEE 802.11. 2016. *IEEE Standard for Information Technology–Telecommunications and information exchange between systems, Local and metropolitan area networks–Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.* Available at https://standards.ieee.org/content/ieee-standards/en/standard/802_11-2016.html.

IEEE 802.15.4. 2006. *IEEE Standard for Information technology – Local and metropolitan area networks-- Specific requirements-- Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (WPANs).* Available at https://standards.ieee.org/search-results.html?q=IEEE+802.15.4.

IEEE C37.118.1. 2011. *IEEE Standard for Synchrophasor Measurements for Power Systems.* Available at https://standards.ieee.org/standard/C37_118_1-2011.html. .

Ke, Xinda, Nader Samaan, and Jesse Holzer. 2018. "Coordinative real-time sub-transmission volt-var control for reactive power regulation between transmission and distribution systems." *The Institution of Engineering and Technology, DOI: 10.1049/iet-gtd.2018.5850.*

Kuzlu, M, and M Pipattanasomporn. 2013. "Assessment of Communication Technologies and Network Requirements for Different Smart Grid Applications ." *IEEE PES Innovative Smart Grid Technologies Conference.* Washington, DC.

Kuzlu, M, Pipattanasomporn, M, Rahman, S. 2014. "Communication network requirements for major smart grid applications in HAN, NAN, and WAN." *Computer Networks* 67: 74-88.

Liu, N, M Panteli, and P.A. Crossley. 2014. "Reliability Evaluation of a Substation Automation System Communication Network Based on IEC 61840." *12th IET International Conference on Developments in Power System Protection.* Copenhagen.

North American Electric Reliability Corporation. 2016. "Cyber Security- BES Cyber System Categorization (CIP-002-5.1)." Available at https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-002-5.1a.pdf.

North American Electric Reliability Corporation. 2017. "Distributed Energy Resources: Connection Modeling and Reliability Considerations." Available at https://www.nerc.com/comm/Other/essntlrlbltysrvcstskfrcDL/Distributed_Energy_Resources_Report.pdf.

North American Electric Reliability Corporation. 2011. "Guidance for secure remote interactive access." Available at https://www.nerc.com/pa/rrm/bpsa/Alerts%20DL/2011%20Alerts/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf.

PNNL. 2015. *The Emerging Interdependence of the Electric Power Grid & Information and Communication Technology.* PNNL-24643, Pacific Northwest National Laboratory, Richland, Washington. Available at https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-24643.pdf.

Reiter, Emerson, Kristen Ardani, Robert Margolis, and Ryan Edge. 2015. *Industy Perspectives on Advanced Inverters for US Solar Photovoltaic Systems: Grid Benefits, Deployment Challenges, and Emerging Trends.* National Renewable Energy Laboratory. Available at https://www.nrel.gov/docs/fy15osti/65063.pdf.

SunSpec. 2019. *Advanced Inverter Communication.* April 29. https://sunspec.org/csi-4/.

Taft, Jeff, Paul De Martini, and L Kristov. n.d. *A Reference Model for Grid Control in the 21st Century.* PNNL-24463, Pacific Northwest National Laboratory. Available at https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-24463.pdf.

Tigo Energy. 2019. *Tigo Smart Inverter.* https://www.tigoenergy.com/products/#smart-modules-ts4-r-duo.

Pacific Northwest National Laboratory

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99354
1-888-375-PNNL (7665)

www.pnnl.gov