White Paper

Scaling Your SCADA Architecture for Distribution Automation

Aclara.com

800 297 2728
info@aclara.com

Table of Contents

Introduction 1

DNP3 Overview 1

Network Architecture 1

Option #1 - Direct Connection into SCADA 2

Option #2 - Traditional De-Centralized Approach 1

Option #3 - Centralized Architecture 1

Aclara Grid Monitoring Platform – A Centralized Architecture For Smart Grid Sensors 9

Additional Benefits of Aclara's Grid Monitoring Platform 11

Advanced Analytics 11

Management of Communications 12

Fault Waveforms 12

Remote Programming and Upgrades 13

Conclusion 14

Aclara™

Scaling Your **SCADA** Architecture for Distribution Automation

White Paper

Introduction

In the U.S., over 90 percent of electrical outages occur on the distribution portion of the network. To improve reliability, many utilities are looking to deploy smart grid technologies to bring real-time situational awareness to their crews, engineers and planners. For many, this means their Distribution Automation (DA) system may easily need to grow to thousands of new endpoints very rapidly with a mix of communicating smart grid sensors, reclosers, and capacitor controllers.

How will you best deploy and scale your DA system? Will you continue using the more traditional technique of installing Remote Terminal Units (RTUs) out in the field that is typical in today's Supervisory Control and Data Acquisition (SCADA) deployments at substations? Or, does your architecture need to mirror that of an Advanced Metering Infrastructure (AMI) system, which is designed to scale up to millions of endpoints by sending meter data to centralized software that analyzes and processes it so that it doesn't flood other backend systems? What is the best approach to future proof your automation build and investment? In this whitepaper, we weigh the pros and cons of the three most popular DA architectures that have adopted the industry standard DNP3 protocol:

- **Option #1:** Directly connecting the end-points from thousands of DA field devices into your SCADA, Distribution Management System (DMS) or Outage Management System (OMS) without any centralized processing or analysis
- **Option #2:** Deploying de-centralized physical concentrators in the field between endpoints and your SCADA, DMS or OMS systems
- **Option #3:** Deploying one centralized concentrator that analyzes all the data from endpoints and integrates into your SCADA, DMS or OMS systems using DNP3

As many have learned with their AMI deployments, the architectural impacts of deploying and scaling thousands of new endpoints into your network required planning and adoption of new techniques. This paper shares best practices for deploying, scaling and managing thousands of devices on your DA network.

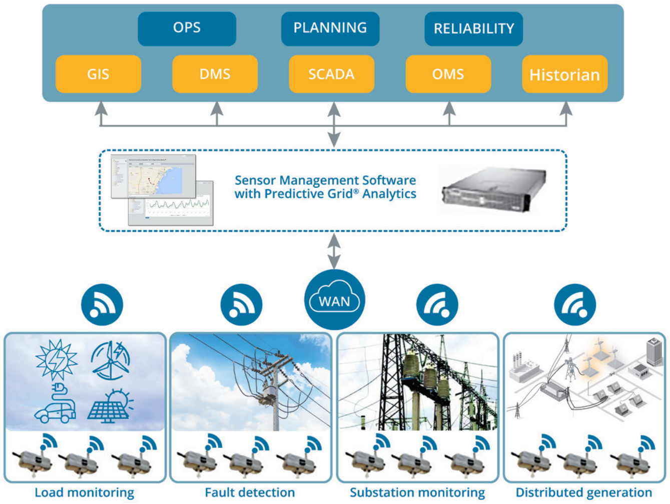

Figure 1: Example of a centralized architecture with Smart Grid Sensors as the DA field devices

DNP3 Overview

Because all architectures descriptions leverage the standards-based DNP3 protocol, it is important that we first cover an overview of this critical communication protocol and how it is used between various types of data acquisition and control equipment. DNP3 plays a crucial role in the modernization and automation of the electric grid by allowing sensors, reclosers and switches, capacitor banks and circuit breakers to communicate with the control centers within the System Operating department. This immediate notification and control beyond the substation level is the backbone of what is required for a smarter grid.

The DNP3 protocol was developed by Westronic using the early versions of the IEC 60870-5 standard protocol specifications. Now the protocol is controlled by the DNP Users Group at at www.dnp.org. The protocol is serial based, and as such, many implementations use RS-232 and RS-485 over copper or even fiber optics. DNP3 can also be used over packet-oriented networks such as TCP/IP and UDP/IP in which Ethernet may be used. The DNP3 message is tunneled over TCP/IP or UDP/IP. The protocol defines a field device such as a capacitor controller as the outstation or slave device. The control center system is labeled the master device.

DNP3 supports advanced functionality, including:

- Standard list of objects and variations
- Unsolicited Responses
- Data points can include a time stamp
- Status flags for individual points
- Performs time syncs
- Supports analog deadbands
- Integrity polls and event polls (events are stored until requested by the Master)
- Assign points to classes
- Ability to freeze counters and analogs
- File Transfers

Network Architecture

In this whitepaper, we will analyze the three most popular architectures used to support a DA deployment. These include:

- **Option #1:** Direct Connection into SCADA
- **Option #2:** Traditional De-centralized Approach
- **Option #3:** Centralized Architecture

We will discuss these architectures in more detail below. The transport method (wireless or wired) will not be explicitly mentioned as the overall architecture is the same for both.

Option #1: Direct Connection into SCADA

In this architecture, thousands of field devices communicate directly to SCADA servers. The outstation or slave devices are polled directly by the control center systems such as a Distribution Management System (DMS) or Outage Management System (OMS). These systems typically have a Front End Processor (FEP) that does the polling and listens for unsolicited messages.

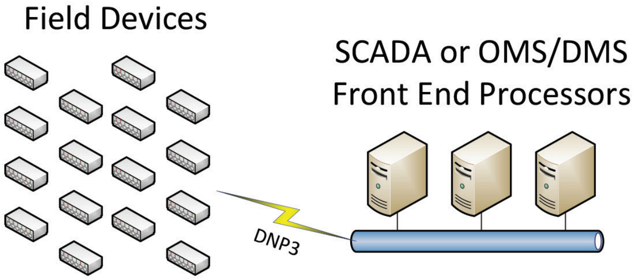

Figure 2: Example of a centralized architecture with Smart Grid Sensors as the DA field devices

Benefit

The architecture allows for a simplified deployment as there are only two locations to program and maintain. The architecture uses DNP3 protocol for all communications, with no other software or concentrator hardware required.

Architectural Considerations

While seemingly simple at the outset, there are several concerns with this design:

1. **Will the team that supports your SCADA system be willing to support and maintain thousands of new devices in the field?**
   The team that supports your current SCADA system will need to establish, support and maintain a dedicated connection to each device in the field. This could mean that thousands of IP addresses and devices need to be separately maintained.

2. **Will you want engineering, maintenance and power quality groups to have direct access to data through SCADA?**
   Many users who normally don’t have access to the SCADA system (engineering, maintenance, power quality, IT department) would need to access the core SCADA network in this architecture to obtain the ancillary data on the devices such as waveforms, logs, communication settings and even perform firmware updates. If the system is designated as a NERC Critical Infrastructure Protection (CIP) Critical Cyber Asset, there may be significant costs to have each user cleared to access the network (security and background checks) along with the yearly costs for continual re-certification.

3. **Security**
   This design also requires thousands of individual connections made directly to the core SCADA servers, presenting additional cybersecurity concerns. If multiple computer systems such as OMS, DMS and SCADA are used, many DNP3 connections will need to be made to the same device. Firewall rules and intrusion detection capabilities need to be established for each device and each separate DNP3 connection. The monthly cost of the intrusion detection system is usually based on the number of connections it is monitoring. If you have thousands of endpoints deployed, these costs could accumulate quickly. Also, DNP3 supports unsolicited messages to keep data usage costs down for wireless systems. Most utilities will not enable unsolicited messages into their core SCADA network as this presents a security risk. However, operators who need to know when trips and lockouts occur as soon as they happen will have to face opening up a security risk in this architecture.

4. **Will you still be in compliance with NERC CIP?**
   Most utilities implement change control processes as required in NERC Critical Infrastructure Protection (CIP) standard. Connections cannot be added and commissioned when it is convenient for the field crews installing the equipment. They may need to make a return trip to commission the device once it is available in the system.

5. **Can your DMS handle it?**
   Many DMS systems were not designed to take direct connections from thousands of end devices in the field. If your ultimate goal is integration with DMS, this is an important question to ask your DMS provider.

6. **Data Accuracy**
   Some of the data gathered by field equipment may not necessarily be “accurate” right out of the device and could benefit from “post-processing” analysis to determine its accuracy and conduct some event correlation that can lead to more meaningful situational awareness requiring less work from crews and engineers to interpret results.

Bottom-line for Option #1:

Many utilities favor this option as they enter the exploratory phase of initial architectural design concepts. But once the advantages are weighed against the disadvantages, most abandon this option in light of one of the two options we'll explore next.

WHY UTILITIES LIKE THIS ARCHITECTURE	KEY CONSIDERATIONS
• Direct connection into you SCADA or DMS system means there is not additional third party software to license, host or manage.	• Will your SCADA team support and maintain thousands of new connections into your core SCADA network? • Do you want to grant more direct users who need the data direct access into your SCADA system? • This architecture opens up new security and NERC CIP compliance vulnerabilities, have you weighed the risks? • Was your DMS designed to handle thousands of new connections directly, or would it perform better if there was a concentrator processing data requests first before it handed off into the DMS?

Option #2: Traditional De-Centralized Approach

In this architecture, the outstation or slave devices are polled by a physical concentrator or Remote Terminal Unit (RTU). This topology is typically found at a substation where several circuit breakers are connected to a SCADA concentrator. The substation is then polled by the DNP master at the control center.

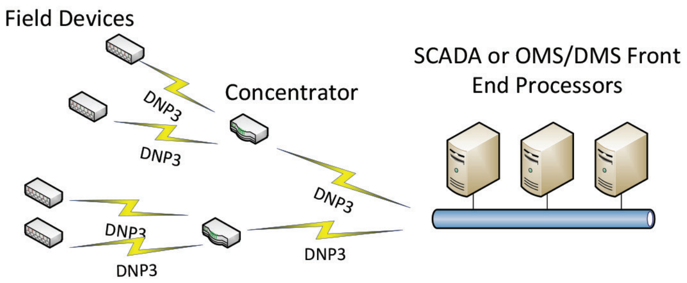

Figure 3: Traditional de-centralized approach

For sensors, capacitor controllers, and reclosers installed on distribution lines, a concentrator may exist at a common area such as the nearest substation or the concentrator may be installed at each of the crew quarters and then backhauled to the central control room. A remote concentrator in the substation can be programmed to poll field devices on a frequent basis or accept unsolicited messages as an aid to help keep data usage costs down. The SCADA front end processors then poll the concentrators on a frequent basis and can also accept unsolicited messages.

Benefit

This is the typical architecture that has been used for substation configuration the past 30 years. The concentrator can be maintained independent of the SCADA network which is security improvement over Option #1.

Architectural Considerations

While a "tried and trusted" method for substation configuration, this architecture creates a number of concerns and new costs when expanded to thousands of field devices:

1. **Security risks?**
   Most utilities will not enable unsolicited messages into their core SCADA network as this presents a security risk. If you will want to know when trips and lockouts occur as soon as they happen, your organization will have to weigh the benefits of having real-time data against security and compliance risks.
2. **Disaster recovery?**
   Physical field concentrators have redundant power supplies and network connections, but still create a single point of failure. For disaster recovery, each concentrator needs a separate configuration file for the devices it is going to poll. Managing hundreds of configuration files and troubleshooting each one will be an additional burden on the business line.
3. **Who is going to manage all of the hundreds of new field concentrators?**
   Physical SCADA RTUs or concentrators are designed to accommodate the number of devices normally found at a single substation, usually up to 150 devices. When utilities deploy thousands of DA field devices, they require hundreds of concentrators installed at substations or in racks at the datacenter to support them. This inevitably will begin to put a burden on SCADA administrators who'll need to manage hundreds of RTUs, connections through firewalls and backup configuration files.
4. **New costs?**
   This architecture is dependent on the deployment of field concentrators. The typical concentrator is designed to scale to 150 devices. So, if your deployment is planned to grow to thousands of end devices, this will be hundreds of concentrators that will need to be purchased and maintained. On top of the hardware costs, there will be added business costs as the SCADA team will need to take on new maintenance activities to keep this architecture operational.
5. **Can your DMS handle it?**
   Many DMS systems were not designed to take direct connections from hundreds of concentrators in the field. If your ultimate goal is integration with DMS, this is an important question to ask your DMS provider.

Bottom-line for Option #2:

Many utilities favor this option because it is the traditional way to configure substations for the last few decades. While it is a good option, there are some new costs and security risks that will need to be considered.

Why Utilities Like This Architecture	Key Considerations
• "Tried and trusted" method – same architecture used for substation configuration the last 30 years • The concentrator allows SCADA to be managed separate from the SCADA system – this avoids many of the security risks outlined in Option 1.	• Will your SCADA team support and maintain hundreds of new SCADA concentrators? • How data is handled will be privy to new security risks which will need to be weighed against the needs of the business. • New costs – you'll need a new field concentrator for every 150 field devices, this will introduce new hardware costs over and above the costs of the field devices. • Impacts on your DMS system

Option #3: Centralized Architecture

In this architecture, field devices talk to a server-based centralized concentrator that is located at a datacenter either hosted in the cloud or located at the utility's facility. The centralized concentrator provides a front end to process and analyze data before it is passed over DNP3 to SCADA, DMS or OMS systems.

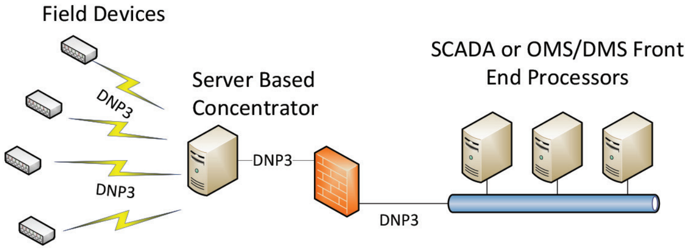
Field Devices
DNP3
DNP3
Server Based Concentrator
DNP3
DNP3
SCADA or OMS/DMS Front End Processors

Figure 4: Centralized architecture

This architecture utilizes DNP3 or another proprietary protocol between the field devices and the concentrator server, minimizing the data traffic on your DA network. The concentrator then acts as the DNP slave or outstation to the master SCADA, DMS or OMS system installed at the control center.

The server-based centralized concentrator is designed to host many field devices into one DNP3 connection to SCADA, DMS or OMS. If needed for disaster recovery, additional servers can be deployed for redundancy. Servers automatically load balance and fail over if a server is offline due to a failure or system maintenance. In either case, only a few connections are needed to the SCADA or DMS system.

For most DMS systems, this is the preferred design. By reducing the number of connections you can significantly reduce firewall rules and costs for intrusion monitoring. This makes it easier to comply with NERC CIP standards as fewer connections need to be vetted when doing architecture reviews and during audits and it is more secure. The concentrator supports multiple masters simultaneously polling, such as a DMS and Historian.

Because the concentrator is connected to the utilities' internal network, data costs and latency are no longer a concern. For example, the SCADA system can perform DNP3 event and integrity polls every two seconds just like they have been using in their Modbus SCADA systems. The concentrator will respond with the same analog data until it is updated from the field devices. However, if an outage occurs, the field devices can immediately send their data to the concentrator. If SCADA polls every two seconds, it will pick up the state change and alert the operator. This eliminates the need to have DNP3 unsolicited messages enabled in the SCADA system.

Benefit

There is only one concentrator to manage and because it is software that runs on a computer server, it can be easily maintained by the IT department or hosted on the utility's behalf. Additionally, there are a number of security and NERC CIP benefits, because the concentrator can be maintained independent of the SCADA network (no need for users to access your SCADA network to get data) and there are fewer connections to maintain (which is also a blessing for your DMS vendor). With a software analytics package, you can eliminate false positives and correlate events to give users more meaningful information. Finally, because the concentrator can manage thousands of devices at a time, there is less hardware to buy when compared to Option #2.

Architectural Considerations:

While there are a number of benefits for adopting this approach over Options #1 and 2, there are a couple of architectural considerations to evaluate in your planning:

1. **Who is going to maintain and support the concentrator?**
   Unlike Options #1 and #2, you do not need to have your SCADA administrators manage the centralized concentrator but it still needs to be supported. Because the concentrator is server-based on a common IT platform, maintenance should be minimized. Even better, because it can be hosted in the cloud, you can outsource the support and maintenance costs to a third-party service provider.
2. **Are there any negative impacts from if I use a proprietary protocol from devices to the concentrator?**
   This architecture may utilize a proprietary protocol using TCP/IP between the field devices and the concentrator server such as the one used in the Aclara system. This protocol was designed for low overhead so that it could host as many 5,000 field devices in one concentrator significantly reducing the hardware costs in Option #2. This is similar to many AMI solutions where there can be proprietary protocols in place between the meter and the concentrator to maximize performance and bandwidth constraints but standard protocols are in place between the concentrator and back-office systems.

Bottom-line for Option #3

This option offers many benefits to reduce costs while increasing scalability and security over Options#1 and #2. The immediate hurdle is the idea of the "proprietary protocol" from field devices to the concentrator. But, once the cost and security advantages of the proprietary protocol are weighed and utilities can still achieve a seamless integration from the concentrator to this SCADA, DMS and OMS systems over DNP3, this objection can most likely be overruled.

Why Utilities Like This Architecture	Key Considerations
• Better security • Easier compliance with NERC SIP • Lower hardware costs over Option #2 • Fewer connections into your SCADA or DMS • IT can maintain instead of your SCADA team • Cloud-based hosting is available for utilities who would like to outsource maintenance and support • Better data accuracy over Option #1 • Eliminates the need to have DNP3 unsolicited messages enabled in the SCADA system.	• Will you support in-house with your IT department or outsource? • What impact, if any, will the proprietary protocol have on the deployment?

Aclara Grid Monitoring Platform – A Centralized Architecture for Smart Grid Sensors

Aclara's Grid Monitoring platform offers a smart grid sensor solution based on Option #3 – a centralized deployment architecture. The Aclara Sensor Management System (SMS) is a centralized concentrator that can support up to 5,000 sensors thanks to the low overhead of a proprietary protocol.

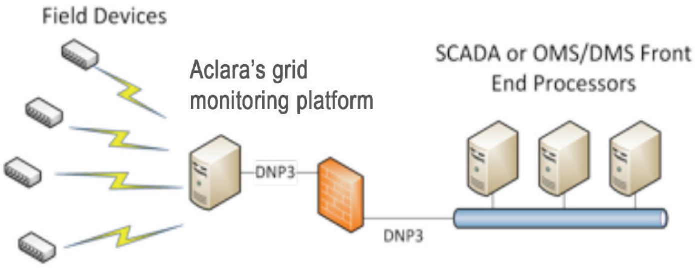
Field Devices
Aclara's grid monitoring platform
DNP3
DNP3
SCADA or OMS/DMS Front End Processors

Figure 5: Aclara's Smart Grid Sensor architecture

Aclara's Distribution Grid Monitoring platform – a next generation grid modernization technology consisting of Aclara's Smart Grid Sensors, a Sensor Management System (SMS) and Predictive Grid® Analytics software. The platform enables grid operators to proactively monitor the distribution network, improve reliability and safely bring distributed energy resources onto the grid. The platform encompasses all of the benefits of the architecture of Option #3 including:

- **Easier Compliance:** Fewer connections are needed to the SCADA system – easier maintenance, better security and better compliance to NERC CIP
- **Better Disaster Recovery:** Additional servers can be deployed for redundancy. Servers automatically load balance and fail over if a server is offline due to a failure or system maintenance.
- **Better Security:** There is no need to send unsolicited messages to SCADA for fault events – better security
- **Better Operations:** All users of the Aclara system access the sensors and data from outside the SCADA environment
- **Better Accuracy:** The Predictive Grid Analytics package is able to process data before it is passed on to other systems to improve data accuracy over alternative solutions

Aclara's Medium Voltage (MV) sensors provide the ideal combination of outage and fault detection with the additional benefits of configurable threshold alarming, real-time load and power quality monitoring and auto-phase detection that can be used for a wide variety of distribution grid applications. Aclara's line sensors quickly clamp directly onto overhead conductors and provide real-time data about faults and alarms about other grid conditions to get proactive about preventing outages.

We purpose-built our sensors to offer utilities the easiest installation process available. Only one lineman is needed with a hot stick or insulated gloves and sensors are deployed on the line in a matter of minutes. Deployment is quick and easy because our sensors do not require calibration, are lightweight and don't require access to cabinets. In addition, there are no solar panels to manage and nothing else to hang on the pole.

The Aclara's platform includes our Sensor Management System (SMS) software with Predictive Grid Analytics. This is a server based application that forms the centralized concentrator for all platform's data and events provided by our sensors. This software is provided by Aclara (and can be hosted for you). The software is a turnkey package that enables:

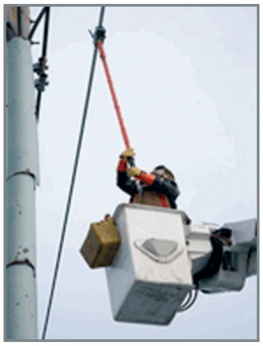

Figure 6: Aclara Smart Grid Sensor installation

- Fault detection and location analytics
- Sensor maintenance functions such as diagnostics, parameter settings, and firmware upgrades
- User Interface (UI) and visualization tools (for example, Google® Maps)
- Reporting dashboards and alarms
- Analytics functions to filter out or suppress data before it is passed to higher level systems
- DNP3 integration to SCADA, Historians, DMS, etc.
- An archive database of waveforms and fault events, available anytime to your engineers for post-event analysis

Planners, engineers, operations and field crews can interface directly with our Aclara Sensor data in two ways to monitor load or faults:

1. Directly through SMS
2. Passing SMS data through DNP3 to higher level systems (e.g. Historian, SCADA or DMS).

First, with browser-based access to SMS, your users can have full access to fault monitoring, fault location and maps, load monitoring and waveforms for investigative purposes or analysis. SMS provides RMS fault current, power quality events, and waveforms to analyze disturbances from virtually any type of device (e.g. PC, laptop, tablet, cell phone).

Second, you can integrate information from SMS into your Historian, SCADA, and DMS systems through our DNP3 interface. Here, SMS offers a competitive advantage because it first aggregates all information coming in from ALL sensors (that have been time-synched). SMS with Predictive Grid Analytics then analyzes the data to classify what types of events are occurring (filters out the false positives that FCIs or sensors that send their data directly to back-end systems produce) and indicates where the faults are located (e.g. using GPS or RMS Fault Current) on your network so you have actionable intelligence.

Finally, events that do not cause immediate outages, like momentaries or line disturbances, are logged in SMS so your engineers can continue to mine this data to learn more about your network and prevent future outages. Here, they have full access to waveforms and event data for post-event forensic analysis. Using this data, you can send crews to investigate potential problems before they cause an outage. Many of our customers have been able to prevent outages using SMS data in this manner.

Additional Benefits of Aclara's Grid Monitoring Platform

Additional benefits of the Grid Monitoring platform include:

- Advanced analytics
- Management of communications
- Fault waveforms
- Remote programming and upgrades
- Low power usage

Each is described in more detail below.

Advanced Analytics

The SMS takes the data from all of the sensors and processes it with our Predictive Grid Analytics software, including fault current and electrical position on the circuit to determine the root cause and direct the lineman to the appropriate location to look for the problem. This also prevents false positives where another source of fault current such as a distributed generator or delta connected transformer bank may have tripped the sensors. Aclara's Grid Monitoring platform compares the results of all sensors to determine the path to the real fault.

This advanced logic cannot be performed if each line sensor has separate logic onboard and doesn't know what its neighboring sensors are seeing. Each one will separately report what they think is the problem. In some cases, for a feeder lockout, 10 or 20 sensors may be reporting events and what they believe happened. Some will say that a fault occurred while others will say the power went off. The Aclara solution provides the intelligence to take all of these inputs and determine the source of fault.

Management of Communications

Incorporated in the platform protocol is the ability to retrieve and track communication status and other statistics. The communication statistics are transmitted on every interval load reading. This includes information about signal strength, signal to noise ratio, and if the cellular modem is roaming. This data can be trended over days or weeks to look for connectivity issues such as signal degradation due to vegetation growth. Also, alarms can be generated if a sensor has not communicated in a specified period of time. When managing hundreds or thousands of endpoints, these alarms are needed so that administrators don't need to manually look for problems.

For other systems, a separate piece of software is required to manage the radio or fiber optic network with a separate administrator and training. There are usually significant O&M costs for licensing and upgrades. Separate servers need to be installed to host the software. They are usually managed by an IT group or services organization that doesn't interact normally with the system operators. When a sensor or recloser DNP point shows as failed in SCADA, they don't know if it is a communication issue or something power related.

Fault Waveforms

The platform's protocol is designed to download fault waveforms after every event. This is a key feature as the waveforms are analyzed against the other sensors that are reporting to determine the root cause of the problem. All waveforms are available to users and can be exported to Excel or as a Comtrade file for analysis by protection engineers or reliability engineers.

The DNP3 protocol supports the transfer of waveforms. However, this type of information is usually not needed by the system operators to restore outages. In the first two architectures, the data would go to the central SCADA system where it would need to be stored or passed to another system so that engineers can access the data. Some utilities have installed a second radio for engineering access so that it doesn't interfere with SCADA which adds complexity and costs.

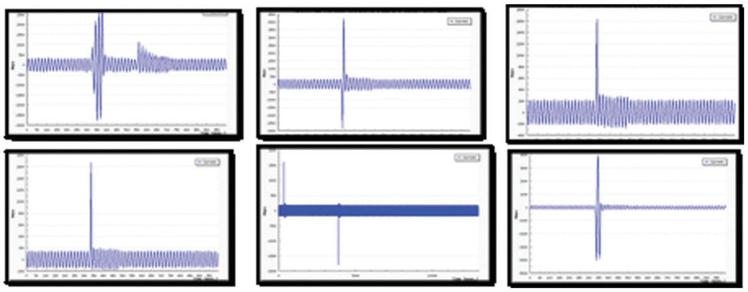

Figure 7: Waveform analysis showing a failing underground cable

Most equipment is not designed to download the waveforms automatically. The users must log into the sensor or recloser and manually retrieve the data. Most vendors supply their own software to do this. This software must be installed on each person's computer and is not visible to all users once downloaded. It is usually just on that person's computer. Depending on the equipment, the data may not be able to be downloaded remotely. The engineer may need to connect to the SCADA network to access the devices or may need to drive to the sensor or recloser and connect locally to manually download waveforms. With Aclara's platform, fault waveforms are automatically stored in SMS and available online at any time to all users.

Remote Programming and Upgrades

The Aclara platform protocol allows for remote programming of all settings and supports firmware upgrades. In fact, the sensors cannot be programmed in the field saving significant costs for commissioning engineers. If a line is reconfigured due to the installation of a new line or substation, the sensors can be re-programmed in a matter of minutes by an engineer sitting at their desk. Also, as Aclara continues to release industry leading features, the new firmware can be deployed to the entire population of sensors with one click on the SMS system.

DNP3 supports programming of some points remotely. These are typically analog setpoints such as trip settings. However, completely programming a sensor or recloser is not typically done using DNP3 only. DMS and OMS systems are not designed to be used to manage programming or firmware. The vendor's propriety software is required. Again, the engineer will either need to connect to the SCADA network or drive to the location to locally program the unit. If thousands of sensors are deployed, this will become unmanageable and cost prohibitive.

Conclusion

Taking these planning considerations into your DA architecture is critical to maximize your ability to scale, secure and use real-time data from field devices like smart grid sensors:

Option #1: Direct Connection from Field Devices into SCADA

Why Utilities Like This Architecture	Key Considerations
• Direct connection into you SCADA or DMS system means there is not additional third party software to license, host or manage.	• Will your SCADA team support and maintain thousands of new connections into your core SCADA network? • Do you want to grant more direct users who need the data direct access into your SCADA system? • This architecture opens up new security and NERC CIP compliance vulnerabilities, have you weighed the risks? • Was your DMS designed to handle thousands of new connections directly, or would it perform better if there was a concentrator processing data requests first before it handed off into the DMS?

Option #2: Traditional De-centralized Approach

Why Utilities Like This Architecture	Key Considerations
• "Tried and trusted" method – same architecture used for substation configuration the last 30 years • The concentrator allows SCADA to be managed separate from the SCADA system – this avoids many of the security risks outlined in Option 1.	• Will your SCADA team support and maintain hundreds of new SCADA concentrators? • How data is handled will be privy to new security risks which will need to be weighed against the needs of the business. • New costs – you'll need a new field concentrator for every 150 field devices, this will introduce new hardware costs over and above the costs of the field devices.

Option #3: Centralized Architecture

Why Utilities Like This Architecture	Key Considerations
• Better security • Easier compliance with NERC CIP • Lower hardware costs over Option #2 • Fewer connections into your SCADA or DMS • IT can maintain instead of your SCADA team • Cloud-based hosting is available for utilities who would like to outsource maintenance and support • Better data accuracy over Option #1 • Eliminates the need to have DNP3 unsolicited messages enabled in the SCADA system.	• Will you support in-house with your IT department or outsource? • What impact, if any, will the proprietary protocol have on the deployment?

About Aclara

Aclara is a world-class supplier of smart infrastructure solutions (SIS) to more than 800 water, gas, and electric utilities globally. Aclara SIS offerings include smart meters and other field devices, advanced metering infrastructure and software and services that enable utilities to predict and respond to conditions, leverage their distribution networks effectively and engage with their customers. In 2016 Aclara won a Frost & Sullivan Global Smart Energy Networks Enabling Technology Leadership Award and was named a finalist in three categories of the Platts Global Energy Awards. Aclara is owned by an affiliate of Sun Capital Partners.

Contact Information

Phone: 800 297 2728
Email: info@aclara.com
@AclaraSolutions

www.Aclara.com