How can I ...

Utilize telemetry and remote SCADA architecture for distributed infrastructure?

System Technical Note
PlantStruxure Reference Architecture

Design
Your architecture
**Important Information**

People responsible for the application, implementation and use of this document must make sure that all necessary design considerations have been taken into account and that all laws, safety and performance requirements, regulations, codes, and applicable standards have been obeyed to their full extent.

Schneider Electric provides the resources specified in this document. These resources can be used to minimize engineering efforts, but the use, integration, configuration, and validation of the system is the user's sole responsibility. Said user must ensure the safety of the system as a whole, including the resources provided by Schneider Electric through procedures that the user deems appropriate.

**Notice**

This document is not comprehensive for any systems using the given architecture and does not absolve users of their duty to uphold the safety requirements for the equipment used in their systems, or compliance with both national or international safety laws and regulations.

Readers are considered to already know how to use the products described in this document.

This document does not replace any specific product documentation.

The following special messages may appear throughout this documentation or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.

⚠️ The addition of this symbol to a Danger or Warning safety label indicates that an electrical hazard exists, which will result in personal injury if the instructions are not followed.

⚠️ This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.

<table>
<thead>
<tr>
<th>DANGER</th>
</tr>
</thead>
<tbody>
<tr>
<td>DANGER indicates an imminently hazardous situation which, if not avoided, <strong>will result in</strong> death or serious injury.</td>
</tr>
<tr>
<td>Failure to follow these instructions will result in death or serious injury.</td>
</tr>
</tbody>
</table>
Before You Begin

This automation equipment and related software is used to control a variety of industrial processes. The type or model of automation equipment suitable for each application will vary depending on factors such as the control function required, degree of protection required, production methods, unusual conditions and government regulations and so on. In some applications more than one processor may be required when backup redundancy is needed.

Only the user can be aware of all the conditions and factors present during setup, operation and maintenance of the solution. Therefore only the user can determine the automation equipment and the related safeties and interlocks which can be properly used. When selecting automation and control equipment and related software for a particular application, the user should refer to
the applicable local and national standards and regulations. The National Safety Council’s Accident Prevention Manual also provides much useful information.

Ensure that appropriate safeties and mechanical/electrical interlocks protection have been installed and are operational before placing the equipment into service. All mechanical/electrical interlocks and safeties protection must be coordinated with the related automation equipment and software programming.

**Note:** Coordination of safeties and mechanical/electrical interlocks protection is outside the scope of this document.

**START UP AND TEST**

Following installation but before using electrical control and automation equipment for regular operation, the system should be given a start up test by qualified personnel to verify the correct operation of the equipment. It is important that arrangements for such a check be made and that enough time is allowed to perform complete and satisfactory testing.

<table>
<thead>
<tr>
<th>WARNING</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>EQUIPMENT OPERATION HAZARD</strong></td>
</tr>
<tr>
<td>• Follow all start up tests as recommended in the equipment documentation.</td>
</tr>
<tr>
<td>• Store all equipment documentation for future reference.</td>
</tr>
<tr>
<td>• Software testing must be done in both simulated and real environments.</td>
</tr>
</tbody>
</table>

**Failure to follow these instructions can cause death, serious injury or equipment damage.**

Verify that the completed system is free from all short circuits and grounds, except those grounds installed according to local regulations (according to the National Electrical Code in the USA, for example). If high-potential voltage testing is necessary, follow recommendations in the equipment documentation to prevent accidental equipment damage.

Before energizing equipment:

- Remove tools, meters, and debris from equipment
- Close the equipment enclosure door
- Remove ground from incoming power lines
- Perform all start-up tests recommended by the manufacturer
OPERATION AND ADJUSTMENTS

The following precautions are from NEMA Standards Publication ICS 7.1-1995 (English version prevails):

Regardless of the care exercised in the design and manufacture of equipment or in the selection and rating of components; there are hazards that can be encountered if such equipment is improperly operated.

It is sometimes possible to misadjust the equipment and thus produce unsatisfactory or unsafe operation. Always use the manufacturer’s instructions as a guide for functional adjustments. Personnel who have access to these adjustments should be familiar with the equipment manufacturer’s instructions and the machinery used with the electrical equipment.

Only those operational adjustments actually required by the operator should be accessible to the operator. Access to other controls should be restricted to prevent unauthorized changes in operating characteristics.

⚠️ WARNING

UNEXPECTED EQUIPMENT OPERATION

- Only use software tools approved by Schneider Electric for use with this equipment.
- Update your application program every time you change the physical hardware configuration.

Failure to follow these instructions can cause death, serious injury or equipment damage.

INTENTION

This document is intended to provide a quick introduction to the described system. It is not intended to replace any specific product documentation, nor any of your own design documentation. On the contrary, it offers information additional to the product documentation on installation, configuration and implementing the system.

The architecture described in this document is not a specific product in the normal commercial sense. It describes an example of how Schneider Electric and third-party components may be integrated to fulfill an industrial application.

A detailed functional description or the specifications for a specific user application is not part of this document. Nevertheless, the document outlines some typical applications where the system might be implemented.
The architecture described in this document has been fully tested in our laboratories using all the specific references you will find in the component list near the end of this document. Of course, your specific application requirements may be different and will require additional and/or different components. In this case, you will have to adapt the information provided in this document to your particular needs. To do so, you will need to consult the specific product documentation of the components that you are substituting in this architecture. Pay particular attention in conforming to any safety information, different electrical requirements and normative standards that would apply to your adaptation.

It should be noted that there are some major components in the architecture described in this document that cannot be substituted without completely invalidating the architecture, descriptions, instructions, wiring diagrams and compatibility between the various software and hardware components specified herein. You must be aware of the consequences of component substitution in the architecture described in this document as substitutions may impair the compatibility and interoperability of software and hardware.

⚠️ CAUTION

EQUIPMENT INCOMPATIBILITY OR INOPERABLE EQUIPMENT

Read and thoroughly understand all hardware and software documentation before attempting any component substitutions.

Failure to follow these instructions can result in injury or equipment damage.
This document is intended to describe architectures for telemetry and remote SCADA systems.

---

**DANGER**

**HAZARD OF ELECTRIC SHOCK, BURN OR EXPLOSION**

- Only qualified personnel familiar with low and medium voltage equipment are to perform work described in this set of instructions. Workers must understand the hazards involved in working with or near low and medium voltage circuits.
- Perform such work only after reading and understanding all of the instructions contained in this bulletin.
- Turn off all power before working on or inside equipment.
- Use a properly rated voltage sensing device to confirm that the power is off.
- Before performing visual inspections, tests, or maintenance on the equipment, disconnect all sources of electric power. Assume that all circuits are live until they have been completely de-energized, tested, grounded, and tagged. Pay particular attention to the design of the power system. Consider all sources of power, including the possibility of back feeding.
- Handle this equipment carefully and install, operate, and maintain it correctly in order for it to function properly. Neglecting fundamental installation and maintenance requirements may lead to personal injury, as well as damage to electrical equipment or other property.
- Beware of potential hazards, wear personal protective equipment and take adequate safety precautions.
- Do not make any modifications to the equipment or operate the system with the interlocks removed. Contact your local field sales representative for additional instruction if the equipment does not function as described in this manual.
- Carefully inspect your work area and remove any tools and objects left inside the equipment.
- Replace all devices, doors and covers before turning on power to this equipment.
- All instructions in this manual are written with the assumption that the customer has taken these measures before performing maintenance or testing.

Failure to follow these instructions will result in death or serious injury.
The STN Collection

The implementation of an automation project includes five main phases: Selection, Design, Configuration, Implementation and Operation. To help you develop a project based on these phases, Schneider Electric has created the Tested, Validated, Documented Architecture and System Technical Note.

A Tested, Validated, Documented Architecture (TVDA) provides technical guidelines and recommendations for implementing technologies to address your needs and requirements. This guide covers the entire scope of the project life cycle, from the Selection to the Operation phase, providing design methodologies and source code examples for all system components.

A System Technical Note (STN) provides a more theoretical approach by focusing on a particular system technology. These notes describe complete solution offers for a system, and therefore support you in the Selection phase of a project. The TVDAs and STNs are related and complementary. In short, you will find technology fundamentals in an STN and their corresponding applications in one or several TVDAs.

Development Environment

Each TVDA or STN has been developed in one of our solution platform labs using a typical PlantStruxure architecture.

PlantStruxure, the process automation system from Schneider Electric, is a collaborative architecture that allows industrial and infrastructure companies to meet their automation needs while at the same time addressing their growing energy efficiency requirements. In a single environment, measured energy and process data can be analyzed to yield a holistically optimized plant.
Table of Contents

1. Quick start guide
   1.1. Purpose
   1.2. Customer challenges
   1.3. Glossary
   11

2. Introduction
   2.1. Purpose
   2.2. Customer challenges
   2.3. Glossary
   13

3. Remote SCADA overview
   3.1. What is a telemetry and remote SCADA system?
   3.2. Differences between process SCADA and remote SCADA
   3.3. What is an RTU?
   3.4. RTU market and customer requirements
   3.5. RTU device categories
   3.6. Remote communication networks
   3.7. Telemetry and optimization
   3.8. Telemetry protocols
   3.9. Remote SCADA for telemetry
   17

4. System presentation
   4.1. Reference architecture
   4.2. Enterprise and asset management integrated systems
   4.3. ClearSCADA
   4.4. Trio data radios for wireless infrastructure
   4.5. RTU solutions
   4.6. Standard SCADAPack RTU
   4.7. SCADAPack E smart RTU
   4.8. M340 PAC with RTU module
   4.9. Accutech wireless instrumentation
   35

5. System requirements
   5.1. General system requirements
   5.2. System architecture
   5.3. Business interface
   5.4. Control room subsystem
   5.5. Telemetry protocol
   79
6. **Selection**

   6.1. *Business network interface architecture for remote SCADA* 121
   6.2. *Control room architecture for remote SCADA* 126
   6.3. *Multi-site systems* 133
   6.4. *Remote communication network architecture* 140
   6.5. *Remote site architecture* 152

7. **Appendix** 161
1. Quick start guide

The goal of this System Technical Note (STN) is to provide recommendations, guidelines, and examples to help users in different roles to select an architectural framework, design, implement and maintain a telemetry and remote SCADA system.

To get the most out of this STN, please consider the following suggestions:

1. If this is the first time you are using a Schneider Electric telemetry and remote SCADA solution, we recommend that you read the entire STN before proceeding.

2. If you are familiar with remote SCADA and RTU technology and want to learn about Schneider Electric’s telemetry and remote SCADA Solutions offer, you can start at chapter 4.

3. If you are already familiar with RTU technology and want to understand how requirements affect a solution, you can start at chapter 5.

4. If your requirements are understood and you want to choose solution architectures, you can start at chapter 6.
2. **Introduction**

2.1. **Purpose**

This System Technical Note (STN) describes how to utilize telemetry and remote SCADA for managing widely distributed infrastructure. It describes the customer challenges, the industry environment and requirements, concepts and architectures using Schneider Electric telemetry and remote SCADA solutions to meet those industry challenges.

2.2. **Customer challenges**

![Diagram of customer challenges]

**Figure 1: Remote infrastructure management: customer challenges**

For customers in industries that require remote SCADA solutions, the challenges include the following:

- Minimize cost along lifecycle of remote assets
- Minimize risk of managing and operating remote assets
- Optimize remote equipment operation and production
- Make the most of your remote assets
2.2.1. Minimize cost along lifecycle of remote assets

Scalability and flexibility
- Choose a cost effective type of remote communication: permanent vs. non-permanent
- Accommodate the number of remote sites in a system
- Understand the services needed: event, alarming, data logging, time stamping accuracy

Simplicity and open standards
- Use the communication protocol specified by customer, appropriate to the region and that suits the application requirements. E.g. DNP3, IEC 60870, Modbus

2.2.2. Minimize risk of managing and operating remote assets

Safe operation and compliance
- Monitor critical items
- Record and calculate the correct data for compliance reporting

Reliability and security
- Choose the right level of security for defense in depth and best practices
- Choose the right remote communication infrastructure for critical systems

2.2.3. Optimize remote equipment operation and production

- Monitor energy efficiency (a key aspect of Schneider Electric’s EcoStruxure strategy)
- Maximize operational efficiency
- Minimize equipment downtime

2.2.4. Make the most of your remote assets –Connectivity and integration

- Turn SCADA data into business information
- Understand the benefits of remote site configuration management
- Provide meaningful and accurate reports to the enterprise
- Use open standards for connecting to business systems
2.3. **Glossary**

A glossary is available in the appendix chapter of this document. Please refer to it whenever necessary.
3. Remote SCADA overview

To give users an overview of telemetry and remote SCADA and remote asset management solutions, we will introduce:

- What is a telemetry and remote SCADA system?
- Differences between process SCADA solutions and remote SCADA solutions
- What is an RTU?
- RTU market and customer requirements
- RTU device categories
- Telemetry protocols
- Remote SCADA for telemetry

3.1. What is a telemetry and remote SCADA system?

A telemetry and remote SCADA system provides the software, equipment, linkages and communication infrastructure to deploy an entire solution for managing distributed assets and infrastructure.

The Schneider Electric offer for telemetry and remote SCADA includes ClearSCADA enterprise SCADA server and display client solutions, remote communication networks including Trio data radio devices, SCADAPack and SCADAPack E smart RTU devices utilizing the latest in open telemetry protocol standards, and Accutech wireless instrumentation. Schneider Electric’s focus on open standards ensures connectivity with business systems and a wide range of industry equipment, working together in an integrated enterprise to field solution.
3.2. Differences between process SCADA and remote SCADA

Process solutions and remote solutions have similarities, but differ in important ways. The table, diagrams and descriptions below highlight the differences.

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Process SCADA</th>
<th>Remote SCADA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Geography</td>
<td>100s meters across a process installation</td>
<td>100s to 1000s kilometers across a system</td>
</tr>
<tr>
<td>System size</td>
<td>10s to 100s of devices</td>
<td>Scalable from 100s to 1000s of remote sites</td>
</tr>
<tr>
<td>Communication design</td>
<td>Permanently connected, high availability by duplication</td>
<td>Non-permanent or connection-on-demand, improved availability by communication link diversity (e.g. radio + cellular)</td>
</tr>
<tr>
<td>Communication type</td>
<td>Local area, high speed e.g. Ethernet</td>
<td>Widely distributed, low speed e.g. radio, cellular, satellite, dial-up, leased services</td>
</tr>
<tr>
<td>Communication speed</td>
<td>100 ~ 1000 M bits/second</td>
<td>10 ~ 100 K bits/second</td>
</tr>
<tr>
<td>Data acquisition</td>
<td>High-speed sequential polling</td>
<td>Event-based telemetry communication</td>
</tr>
<tr>
<td>Control room / operations center</td>
<td>Locally at process site</td>
<td>• Co-located in a process control room (small systems)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Centralized close to business operations (medium-sized systems)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Duplicated, independent control centers for business continuity (large systems)</td>
</tr>
<tr>
<td>Functionality</td>
<td>Logic and data handling coded in PAC / PLC and SCADA host</td>
<td>Logic optional; Data processing and communication functionality built-in to RTU and remote SCADA master. Set by Configuration, not Logic</td>
</tr>
<tr>
<td>Maintenance and fault detection</td>
<td>Local at PLC or other process automation equipment</td>
<td>Remote from site equipment, using Remote Communication Network; and Local at site</td>
</tr>
<tr>
<td>Upgrades</td>
<td>Local at process automation equipment, commonly performed during scheduled system shutdown</td>
<td>Deployed remotely without reloading configuration</td>
</tr>
</tbody>
</table>

Table 1: Differences between typical process SCADA and remote SCADA systems
3.2.1. **Process SCADA and remote SCADA in the control room**

In the control room, both process SCADA and remote SCADA deliver visualization to operators, presenting operational status, historical data and alarm management facilities, as well as integration with enterprise applications.

While process SCADA typically provides a concentration of system servers and operator displays in the control room and other locations throughout the process, remote SCADA is often required to provide these services in different operational locations, in an integrated way. Remote SCADA typically provides coordination of system client and server activities over wide area network (WAN) communication links.

A focus on operational and historic data in the control room for both process and remote systems ensures accuracy of the data presented and recorded. Data is delivered from a process automation system to the control room in real time on high speed reliable communication networks, recording the current data as it arrives. In the case of remote SCADA, the data from widely distributed remote sites may experience delays or interruptions before being delivered to the control room. The remote SCADA solution provides visualization and historical accuracy of the remote data through the use of timestamped and quality tagged data, annunciating alarms.
Remote SCADA manages data that can be received any time from minutes to days after its collection in the field. Remote SCADA presents and manages that delayed data as if it had been received in real time.

Schneider Electric’s PlantStruxure architecture defines communication infrastructure used by process SCADA, based on LAN and fieldbus networking. Remote SCADA interfaces to remote communication network technologies. While similarly including Ethernet and TCP/IP WAN networks, common remote communication network infrastructure such as radio, leased-line modems, GPRS, PSTN (dial-up), is supported. Communication with critical remote sites can use independent fail-back communication infrastructure. Remote SCADA deals with multiple types of communication paths, including to the same site.

Figure 3: Typical process automation architecture based on PlantStruxure

Remote SCADA systems that monitor widely dispersed sites are often required to interact with process sites. The multi-site approach to operating this type of system can be provided in a number of ways. Remote SCADA’s role as a distributed operational platform can be extended to include visualization of an automation process as one approach for multi-site operation. Alternatively, data can be collected by remote SCADA from a process automation system in the
same way as other remote sites and be used by operators in the same way. Further details of these alternatives are presented in 6.3.

Figure 4: Typical remote SCADA architecture
3.2.2. Process networks and remote communication networks

Process automation solutions are architected to take advantage of high bandwidth and high reliability connections in a contained area. These systems can be extended locally by using wide area communication technologies such as Wi-Fi. Availability improvements can be made in process networks by duplicating communication device hardware, network communication cabling, and so on.

In general, process network systems can be characterized as permanently connected networks. A process network may support communication with 10s to 100s of devices.

In contrast, remote communication network solutions are architected to cope with challenges of lower bandwidth and lower reliability, across long distances and in remotely distributed systems. In many cases, devices need to establish connection prior to communication. Availability improvements are sometimes made in remote networks for critical sites through the addition of independent communication technologies.

A remote communication network may support communication with 10s to 1000s of remote sites. Also see 3.6.

3.2.3. Communication methodology

Process automation communications are driven by the SCADA servers and, in most cases, use protocols suitable for direct connection to process equipment, including Modbus, Modbus/TCP, and Ethernet/IP. These protocols are efficient in the process environment and operate best on high bandwidth reliable channels.

Remote SCADA provides specialty in long distance, lower reliability channels, providing very efficient communication methodologies with a focus on NO LOSS OF DATA even when remote communication links are not available. Event driven telemetry protocols such as DNP3 and IEC 60870-5 operate on the remote communication networks between the remote SCADA servers and field RTUs. These protocols provide an accurate timestamped representation of field data changes. They are ideal for operating in a low bandwidth environment, and where communications can be disrupted due to the remote nature of the sites. Adaptations of Modbus can also provide some of this functionality, and in particular there is an established product base offering intelligent data based on Modbus for the Oil & Gas sector Electronic Flow Measurement (EFM).

Where timestamped events are used, telemetry communication methodologies are employed to collect field data. This can include polling for events more frequently than polling for the current values of all data points. Some protocols and communication media support unsolicited reporting for rapid delivery of alarm conditions even in low bandwidth and low polling rate systems. Some communication media provides multi-drop communication, allowing a cost effective means to
reach widely distributed remote sites. Some system architectures can provide inter-site connection strategies to minimize communication cost and maximize reliability.

3.2.4. Devices at process and remote sites

Process automation solutions use PAC or PLC devices to automate process control through connection with field devices. Important characteristics of PLCs in the process environment include determinism of control algorithms, I/O performance and interconnectivity with field bus technologies. The communication aspect of process automation is important, with the solutions building robust local area communication systems as a service for the PLC devices. A typical process automation communication solution distributes PLC devices in a local area, providing sophisticated control at each field location.

Remote solutions use RTUs to collect data from field equipment and field devices. An important characteristic of RTUs in the remote field environment is communication capability. Due to the characteristics of remote communication networks, RTUs provide sophisticated communication features to overcome the unreliable, non-permanent and low bandwidth nature of many remote communication solutions. RTUs often integrate data from a wide variety of local devices (typically requiring the RTU to support multiple integrated communication protocols). They perform all these functions whilst preserving information integrity (i.e. no lost data).

Remote sites using an RTU typically contain a lower density of equipment and simpler controls compared with a process automation system. While similar control logic capabilities are provided in an RTU as in a PLC (such as IEC 61131-3 control languages), the primary focus of an RTU is its data gathering, data manipulation, event buffering and remote communication capabilities.

Spread over a very large geographic area with potentially thousands of remote sites, these can be difficult and time consuming to access, and are unattended a majority of the time. An important aspect of an RTU is its ability to be remotely managed. RTUs are optimized for operating remotely, including over low bandwidth and non-permanent communication links.

Features supporting this functionality include:

- Read, modify and write configuration including logic applications
- View operational data
- Debug control logic applications
- Upgrade system firmware
- Capture and return diagnostic logs
- Centrally manage and deploy configuration to smart RTUs
3.3. What is an RTU?

An RTU (Remote Terminal Unit) is an electronic device located in a remote field installation which operates as a data acquisition and control unit. It often interfaces with local equipment through I/O (Input/Output) physical connections, as well as interfacing with local intelligent devices through communication interfaces.

RTUs aid in monitoring and controlling equipment by gathering and updating data from the process equipment installed at remote locations. An RTU manages connection across a remote communication link to a control room (typically to a remote SCADA server), providing robustness and security in unreliable, non-permanent and low bandwidth communication environments (e.g. radio, GPRS, modem connections).

Along with the communication connection with a remote SCADA server, there can be communication connections to other RTUs (peer-to-peer communication). The RTU can also route communication packets to other RTUs, or collect data from other RTUs in data concentrating sub-master hierarchies, forming a network structure for distributed communication to sites which may not be accessible directly from the control room.

![Figure 5: RTUs in telemetry and remote SCADA architecture](image)

Key RTU facilities may include updating of configuration, control programs and deploying of firmware updates from the remote SCADA server, as well as being managed locally using RTU configuration tools.
Telemetry protocols such as DNP3, IEC 60870-5 and Modbus are standard communication protocols that allow the remote measurement, monitoring, control and data transfer of infrastructure scattered over a large area, or that are hard to access from a central system.

RTUs solve the challenges of remote monitoring and control by optimizing data collection and transmission, and by managing data communication so that a large number of remote devices can communicate within a system using cost effective remote communication links.

3.4. **RTU market and customer requirements**

RTU systems address the remote communication needs of the Water & Wastewater (WWW), Renewable Energy, Oil & Gas (O&G) and other industries. Remote monitoring and control are critical to these large systems and widely dispersed sites.

3.4.1. **Specific requirements for WWW applications**

Requirements for remote stations:

- Ready-to-use solutions for telemetry and control applications for geographically dispersed pump station and booster station monitoring and control
- Conformal coating of electronics in some applications (e.g. wastewater H₂S environments)
- Extensive event logging for operational analysis and auditing
- Time-stamp event management in the order of 100 - 200ms, with clock synchronization
- Remote diagnostics and configuration management
- Critical infrastructure asset resilience against cyber attacks
- Inter-site control coordination for energy management, environmental protection and reliable water supply

Requirements for the remote communication infrastructure:

- Networks supporting dozens to thousands of remote stations
- Powerful telemetry SCADA master with communication scheduler
- Flexibility to support a choice of communication options, including use of cellular and wire-line public networks and private wireless communication
- Conformance certified to locally accepted standards (IEC 60870-5 in Europe, the Middle East and some parts of Asia, DNP3 in the Americas, China, Australia, UK)
- Modem management
- Scalability from dozens to thousands of remote sites
3.4.2. Specific requirements for O&G applications

Requirements for remote stations:

- Simple to use ladder logic programming
- Flexible Modbus device interfaces
- Remote data accessibility due to remote systems scattered over a wide geographical area and hard to access locations
- Extreme ruggedness (low and high temperatures)
- Operational in hazardous environments (hazardous and explosive atmosphere requirements, conformal coating for operation in corrosive gas environments)
- Challenging operating conditions (requiring compact design with low power consumption)
- Maximum availability required (production environments)
- Gas flow computer functionality providing certified algorithms and custody transfer auditing features (geography dependent), including hourly and daily history reporting

3.5. RTU device categories

RTU devices are available in two general forms:

- Compact RTU
- Modular RTU

Due to the nature of remote sites, many suit a **Compact RTU** solution, typically requiring the following features:

- Compact size
- High level of functionality in a single device
- Low power consumption
- High environmental specifications
- Expandable I/O options
- Multiple, integrated communication options
Schneider Electric’s compact RTU range includes SCADAPack Smart RTU and SCADAPack E Smart RTU devices.

![Image of SCADAPack devices]

**Figure 6: SCADAPack and SCADAPack E Compact RTUs**

Schneider Electric SCADAPack and SCADAPack E RTUs provide the advantages of a highly integrated RTU in a cost effective, compact solution.

Standard SCADAPack RTUs are best suited to Oil & Gas applications, including gas flow measurement and auditing applications, and where the remote communication protocol is typically Modbus. They are best suited to low and medium complexity applications using simple ladder or IEC 61131-3 programming, or where specialist C/C++ application development is required. Examples include gas well head control and electronic flow measurement.

SCADAPack E RTUs are best suited to Water and Renewable Energy applications, including applications with site-to-site interaction for optimizing control, in hierarchical architectures requiring message routing and data concentrating (sub-master), and where the remote communication challenges are solved using open telemetry protocols such as DNP3 or IEC 60870-5. They are suited to low and medium complexity applications using the strengths of one or more applications in IEC 61131-3 languages. Examples include pumping installations and small process sites.

**Modular RTUs** are typically used in more complex control applications in large autonomous remote sites.

They provide features such as:

- High speed processing and determinism for complex control algorithms
- I/O expansion through the addition of modules
- Communication expansion through the addition of modules

The M340 PAC is suitable for Oil & Gas applications, for example in pipeline control and compressor station applications, and where complex control is required with field bus.
communication. The additional M340 RTU module provides an interface between the control application and a telemetry system using DNP3 or IEC 60870-5 protocols.

Figure 7: Modicon M340 PAC with the RTU module option

In Water applications, the M340 is suited to solutions described in the Schneider Electric Water Solutions structure for remote sites. In particular the “R3” remote site type is suited to M340 applications typically in large pumping stations with complex control requirements. Other applications include small wastewater treatment plants and small hydro-electric power plants. The M340 PAC with its additional NOR0200H RTU module provides an interface between a control application and a telemetry system using DNP3 or IEC 60870-5 protocols.

3.6. Remote communication networks

There are three broad types of remote communication networks:

- **Permanent**
  - Where the data path is always available from a SCADA master to the remote device
  - Typically a dedicated service, point-to-point communication
  - Data is available immediately
  - Examples include: Ethernet, Fiber Optic, DSL WAN, and so on

- **Non-Permanent**
  - Where the data path becomes available soon after it is requested
  - Typically a shared service, subject to loss of availability or quality
  - Data is slightly delayed
  - Examples include: Private data radio, Landline, GPRS, Satellite

- **Connection on demand**
  - Where the connection must be established between communicating devices
  - Data is delayed
  - Examples include: PSTN, GSM
3.7. Telemetry and optimization

A challenge in remote systems is the broad variance in potential communication network solutions. A uniform approach to sending data across this broad variance of remote network types is preferred over individual solutions for different technologies. This is particularly important for the long term viability of remote asset monitoring as communication technologies evolve. In addition, the approach needs to be highly scalable to suit system sizes from dozens to thousands of remote sites.

Open telemetry protocols provide this uniform approach as well as a key benefit in the optimization of both data gathering and data transmission.

The role of the smart RTU, after collecting raw data from local I/O or attached devices, is to derive useful information from that data. Transforming the data into information occurs in several ways: through manipulation using control logic; through the presentation of data as real world values rather than just as computer represented numbers; and through the detection of interesting changes in data, recording the times that those changes occurred.

Figure 8: Remote communication network in remote SCADA architecture
Smart RTUs capture “interesting changes” in data using “Events.” Events may be recorded by an RTU when:

- A point state change occurs (e.g. a digital point changing its state from Off to On)
- A change in data quality (e.g. a value has gone out of range and is no longer valid, a local instrument from which data was being gathered is no longer communicating)
- A value has deviated by more than a specific amount since the last time the value was reported (e.g. a sudden deviation in a value that makes it significant to report); this is an absolute or percentage deviation
- A value changing slowly is reported occasionally, but when it starts to change more quickly, it should be reported more often; this is an integration deviation
- A value is expected to be changing but has not changed, indicating a process problem or instrumentation failure
- A value is increasing or decreasing too rapidly
- A value has exceeded operating limits, requiring an alarm to be raised

When an RTU records an event, it typically records the time at which the event (interesting data change) occurred.

Telemetry optimizes bandwidth through efficient representation of information, taking the stored “interesting” data and transmitting as events. Where the events include individual timestamps, the control center receiving this can reconstruct the field data accurately, independent of how often the data is transmitted or whether the communication link was inoperable for a period of time.

This provides significant data resilience, optimizing the availability requirements of the remote communication network without compromising data integrity.

Telemetry provides services that enable a control center to collect data from remote RTUs in a number of ways. The concept of classical data polling, where the master requests data and the RTU returns what is requested, is extended for telemetry whereby data can be organized in Classes, allowing different types of data to be requested at different rates. Where data is provided by the RTU in the form of events, significant bandwidth and response time gains can be made across a system where the data is only periodically changing. Occasionally, a master will send an Integrity Poll to retrieve all events and all current values of points in the RTU to ensure ongoing synchronization of all data between the devices. Another data transmission service provided by telemetry protocols is that of the Unsolicited Response which allows an RTU to transmit event data without being polled. There are design and configuration considerations when using Unsolicited Responses in a system, but this can provide significant performance improvement in response time for critical data.

The telemetry protocol defines the format and semantics of the communication mechanisms.
3.8. Telemetry protocols

In the remote SCADA industry, a number of different protocols are used for communication between control centers (using SCADA) and widely separated (remote) assets monitored and controlled by an RTU. Proprietary protocols, and now commonly, international standard protocols are used for telemetry. The most popular standard protocols are DNP3 (Distributed Network Protocol, also known as IEEE 1815) and IEC 60870-5-101/-104 (from the International Electrotechnical Commission). Many proprietary solutions for telemetry protocols use privately extended derivatives of Modbus protocol.

![Telemetry Protocols](image)

Figure 9: Telemetry protocols in remote SCADA architecture

A key value of standard protocols, compared to proprietary protocols, is that they ensure a high level of interoperability with devices from multiple manufacturers. DNP3 is dominant in North America, Australia, the UK and parts of Asia. IEC 60870-5 protocols are part of the IEC suite and are associated with legislative requirements in some European countries. IEC protocols are also used in some parts of the Middle East. In parts of Asia and South America, both DNP3 and IEC 60870-5 protocols are used.

The basic set of telemetry services provided by DNP3 and IEC 60870-5 protocols is similar. They are both particularly suited to “non-permanent communications” (modem, radio and so on) and low bandwidth data exchanges, as they provide high efficiency and robustness in data transfer between SCADA systems and RTU devices. They are fundamentally “event driven” protocols,
using a data generation technique known as *Report by Exception*. Events capture important (or interesting) changes in data being monitored, and can be recorded along with information such as time of occurrence and data quality. The feature set of DNP3 is larger than IEC 60870-5 which can be advantageous in some system architectures.

It is important to understand the difference between *Report by Exception* and *Unsolicited Responses* which both relate to event management. *Report by Exception* is a data generation technique used by RTUs (producing events). An *Unsolicited Response* describes the spontaneous transmission of data and is only one of several data reporting techniques used by RTUs (transmitting events). There are other ways of reporting event data that do not require unsolicited responses (polling from a master).

Compared to traditional polling protocols, these event management aspects of DNP3 and IEC 60870-5 protocols significantly contribute to reducing and optimizing data traffic for non-permanent and connection on-demand remote communication networks, but they also bring efficiency and robustness to all types of communication networks, including those supporting permanent communications (for example, robustness in the form of recovery of data following the loss of communications).

DNP3 and IEC 60870-5 protocols can operate over a broad range of remote communication networks including multi-drop networks such as serial lines, radio, leased-line and PSTN (dial-up); and point-to-point or connection-oriented networks such GSM, cellular IP (GPRS, EDGE, HSDPA, and so on), DSL, LAN and more.

### 3.9. Remote SCADA for telemetry

The role of the remote SCADA environment is to centralize information received, via telemetry, from remote sites for the purpose of providing human and machine interfaces for operating a system through visualization, alarming, archiving and control.

The remote SCADA comprises servers that collect data from remote sites. These are typically located in data centers, often replicated for disaster recovery and business continuity.

Remote SCADA also comprises clients for the human and machine interfaces to the collected data, presenting both current and historical information. Where operated with human supervision and intervention, remote SCADA clients are often present in a control center along with other business information applications needed for operating a system. Control centers may be replicated for disaster recovery, or be distributed according to function.

A challenge for remote SCADA solutions is providing a scalable architecture that suits systems that are small in size (dozens of remote sites managed from a single desktop) up to very large systems (thousands of remote sites managed across multiple control centers, interacting in real
time with other business applications). Object-oriented techniques are used in modern systems to significantly simplify scalability. Data communication aspects to handle telemetry protocols, with native handling of data quality, time stamps and native backfilling of data into history and event logs, are critical to system scalability. Information received from a low capacity link, or after restoration of a remote link, is presented as if it had been received in real time. This scalability requires the support of a full range of communication technologies, including automatic switching to backup links, operation on permanent, non-permanent and connection-on-demand services and the flexibility to dynamically optimize communications based on link congestion, adverse weather conditions and operational scheduling.

Figure 10: Remote SCADA

Further, the information collected by remote SCADA is valuable for making business decisions and the architecture must provide scalability for distribution of data across an organization, for up to potentially hundreds of concurrent users. The solutions provided for human interaction with a system need to operate centrally within a high speed business network, but also be optimized for operating over slower communication links, such as mobile equipment or at remote locations. Notification of system issues through a range of technologies is often sought for ensuring operational efficiency. This includes SMS, email, web and mobile access. Paramount is a strong system security model at all levels of operation.

Today’s challenges also include operating a business in a dynamic environment where the number of remote sites, control centers and users of business data alike are expanding. It is crucial that the remote SCADA infrastructure and the data it presents, like the rest of the business, be augmented and upgraded online, providing new information immediately without
disrupting the operation of the business. Requirements extend to remotely managing field equipment for operational efficiency and augmenting system security. Remote SCADA can provide this efficiency through centralized configuration management of remote RTUs, for example through the centralized management of RTU configuration changes and firmware upgrades. These can be managed locally and deployed remotely, and in a secure manner, without disrupting system operation and with better workforce efficiency.

Business efficiency challenges mean that previously isolated automation systems need to work together, be operated, managed and presented as a single system so better decisions can be made and energy management can be optimized. A good remote SCADA can take the view of multiple distributed remote SCADA systems and present them in a single system view, providing combined display, navigation, trend and alarm information.
4. System presentation

A **High Level Reference Architecture** is an integration of a large-scale automation network; in this case, defining the architecture for telemetry and remote SCADA. In this remote oriented network architecture, the focus is on the unreliable, non-permanent and low bandwidth nature of remote communications. Solutions are described for all levels of the telemetry and remote SCADA architecture: the business network, control room, remote communication network and remote sites. The High Level reference architecture is consistent with the philosophy of the PlantStruxure reference architecture framework.

This section introduces the Telemetry and Remote SCADA Solutions offer at each layer in the integrated telemetry system architecture.

4.1. Reference architecture

The guide uses high level reference architecture to demonstrate examples and guide users in the requirements, design and implementation of telemetry and remote SCADA networks supporting various services to support simple through to complex applications.

4.1.1. Telemetry and remote SCADA reference architecture

- **A. Choose a business system interface architecture for remote SCADA**
  See section 6.1

- **B. Choose a control room architecture for remote SCADA**
  See section 6.2

- **C. Choose a remote communication network architecture**
  See section 6.3

- **D. Choose a remote site architecture**
  See section 6.4

Figure 11: Choosing telemetry and remote SCADA solutions architecture
4.1.2. Benefits of telemetry and remote SCADA solutions

Schneider Electric's products for telemetry and remote SCADA adhere to open standards in order to maximize interoperability when any individual product is used in conjunction with third party devices. The telemetry and remote SCADA solution structure provides additional benefits when Schneider Electric products are used together. This STN describes solutions based on a system approach, providing examples that bring additional benefits when the telemetry and remote SCADA products are used together.

Both operational and maintenance benefits are achieved by using a systems approach that combines the use of multiple telemetry and remote SCADA products. Examples include:

- System using best-in-class open standards
- Confidence that the components will work together, reliably, as a system
- Application examples provided by Schneider Electric based on field systems
  - Can be used in training or as a starting point for similar customer applications
  - Tested Validated Documented Architectures (TVDA) provided by Schneider Electric provide system performance data and configuration information for applications
- Enhanced diagnostics
- Providing clear information on operational issues, configuration problems or fault scenarios
- Centrally managed configuration
  - Easing maintenance and providing long-term system performance
  - Reducing engineering effort
  - Reducing site visits by managing changes centrally and deploying validated configuration uniformly across a system
- Better integrated systems when using products from Schneider Electric
  - ClearSCADA integrated with Trio diagnostics
  - ClearSCADA integrated configuration, firmware upgrade and real-time diagnostics management for SCADAPack E RTUs
  - ClearSCADA integrated configuration management for SCADAPack Realflo gas flow computers
  - ClearSCADA integrated with OFS communication suite for Schneider Electric PAC and PLC devices
  - SCADAPack RTU, SCADAPack E RTU and M340 PAC communication with Accutech Wireless Instrument network
4.2. Enterprise and asset management integrated systems

Schneider Electric’s architecture includes powerful and open interfaces for connecting telemetry and remote SCADA solutions to business systems. Enterprise management systems and asset management systems can process data aggregated and presented by remote SCADA, adding significant value to business information.

Integration with enterprise systems is provided through reporting, database access and other means, allowing a wide range of business applications to interface with Schneider Electric’s offer. Open standards are a key to this integration.

Schneider Electric also provides a number of domain focused enterprise level solutions.

4.2.1. Schneider Electric EcoStruxure web services

A major enabler in enterprise application integration is provided by a Schneider Electric’s EcoStruxure solution: EWS – Schneider Electric EcoStruxure web services.

EWS is a data exchange mechanism based on SOAP / XML that enables specialist business systems to interact. It is simple to use and configure.

A number of Schneider Electric enterprise solutions, including ClearSCADA for telemetry and remote SCADA, support the EWS standard. Applications include leakage detection, energy management and building management that allow integration with remote SCADA data to realize cost savings through energy optimization.
4.2.2. AQUIS water network simulation platform

Schneider Electric's Hydraulic Simulation and Optimization software (AQUIS) is a domain enterprise platform that is complementary to telemetry and remote SCADA. It integrates with ClearSCADA using EcoStruxure Web Services (EWS) to obtain real-time data from telemetry, and can gather data from other sources to optimize water distribution network operation.

AQUIS is an advanced, powerful and extensive water network simulation platform designed to improve:

- Hydraulic performance
- Water quality
- Safety of operation

while reducing:

- Water supply costs
- Energy and CO₂ emissions
- Leakage (Non-Revenue Water)
- Customer complaints
- Capital investment

ClearSCADA provides a single, integrated user interface for remote SCADA and AQUIS water network simulation.

For more information see www.7t.dk

4.3. ClearSCADA

ClearSCADA is an extensible and open client/server enterprise platform designed for use in SCADA systems with multiple, remotely located controller and sensor installations. Real-time and historical data is collected by single or redundant servers over dedicated long-distance communication infrastructure and made available to local and remote users via integrated clients or third-party data management applications.

Key value propositions of ClearSCADA include:

- Optimized for dynamic business environments
  - Business continuity provided through highly available system architectures
  - Online system configuration changes available immediately across an enterprise
  - Low client/server bandwidth requirements for deployment across multiple business locations
4 – System presentation

- Significant functionality built in for operating and managing remote SCADA
- System presentation and management using object orientation
  - Rapid system deployment
  - Low total cost of ownership
  - Vector graphics automatically adapt visualization to different environments (control room, laptop, desktop)
- Open standards access for all client, server, database and communication interfaces
- Comprehensive integrated historian
- Extensive security model
- Integrated telemetry drivers for open standard protocols (DNP3, IEC 60870-5)
  - Native handling of non-permanent and connection on demand communications
  - Native historical data backfilling from buffered RTU data
  - Centralized configuration management of remote RTUs and applications
- Full function display client (ViewX) integrates secure engineering management tool
- Integrated web server immediately provides active content to web users
  - Same look and feel as full function client
  - No publishing to an external web server
- Extensive integrated alarm management and reporting
  - Prioritized alarm redirection via email, SMS, pager, escalation
  - Alarm handling time management for rosters, duty shifts, calendar events

4.3.1. Vector graphics

Providing independence from PC display resolution for full function display and web display, the ClearSCADA vector graphics engine provides significant operational benefits. Automatically scaled vector graphic objects ensure display configurations created today suit changes in display technology in the future.
The full-featured graphics capability of ClearSCADA displays include zooming, panning, automatic de-cluttering, and provides the ability to turn on and off selective graphic content using layers. The result is simplified graphics for clear systemic views, with more detail easily displayed to look deeper into operational states.

Graphic displays can be imported from DXF multi-layer graphic files, allowing external graphical content to be imported (maps, schematics, spatial asset information).

4.3.2. Alarm management

Integrated alarm management allows ClearSCADA to integrate with a customer’s business operations, adding value by directing alarms to the correct personnel for problem rectification and maintenance planning. This is particularly important for operational and maintenance aspects of remote assets, ensuring efficiency by notifying the correct personnel at the correct time.

ClearSCADA provides alarm redirection for distributing alarms via email, SMS and pager systems. Alarms can simply notify or require acknowledgment via ClearSCADA login, email or SMS. Unacknowledged alarms can be escalated to different operational personnel if not acknowledged, escalated to maintenance personnel if remaining unresolved, and so on.

Personnel rosters and contact priority can be established in flexible groupings as required. Calendar-based roster management allows time varying rosters to be planned in advanced, accounting for holiday periods. ClearSCADA alarm facilities are suited to both manned and unmanned operation control centers and distributed field maintenance personnel common in systems with widely distributed assets.

Alarm management can be managed at all operational levels on a system, group, device and an individual alarm basis, as required.

4.3.3. Object oriented

Object oriented by design, the ClearSCADA architecture provides a hierarchy of objects, grouped functionally to maximize configuration standardization and re-use through templates and instances. Online database configuration and management provide an enterprise platform for critical infrastructure with 24x7 operations.
4.3.4. **Templates**

Bringing engineering efficiency in configuration and significant reductions in system configuration maintenance, ClearSCADA object templates encourage and simplify the deployment of standardization.

Objects are managed in configuration groups, for example by equipment or site type. These groups form templates representing the standard configuration for a piece of equipment. Templates can themselves be part of other templates in a standard configuration for a site. Each set of configuration representing field equipment or a remote site is created as an instance of a standard template. Instances can be created from the same template for as many sites as needed, each instance representing a separate remote site. Naturally, to account for specific configuration variations between sites, instances can be individually varied as needed.

Templates can contain points, mimics, trends, logic, reports, alarm strategies, communication definitions to remote sites and more. When a new site is added to the system, the template is simply instanced as all associated configuration is automatically created.

The common configuration between sites is centrally managed from the template. Management of remote asset configuration and operation is significantly simplified. Configuration can be expanded, alarm strategy modified, all from a template from which the configuration change automatically flows to each instance.

When including SCADAPack E RTU configuration in a template, for example, the creation of an instance for a new site automatically creates the RTU configuration. If the site will use a standard IEC 61131-3 application with the RTU, the IEC 61131-3 application is also created. These configurations and applications can be automatically downloaded to the RTU across the remote communication network.

4.3.5. **Security model**

The ClearSCADA security model is uncompromising but easy to set up and manage. Fully integrated with the database object model, instances and templates, it provides security granularity at the point, object, device, site and system levels, with functional restrictions per user or user group. Security applies to ViewX, WebX and open interface connections.

Secure connection through an extensive set of open interfaces provides operational information for critical infrastructure to the enterprise. Integrated reporting provides printed, emailed and data-
push options for SCADA data into the enterprise. Additionally, open interfaces provide real-time and historical data access to enterprise applications, including smart applications pushing data and configuration into ClearSCADA and beyond, into the telemetry and remote SCADA system.

4.3.6. Server architecture

ClearSCADA server architecture provides an extensive redundancy model capable of operating on LAN and across WAN links, with remote server management.

It supports highly available architectures with dual network capability, main/standby, triple standby, performance server and DMZ server capabilities. Online database changes are propagated transparently across the system.

Main/standby/triple standby servers

Main/standby and triple standby server architectures increase system availability for a wide range of remote SCADA applications, including critical infrastructure management. ClearSCADA optimization for wide area links between servers provides customers with a choice of options for enterprise network integration, distributed equipment and distributed control centers consistent with business continuity strategies.

ClearSCADA redundancy architecture supports local redundancy and widely distributed redundant servers, for example as used in pipeline management and water infrastructure systems.

Main/standby and triple standby servers use online replication between ClearSCADA databases to ensure smooth system operation during a transition between a main server and standby server. Replication is optimized for use across Wide Area Network or LAN links. These ClearSCADA servers automatically arbitrate which server will be “Main” and, therefore, responsible for data collection (e.g. from RTUs, PLCs, and so on), for data processing, historical processing, logic control and report generation.

Figure 12: ClearSCADA main/standby servers
Each main/standby/triple standby server presents a mirror copy of the same configuration, real-time and historical data. Full display clients, web display clients and applications can connect to any of these servers. Full display clients can prioritize connection to servers (for best performance or lowest cost to access a link, for example) with automatic changeover to alternate servers should the preferred server become unavailable. Online configuration changes, additions to historical data and real-time data changes are transparently propagated between the servers. Configuration of standby servers is simple and secure. See example architectures in 6.2.2.

**Performance servers**

Performance servers are used in ClearSCADA architectures to enhance processing capacity for serving distributed users and distributed business applications. A performance server is an online replication of the ClearSCADA main/standby/triple standby servers. A performance server does not arbitrate to become a main server. However, it does mirror the main and standby ClearSCADA servers by replicating real-time data, configuration and historical updates. Replication is optimized for Wide Area Network and LAN links.

All the open standard interfaces presented for ClearSCADA data access are secured using the ClearSCADA security model. Applications, full display clients and web clients can connect to a performance server. Full display clients can prioritize connection to servers (for best performance or lowest cost to access a link) with automatic changeover to alternate servers.

Applications and display clients connecting to a performance server are authorized for system access and have full function capability, subject to security privileges.

Up to four performance servers can be added to a main/standby system (maximum three on a main/standby/triple standby system).
DMZ servers

DMZ (de-militarized zone) servers are similar to performance servers in ClearSCADA architectures, enhancing processing capability for serving distributed users and distributed business applications. DMZ servers deploy an additional security layer that allows READ-ONLY access to ClearSCADA data. The ClearSCADA security model continues to apply to protect system and data access; however, regardless of the security privileges allowed by an authorized user or application, the DMZ server will not allow data to be changed, nor configurations modified.

DMZ servers are often used in deploying remote SCADA data access throughout an organization for operational analysis, or where a ClearSCADA server is deployed in an IT DMZ network for broadly exposing data to wide area networks.

See example architectures in 6.1.3.

Figure 14: ClearSCADA DMZ server

To add a DMZ server to a ClearSCADA system, simply configure a performance server and select the DMZ option.

Further scaling up the ClearSCADA architecture

ClearSCADA system architecture can be further scaled up using multiple main/standby/performance / DMZ server sets. Each set manages an independent database;
however, display clients and applications can integrate data from multiple server sets. For example, ViewX combines alarm, mimic and trend displays for a seamless user view of large enterprise remote SCADA systems.

ClearSCADA’s Database Manager facility allows multiple ClearSCADA servers to reside on a single physical server. This suits architectures where multiple performance servers are centralized, leading to efficiencies such as less hardware, simpler system management and lower energy consumption in a central data center.

4.3.7. Connectivity

Open standard business application interfaces supported by ClearSCADA are described in 5.3. A key aspect of remote SCADA is its communication capability with RTUs. ClearSCADA provides industry leading remote communication functionality. The flexibility and comprehensive support provided by ClearSCADA are integrated with standard remote SCADA protocols:

- **DNP3**
  - DNP3 Master and DNP3 slave (conformance certified) drivers
  - Serial links for direct, radio, PSTN connection
  - DNP3/UDP and DNP3/TCP for IP networks (also known as DNP3/IP)
  - DNP3 subset Level 4 features
  - Additional features from the DNP3 standard including File Transfer, Virtual Terminal
  - DNP3 secure authentication
  - Dual network and redundant connection with shared or switched operation
  - SCADAPack E smart RTU integrated configuration management
- **IEC 60870-5**
  - Master and slave drivers
  - IEC 60870-5-101 serial for direct, radio connection
  - IEC 60870-5-104 for TCP/IP networks
  - File transfer
  - Dual network and redundant connection with shared or switched operation
  - KEMA certified protocol implementation
- **Modbus**
  - Master and slave drivers
4.3.8. **Historian**

Using a telemetry and remote SCADA system can present challenges for customers managing remote assets and integrating information they have collected from those assets with their enterprise IT system.

In a typical organization managing remote infrastructure:

- The amount of data stored in a SCADA system can be greater than in the IT system
- SCADA data arrives continuously and must be processed and stored immediately. In comparison, data from an organization’s IT system may arrive sporadically and may be processed and stored after some delay (e.g. from seconds up to hours)
- SCADA data is retrieved as large time-based data sets using simple queries. IT data is typically retrieved as smaller, relational data sets using complex queries and filters

ClearSCADA addresses these challenges by providing an integral historian suited to remote SCADA data, with powerful query optimization processing and standard database interfaces for use through the ClearSCADA display clients as well as for interacting with IT systems.

The ClearSCADA historian records data associated with historical trend data and log data.
Historical trend data

- Stored with value, units, quality, alarm status and timestamp information
- Automatically backfilled from telemetry protocols (DNP3, IEC 60870-5, and so on)
- Capable of being securely modified and annotated from users or external applications
- Pan and zoom trend graph regions, multi-axis, X-Y plots, display alarm limits

Log data

- Auditable actions from interactive user, system and external application causes
- Alarm transactions
- System communication transactions

Accessing historical and log data

From ClearSCADA display clients, users can access alarm lists, event logs, historical lists and configuration data lists through pre-defined queries. These are available as simple select and click actions available at point, device and site levels on the navigation browser, or from mimic displays. More complex queries can be built through data access wizards that are easy to use for extracting operational data. For database experts, an advanced mode shows the equivalent SQL query which can be edited to extended queries directly.

Figure 15: SCADA historical trending

Access to the same ClearSCADA historical data is available through the external data access interfaces. Optional data access clients can be purchased as needed to provide external data access to the ClearSCADA servers.
When accessing ClearSCADA historical data externally, standard open database interfaces for ClearSCADA include:

- SQL
- ODBC
- OLE/DB
- OPC-HDA
- OPC-AE

ClearSCADA provides a set of predefined data aggregates and data views as well as customizable data aggregates and data views that can provide significant efficiency gains through pre-processing when externally accessing historical data.

External applications can also perform complex queries across historical, real-time data and configuration data tables through the same ODBC/SQL and OLE/DB SQL connections.

With replication of historical databases included in the ClearSCADA multi-server architecture, any ClearSCADA server can be used to serve historical remote SCADA data through these interfaces. The ClearSCADA security model applies to historical access, ensuring applications and external data users only have access to the intended data for their application.

### 4.4. Trio data radios for wireless infrastructure

![Figure 16: Trio data radio equipment](image)

Trio data radios provide long range wireless communication solutions ideally suited to telemetry and remote SCADA. License-free and licensed data radio solutions are available for a wide range of applications, providing serial and Ethernet communication.
4.4.1. **License-free data radios**

Trio frequency-hopping, spread-spectrum data radios set the standard for reliable and secure Ethernet and serial data communication in the license-free 900MHz and 2.4GHz ISM bands.

With unique features like LinkXtend™ for single radio store-and-forward, and ChannelShare™ collision-avoidance for support of spontaneous SCADA messages, Trio license-free radios provide the flexibility to allow implementation of even the most complex wireless solutions with virtually unlimited expansion capability. The Trio K-Series is ideally suited for serial-only applications, while the Trio J-Series provides both serial and Ethernet connectivity.

Important features of the Trio license-free range include:

- **KwikStream™** high-speed single radio repeater mode
- **Dual antenna LinkXtend™** technology increases usable range
- **ChannelShare™** collision avoidance for unsolicited remote transmissions, allowing simultaneous polling and spontaneous reporting
- **SmartPath™** technology for enhanced mesh-like redundancy in network configuration
- **1 Watt (+30dBm) maximum allowable transmitter power** (500mW with 2.4GHz version)

Features specific to the J-Series Ethernet and serial data radio include:

- 900MHz version: 512kbps high speed over-air data rate or 256k, 128k or 64k for longer range. 2.4GHz version: 256k/128k/64k
- Dual independent Ethernet ports (Auto MDI/MIDX)
- Optimized Ethernet connectivity with smart peer-to-peer repeating, broadcast filtering and data compression
- Legacy RS-232 serial support via embedded terminal servers (UDP/TCP) and MODBUS/TCP gateway
- SNMP V1/V2c access to radio diagnostics, including trap generation for radio alarms

Features specific to the K-Series Ethernet and serial data radio include:

- 256kbps high speed over-air data rate (can be reduced to 128k, 64k or 32k for longer range)
- Advanced error-free data delivery with CRC plus selectable FEC and ARQ
- MultiStream™ simultaneous data stream delivery allows for multiple vendor devices/protocols to be transported on the one radio network - compatible with Trio E-Series and M-Series
- Small form factor DIN rail mounting options
- Available as an embedded option in SCADAPack and SCADAPack E RTU models
4.4.2. Licensed data radios

Trio licensed radios provide both Ethernet and serial communications for the most complex and demanding applications in point-to-point and point-to-multipoint (Multiple Address Radio) telemetry and remote SCADA systems using the licensed 450MHz band.

Available in Ethernet and serial (ER45e) and serial-only (ER450 and MR450) versions, the Trio licensed radios offer unique features to efficiently transport telemetry and SCADA data over long distances. Base/repeater stations are also available and offer high duty cycle capable of coping with operational stresses at critical sites.

Important features of the Trio licensed range include:

- 380 – 518MHz (various sub-frequency bands available)
- True 19,200 bps over-air data rates in 12.5kHz FCC channels (also 9600 bps)
- 128-bit AES encryption (export restrictions may apply)
- 12.5 or 25kHz channel operation
- Compatible with most industry-standard data protocols, e.g. DNP3, IEC 60870-5, Modbus, SEL protection relay mirrored bits, and so on
- Multistream™ simultaneous data streams allow for multiple vendor devices/protocols to be transported on the one radio network
- Internal repeater operation – single radio store and forward
- Channelshare™ unique integrated C/DSMA collision avoidance technology permits simultaneous polling and spontaneous alarm reporting operation in the same system
- Remote, fully transparent network management and diagnostics
- Legacy RS-232 serial support via embedded terminal server (UDP/TCP)
- Separate online system port avoids the need to interrupt user data for configuration access
- Maximum narrowband channel utilization with smart peer-to-peer repeating, broadcast filtering and data compression
- Advanced commissioning tools and remote diagnostics including SNMP
4.4.3. Configuration and diagnostics

Trio radio configuration and diagnostics are provided by the TView+ package. Trio radios are configured through connection of TView+ running on a PC or laptop onto the system port on a remote radio or radio base.

Additionally, the J-Series radios can be configured through a web browser interface to the onboard web server using Ethernet.

Diagnostic information provided by all Trio radios includes:
- Radio alarm status
- Transmit power
- Receive signal strength
- Frequency deviation
- Reflected power (VSWR)
- Temperature
- Power supply voltage

Trio radio diagnostics are available using the TView+ package through a number of interfaces:
- Locally to a remote radio or radio base through connection to the system port
- Remotely across a radio network to remote radios and radio bases

Additional diagnostics are provided by Trio base radios to assist in managing the remote communication networks.

SNMP Trio diagnostics

Radio diagnostics information is also available through the open SNMP protocol over IP networks for the J-Series and Ethernet E-Series radios. SNMP V1 and V2c are supported. SNMP provides the ability to integrate status, alarm and configuration capability with IT Network Management System (NMS) infrastructure.

Real-time radio diagnostics information is also available via SNMP notifications. This eliminates the need for polled base radio alarm status monitoring to maximize the available channel bandwidth for critical SCADA applications.

User configurable flexibility is provided for all key radio parameters including temperature, supply voltage, received signal strength (RSSI), transmit power, VSWR and error states, as well as customized alarm limits to ensure that important alarms are generated and sent to the user’s SNMP agent.
ClearSCADA Trio diagnostics

ClearSCADA integrates Trio diagnostics into a remote SCADA environment using one of two methods:

- **ClearSCADA Trio Diagnostic driver**
  
  Using the native ClearSCADA Trio Diagnostic driver, ClearSCADA connects to the Trio radio diagnostics interface using either a serial interface or encapsulating the serial traffic within a UDP datagram for transmission via an Ethernet interface. From this connection it can obtain diagnostics for all interconnected Trio radios in a remote communication network.

- **SNMP**
  
  By using the SNMP client objects in ClearSCADA, Trio diagnostics can be collected via SNMP (for the Trio J-Series and Ethernet E-Series radios)

Diagnostic information collected by ClearSCADA, using either of these methods, is available for utilization with full ClearSCADA functionality, including historical recording, alarming and escalation, event logging, display to an operator, access by external applications for analysis, and so on.

4.5. RTU solutions

SCADAPack smart RTUs (also known as standard SCADAPack), SCADAPack E smart RTUs and M340 PAC with an additional RTU module provide a comprehensive RTU feature set for field installations requiring local control logic, connection with I/O and intelligent field equipment, telemetry communication via remote communication networks and standard protocol support for operation with a wide range of remote SCADA systems.

Important features of the standard SCADAPack RTU range for solutions include:

- Power management modes well suited to low power applications
- Choice of basic ladder logic (Telepace) applications or IEC 61131-3
- C/C++ applications, allowing complex algorithm development by sophisticated users
- Specifications well suited to harsh environments

Important features of the SCADAPack E RTU range for solutions include:

- Native data processing providing in-built functionality without user logic programming
- Remote configuration management allowing manual and automatic configuration and logic management using ClearSCADA; including efficient remote firmware updating
- Native IEC 61131-3 logic with comprehensive system services for control, communication applications and interacting with the SCADAPack E RTU database
• Comprehensive diagnostics available locally to the RTU and remotely across telemetry links
• Enhanced security using open DNP3 Secure Authentication
• Specifications well suited to harsh environments

The M340 PAC with its additional RTU module provides an interface between a control application and a telemetry system using DNP3 or IEC 60870-5. It is suited to a complex control logic application where derived data is to be presented to a remote telemetry system.

4.5.1. Applications for RTUs

The choice of compact or modular RTU is typically made based on complexity and size of individual remote site applications, but may also be influenced by factors such as low power requirements, environmental conditions and remote configuration management requirements.

The choice of standard SCADAPack and SCADAPack E is typically made based on application sector (Oil & Gas or Water & Wastewater) or telemetry protocol (Modbus, DNP3, IEC 60870-5).

The choice of RTU device model is typically made based on the complexity and size of individual remote site applications.

For example, for gas flow with full operational audit traceability with one or two flow runs using Modbus protocol, a SCADAPack 300 fitting the required I/O mix is ideal. For an application with eight or 10 flow runs, a SCADAPack 32 RTU may be chosen.

**Note:** The M340 PAC gas flow calculation library does not provide the traceability facilities normally required for electronic flow measurement applications. For a gas pipeline application requiring a control solution for a compressor station with a requirement for remote communication using DNP3, for example, an M340 PAC with an additional RTU module could be chosen, providing control and an interface to a telemetry system.
A water application with a small to medium I/O count for a small pumping application would result in the choice of a SCADAPack 300E. A more complex application (larger pumping station, combination pumping / dosing system, or site with multiple instrument connections or communication links) may result in the selection of a SCADAPack ES. A treatment plant with complex drive control and requiring a large number of fieldbus I/O may use an M340 PAC with an additional RTU module as the interface to bring data into the telemetry system.

The Schneider Electric Modicon M340 PAC is a versatile device suitable for a number of higher complexity control applications. Its additional RTU module provides an interface to a telemetry system using open protocols. As a general purpose control device it may not be optimized for all applications. The high level of built-in remote SCADA functionality and configuration management of SCADAPack E RTUs makes them ideal for a wide range of Water & Wastewater applications. The low power and rugged environmental specifications of standard SCADAPack RTUs make them ideal for a wide range of Oil & Gas applications. The M340 PAC specifications, as shown by the yellow arrows in Figure 17, indicate that it may not be suited to applications with severe environmental constraints, such as those with very low temperature and very low power consumption requirements.

**Figure 17: Choosing an RTU based on application**
4.5.2. Remote communication

Remote SCADA platforms such as ClearSCADA provide SCADA server and operator stations for remote asset visualization (monitoring, alarm reporting), alarm signaling (with on call personnel), and central databases (alarm or data archiving, reporting, enterprise interface) for the purpose of aggregating remote asset data. The ClearSCADA server also provides facilities in a key role as telemetry master station, providing remote SCADA communication to RTU devices across remote communication networks.

It is the role of the RTU to collect the data from field instruments and devices and report that information to the telemetry master station. SCADAPack RTUs, SCADAPack E RTUs and M340 PAC with an additional RTU module provide open telemetry protocols for the remote communication between the master station and the RTU.

Standard SCADAPack RTUs provide access to open protocols (Modbus with extensions, DNP3) across a variety of communication media:

- Serial links (RS232 to a modem or other device for remote communication)
- Trio data radio via serial or Ethernet
- Other wire-line or wireless solutions such as leased line and audio radio
- PSTN and cellular (GSM) dial-up with external modem
- DSL services with external modem/router
- Other IP infrastructure

SCADAPack E RTUs provide access to open telemetry protocols (DNP3, IEC 60870-5) across a variety of communication media:

- Serial links (RS232 to a modem or other device for remote communication)
- Trio data radio via serial or Ethernet
- Other wire-line or wireless solutions such as leased line and audio radio
- PSTN and cellular (GSM) dial-up with external modem
- Cellular IP (GPRS, 1xRTT, EDGE, HSDPA, and so on) with external modem
- DSL services with external modem/router
- Other IP infrastructure

A solution using the M340 PAC with its additional RTU module provides an interface for open telemetry protocols (DNP3, IEC 60870-5) using:

- Serial links (RS232)
- Trio data radio via serial or Ethernet
- Cellular IP (GPRS, 1xRTT, EDGE, HSDPA, and so on) with external modem
- DSL services with external modem
- Other IP infrastructure

Where supported by the communication protocol and specific device, SCADAPack, SCADAPack E and M340 solutions can variously provide flexible communication such as:

- Interchanging data with other remote sites (peer-to-peer coordination for site-to-site control synchronization)
- Data concentrating (a hierarchy of collecting and serving data, mapping data including events)
- Remote diagnostics, control logic debugging, software upgrades, configuration management from an engineering terminal

The following table shows the remote communication capabilities of standard SCADAPack Smart RTU, SCADAPack E Smart RTU and M340 PAC with RTU module.

<table>
<thead>
<tr>
<th>RTU communication</th>
<th>SCADAPack</th>
<th>SCADAPack E</th>
<th>M340 PAC with RTU module</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serial ports support RS232</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Serial ports support RS485 for telemetry protocols</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Serial ports support radio keying</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Serial ports support multi-drop with collision avoidance</td>
<td>With external modem</td>
<td>✓ (DNP3)</td>
<td>✓</td>
</tr>
<tr>
<td>Multiple IP protocols on Ethernet port</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>DNP3 slave – serial</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>DNP3 slave – PSTN, GSM</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>DNP3/IP slave (DNP3/UDP and /TCP)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>DNP3 slave connection to multiple masters</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>DNP3 Secure Authentication</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Encryption of DNP3 protocol (AGA12*)</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>*subject to export restrictions</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNP3 – peer-to-peer (site-to-site)</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>DNP3 file transfer</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>DNP3 serial data concentrating (sub-master)</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>DNP3/IP data concentrating (sub-master)</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>DNP3 message routing</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>IEC 60870-5-101 slave (serial)</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
### 4.5.3. Site data acquisition, processing and storage

The following table shows the various mechanisms available to the SCADAPack RTU, SCADAPack E RTU and M340 PAC with additional RTU module, for acquiring and processing data at a remote site.

The available communication options on Schneider Electric RTUs allow for interconnectivity with a wide range of fields devices including Schneider Electric Accutech wireless instrument systems, I/O systems, Altivar variable speed drives, Ion power meters, and so on. Also see 6.5.2.

The table also shows available data processing, logging and storage mechanisms, ability to interact with local HMI, time-synchronization and diagnostic capability.

<table>
<thead>
<tr>
<th>RTU communication</th>
<th>SCADAPack</th>
<th>SCADAPack E</th>
<th>M340 PAC with RTU module</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEC 60870-5-104 server (IP)</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>IEC 60870-5 connection to multiple masters</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>IEC 60870-5-101 (serial) data concentrating (sub-master)</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>IEC 60870-5-104 sub-master client (IP)</td>
<td></td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>IP protocols over Cellular IP</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>GPRS Dynamic IP</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP protocols over CDMA 1xRTT (serial PPP)</td>
<td></td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>IP routing (basic)</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modbus RTU – serial (RS232, RS485), master and slave</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Modbus proprietary extensions for telemetry</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modbus store-and-forward</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modbus – PSTN, GSM</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modbus/TCP – client and server</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Modbus RTU in TCP – master</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modbus RTU in TCP – slave</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modbus ASCII – master and slave</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modbus/UDP – client and server</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modbus RTU in UDP – master and slave</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gas Modbus (Enron)</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 2: RTU remote communication capability
<table>
<thead>
<tr>
<th>RTU feature</th>
<th>SCADAPack</th>
<th>SCADAPack E</th>
<th>M340 PAC with RTU module</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data acquisition from I/O and processing by logic application</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Data processing features without need for user logic programming</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Event management, alarming, time-stamping</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Data acquisition from Modbus and Modbus/TCP devices</td>
<td>✓</td>
<td>✓</td>
<td>(on PLC CPU or comm. module port)</td>
</tr>
<tr>
<td>Data acquisition from Fieldbus devices</td>
<td></td>
<td></td>
<td>✓ (on PLC CPU port or Fieldbus module)</td>
</tr>
<tr>
<td>Data acquisition from DNP3 devices (as a sub-master)</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Data acquisition from IEC 60870-5 devices (as a sub-master)</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Data acquisition from devices with custom communication</td>
<td>✓ (user C/C++ coding required)</td>
<td>✓ (user IEC 61131-3 coding required)</td>
<td></td>
</tr>
<tr>
<td>Visualization of RTU data to local HMI</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Notification via SMS</td>
<td>✓ (user C/C++ coding required)</td>
<td>✓ (user IEC 61131-3 coding required)</td>
<td>✓</td>
</tr>
<tr>
<td>Notification via SMTP (email)</td>
<td>✓ (user C/C++ coding required)</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Timed data logging with Modbus transfer</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Timed data logging with DNP3 transfer</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Data logging to internal file system</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Data logging to external file media</td>
<td>✓ (SP300) USB</td>
<td>✓ (SP ES) CompactFlash (user IEC 61131-3 coding required)</td>
<td>(Configuration by Web Designer)</td>
</tr>
<tr>
<td>FTP access to files</td>
<td>✓ (SP 300)</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Time synchronization from telemetry protocol</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Time synchronization from serial port GPS</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Time synchronization from NTP</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>SNMP diagnostic information</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>
### 4 – System presentation

<table>
<thead>
<tr>
<th>RTU feature</th>
<th>SCADAPack</th>
<th>SCADAPack E</th>
<th>M340 PAC with RTU module</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local diagnostic stream and diagnostic files</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Remote diagnostic stream and diagnostics files</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Remote firmware upgrade management</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

*Table 3: RTU data handling features*

#### 4.5.4. Site control logic

Standard SCADAPack RTUs support integrated basic ladder logic (Telepace) or IEC 61131-3 control languages. Either logic environment can be supplemented by C/C++ applications for data processing and local control of site process equipment. Ladder logic, IEC 61131-3 logic and C applications can be managed remotely across remote telemetry links.

SCADAPack E RTUs support integrated IEC 61131-3 ladder logic with an extensive set of RTU services available to the IEC 61131-3 languages. IEC 61131-3 logic applications can be downloaded across remote telemetry links, including through ClearSCADA centralized configuration management capability. IEC 61131-3 logic applications can also be debugged remotely across the telemetry protocol links.

The M340 PAC supports features provided by the Unity platform, including IEC 61131-3 and LL984 basic ladder logic, with specialist function block development using C programming.

<table>
<thead>
<tr>
<th>RTU Logic Capability</th>
<th>SCADAPack</th>
<th>SCADAPack E</th>
<th>M340 PAC with RTU module</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data acquisition from I/O and processing by logic application</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Basic ladder logic environment (Telepace)</td>
<td>✓</td>
<td></td>
<td>(Unity LL984)</td>
</tr>
<tr>
<td>IEC 61131-3 logic environment</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Offline logic editing and management</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Online logic editing and management</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>User Defined Function Blocks</td>
<td>Limited</td>
<td>✓</td>
<td>(using IEC61131-3 languages)</td>
</tr>
<tr>
<td>C/C++ language development (C/C++ applications)</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote logic download across Modbus telemetry link</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
4.5.5. Remote and centralized configuration management

Remote configuration management is the ability to view, modify, upload and download RTU configuration and control logic remotely from the RTU, across a telemetry protocol.

Centralized configuration management is the ability to modify and download RTU configuration, and download control logic for multiple RTUs from the master station. ClearSCADA provides integrated configuration management services for SCADAPack RTUs. In particular:

- SCADAPack E remote management of the full RTU configuration between the ClearSCADA server and remote RTUs, including loading IEC 61131-3 application programs, synchronizing point configurations, coordinating firmware upgrades and so on
- Realflo configuration management for downloading configuration parameters for SCADAPack gas flow computer settings

<table>
<thead>
<tr>
<th>RTU Logic Capability</th>
<th>SCADAPack</th>
<th>SCADAPack E</th>
<th>M340 PAC with RTU module</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote logic download across DNP3 telemetry link</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Remote logic download across IEC 60870-5 telemetry link</td>
<td></td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Centralized configuration management for logic from ClearSCADA</td>
<td></td>
<td>✔</td>
<td></td>
</tr>
</tbody>
</table>

Table 4: RTU logic features

<table>
<thead>
<tr>
<th>RTU configuration management</th>
<th>SCADAPack</th>
<th>SCADAPack E</th>
<th>M340 PAC with RTU module</th>
</tr>
</thead>
<tbody>
<tr>
<td>Offline RTU configuration management</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Online RTU configuration management</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Configuration and logic download and debugging across a remote Modbus telemetry link</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configuration and logic download across remote DNP3 telemetry link</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Logic debugging across remote DNP3 telemetry link</td>
<td></td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Configuration and logic download across IEC 60870-5 telemetry link</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firmware upgrade across remote DNP3 telemetry link</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firmware upgrade across remote IEC 60870-5 link</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
4.6. **Standard SCADAPack RTU**

The standard SCADAPack smart RTU range caters for generic telemetry applications and specializes in features to meet Oil & Gas sector requirements, including Schneider Electric's ProductionPlus solution.

![Oil & Gas](../images/oil_gas.png)

Standard SCADAPack RTU models include:

- SCADAPack 100 RTU (SP100)
- SCADAPack 300 RTU range (SP300)
- SCADAPack 4102 transmitter
- SCADAPack 4203 flow computer
- SCADAPack 32 RTU range (SP32)

---

Table 5: RTU configuration management capability

<table>
<thead>
<tr>
<th>RTU configuration management</th>
<th>SCADAPack</th>
<th>SCADAPack E</th>
<th>M340 PAC with RTU module</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firmware upgrade preserves configuration</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Centralized RTU configuration, logic and firmware management from ClearSCADA</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Centralized application management from ClearSCADA (Realflo)</td>
<td>✓</td>
<td>✓</td>
<td>(Customized via file management)</td>
</tr>
</tbody>
</table>

© 2012 Schneider Electric All Rights Reserved
4.6.1. Standard SCADAPack features

The standard SCADAPack RTU family features simplicity of use and optimized features:

- Simple ladder logic development environment (Telepace)
- IEC 61131-3 development environment
- Strong Modbus communication capability
- Internal file system (SCADAPack 300 range)
- External file system via USB host memory stick (SCADAPack 330,334,350,357)
- File management via Modbus and FTP
- DNP3 protocol support (Level 2 Subset)
- Local configuration connection using USB device port
- Remote configuration loading via Modbus or DNP3
- C/C++ application development
- Optional Gas flow computer application (Realflo)

Figure 18: Standard SCADAPack 334 RTU
4.6.2. Standard SCADAPack tools

Telepace Studio

To configure a SCADAPack RTU and program user logic using simple ladder logic, install and use the SCADAPack Telepace Studio tool set for local and remote operation to:

- Build RTU configurations offline
- Modify RTU configurations online
- Write configurations to an RTU
- Read configurations from an RTU
- Write a ladder logic program
- Transfer a ladder logic applications to an RTU
- Configure port settings
- Configure telemetry protocol settings
- View online RTU data
- Browse RTU file system, transfer log files
- Upgrade system firmware

IEC 61131-3 Logic

To configure a SCADAPack RTU and program its user logic using IEC 61131-3 languages, install and use the SCADAPack IEC 61131-3 Workbench tool set (requires purchase of an activation license).

Use the IEC 61131-3 logic tool set to:

- Write programs in a mixture of up to four different IEC 61131-3 languages (ladder diagram, function block diagram, structured text, sequential function chart)
- Interact with RTU system services through I/O boards, variables and function blocks
- Compile, download, debug logic IEC 61131-3 applications
- Visualize RTU and logic application data through tabular or graphical displays
Realflo

Realflo is an application that enables custody transfer gas flow measurement of up to 10 flow runs in SCADAPack controllers. The application provides Electronic Flow Measurement (EFM) functionality independent of, yet concurrent with, SCADAPack Telepace Studio Ladder Logic or IEC 61131-3 logic; and C/C++ user application programmability.

Realflo supports concurrent AGA-3 (orifice plate), V-Cone, Wafer Cone, AGA-7 (turbine meter) flow measurements with AGA-8 or NX-19 gas density calculations.

Meeting the requirements of API 21.1 audit traceability, Realflo provides 35 days of hourly and daily averages, 700 user changes and events, as well as 300 alarms.

The software's user interface offers efficient production gas well deployment utilizing wizards and templates minimizing entry tasks required by operators and measurement technicians. The user also has the ability to export EFM data with customizable file naming conventions to ease file organization, and tamper proof file signatures for better data integrity.

Realflo also offers functionality to support gas transmission (pipeline) system measurement. The functionality provided by Realflo meets the operational needs of the Oil & Gas industry, including audit trails, hourly and daily history and features, exceeding the capabilities of flow calculation libraries provided on other PLC devices.

C/C++ tools

To develop applications for the standard SCADAPack RTU using C or C++ languages, install and use the SCADAPack C/C++ tool set (requires purchase of the SCADAPack C/C++ tool set for the appropriate SCADAPack controller model). User developed applications can be used in conjunction with ladder logic (from Telepace Studio), IEC 61131-3 logic (from SCADAPack IEC 61131-3 tools) and SCADAPack gas flow computer.

Other tools

Other freely available tools may be useful, in conjunction with standard SCADAPack tools, to assist installation, commissioning, operation and diagnosis activities:

- SCADAPack Firmware Loader for upgrading firmware
- FTP client software to browse the file system, transfer log files
- Ethernet packet analyzer software for communication diagnostics, traffic analysis
4.7. SCADAPack E smart RTU

The SCADAPack E smart RTU range caters for highly scalable telemetry applications with advanced remote management, supports integrated configuration with ClearSCADA, and specializes in advanced features to meet a wide range of industry requirements.

The SCADAPack E smart RTU range provides comprehensive services for generic telemetry applications with open protocols and features to meet Water & Wastewater sector requirements, including irrigation, flood and environmental monitoring, integrated with Schneider Electric's remote water solutions.

The SCADAPack E smart RTU can be used in Renewable Energy applications and in solutions for other complementary sectors such as Hydro Power and some Power Distribution applications.

SCADAPack E provides the following families of RTU models:

- SCADAPack 300E range (SP300E)
- SCADAPack ES range (SP ES)
4.7.1. **SCADAPack E features**

Key features of the SCADAPack E controllers include:

- Full featured RTU for simple to demanding applications
- RTU data processing built in without requiring user logic
  - Point database
  - Raw integer values and scaled engineering values
  - Alarm limits, over/under-range alarms, rate-of-change and no-change alarms
  - Alarm time and value dead bands
  - Individual point protocol settings (data type, unsolicited operation)
  - Description field, user managed or automatically linked to ClearSCADA point name
- IEC 61131-3 development environment
  - Online editing
  - Remote debugging
  - Access to RTU system functions from logic applications
  - Dual logic applications for precise timing algorithms or separation of logic responsibility
- Extensive DNP3 communication capability (Level 4 Subset +)
  - DNP3 Conformance Certified
- DNP3 Secure Authentication (option)
- Peer-to-peer communication
- Message routing
- Data concentrator (option)
- File transfer
- AGA12 encryption security (option)
- IEC 60870-5-101 and IEC 60870-5-104 communication support
  - KEMA certified protocol operation
  - File transfer capability
- GSM, GPRS and other cellular IP connections supported
- Dual Ethernet ports (SCADAPack ES)
- Internal file system
- External file system via Compact Flash (SCADAPack ES)
- File management via DNP3, IEC 60870-5 and FTP
- Local configuration connection using USB (device)
- Time synchronization from telemetry protocols, NTP and GPS serial
- Extensive diagnostic features, available locally and remotely
- Locally and remotely managed configuration, firmware upgrades
- Centralized configuration management using ClearSCADA

4.7.2. SCADAPack E tools

**SCADAPack E Configurator**

To configure, maintain and diagnose the SCADAPack E RTU, install and use the SCADAPack E Configurator tool set. Use the SCADAPack E Configurator for local and remote operation to:

- Build RTU configurations offline
- Modify RTU configurations online
- Write configurations to an RTU
- Read configurations from an RTU
- Transfer one or two independent IEC 61131-3 applications (resources) to an RTU
Configure port settings
Configure telemetry protocol settings
Configure point characteristics and point processing parameters
View online RTU data
Interact with the RTU command line remotely
Upgrade system firmware
Upgrade RTU licensed features
Transfer trend (data log) files from the RTU

Figure 20: SCADAPack E Configurator

The SCADAPack E tool set also includes a firmware Difference Generator application to produce firmware patch files for efficient transfer and remote upgrade of system firmware.

IEC 61131-3 logic

The programming of control logic for the SCADAPack E RTU is performed using IEC 61131-3 languages with the SCADAPack E Utilities tool set. (SCADAPack IEC 61131-3 Workbench environment requires purchase of an activation license).
Use the SCADAPack Workbench logic tool set to:

- Program one or two independent applications (resources) for SCADAPack E RTUs
- Write programs in a mixture of up to four different IEC 61131-3 languages (ladder diagram, function block diagram, structured text, sequential function chart)
- Interact with RTU system services through I/O boards and function blocks
- Compile, download, debug IEC 61131-3 logic applications
- Visualize RTU and logic application data through tabular or graphical display windows

![Figure 21: SCADAPack Workbench for IEC 61131-3 programming](image)

**Security administrator**

To manage security configurations for DNP3 Secure Authentication and AGA12 Encryption options on SCADAPack E controllers, use the Security Administrator tool (activation license option required).
Other tools

Other freely available tools may be useful, in conjunction with SCADAPack E tools, to assist installation, commissioning, operation and diagnosis activities:

- FTP client software to transfer files to and from the RTU: firmware, diagnostic logs, trend (data log) files, configuration, logic applications
- Telnet client software for Ethernet or remote IP access to: the RTU’s command line for file management, diagnostic status; the RTU’s diagnostics stream for protocol analysis, operational messages
- Terminal emulator software (may be available with integrated Telnet client) for local serial port access to: the RTU’s command line for file management, diagnostic status; the RTU’s diagnostics stream for protocol analysis, operational messages
- Ethernet packet analyzer software for communication diagnostics, traffic analysis
4.8. **M340 PAC with RTU module**

The Modicon M340 Process Automation Controller’s NOR0200H RTU module allows data from a complex control application to be integrated into a telemetry and remote SCADA system.

The NOR0200H RTU module provides a range of communication services, including open protocols, for operating in a telemetry and remote SCADA environment. It is suitable for use in applications where the control complexity requires the power of the M340 PAC including water & wastewater, renewable energy, gas transportation, and so on.

4.8.1. **NOR0200H RTU module features**

Key features of the NOR0200H RTU module include:

- DNP3 (subset Level 3), IEC 60870-5
- Time synchronization via telemetry protocols and NTP
- Ethernet port supporting:
  - DNP3/IP over TCP and UDP slave operation
  - Or, IEC60870-5-104 slave operation
  - DNP3/IP over TCP and UDP master operation from IEC 61131-3 logic
  - Or, IEC 60870-5-104 master operation from IEC 61131-3 logic
  - Modbus/TCP communication to the M340 PAC processor
  - Web server for configuration and diagnostics
  - SMTP email notification
  - SNMP agent for monitoring module status
  - FTP file transfer for data logs
  - SOAP / XML with Modbus XMLDA and Symbolic XMLDA services
  - PPPoE for DSL (using external modem)
- Serial port supporting:
  - RS232 or RS485 communication
  - DNP3 slave protocol
4 – System presentation

- Or IEC 60870-5-101 slave protocol
- Modem operation from IEC 61131-3 logic
- External GPRS / PPP modem
- DNP3 master protocol (RTU module as a DNP3/IP slave)
- Or IEC 60870-5-101 master protocol (RTU module as IEC 60870-5-104 slave)
- SMS notification (using external modem)
- Telemetry protocol access to M340 PAC variables
- Communication status available in M340 PAC variables
- Up to 100,000 events buffered, up to 10,000 events retained over power failure
- Local firmware upgrade capability
- SMS / email service for alarm notification, maintenance reminders, production reports, equipment status updates, other process information derived from the M340 PAC processor
- Data logging to CSV files

4.8.2. Tools for M340 PAC with RTU module

Web browser

Use a web browser through the Ethernet port of the NOR0200H RTU module to:

- Logon with a username / password for accessing the module
- Diagnose RTU protocol session status
- Configure the RTU module communication port settings
- Configure communication sessions to a remote SCADA master
- Configure sub-master communication sessions to downstream devices
- Configure the telemetry protocol mappings to M340 PAC variables
- Monitor and edit M340 PAC variable data
The programming of control logic and configuration for the M340 PAC is managed by Unity Pro. Connection to the M340 for Unity Pro can be via the processor USB port, a processor Ethernet port, an Ethernet module port or via the RTU module Ethernet port.

Use the Unity Pro tool set to:

- Program, compile, download and debug the control application for the M340 PAC
- Configure the M340 module bus for the NOR0200H RTU module
- Manage field bus devices associated with the control application
- Program logic to control RTU module sub-master communications
- Visualize application data through tabular or graphical display windows
Figure 24: Unity Pro for M340 PAC programming and configuration

Web Designer software

Use the Web Designer software tool supplied with the NOR0200H to:

- Configure the SMS notification service
- Configure the email notification service
- Configure the data logging service
Other tools

Other freely available tools may be useful, in conjunction with the M340 and RTU module tools, to assist installation, commissioning, operation and diagnosis activities:

- Schneider Electric OS Loader for upgrading firmware
- Ethernet packet analyzer software for communication diagnostics, traffic analysis

4.9. Accutech wireless instrumentation

The self-powered wireless Accutech range allows for rapid deployment of instrumentation solutions for remote sites.
With a wide range of available instruments for temperature, pressure, flow, level, valve control and more, Accutech is ideally suited to many industrial applications including upstream oil & gas, and applications in water & wastewater that are “outside the process.”

Distance, hazardous environments and absence of power are some of the hurdles faced when process variables are difficult to reach and expensive to support. With operational efficiency as the primary goal, the deployment of self-powered wireless instrumentation provides process knowledge in a cost effective manner.

Supporting a range up to 1500m (5000 ft) from an Accutech base station, the Accutech wireless sensors are easily configured in a highly scalable deployment. Up to 10 years operation on a single battery eases maintenance. Each Accutech base radio can support up to 100 field instruments with up to 1 second sampling. Up to 256 base radios are supported.

Over the air configuration and firmware upgrade are available from the Accutech Manager software configuration tool.

Integrate the Accutech remote instrumentation network with an RTU, PLC, DCS or SCADA master through Modbus communication with the base radio, or through analog and switch output modules.

The BR20 base radio option for integrated Trio K-Series backhaul radio allows an Accutech system to connect directly on a Trio K-Series wireless network without the need for additional communication equipment.

4.9.1. Accutech tools

Use Accutech Manager to configure, maintain and diagnose an Accutech wireless instrumentation system:

- Configure an Accutech wireless instrument system
- Manage an Accutech wireless instrument system
- Configure Accutech base radio
- Configure Accutech field unit
- Transfer Accutech configurations
- Upgrade Accutech firmware
4.9.2. Accutech system architecture

The sample Accutech system architecture shown depicts a typical gas production installation. The architecture includes a number of Accutech wireless instruments, a BR20 base station module and a SCADAPack 334 RTU interconnecting with a SCADAPack 4102 multi-variable transmitter (labeled as Wellhead Separator Outlet Gas Flow).

Figure 27: Accutech Manager

Figure 28: Accutech system architecture
5. System requirements

5.1. General system requirements

The following sections describe the subsystems that make up a remote SCADA solution. Details relevant to the architecture of the subsystems highlight the important considerations when designing, deploying and operating a telemetry and remote SCADA system.

5.2. System architecture

Typical system architectures comprise layers that are interconnected. Telemetry and remote SCADA architectures interconnect:

- A Business system interface architecture
- Control Room architecture
- Remote Communication Network architecture
- Remote Site architecture

Typical architectures for small, mid-size and large systems, composed of these layers, are shown in the following sections. Detailed architecture options for each layer are described throughout Chapter 6.

5.2.1. Typical small remote SCADA system

Small remote SCADA systems typically satisfy applications with small numbers of remote field assets (e.g. less than 50 remote sites). See Figure 29.

Examples of these typical systems can be found in many sectors including Oil & Gas production, municipal Water & Wastewater, Mining, Environmental Monitoring and so on.
5.2.2. Typical mid-sized telemetry and remote SCADA system

Mid-sized remote SCADA systems are typically found in larger municipal and regional based organizations and in systems with widely distributed assets. See Figure 30.

There may be a large number of remotely located field assets (e.g. up to several hundred) and more sophisticated communication infrastructure. Examples of these typical systems can be found in many sectors including Oil & Gas pipelines, Water & Wastewater, Flood Monitoring and Mitigation, Renewable Power Generation, Power Transmission, Power Distribution and so on.
Typical large telemetry and remote SCADA system

Large telemetry and remote SCADA systems are typically found in regional and state based organizations, in systems with large concentrations of assets or large numbers of widely distributed field assets (hundreds to thousands of sites). See Figure 31. A wide variety of communication infrastructure methods are typically deployed. Examples of these typical systems can be found in sectors such as Oil & Gas pipelines, Water & Wastewater, Renewable Energy, Power Transmission, Power Distribution, and so on.
Figure 31: Typical large remote SCADA system
5.3. **Business interface**

The telemetry and remote SCADA architecture includes interfaces that provide business information from the remote SCADA system.

For some applications, the remote SCADA system can provide business information and key performance indicators directly. Visibility to this type of business information can be made available directly from the remote SCADA. Alternatively, this data may be transferred to business software for external visualization.

For other applications, the remote SCADA system can provide processed information or raw data for external business software to collate, analyze and present. Open software interfaces are used for the transfer of data between remote SCADA and business applications. Examples of this can include alarms for work order management, performance data for asset management, real-time data for operational system modeling, historical data for long term planning and modeling, real-time and historical data for energy management.

5.3.1. **Remote SCADA connectivity with business systems**

Network connectivity between remote SCADA and business systems is consistent with, and integrates with, enterprise IT network connectivity. Open interfaces such as OPC, ODBC/SQL, OLE-DB, SOAP/XML web services, .NET, and so on, allow remote SCADA to interface with a wide variety of business systems.

Remote SCADA infrastructure leverages wide area enterprise IT networks for integration with business operations. Remote SCADA servers located in enterprise data centers, including geographically separated locations interconnected via WAN networks, ensure integration of remote SCADA operations with business continuity strategies. Full-time and part-time, local and after-hours remote access to telemetry and remote SCADA operations leverage enterprise network connectivity across wide area business communication links.

After-hours maintenance capability is provided through remote access for SCADA server configuration and diagnostics, remote communication network diagnostics and remote RTU diagnostics.

Security is an essential requirement for telemetry and remote SCADA. Security is built in to the Schneider Electric telemetry and remote SCADA solution at all levels, not added as an afterthought.
5.4. Control room subsystem

5.4.1. Operations center

Control room operations monitor and process information that is collected from remote assets. This function is often combined with other business operations. Operations related to remote assets can include production monitoring, analysis of asset status based on received alarms, and system control. It can also include use of performance information derived from remote sites, data processed by the remote SCADA master station, or information derived and collated by an enterprise application.

Alarm management is aided by ClearSCADA features such as severity prioritization, areas of interest to categories alarms for different operations groups, responsibility division, alarm escalation based on actions (or lack of actions), alarm distribution by the remote SCADA to SMS, paging and email interfaces.

System control carried out by the operations center uses alarm management, visualizing remote process operating parameters, historical trending and consolidated data reporting.

As a scalable platform for managing remote assets, the ClearSCADA ViewX display client plays an important role in all aspects of the control room described above. It is optimized for use as a single display terminal for a single operator, as well as providing a feature-rich environment as a multi-head control console in a multiple operator, multi-disciplined control center. Architectures for optimized, through to highly-available and enterprise-wide control center solutions, are described in 6.2.

5.4.2. Data center considerations

There are a number of architectures possible for managing the servers or other computers associated with a SCADA master station system. For a simple system this may just be the computers used in a control room. In many cases, the architecture will be more substantial and make use of enterprise computer networks and resources, separated from the control room display clients.

When locating SCADA master station servers, the ClearSCADA distributed server architecture should be taken into account. For example, ClearSCADA supports distributed main/standby servers that should be physically placed to best take advantage of location diversity as part of the enterprise business continuity strategy. Similarly, ClearSCADA performance servers distribute SCADA user load and should be located across an enterprise network for minimizing WAN bandwidth requirements while improving communication efficiency in serving clusters of users (or applications).

ClearSCADA server architectures are described in 6.2.
Main and standby ClearSCADA servers include the facilities for remote SCADA data collection from remote sites (across the remote communication networks). As such, they require connectivity with the remote communication network. When deploying main/standby SCADA servers in diverse locations for business continuity, the design must consider the access requirements to the remote communication networks from all the diverse locations that can become a “main” server (i.e. a standby or triple standby server). Linkage to the remote communication network from each SCADA server location should be independent of the linkage from other server locations to ensure a robust remote SCADA solution. This is described further in 6.4.

ClearSCADA servers are responsible for managing communication with remote sites. The communication drivers providing this functionality are active on the “Main” ClearSCADA server and communicate using telemetry protocols to remote devices such as RTUs. ClearSCADA “Standby” servers have inactive communication drivers that are ready to start, in the event of a transition of responsibility to “Main” status. Telemetry protocols are discussed in 5.5.

As part of an enterprise’s computing and operational infrastructure, it is recommended that the health of the SCADA servers be routinely monitored. Server class computers usually support an SNMP interface for system monitoring and control which can be coupled to a Network Monitoring System (NMS). ClearSCADA servers support the ability to use SNMP to monitor network and computer equipment in a similar way to an NMS. ClearSCADA also supports the ability to monitor servers through the operating system performance monitor. It can monitor a diverse range of statistics, including trending over time, to ensure system health and aid in the maintenance of the computing infrastructure. For example: CPU load, memory usage, disk capacity, network performance, hardware errors, operating system performance and so on.

5.5. Telemetry protocol

5.5.1. Role of the telemetry protocol

A telemetry protocol encodes communication messages generated from the SCADA server for delivery to the RTU (requests), and encodes data collected by an RTU for transmission to the SCADA server (responses). The encoding includes error checking to ensure robust delivery of the communication message data across a system. Some telemetry protocols encode simple data values only while others encode, and self-describe, rich data types. Some telemetry protocols include addressing information that allows messages to be directed between different pairs of devices, or routed in a hierarchical network.
5.5.2. Which protocol should I choose?

Telemetry and remote SCADA architecture can be impacted by the protocol used in a system. The protocol choice may be dictated by one or more of the following factors:

1. Region
2. Industry sector (e.g. WWW, O&G)
3. Customer preference
4. Country legislation (particularly in some parts of Western Europe for specific sectors)
5. Requirement for telemetry protocol security
6. Feature requirements
7. Compatibility with existing equipment

Many system deployments extend, or must coexist with, legacy systems. It is important to determine system constraints such as:

- Requirements to integrate with an existing system
- Transition strategy (e.g. piece-by-piece replacement while existing system is running)

Where there is a protocol choice in a system, the flexibility, feature set and RTU support for a protocol should be considered.
5.5.3. Telemetry protocol features

<table>
<thead>
<tr>
<th>Protocol features</th>
<th>DNP3</th>
<th>IEC60870-5</th>
<th>Modbus</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multi-layer protocol, optimized for remote communication</td>
<td>✔</td>
<td>✔</td>
<td>⬗</td>
</tr>
<tr>
<td>Independent protocol verification programs</td>
<td>✔</td>
<td>✔</td>
<td>⬗</td>
</tr>
<tr>
<td>Time synchronization &amp; time-stamped events</td>
<td>✔</td>
<td>✔</td>
<td>⬗</td>
</tr>
<tr>
<td>Data quality reporting</td>
<td>✔</td>
<td>✔</td>
<td>⬗</td>
</tr>
<tr>
<td>Multiple masters and peer-to-peer operation on same communication channel</td>
<td>✔</td>
<td>⬗</td>
<td>⬗</td>
</tr>
<tr>
<td>Segmentation of messages</td>
<td>✔</td>
<td>⬗</td>
<td>⬗</td>
</tr>
<tr>
<td>Secure Authentication</td>
<td>✔</td>
<td>�oliberal may not yet be commercially available</td>
<td>⬗</td>
</tr>
<tr>
<td>File transfer</td>
<td>✔</td>
<td>✔</td>
<td>⬗</td>
</tr>
<tr>
<td>Strongly typed, rich protocol data types</td>
<td>✔</td>
<td>⬗</td>
<td>⬗</td>
</tr>
<tr>
<td>User defined, self describing data objects</td>
<td>✔</td>
<td>⬗</td>
<td>⬗</td>
</tr>
<tr>
<td>Unsolicited operation: multi-drop and point-to-point</td>
<td>✔</td>
<td>⬗</td>
<td>⬗</td>
</tr>
<tr>
<td>Hierarchical network options: routing, peer-to-peer, store &amp; forward, data concentrating</td>
<td>✔</td>
<td>⬗</td>
<td>⬗</td>
</tr>
<tr>
<td>Data concentrating preserves</td>
<td>Value, Quality, Timestamp</td>
<td>Value, Quality, Timestamp</td>
<td>Value only</td>
</tr>
</tbody>
</table>

Table 6: Telemetry protocol comparison

*Protocol features indicated as “X” (not supported) may be available as private extensions to the protocol. This is popular among manufacturers using Modbus protocol, for example; the standard SCADAPack RTU range provides many features to enhance its capability for remote SCADA this way.

5.5.4. DNP3 (Distributed Network Protocol) standard

Also known as IEEE1815, DNP3 provides extensive services for remote telemetry communication.

DNP3 protocol provides telemetry services optimized for remote communication networks. The key values include the ability to multi-drop devices for efficient use of remote communication links, event handling to optimize volume and accuracy of data as shown in Figure 32, and the interoperability that standardization brings.
Figure 32: Backfilling historical data from DNP3

DNP3 is defined for operation over a wide range of communication media:

- Serial
  - RS232, RS485
  - Leased line modems
  - Serial data radios
- TCP/IP
  - DNP3 over UDP
  - DNP3 over TCP
  - Operation over Ethernet, Ethernet data radios, GPRS, DSL, IP Satellite links
- PSTN
  - Operation with modems over public telephone system
  - Operation with GSM cellular modems

Standard SCADAPack and SCADAPack E smart RTUs, and M340 PAC with additional RTU module support DNP3. Differences between the DNP3 features include:

- Standard SCADAPack supports DNP3 Level 2 subset features and additionally:
  - Support for communication with multiple masters (same data for each master)
- SCADAPack E supports DNP3 Level 4 subset features and additionally:
  - Support for communication with multiple masters (flexible data definition for each master)
  - DNP3 file transfer for configuration, retrieval of trend files, firmware upgrade
  - Compliance tested to latest DNP3 standards
5.5.5. **IEC 60870-5 protocols**

Similar to DNP3, IEC 60870-5 protocols provide telemetry services optimized for remote communication networks. The key values include the ability to multi-drop devices for efficient use of remote communication links, event handling to optimize volume and accuracy of data, and the interoperability that standardization brings.

The IEC 60870-5-101 and IEC 60870-5-104 protocol standards provide services for remote telemetry communication and are defined for operation over the following communication media:

- Serial (IEC 60870-5-101)
  - RS232, RS485
  - Leased line modems, serial data radios
- TCP/IP (IEC 60870-5-104)
  - IEC 60870-5-104 using TCP
  - Operation over Ethernet, Ethernet data radios, GPRS, DSL, IP satellite links

SCADAPack E smart RTU and M340 PAC with its additional RTU module supports IEC 60870-5-101 and IEC 60870-5-104 protocols. Differences between the IEC 60870-5 features include:

- SCADAPack E:
  - Support for communication with multiple masters (IEC 60870-5-101 and -104, same data for each master)
  - File transfer for configuration, firmware upgrade (preserves configuration)
  - Compliance tested to KEMA IEC 60870-5 standards
  - IEC 60870-5-101 communication on serial ports using RS232 or RS485
5.5.6. Modbus protocols

While not generally regarded as a telemetry protocol, variants of Modbus with proprietary extensions are used in telemetry applications, in particular in the Oil & Gas sector.

- Standard SCADAPack smart RTUs provide a full featured set of current and legacy Modbus protocol facilities and extensions for telemetry communication, as well as device communication including:
  - Master (Client) and slave (Server) communications for:
    - Modbus RTU
    - Modbus ASCII
    - Modbus/TCP, Modbus RTU in TCP
    - Modbus/UDP, Modbus RTU in UDP
    - Gas Modbus (Enron)
    - Modbus extensions for SCADAPack configuration; extended device addressing (up to 65534 devices), file transfer, gas flow computer history upload and configuration

- SCADAPack E RTUs provide the following Modbus protocol facilities for device communication (instruments, drives, HMI, and so on):
  - Modbus RTU (Master and Slave)
  - Modbus/TCP (Client and Server)
  - Modbus RTU in TCP (Client)

- M340 PAC with additional RTU Module provides the following Modbus protocol facilities for device communication (instruments, drives, HMI, and so on):
  - Modbus RTU (Master and slave, with appropriate CPU model or communication module)
  - Modbus/TCP through RTU module, CPU and optional Ethernet modules
5.5.7. Using telemetry protocols

Time zone management

Both local time and UTC time are available at the RTU when using UTC as the coordinated system time. Use UTC time synchronization to the RTU (e.g. from the remote SCADA master station or local time source such as NTP or GPS). Configure the local time zone offset at the RTU and use the Daylight Savings control to adjust the “local” time in the RTU.

Time-of-day control and time-stamped event reporting in remote SCADA solutions rely on accurate time synchronization between a remote SCADA master station and remote RTUs.

The use of best-practice time management is part of Schneider Electric’s energy management solutions, offering customer benefits in process and remote SCADA systems.

A common question for time management is “In which time zone should my devices operate?”

Remote SCADA operates smoothly when using UTC (Universal Coordinated Time). Best-practice time management has all devices and systems synchronized to UTC time. Time-of-day operations are a local factor and should be offset from UTC at each RTU device.

DNP3 specifies that the “time” to be used for time synchronization and event time stamps is UTC.

Using UTC time at the RTU provides:

- No disruption of historical data during Daylight Savings transitions
- Common time reference in the same system, and interconnected systems, for RTUs and master stations operating across multiple time zones
- Common time format regardless of the time source. E.g. UTC is uniformly used in DNP3 protocol, IEC 60870-5 protocol, NTP time synchronization (IP), time synchronization from a locally connected GPS device
- Aligned diagnostics between RTUs and remote SCADA master stations in different time zones
- Uniform time information for auditing purposes (operational audit, security audit and so on)

Many remote SCADA master stations use UTC time internally. RTU time management from the master station is simplified if UTC time is used to all remote devices.

Smart RTUs typically provide built-in facilities for dealing with both UTC and local time at the RTU.

Standard SCADAPack, SCADAPack E and M340 PAC with additional RTU module are all designed to synchronize time using UTC. Events that are time-stamped at each RTU are internally recorded using UTC. For time-of-day control, each RTU provides configuration for local time-zone offset and Daylight Savings control to allow local time to be available at the RTU. This
provides both UTC and local time at every RTU, adhering to the remote SCADA best practice and telemetry protocol standards for the use of UTC time synchronization.

**Impact of multiple protocols**

A common requirement in remote SCADA systems is to optimize the use of a physical communication channel by simultaneously supporting communication of multiple protocols. This is often required when multiple brands of legacy devices are installed in remote sites within the same system. This can occur when an existing system is upgraded or when parts of a system are replaced with equipment that uses a different protocol.

In general, attempting to use multiple protocols on the same communication link should be examined carefully as incompatibilities can cause unintended operation. For example, interleaved messages can be incorrectly rejected, message integrity checking can be compromised, message addressing and data content can be confused, or simultaneous polling from multiple sources can cause collisions and communication inefficiency.

A communication technology should be chosen that can easily separate multiple protocols in order to avoid problems. For example, Schneider Electric’s Trio radio solutions allow multiple virtual communication streams to operate on the same physical radio channel. This segregates different protocols such that individual streams operate as if there were the only protocol present on the channel. Trio serial radio solutions (K-Series and E-Series radios) provide this capability using Trio’s MultiStream™ feature. Trio IP radio solutions (J-Series and ER45e radios) provide this capability through IP connection handling.

### 5.6. Remote communication network subsystem

This section provides information to consider when choosing remote communication network infrastructure.

Remote communication network types (permanent, non-permanent and connection on-demand) are described in section 3.6.

<table>
<thead>
<tr>
<th></th>
<th>Permanent</th>
<th>Non-permanent</th>
<th>Connection on-demand</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example Network</td>
<td>Ethernet, fiber optic, extension of business network</td>
<td>Data radio, GPRS, leased-line, audio radio, satellite</td>
<td>PSTN (dial-up) GSM</td>
</tr>
<tr>
<td>Data Collection</td>
<td>Current values and time-stamped events</td>
<td>Time-stamped events</td>
<td>Time-stamped events</td>
</tr>
<tr>
<td>Availability of Data</td>
<td>Immediate</td>
<td>Slightly delayed</td>
<td>Delayed</td>
</tr>
</tbody>
</table>
### Polling Methodology

<table>
<thead>
<tr>
<th>Permanent</th>
<th>Non-permanent</th>
<th>Connection on-demand</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrity polls (events and current values)</td>
<td>Event polls</td>
<td>Integrity poll after connection</td>
</tr>
</tbody>
</table>

### High Priority Alarms

<table>
<thead>
<tr>
<th>Permanent</th>
<th>Non-permanent</th>
<th>Connection on-demand</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collected by polling</td>
<td>Collected by event poll or unsolicited response</td>
<td>By polling, or unsolicited response if the site can dial in</td>
</tr>
</tbody>
</table>

### Inter-site Connection (DNP3 protocol)

<table>
<thead>
<tr>
<th>Permanent</th>
<th>Non-permanent</th>
<th>Connection on-demand</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct peer-to-peer</td>
<td>Multi-drop peer-to-peer</td>
<td>Site-to-site dialing</td>
</tr>
<tr>
<td>Multiple masters to the same RTU</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Table 7: Remote communication network use - case comparison

In broad terms, the cost and bandwidth dimensions for various remote communication networks can be characterized as follows:

<table>
<thead>
<tr>
<th>Permanent</th>
<th>Non-permanent</th>
<th>Connection on-demand</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low CapEx</td>
<td>Med-High CapEx</td>
<td>Low OpEx</td>
</tr>
<tr>
<td>LAN/WAN</td>
<td></td>
<td>Med-High OpEx</td>
</tr>
<tr>
<td>DTS</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Non-Permanent                 |                        |                      |
| Landline                      | ★                       |                      |
| GPRS                          | ★                       | ★                     |
| Radio                         | ★                       | ★                     |
| Satellite                     | ★                       | ★                     |

| Connection on-Demand          |                        |                      |
| PSTN                          | ★                       | ★                     |
| GSM                           | ★                       | ★                     |

#### Table 8: Remote communication network operational comparison

**Note:** Where a public infrastructure communication network (primarily including Internet infrastructure, but including other infrastructure as well) is used to interconnect parts of a remote SCADA system, careful attention should be paid to system security. Best practice and defense-in-depth security should be deployed.
5.6.1. **Wireless communication**

Schneider Electric’s Trio data radio products are optimized for remote communication networks between control center remote SCADA master station and remote sites.

Both licensed band and license-free product ranges are available to accommodate a wide range of applications and locations around the world. Serial and Ethernet models are available in both licensed and license-free ranges to accommodate various remote site solutions. Trio Ethernet data radios also provide a serial connection for supporting mixed technology networks. For more information see 4.4.

Telemetry radios can be used in simple flat architectures (Figure 33) and geographically widespread hierarchical model architectures (Figure 34). Also see 6.4.1.

![Figure 33: Flat wireless architecture](image_url)

![Figure 34: Hierarchical wireless architecture](image_url)

5.6.2. **Cellular IP**

Public telecommunications providers offer cellular communication services in a variety of ways. Some offer IP connectivity as part of their Internet infrastructure. Others offer IP services as part of business VPN services.

Where a public infrastructure communication network (primarily including Internet infrastructure, but including other infrastructure as well) is used to interconnect parts of a remote SCADA system, careful attention should be paid to system security. Best practice and defense-in-depth security should be deployed.

In addition to security considerations, availability and reliability requirements of your application should be carefully considered when using shared public telecommunication infrastructure. For critical infrastructure addressed by remote SCADA, cellular communication, for example, may not provide the level of service needed to guarantee network access when needed. For example, events such as storms and other severe weather activity, civil emergencies and so on can impact
the availability of public communication networks. For critical infrastructure applications, system availability particularly at these times may be a key requirement.

A number of telecommunication network standards are in use for cellular IP networks. These include GPRS, EDGE, HSPA, and LTE. Your telecommunications provider can help you determine the type of modem and plan that suits your current and future needs.

The telecommunications provider may offer cellular modem equipment for the remote sites along with the service agreement, or it may be up to the user to provide their own modem equipment. If you provide your own equipment, check with the telecommunications provider which technology is required for the service (e.g. GPRS) and how you provision the equipment for connection to their network (e.g. they may provide you with SIM cards).

Figure 35: RTUs using a cellular network for remote communication

When used with SCADAPack E smart RTUs, serial cellular IP modems provide connectivity to the RTU using PPP serial communications. Full RTU IP functionality is provided by these modems. When using a PPP serial link between a cellular IP modem and the RTU, the functionality provided to the RTU is equivalent to that of an Ethernet link from an external Ethernet modem. Further, the service provided may include allocation of static IP addresses as part of the service agreement, or may require the use of dynamic IP addresses.

Remote SCADA and cellular static IP addressing

In general, an offer that provides static IP addresses is better suited to remote SCADA. An increasing number of telecommunication providers around the world are addressing machine-to-machine (M2M) challenges, which are similar to some of the remote SCADA challenges. The classic IT model for distributed applications uses a large central server at a known IP address and small distributed clients with dynamic IP addresses. In classic IT terms, the RTU at each remote site is a “server.” Remote SCADA architecture results in a large number of small distributed servers. Typically, each system has only one (or a very small number) of clients, for example the remote SCADA master station.

Static IP better suits this remote SCADA architecture by allowing lower cost, simpler modem devices to be used at remote sites. Such modem devices can typically be configured automatically from an RTU (e.g. SCADAPack E RTU connecting to a serial cellular IP modem).

Connection from a telecommunications provider’s cellular IP network (supporting static IP addressing) to the SCADA LAN can take one of two forms:

- Cellular IP modem connected to the SCADA LAN
- Backhaul IP connection from the telecommunications provider to the SCADA

See 6.4.2. for more information.
Remote SCADA and cellular dynamic IP addressing

When only dynamic IP addresses for a cellular network are available from the telecommunications provider, choose from one of the two following methods:

- Obtain cellular modem equipment and service from the telecommunications provider that supports operation with dynamic IP, providing either a known IP address or an externally resolvable name (e.g. using a DDNS service with corresponding software and configuration for computers on the SCADA LAN). In general, the telecommunications provider will pre-configure the equipment for each site, or include detailed instructions on how to configure the individual modem cellular devices. Other service options such as VPN may also be available. Consideration should be given to the long term maintenance and replacement impact of this option.

- Use a solution that tracks the changes in the IP address of the connection to the RTU. Section 6.4.2. describes a system architecture using DNP3 protocol with a SCADAPack E Gateway RTU on the SCADA LAN and SCADAPack E RTUs at remote sites.

5.6.3. IP communication infrastructure

Remote SCADA can utilize conventional IT communication services to remote sites, if available. In general, business IT communications is going to be available for remote sites only in a small number of cases. Typically, this might occur at a major site where IT infrastructure is provided for other business purposes. While bandwidth is typically not an issue, one aspect to consider when sharing IT infrastructure with SCADA operations is availability; IT networks may not be available at all times when required for remote SCADA operations.

In some applications, telecommunications networks can provide dedicated IP connections to remote sites. There are a number of alternatives available. Both the cost to install and the cost to operate these links should be considered.

Such IP connections are usually provided by means of a modem or transceiver with an Ethernet connection, for example DSL, VSAT satellite, and so on. Although the bandwidth will be limited, the operation for remote SCADA will in some ways be similar to that of a direct Ethernet connection. Talk to your telecommunications provider for more information.

5.6.4. Landline / dialup

Wire-line services are a classic connection method used in remote SCADA for communication between a master station and remote sites. In some countries, telecommunications providers are phasing out wire-line services for business in favor of other forms of IP services (cellular, DSL, and so on).
Several forms of wire-line services can be used for remote SCADA communication:

- Point-to-point leased line
- Point-to-multi-point leased line
- PSTN (dial-up line)

In each case, some form of serial modem equipment is necessary, either supplied by the telecommunications provider or provided by the user.

Private wire-line services can also be used (similar to leased landline services).

Data speed across classic wire-line services is typically slow (typically 1200bps – 9600bps) and while a minimum line quality can be expected, it can be variable. Some telecommunications providers offer a premium line option providing better quality and potentially higher speed.

**Leased landlines**

In the case of a leased point-to-point line, full duplex modems may be used, providing transparent serial data communication between the two devices on the line. Data transmitted by one device is received by the other, and vice versa, with minimal latency. The external modems are transparent to the applications (e.g. remote SCADA master station and RTUs) which communicate as if there were a direct RS232 serial connection between the devices. Depending on the modems, the data rate across the line may be more limited than a direct serial connection.

In the case of a leased point-to-multi-point line, the devices connecting to the modems may be required to provide serial hardware control lines to activate the modem for transmission, detect carrier for collision avoidance, and so on. Care must be taken to ensure that the RTU or remote SCADA master station device to which such a modem is connected provides the correct control of the modem hardware lines. RTU devices such as the standard SCADAPack and SCADAPack E RTUs provide such features. Remote SCADA software such as ClearSCADA can also control a PC serial port in the same way.

Care should be taken when using terminal server and other port server equipment for the remote SCADA master station: many do not provide real-time software control of the hardware control lines necessary for controlling multi-point modems.

Point-to-multi-point systems often use a master-slave communications relationship such that the “master” controls the communication with the “slave” devices, transmitting a response only when a message is first received that is addressed to them. Systems using protocols such as Modbus and IEC 60870-5-101 naturally use this mechanism. When using DNP3, care must be taken to generally avoid the use of multi-master communication on a shared link, unsolicited messaging and peer-to-peer communications unless specific collision avoidance mechanisms are available. (Many leased services and multi-drop modems may not provide the necessary support for data carrier detection to indicate when anyone on the line is transmitting).
PSTN and cellular dial-up

Dial-up connections offer a mechanism for point-to-point communication that is straightforward to deploy. Classic dial-up modems connect onto a regular telephone circuit and interface with a smart RTU through a serial port using what is known as a Hayes Modem command set. The same concept is available using cellular networks (in the same way a cellular telephone dials a telephone number). A cellular modem (e.g. GSM modem) also connects to a smart RTU through a serial port and uses a Hayes Modem command set.

PSTN dial-up landline and cellular modems pass serial protocols transparently once a connection has been established. A “phone number” for the target device is required by the initiating device in order to establish the connection. In many cases, this means that the remote SCADA master station will be configured with a phone number of the remote site. Depending on the protocol and the device, an RTU may be able to initiate communication with the remote SCADA master station or with peer devices (e.g. DNP3). In these cases, the RTU will be configured with the phone numbers of the remote SCADA master station and the peer RTUs that it can call.

Compared to other remote communication techniques, the dialing and connecting process from one modem to another is generally very slow (e.g. 15 seconds to call and connect). Communication design should account for this long establishment time for every connection.

One way to mitigate the long connection process is by installing one or more dial-up modems at the remote SCADA master station. Multiple communication connections can be established at the same time in such circumstances. PSTN modems may be used for scheduled outgoing connections (dial-out) and incoming connections (dial-in) initiated from remote sites. Some communication architectures may also allow remote sites to establish connections for sending data to other remote sites (e.g. SCADAPack E allows this peer-to-peer communication using DNP3 protocol).
Figure 36: RTUs using a dial-up network for remote communication

Once a connection is established, it remains open while communication proceeds. In most applications, the link should be disconnected after communication is complete in order to allow the connection to be used for communication with other remote sites, or to minimize communication operating costs.

Remote SCADA master stations and smart RTUs supporting PSTN communication typically manage modem disconnection through RS232 hardware control lines. At times, external modem operation may be subject to disturbance through wired-line interference, power fluctuation and so on. This may require the modem to support features such as:

- Hard restart upon deactivation of a hardware control line (e.g. DTR)
- Internal watchdog features for recovery
- Installation support to power down of the external modem

Wiring the power to an external modem through an RTU relay, for example, may be necessary to ensure robust operation: user logic in the RTU could detect failure of the modem to respond, then deactivate and reactivate a relay in an attempt to restore operation of the external modem.

5.6.5. **High availability**

A number of the communication methods described can be used to provide communication for remote SCADA. Small systems may use only a single method (e.g. remote wireless network using Trio radios). Medium and large systems may use multiple methods in the same system to provide cost-effective communication coverage to all remote sites (e.g. remote wireless network
with coverage to the majority of remote sites, with cellular IP to the few outlying sites not within the wireless coverage area or with marginal signal to the remote wireless network).

Some remote sites may be determined to be more critical to business and system operation than others. Despite a reliable primary communication link, it may be appropriate to provide an additional (fall-back) communication link to a critical site for remote communication system availability.

For example, a system using wireless communication may choose to provide a dial-up cellular fall-back link to each critical site. Fall-back links should be chosen to maximize the independence of communication. (For example, a primary landline communication link and a fall-back cellular IP link may have dependencies on the telecommunications network resulting in common failure conditions whereby both systems become unavailable at the same time). Further, it is preferable that the RTU connect with the primary and fall-back links directly, reducing the external influences and dependencies on communication availability.

5.6.6. Extending a remote communication network using IT infrastructure

Many of the remote communication network systems described can directly use IP communication, or have the ability to be accommodated in the context of IP (for example using a terminal server for serial ports). As a result there can be a correspondence between a remote communication network and an IT infrastructure network.

Fundamental differences between the operational requirements of a remote communication network and an IT network need to be taken into account (availability, variable load causing undesirable communication performance, maintenance scheduling, security concerns, and so on). In many cases, it is not necessary or desirable to couple remote communication and IT networks, however there are some instances where efficiencies can result.

For example, business IT infrastructure in place to service front-office, back-office, process SCADA, and so on, may provide private network capability to the business over a wide area. Where remote sites are in similar geographic areas to these wide area business operations, the business IT infrastructure could be considered the backbone of a remote communication network. Each of the appropriate business sites could then become the connection point for a network for the remote sites in that area. This may allow remote communication solutions such as radio, DSL and dial-up to be optimized. Communication via the closest business site may be more effective than extending the remote communication network separately to the SCADA LAN. As described above, operational constraints that the business network might exert on the remote communication network need to be examined carefully.
5.7. Remote site subsystem

A “remote” asset or site often requires the facilities of a device that integrates equipment and data interfaces from various pieces of equipment. Such demands often require a smart RTU because of its remote communication features, logic for autonomous control, as well as interaction with other remote sites and configuration management.

5.7.1. Design considerations

The following are considerations for selecting a smart RTU and designing a telemetry and remote SCADA system:

- Remote telemetry protocol choice. Also see 5.5.
- Managing remote communications which can be unreliable, or only “periodically connected” by design. Goal should be “No lost data”
- Protocols for connecting to peripherals. Also see 5.7.3.
- Configuration vs. coding
- Logic for deriving data and autonomous control
- Alarm management
- Requirements for remote management: configuration, diagnosis, logic debugging, firmware upgrade
- Telemetry protocol Security. Also see 5.8.7.
- Application content:
  - Standard SCADAPack: Oil & Gas content (Realflo gas flow measurement, ProductionPlus solutions), general control at a remote site
  - SCADAPack E: Water & Wastewater, Irrigation, Renewable Energy, general control at a remote site
  - M340 PAC with additional RTU module: complex Oil & Gas control, Water or other general control applications
  - Physical I/O requirements, including planned expansion
5.7.2. Wireless instrumentation

In many field installations, access to remote sensors can be problematic. Extending power and communication services to remote equipment can be expensive to the extent of being prohibitive. The Accutech wireless instrument solution can provide a solution to both power and communication challenges, allowing integration of data from remote equipment more effectively, and, in some cases, where it was not previously possible.

Based on an architecture of a base radio and remote, self-powered wireless sensors, Accutech provides an easy to install and easy to integrate environment wireless sensor network.

The Accutech base radio is configured to manage a system of remote instrument units, collecting data for easy access from an external RTU or PLC device, from a SCADA master station or other control system. The external communication interface on an Accutech base radio communicates using Modbus RTU protocol on an RS485 connection. This allows direct connection with a SCADAPack RTU, a SCADAPack E RTU or a PLC. The Accutech BR20 base radio includes an option for an integrated Trio wireless radio suitable for use on a Trio K-Series system. With the use of an appropriate RS232 / RS485 converter, an Accutech wireless instrument solution can be connected through other Trio wireless networks or to a ClearSCADA server.

5.7.3. Connecting to field devices

A smart RTU is capable of supporting connection to a wide variety of field device equipment interfaces.

Compact RTUs, for example, typically provide a number of RS232 and RS485 serial ports and/or Ethernet interfaces for connecting to field device equipment or interfaces.
Figure 37: Smart RTU connecting to field devices

When a smart RTU is used to extract data from an external device, it is typically known as the “Master” or “Client.” Examples include connection to a variable speed drive, power meter, flow computer, external PLC or fieldbus converter. Commonly used communication protocols for field device connection in this situation are:

- Modbus RTU (serial) Master using RS232 or RS485
- Modbus/TCP Client using Ethernet
- DF1 protocol Master using RS232 or RS485
- Modbus ASCII Master using RS232 or RS485
- CANopen fieldbus

In these cases, the smart RTU initiates the communication and typically reads data from the connected field device. The smart RTU can also write data to the field device.

Subsection 4.5.2. describes support for these protocols for SCADAPack, SCADAPack E and for M340 PAC with additional RTU module.

Where field devices use fieldbus protocols such as Profinet, CANBus, Foundation Fieldbus and so on, and no direct serial protocol interface is available, an external fieldbus/Modbus converter can be used for interfacing to a smart RTU. Where there is extensive fieldbus connectivity required to an RTU device, consideration can be given to using a process automation solution,
such as the M340 PAC. The additional RTU module can then provide an interface between the control system and the telemetry system.

Another connection scenario uses the smart RTU operating as a “Slave” or “Server.” Examples include a local HMI display unit extracting data, an external PLC, a DCS connection. Commonly used communication protocols for connecting to the smart RTU in this situation are:

- Modbus RTU (serial) Slave using RS232 or RS485
- Modbus/TCP Server using Ethernet
- Gas Modbus Slave using RS232 or RS485

In these cases, the external device initiates the communication and typically reads data from the smart RTU. The external device can also write data to the smart RTU. Although this is typically less frequent than reading data from it.

Subsection 4.5.2. describes support for these protocols for SCADAPack, SCADAPack E and for the M340 PAC with its additional RTU module.

SCADAPack and SCADAPack E smart RTUs support the user authoring their own communication interfaces, allowing communication with external devices that do not support the native protocols of the RTU. For SCADAPack, communication drivers can be written using C/C++ tools. For SCADAPack E, communication drivers can be written using IEC 61131-3 languages.

Other IP connectivity can be enabled on the SCADAPack and SCADAPack E smart RTUs. These smart RTUs support FTP server operation on the RTU providing access to the RTU file system for user defined file handling. This can allow files to be stored on the RTU by external devices (e.g. video security cameras), or transferred to the RTU as part of its configuration (e.g. personality files). These files are under user control, e.g. managed using C/C++ user applications on a SCADAPack, IEC 61131-3 languages on a SCADAPack E RTU. Similarly, the smart RTU can generate data files, with external access via FTP.

5.8. Remote system topology considerations

The topology of a remote communication network can affect how remote devices can interact with the SCADA master station and interact with each other. Particularly in a system with widely dispersed remote sites, the design of the network needs to consider if there are requirements for multiple communication initiators, aggregation of data, separation of communication and interaction between remote sites.

The following sections describe aspects of remote system communication that should be considered in the design of a remote communication network. A number of remote communication network architectures follow from these considerations including:

- Hierarchical topology to suit geographical challenges
5.8.1. Polling

Polling is the standard strategy for acquiring data from remote sites. The master station establishes a schedule to collect data from the remote site RTU. Unlike a Process SCADA (where the goal of polling is to set the update rate as fast as possible), polling should be used in remote SCADA to provide the balance between information updates and the bandwidth consumed on the remote communication network. Keep in the mind that telemetry uses events to report changes, and that the data provided by time stamps on those events collected by an RTU are very accurate.

The majority of communication with a remote asset should yield very little in the way of changes from one poll to the next. Therefore, the majority of communication requests from the master station to remote RTUs should be event polls. If the RTU has no, or very few, changes to report since the last event poll, the response messages should be very short. Event polls should be issued by the master occasionally (e.g. 15 min to 1 hour). Less data and less communication transactions have benefits in scalability and cost (e.g. for cellular communication networks).

RTU data reporting is generally designed and configured for infrequent collection. A smart RTU’s data processing should be used to full advantage to achieve this.

Where multiple classes of events are supported (e.g. in DNP3), a high priority data class containing alarms and more important point changes can be polled more frequently, with lower priority data classes polled less frequently. For example:

- High priority event poll: once every 10 min
- Medium priority event poll: once every 30 min
- Low priority event poll: once every 60 min
Many remote sites will have data that does need to be collected from time to time even if it has not changed, or changed very little. In this case, the data can be made available through time of day scheduled polls, timed event generation, by polling for specific ranges of current value data, or more commonly collected through an integrity poll to which an RTU responds, with all events currently buffered in the RTU as well as a current value report for all data being monitored by the RTU. Integrity polls can result in responses that are generally large and, therefore, should be issued only rarely. For example:

- Integrity poll: once every 8 hours

Where it is necessary to have critical alarms reported more frequently than the high priority event poll, unsolicited responses can be considered. See 5.8.2.

Naturally, communication commands for sending specific messages to an RTU (such as controls, configuration change, and so on) can occur at any time and are given high priority, interrupting the polling cycle to initiate the transaction.

Polling for remote SCADA requires careful consideration. There is high value in being able to have other communication traffic inserted in the remote communication data stream in addition to the polling. The following are examples of non-polling data that can operate on a remote communication network if sufficient “free time” is made available between polls:

- Peer-to-peer communication between remote sites. See 5.8.4.
- Remote diagnostics from maintenance software
- File transfer for remote configuration changes
- File transfer for remote firmware upgrade
- Headroom provided for system expansion

A well-tuned polling regime for remote SCADA can support up to hundreds of remote sites on a single communications link without compromising data integrity or responsiveness to critical events.

### 5.8.2. Unsolicited responses

Unsolicited reporting (also known as spontaneous reporting) is a data transmission mechanism that allows an RTU to send event data to a master without having to wait for an event or integrity poll. It is typically used for transmission of high priority data such as alarm conditions.

It should only be used in conjunction with a remote communication network technology that supports multiple devices concurrently initiating communication. In a multi-drop remote communication environment, the communication network should provide services to avoid collisions between devices that wish to communicate at the same time.
DNP3 supports unsolicited message transmission over multi-drop, point-point, serial and IP communication links. In the case of multi-drop links, collision avoidance should be configured in the RTU or provided by the remote communication network device before attempting using unsolicited reporting. Trio serial and IP data radios provide this feature, for example.

IEC 60870-5-104 (IP communication) can spontaneously send data over a remote communication network from the RTU device to the master station.

IEC 60870-5-101 can spontaneously send data over a communication link from the RTU device to the master station when using balanced link mode (serial point-to-point connections only).

Unbalanced link mode in IEC 60870-5-101 (serial point-to-multi-point connections) cannot spontaneously send data over a link.

**Note:** The use of unsolicited responses can result in added telemetry system complexity and the need for additional communication tuning considerations and performance analysis. When tuned correctly, unsolicited responses can improve system response time, but in general should be restricted to sending data that is considered critical. Normal operational data should typically be collected using event polling with low rate (background) integrity polling. See 5.8.1.

5.8.3. **Routing**

Message routing in a remote SCADA system allows communication across interconnections in a hierarchical architecture, including situations where there are multiple remote communication network links or multiple types of networks to interconnect (e.g. serial, Ethernet, PSTN).
DNP3 message routing on a SCADAPack E

DNP3 supports message routing because its messages carry both a source and a destination address. (Similar in concept to IP network routing).

Figure 38: DNP3 routing using SCADAPack E RTUs

Use a SCADAPack E RTU for routing DNP3 messages in a hierarchical network. Routing of multiple DNP3 messages between multiple devices, across multiple channels and between channel media types is supported concurrently by the SCADAPack E RTUs.

Figure 38 shows an architecture example that uses routing. (The red arrows show where DNP3 routing is occurring in the network). A radio network backbone stretching across a widely distributed geography links sub-networks to provide coverage to remote sites. Routing can be used in many remote communication network architectures. Messages are routed across the network links, allowing the SCADA master station to communicate with remote RTUs, but also allowing other concurrent communication, such as peer-to-peer and remote maintenance between coverage areas. See 5.8.4.

A specific, and limited, form of message routing provided by DNP3 on SCADAPack E RTUs known as store-and-forward allows one device to repeat messages it receives on a communication channel back to the same channel in order to reach a target remote device. This form of routing is primarily used with analog communication channels in order to “boost” or translate a signal to a target device.

Other forms of passing DNP3 messages on SCADAPack E RTUs (e.g. between communication channels) is referred to simply as “routing,” rather than “store-and-forward.”
Standard SCADAPack Modbus store-and-forward

When using Modbus protocols, standard SCADAPack RTUs provide support for Modbus packet forwarding. This is known as store-and-forward on a standard SCADAPack RTU and is supported for Modbus to one level of device beyond the SCADAPack RTU. The limitations of Modbus addressing mean that packet forwarding is limited to a single outstanding Modbus transaction on a communication channel at a time.

IEC 60870-5

Routing and store-and-forward features are not supported for IEC 60870-5 protocols.

5.8.4. DNP3 peer to peer

SCADAPack E RTUs, when used with DNP3 protocol, allow the user’s IEC 61131-3 logic application to request reading of the current value of specific data items, across the remote communication network, from another RTU. Similarly, an RTU can send a control request to change data in a remote RTU. These actions are known as peer-to-peer communication. There is a wide range of applications to which this functionality can be applied.

For example, in water distribution systems, a pumping station can be notified of the level of a tank that it is filling. It can periodically receive or request the level of the tank to determine when to start and stop its pumps. Similarly, it can check the status of valves and other downstream or upstream pipeline conditions prior to making a decision to start pumps.

In a wastewater collection system, a lift station at an environmentally sensitive location can instruct upstream (in-flow) stations to stop pumping in order to avoid a local overflow. Upstream stations can also periodically check operational conditions in their surrounding network, determining when it is appropriate to resume normal operating conditions.

Examples of peer-to-peer communication are shown in Figure 39 and Figure 40, where the red lines indicate the path that the peer-to-peer messages travel. In Figure 40, routing is also occurring as shown by the red arrows where DNP3 messages are being redirected between the remote RTUs. A water supply network, for example, may have zone pressure control sites that are hydraulically linked, but whose geography prevents a single communication network from covering the control sites that need to interact. An architecture using both routing and peer-to-peer communication is applicable in this case, providing robust communication interaction between separated control systems.
Figure 39: DNP3 peer-to-peer using SCADAPack E RTUs

DNP3 peer-to-peer data exchanges differ from other types of DNP3 and IEC 60870-5 communication transactions which usually involve event groups and data classes, along with integrity polls. This is a classic polling methodology for moving higher volumes of device data between an RTU and a SCADA master station or sub-master (for example see 5.8.4.).

Peer-to-peer messages are typically an exchange of small, specific data items using an optimized DNP3 Level 3 feature known as a “point range qualifier.” Typically, peer-to-peer communication uses the same remote communication network links used for RTU communication with a SCADA master station or data concentrator (sub-master). If needed, SCADAPack E RTUs do support peer-to-peer on DNP3 communication channels separate from the SCADA master station.

Using the same communication network for RTU-to-master station and RTU-to-RTU peer communication, peer-to-peer operation requires that the remote communication network technology supports multiple devices concurrently initiating communication. In a multi-drop remote communication environment, the communication network should provide “collision avoidance” services between devices that wish to communicate at the same time. Trio radios provide this feature, for example.
5.8.5. Data concentrator (sub-master)

Data concentrating is a part of an architecture where a sub-master (known as the data concentrator) is used to collect and aggregate (concentrate) data from multiple remote devices. These remote devices are referred to as being “downstream” of the data concentrator. The data concentrator presents the concentrated data (along with data it has collected or derived in its role as an RTU device) to the SCADA master station. The device(s) to which it presents the concentrated data is referred to as being “upstream” of the data concentrator.

DNP3 Data concentrating

When concentrating data from downstream remote devices using DNP3, the SCADAPack E preserves the original sequence of event ordering, event time stamps and point quality information when it presents its data upstream.

For architectures requiring a DNP3 sub-master, a SCADAPack E RTU can be used as the data concentrator. It supports operating as a full DNP3 RTU as well as performing the data concentrating role for downstream devices. In general, a SCADAPack ES is the best SCADAPack E RTU to use.
An optional license is required for a SCADAPack ES data concentrator that communicates with more than 10 remote devices or collects more than 500 remote DNP3 points. With the optional license, SCADAPack E can connect to up to 100 remote devices and support more than 15000 remote data points. SCADAPack 300E models are always limited to communicating with a maximum of 10 remote DNP3 devices, collecting less than 500 points.

SCADAPack E data concentrating supports upstream communication using DNP3 (serial or IP), IEC 60870-5-101 and/or IEC 60870-5-104 protocols when the downstream devices are DNP3 (serial or IP).

When using the M340 PAC with its RTU module as a DNP3 data concentrator, it can connect to up to 32 downstream DNP3/IP devices with up to 5000 words of remote data. The additional RTU module’s data concentrating for DNP3/IP protocol supports upstream communication using DNP3 serial or DNP3/IP communication.

SCADAPack E RTUs, standard SCADAPack RTUs and third party RTU devices can be used as remote DNP3 RTUs in a telemetry and remote SCADA system. The M340 PAC with its additional RTU module provides an interface between a control system application and a DNP3 telemetry system.
IEC 60870-5-104 data concentrating

For architectures using data concentrating (sub-masters) with IEC 60870-5 protocols, use an M340 PAC with an RTU module as the IEC 60870-5 sub-master. When concentrating data from downstream remote devices using IEC 60870-5-104 protocol, the RTU module preserves the original sequence of event ordering, event time stamps and point quality information when it presents its data upstream.

When using the M340 PAC with its additional RTU module as an IEC 60870-5-104 data concentrator, it can connect to up to 32 downstream IEC 60870-5-104 devices with a total of up to 5000 words of remote data. Data concentrating for the IEC 60870-5-104 protocol by the RTU module supports upstream communication using IEC 60870-5-101 or IEC 60870-5-104 protocols.

SCADAPack E RTUs and third party RTU devices can be used as remote IEC 60870-5-104 RTUs in a telemetry and remote SCADA system. The M340 PAC with its additional RTU module provides an interface between a control system application and an IEC 60870-5 telemetry system.

IEC 60870-5-103 data concentrating

For systems using IED devices supporting the IEC 60870-5-103 protocol for electrical protection equipment, use a SCADAPack ES RTU as the data concentrator (IEC 60870-5-103 license option required).

The SCADAPack ES preserves the original sequence of events ordering, event time stamps and point quality information when it presents its data upstream. Upstream communication may use DNP3, IEC 60870-5-101 or IEC 60870-5-104 protocols.

5.8.6. Multiple masters

In some system architectures there are two or more independent masters (also known as a multi-master architecture). This is different from a redundant master system (that while containing several master nodes arranged in a redundant fashion, they appear as a single master).

An example of a multiple master system is where a local master communicates with an RTU as well as a central master (e.g. a local terminal at the remote site that may be using a subset of the configuration of the SCADA master station); or where two separate business entities have independent control rooms with separate communications to the same RTU devices (e.g. pipeline control system).

RTUs supporting multiple masters manage events independently for each master connection.
Connecting multiple masters to SCADAPack E

SCADAPack E Smart RTUs support multiple master connections as follows:

- Up to 3 concurrent DNP3 master connections per RTU, and
- Up to 2 concurrent IEC 60870-5-101 or -104 master connections per RTU, and
- Multiple Modbus RTU serial and Modbus/TCP connections

When using DNP3 protocol, SCADAPack E RTUs can present different data to each master (selected on a per point basis). When using IEC 60870-5 protocols, SCADAPack E RTUs present the same data to all masters.

Multiple master connections may be used concurrently with data concentrating.

Connecting multiple masters to standard SCADAPack

Standard SCADAPack RTUs can support multiple master connections as follows:

- Up to 8 concurrent DNP3 master connections per RTU, and
- Multiple Modbus serial and Modbus/TCP/UDP connections

When using DNP3 protocol, standard SCADAPack RTUs present the same data to all masters.

Connecting multiple masters to M340 PAC with additional RTU module

Adding an RTU module to the M340 PAC provides an interface for multiple master connections as follows:

- Up to 4 concurrent DNP3/IP or IEC 60870-5-104 master connections per RTU module
- Multiple Modbus/TCP connections (for access to M340 processor module data)

Use an appropriate M340 PAC processor or optional external communication module to provide Modbus serial connections.

The M340 PAC additional RTU module presents the same telemetry data to all masters when interfacing with a DNP3 and IEC 60870-5 telemetry system.

Multiple master connections may be used concurrently with data concentrating (with limited protocol combinations).
Addressing cybersecurity aspects of communications to remote assets can be a challenge due to the dispersed nature of remote sites and equipment.

Two types of remote communication security can be applied. These are described below:

- **Authentication security**
- **Encryption security**

Authentication is the process by which a device can verify the identity of another device prior to acting on information it provides. Authentication is not the same as encryption. In many cases, authentication is a preferred security methodology for remote SCADA.

Encryption is the process by which the content of messages passing between two devices is obscured such that an outside observer of the messages cannot discern their content. This involves device processing and communication overhead, typically impacting remote SCADA system performance.

SCADAPack E smart RTUs support both authentication and encryption security for remote SCADA when using DNP3 protocol. These can be used individually or together, depending upon system requirements.
Choosing which security measures to deploy in a system, and where, requires careful consideration due to on-going security management and potential performance impact.

**Architectures for DNP3 secure authentication**

Authentication security is built into the DNP3 protocol standard. ClearSCADA and SCADAPack E smart RTUs support DNP3 Secure Authentication. An optional license is required for SCADAPack E RTU devices using DNP3 Secure Authentication.

It is possible to use ClearSCADA with third party RTUs supporting DNP3 Secure Authentication, and it is possible to use SCADAPack E RTUs with a third party SCADA master station supporting DNP3 Secure Authentication. Compare the DNP3 device profile information for the master and outstation devices when using DNP3 protocol features with combinations of third party products.

When used together, ClearSCADA and SCADAPack E RTUs support advanced configuration management features, including remote management of DNP3 Secure Authentication configuration.

DNP3 Secure Authentication is an end-to-end security solution based on a challenge-response philosophy. Critical messages sent by a SCADA master station are challenged by an outstation (RTU) to verify the authenticity of the master, as shown in Figure 43. Similarly, messages sent by an outstation can be challenged by a master station to verify the authenticity of the outstation.

![Figure 43: DNP3 secure authentication challenge transactions](image)

Secure transactions use security “keys” that are known by the devices that are intended to communicate with each other. For SCADAPack E RTUs, the Security Administrator application allows security configuration files, including keys, to be managed. The key values produced by this application can be used by third party master stations. When used with ClearSCADA, the security configuration files can be remotely deployed to SCADAPack E RTUs, significantly easing one of the maintenance aspects of remote security management.

In a typical configuration, using DNP3 Secure Authentication between ClearSCADA and SCADAPack E smart RTUs, communication initialization establishes a secure session. An alarm
is generated in ClearSCADA if the secure session is not correctly established allowing the detection of unauthorized RTU devices on a system. Thereafter, routine data acquisition exchanges such as class poll requests and poll responses between a master station and an outstation are not typically challenged. This ensures the performance of routine remote SCADA communication is not impacted by the use of Secure Authentication. The secure session between the master station and RTU is periodically re-established to check security integrity.

Every critical message exchange between the master station and RTU, on any DNP3 protocol port on the RTU, is challenged. In particular, any message exchange that can effect outstation operation is classified as “critical” and includes control messages to change point states and values, commands to the RTU, configuration changes, restarting the RTU, setting the time in the RTU, changing unsolicited behavior, upgrading firmware and accessing RTU files (Open, Read, Write, Delete, and so on)

Figure 44: Architecture for remote SCADA authentication security

As the SCADAPack E Configurator uses native DNP3 communication for SCADAPack E RTU configuration, configuration is subject to the rules of the security model through the use of DNP3 Secure Authentication. Security keys for Configurator nodes are also managed by the Security Administrator application, with RTUs having knowledge of authorized configuration computers. The security level for configuration of a remote SCADA system can be further enhanced by enabling security for authorized users. The Security Administrator can manage individual users by name and password, allowing RTUs to require an authenticated individual user, as well as authenticated configuration software, in order to make changes to an RTU’s configuration.

The level of security deployed in a remote SCADA system can be tailored to the system’s needs, including the ability to identify specific sites at which security is required, and other sites at which it is not necessary.

The basic system architecture for using DNP3 Secure Authentication is not physically different from standard remote SCADA architecture as described throughout this STN. See Figure 44.
Security configuration generated by the SCADAPack E Security Administrator sets the protection for the transactions between devices, including remote SCADA master station and RTU, between SCADAPack E remote RTUs (peer-to-peer communication) and between SCADAPack E Configurator and remote SCADAPack E RTUs.

Remote SCADA system architecture using DNP3 can include RTU routers and data concentrators (sub-masters). The physical architectures are the same as those described in Chapters 5. and 6. The transactions between a data concentrator and its remote RTUs work the same way as between the master station and remote RTUs (as described above). The data concentrator uses DNP3 Secure Authentication as an outstation to its master station, and also uses DNP3 Secure Authentication as a master to its remote RTUs.

If authentication and encryption services are both needed to address system security requirements, DNP3 Secure Authentication and AGA12 encryption can be used concurrently in the same system, and on the same remote SCADAPack E RTUs.

**Architecture for AGA12 encryption of DNP3**

Encryption security for remote SCADA communication is provided by the SCADAPack E smart RTU for DNP3 communication using a standard known as AGA12-2 (also known as IEEE 1711). An optional license is required for SCADAPack E RTU devices using AGA12 encryption security.

*Note:* There are export limitations on AGA12 due to the encryption algorithms used.

AGA12 security is supported internally in SCADAPack E smart RTUs. It can be used with any DNP3 capable master station including ClearSCADA, requiring an external SCADAPack ES smart RTU to be used a “security gateway” to a remote SCADA network. See Figure 45.

The security gateway SCADAPack ES RTU takes a standard DNP3 protocol stream from a master station and encrypts it using the AGA12-2 protocol. The AGA12-2 messages are then sent across the remote SCADA network. The receiving SCADAPack E decrypts the message content and processes the DNP3 messages as originally sent by the master station. Similarly, the DNP3 response messages in the RTU are encrypted internally and the AGA12-2 protocol is sent across the remote SCADA network back to the security gateway where it decrypts the message content and passes the DNP3 response to the master station. The SCADAPack ES provides security gateway encryption and decryption for up to 90 remote SCADAPack E RTUs.

Configuration access to remote RTUs is accommodated in the architecture using AGA12 security by connecting the SCADAPack E Configurator to the network behind the security gateway SCADAPack ES RTU. In general, the security gateway RTU should form part of the SCADA master station security perimeter to prevent unauthorized access to the network using unencrypted DNP3.

Each SCADAPack E RTU device using AGA12 security can have a single DNP3 port configured for “local access.” Encryption is not applied to that port to allow the SCADAPack E Configurator to
manage the RTU locally. Routing is disabled on the local access port and it should not be connected to a remote communication device. For a SCADAPack 300E RTU, the USB port is typically configured as the local access port.

Encryption / decryption for AGA12 protected DNP3 peer-to-peer communication between RTUs is performed directly by each SCADAPack E. It does not require messages to pass through the security gateway.

In a typical system, not all RTUs require their message content to be obscured through encryption. In systems where there is a mix of secured and unsecured devices, standard DNP3 and AGA12 encrypted messages can be used together. Devices with AGA12 security configuration can only respond to remote SCADA communication requests using AGA12 protocol. For example, every message transaction with an AGA12 secured device carries the overhead associated with the encryption protocol.

SCADAPack E RTUs using AGA12 encryption can provide message routing for both DNP3 and AGA12 packets, allowing a remote SCADA network using encryption to be architected in a hierarchy using the same message routing capability as described in section 5.8.3. The same SCADAPack E can route both AGA12 encrypted packets and unencrypted DNP3 packets on to other RTUs (but messages processed by the RTU itself and not passed on must be AGA12 encrypted messages. Unencrypted DNP3 message will not be processed by the RTU in this case).

Data concentrator (sub-master) architectures are also supported with AGA12. The physical architecture is the same as described in section 5.8.5.

The AGA12 encryption process uses security “keys” that are known by the devices that are intended to communicate with each other. These are known as “counterparts.” For SCADAPack E RTUs, the Security Administrator application allows security configuration files, including keys and counterparts, to be managed for AGA12 security. When used with ClearSCADA, the security configuration files can be remotely deployed to SCADAPack E RTUs, significantly easing one of the maintenance aspects of remote security management. A security gateway SCADAPack E RTU is still required for the encryption / decryption process at the master station, in this case.
If authentication and encryption services are both needed to address system security requirements, DNP3 Secure Authentication and AGA12 encryption can be used concurrently in the same system, and on the same remote SCADAPack E RTUs.
6. Selection

Architectures are presented in the following sections for each telemetry and remote SCADA Solution layer:

- Business system interface architecture for remote SCADA
- Control room architecture for remote SCADA
- Multi-site systems architectures
- Remote communication network architecture
- Remote site architecture

Based on system requirements, choose an architecture for each telemetry and remote SCADA layer as described in the following sections.

6.1. Business network interface architecture for remote SCADA

The purpose of the business network interface is to facilitate transfer of information from a remote SCADA server to a business network.

**Note:** Where a public infrastructure communication network (including Internet as well as other infrastructure) is used to interconnect parts of a remote SCADA system, careful attention should be paid to system security. Best practice and defense-in-depth security should be deployed.
6.1.1. Interface to an optimized business system

The optimized business system architecture provides a level of functionality that is suitable for an entry level solution or a solution with basic functionality. It provides the network infrastructure for simple connection between the control room SCADA LAN and one or more business application servers.

This architecture is suitable for information transfer such as:

- Printing reports from a remote SCADA server using a business network printer
- Exporting remote SCADA information to files on a business server
- Using a business application to query remote SCADA data using an open interface (e.g. ODBC, OPC, Schneider Electric EcoStruxure Web Services)

![Diagram of Optimized Business System Interface Architecture for Remote SCADA](image)

**Figure 46: Optimized business system interface architecture for remote SCADA**

This architecture is typically used in smaller systems where the majority of information is visualized and acted upon in the control room.

6.1.2. Remote SCADA interface to business systems

![Diagram of Remote SCADA System Interface Architecture for Business Systems](image)

**Figure 47: Business system interface architecture for remote SCADA**
The business system interface architecture provides a comprehensive network infrastructure solution that can address:

- Protection at the connection point of the business network and SCADA networks through the use of a firewall
- Distributing SCADA users across the enterprise network
- Application servers to query and receive remote SCADA information
- Email server access for remote SCADA alarm management
- Protection at the connection point of the enterprise and public networks through the use of a firewall and router supporting VPN functionality
- Access for remote SCADA users external from the enterprise, secured through VPN links
- Managing display clients in a virtualized environment, such as Citrix
- Remote user access to enterprise information, visualize SCADA information through web or full function clients and, if permitted, remotely maintain remote SCADA infrastructure, including SCADA servers, SCADA database, radio equipment, remote RTUs and field devices

This architecture is suitable for:

- Printing reports from a remote SCADA server using enterprise network printers
- Exporting remote SCADA information to files on enterprise servers
- Using enterprise applications to query remote SCADA data using open interfaces (e.g. ODBC, OPC, EcoStruxure Web Services)
- Supporting distributed operation centers
- Supporting business activities using remote SCADA in multiple business locations
- Providing remote access to SCADA for on-call operation and maintenance personnel

This architecture is typically used in medium-sized systems where there are multiple operation and maintenance users, and where remote SCADA information is visualized and used by the enterprise in multiple locations.

Business applications typically use one or more of the following interfaces with ClearSCADA:

- OPC-DA, OPC-XML/DA
- OPC-HDA
- OPC-AE
- ODBC / SQL
- OLE-DB
- SOAP/XML
- Schneider Electric EcoStruxure Web Services
- Programmatic OLE automation interfaces
- Programmatic .NET interfaces
- Data export through report generation: PDF reports, text files, CSV files
- Data export to an external database via SQL
- Email for alarm management

### 6.1.3. Interface to highly available business systems

The highly available business system interface architecture provides a comprehensive network infrastructure solution with enterprise level redundancy that can address the following system requirements:

![Highly available business network architecture for remote SCADA](image-url)

**Figure 48: Highly available business network architecture for remote SCADA**
• High availability business network and high availability SCADA networks

• Protection at the connections between the enterprise and SCADA networks through the use of firewall devices

• Distributing SCADA user access across the enterprise networks for fault-tolerant operations

• Email server access for remote SCADA alarm management

• Distributing remote SCADA users, web users and remote maintenance users beyond the enterprise and SCADA networks through the use of firewall and routers, secured through VPN links

• Remote user access to enterprise information, visualize SCADA information through web or full function clients and, if permitted, remotely maintain remote SCADA infrastructure, including SCADA servers, SCADA database, radio equipment, remote RTUs and field devices

• Managing display clients in a virtualized environment, such as Citrix

• Distributed application servers to query and receive remote SCADA information

• Maximizing the utilization of enterprise IT infrastructure for robustness and distributing access to remote SCADA business information

• Distributing ClearSCADA performance servers across the enterprise network, providing replicated remote SCADA databases close to clusters of users

• Providing secured ClearSCADA DMZ performance servers across the enterprise network for read-only access to remote SCADA data

This architecture is suitable for:

• Using enterprise applications to query and receive remote SCADA data using open interfaces

• Providing distributed, physically separated control rooms

• Supporting business activities using remote SCADA in multiple centers across the enterprise

• Providing remote access to SCADA for on-call operation and maintenance personnel

• Integrating the management of enterprise and SCADA IT infrastructure

Integrated business architectures are typically used in large systems where there are multiple sites providing disaster recovery and business continuity, where IT infrastructure and control room operations are well established. These systems typically have a large number of users of remote SCADA information in multiple sites across the enterprise who may be involved in system operation, modeling, optimization and maintenance. The data provided to the enterprise systems from the remote assets are important for smooth business operation.
6.2. Control room architecture for remote SCADA

The purpose of the control room architecture is to provide the infrastructure for the remote SCADA servers and display clients for remote SCADA operation.

**Note:** Where a public infrastructure communication network (including Internet as well as other infrastructure) is used to interconnect parts of a remote SCADA system, careful attention should be paid to system security. Best practice and defense-in-depth security should be deployed.

6.2.1. Optimized control room

The optimized control room architecture provides a level of functionality suitable for an entry level solution or a solution with basic functionality. It provides a single remote SCADA host system, where a single workstation is used both as the remote SCADA server and the display client.

![Control Room Architecture Diagram](image)

*Figure 49: Optimized control room architecture for remote SCADA*

The operating system for the workstation running ClearSCADA could be Windows XP, Windows 7, Windows 7 x64, and so on.

In this architecture, ClearSCADA provides all database, telemetry communication serving, historical and event log data serving on the same workstation as a ViewX (full function) display client.

The optimized architecture could be applicable for a small system of 10 or less RTUs with around 1000 points or less, with one display client on the workstation and an optional ViewX or WebX external display client. It is suitable where the SCADA data is viewed occasionally and where continuous availability is not a concern – there is no server or communication redundancy. This architecture is suitable where there is overall low system performance and where the system is not critical to the operation of a business.

The optimized control room architecture can support exchanging data with a business system, but as a workstation is not optimized for data serving, it typically could only be used for
connection with a single external data application, and where interaction with that application occurs infrequently.

The business network connection could also provide access to an email server for ClearSCADA alarm management.

This architecture is typically used in smaller, non-mission critical systems where the majority of information is visualized and acted upon solely by an operator in the control room.

This architecture assumes that network security is managed on the business and remote communication networks.

With the addition of a modem for connection to a suitable SMS or paging service, the system can provide SMS or pager notifications for ClearSCADA alarm management.

The connection of the optimized control room architecture to the remote communication network can be through Ethernet or serial connection. The connection may be direct to a remote communication network device, or use an RTU as a communication gateway (e.g. SCADAPack 300 or SCADAPack 300E).

ClearSCADA licenses suitable for this type of system include:

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Equipment</th>
<th>Quantity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server for remote SCADA</td>
<td>ClearSCADA Server (with bundled ViewX display client)</td>
<td>1</td>
</tr>
<tr>
<td>Full function display clients</td>
<td>ViewX client or floating license pack</td>
<td>As needed</td>
</tr>
<tr>
<td>Web server</td>
<td>ClearSCADA base web server license</td>
<td>1</td>
</tr>
<tr>
<td>Web display clients</td>
<td>Concurrent WebX connection pack</td>
<td>As needed</td>
</tr>
<tr>
<td>Data access</td>
<td>ClearSCADA Server includes: ODBC, OLE/DB access ClearSCADA base web server includes: SOAP/XML, EWS access</td>
<td></td>
</tr>
<tr>
<td>OPC connection to server (if required by business application)</td>
<td>ClearSCADA OPC Server</td>
<td>1</td>
</tr>
</tbody>
</table>

Table 9: ClearSCADA equipment for an optimized control room
6.2.2. Highly available control room

Figure 50: Highly available control room for remote SCADA

The highly available control room architecture offers an extensible architecture suitable for many small to medium sized remote SCADA systems.

It offers ClearSCADA servers and multiple ClearSCADA client nodes, and supports main / standby redundancy on the ClearSCADA servers for improved system availability or mission-critical systems:

- Main and standby servers may be collocated on the same business LAN
- Main and standby servers may be located in physically different data centers on a business network
- The server connection between main and standby ClearSCADA servers is optimized for operation across WAN as well as LAN links

The highly available control room architecture can optionally support dual network configurations between ClearSCADA servers and between servers and ViewX clients to increase system availability.

It is strongly recommended for this architecture that the ClearSCADA server machines are based on server grade hardware systems, running a server operating system such as Microsoft Windows Server 2008 or later. See ClearSCADA server specifications for more information. As described in 5.4.2., ClearSCADA servers are often physically located in enterprise data center environments.

Each server can optionally host connections for full function display clients (ViewX) and/or web display clients (WebX).

ClearSCADA ViewX and WebX clients can be distributed across business network LAN and WAN connections.
ViewX is optimized for operation across WAN as well as LAN links

ClearSCADA operator workstations are typically based on Windows XP, Windows 7 or later. See ClearSCADA display client specifications for more information.

In this architecture, ClearSCADA duplicates all database, telemetry communication serving, historical and event log data serving capabilities across two servers. Both ClearSCADA servers can serve requests for data to multiple ViewX and/or WebX display clients and business applications, allowing load on any one server to be reduced. One of the ClearSCADA servers assumes responsibility as the main server and is responsible for managing the remote telemetry communication to collect the data for the system.

The system supports multiple workstations with ViewX or WebX display clients which can operate with the redundant server systems.

Communication redundancy with remote communication networks should be considered independently from ClearSCADA server redundancy. While adding additional resilience to a system, multiple communication links can require additional engineering.

This architecture is suitable for exchanging data with a business system. It typically could be used for connection with several applications. The remote SCADA servers are sharing their load for distributed ViewX clients, WebX clients and application data. This architecture is best suited to business applications that access ClearSCADA data infrequently, thereby avoiding excess load impacting system operation.

The highly available architecture is scalable for small to medium systems with up to 500 RTUs, up to many tens of thousands of points, and with tens of ViewX or WebX display clients. Deploying the correct server hardware and network architectures are necessary to scale up a system such as this. See ClearSCADA server specifications for more information.

This architecture is typically used in small and medium sized mission critical systems where information is visualized and acted upon by fulltime control room operators and distributed business operations centers.

Alarm distribution and management, as an important business operation, is supported using a ClearSCADA server connection to an enterprise email server; or through the connection of modems for an SMS or pager service to a serial port on each ClearSCADA server.

The highly available architecture can easily be extended and scaled using concepts from the scaled performance control room architecture (see 6.2.3. ) and interface to a highly available enterprise system (see 6.1.3. ). For example, a triple standby server, a DMZ server, or performance servers can be added to the highly available control room architecture or enterprise architecture, as required.

This architecture assumes that network security is managed on the business and remote communication networks.
The connection of the highly available control room architecture to the remote communication network can be through Ethernet or serial connection into two points in the remote communication network. The connections may be direct to remote devices, use terminal servers, or use two RTUs as communication gateways (e.g. SCADAPack ES).

ClearSCADA licenses necessary for this architecture include:

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Equipment</th>
<th>Quantity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Main/standby server for remote SCADA</td>
<td>ClearSCADA server (with bundled ViewX display client)</td>
<td>2</td>
</tr>
<tr>
<td>Full function display clients</td>
<td>ViewX client or floating license packs</td>
<td>As needed</td>
</tr>
<tr>
<td>Web server</td>
<td>ClearSCADA base web server license</td>
<td>1</td>
</tr>
<tr>
<td>Web display clients</td>
<td>Concurrent WebX connection packs</td>
<td>As needed</td>
</tr>
<tr>
<td>Data access</td>
<td>ClearSCADA server includes: ODBC, OLE/DB access ClearSCADA base web server includes: SOAP/XML, EWS access</td>
<td></td>
</tr>
<tr>
<td>OPC connection to servers (if required by business application)</td>
<td>ClearSCADA OPC server</td>
<td>2</td>
</tr>
</tbody>
</table>

Table 10: ClearSCADA equipment for a highly available control room

6.2.3. Scaled performance operation centers

The scaled performance control room architecture offers a comprehensive architecture suitable for enterprise remote SCADA systems.

It provides distributed ClearSCADA servers for high availability and business continuity, performance servers for distributing display client and business application load, DMZ server for secure network zones, and distributed ClearSCADA display clients across enterprise networks.

ClearSCADA offers network flexibility with a mix of dual Ethernet and single Ethernet systems as the LAN/WAN network architecture requires.

As described in 5.4.2., ClearSCADA servers are typically located in enterprise data centers, running on enterprise server hardware. ClearSCADA replicates all database, telemetry communication serving, report serving, historical and event log data serving and user serving capabilities across:

- Main server
- Standby server
- Triple standby server
Distributed control rooms may be separated by distances of thousands of kilometers, for example in pipeline systems; or in separate parts of the same city for disaster recovery/business continuity.

ClearSCADA servers for systems distributed across wide area networks can be located close to clusters of SCADA users or business applications (regional office systems for example). ClearSCADA replicates real-time data, configuration data, historical and event log data serving and user serving capabilities across additional servers. These can be located on the control room network, or across the enterprise network as shown in the highly available enterprise system architecture in 6.1.3.:

- Performance server
- DMZ server

Up to a total of six (6) servers are supported in a ClearSCADA server set. Each server can optionally host connections for full function display clients, web display clients and/or business application interfaces.

Distributed ClearSCADA display client workstations are located across the enterprise. Virtualization of client displays is a possible variant of this architecture.

The system supports multiple workstations with ViewX or WebX display clients which can operate with the redundant server systems.

The scaled performance architecture supports up to thousands of remote RTU devices, hundreds of concurrent display client users, multiple business application interfaces, and up to 500,000 database objects.

Figure 51: Scaled performance operation centers for remote SCADA
For systems larger than 500,000 objects, further scaling is provided by the ClearSCADA architecture where a system can be segregated into separate ClearSCADA server sets. The database of each server set can support up to 500,000 database objects. These can be co-located or separated from other ClearSCADA server sets. Each set can support the full ClearSCADA redundancy and distributed performance architectures. ViewX display clients can seamlessly connect with up to 64 separate ClearSCADA server sets.

There are a number of ways of classifying systems for division into multiple server sets:

- By large regional area (e.g. Northern Region, Southern Region remote SCADA)
- By business activity responsibility (e.g. Clean Water, Wastewater remote SCADA)

Information from multiple ClearSCADA server sets can be seamlessly combined for operational display and management through ViewX display clients including:

- Combined alarm lists
- Combined mimic displays
- Combined trend displays
- Integrated system navigation

Enterprise LAN/WAN network design is an important consideration for large systems. The remote SCADA architecture maximizes WAN communication efficiency across an enterprise while delivering distributed functionality to suit business needs. The scaled-performance architecture is typically integrated closely with the enterprise security model.

The connection of the scaled performance operation center architecture to the remote communication network can be through Ethernet or serial connection into two points in the remote communication network. The connections may be direct to remote communication network devices, user terminal servers, or use two RTUs as communication gateways (e.g. SCADAPack ES). The use of RTUs often provides flexibility in managing customized redundancy schemes where multiple communication links are available.

This architecture is suitable for a high level of integration between remote SCADA and business applications. In the same way that the ClearSCADA performance servers can be used to distribute load for users of remote SCADA information across an enterprise network, performance servers can also be used for interfacing to business applications. High intensity business applications (e.g. performing high volume historical enquiries or broad data enquiries across a wide range of asset information) can query performance servers without impacting operational remote SCADA servers. Enterprise work order management system integration with remote SCADA alarms and performance data are other examples of business applications addressed by this architecture.
ClearSCADA licenses necessary for this architecture includes:

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Equipment</th>
<th>Quantity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Main/standby/triple standby server for remote SCADA</td>
<td>ClearSCADA server (with bundled ViewX display client)</td>
<td>3</td>
</tr>
<tr>
<td>Performance server(s)</td>
<td>ClearSCADA server</td>
<td>1 or more*</td>
</tr>
<tr>
<td>Full function display clients</td>
<td>ViewX client or floating license packs</td>
<td>As needed</td>
</tr>
<tr>
<td>Web server</td>
<td>ClearSCADA base web server license</td>
<td>1 per performance server</td>
</tr>
<tr>
<td>Web display clients</td>
<td>Concurrent WebX connection packs</td>
<td>As needed</td>
</tr>
<tr>
<td>Data access</td>
<td>ClearSCADA server includes: ODBC, OLE/DB access</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ClearSCADA base web server includes: SOAP/XML, EWS access</td>
<td></td>
</tr>
<tr>
<td>OPC business application connection to performance server(s)</td>
<td>ClearSCADA OPC server</td>
<td>1 per performance server</td>
</tr>
</tbody>
</table>

Figure 52: ClearSCADA equipment for scaled performance operation centers

* Maximum 4 performance servers, maximum total of 6 ClearSCADA servers in single server set.

E.g. Main, standby, 4 performance servers

E.g. Main, standby, triple standby, 3 performance servers

6.3. Multi-site systems

In remote SCADA solutions, it is often desirable to consolidate data from widely distributed business assets at a high level in the system. Examples include:

- Central reporting of regulatory data
- Consolidating energy consumption data for site performance benchmarking
- Centralized management of critical remote site alarms
- Transparent operation of remote sites from centralized or distributed locations
- Control room operator after-hours responsibility for process and remote site operations
- Maintenance personnel visit both process sites and remote sites in the same shift and need access to all alarms and site information from the same system
- Process automation data and remote site data used to correlate system performance and efficiency to drive operational improvements

For municipal business organizations, multi-site systems can help them comply with regulatory requirements. When reporting for remote process sites (e.g. reporting quality parameters), the
collection and compilation of the process data can be optimized by centralizing data for multiple remote process sites at the control room. This improves data accuracy and reduces the need to send operators to the remote sites.

Regional authority organizations require full reporting and measurement of business performance – including items such as regulatory compliance, energy consumption, water quality, and so on – and benefit from high level consolidation of data from multiple process sites using multi-site system architecture.

Multi-site system support is an extension of remote SCADA solutions. A number of solutions are available depending on the available remote communication infrastructure, remote site size and operational requirements.

### 6.3.1. Data from remote process PLCs

Data can be extracted from a remote process automation system and integrated in a central control room in a number of ways.

**Schneider Electric PACs**

ClearSCADA in a central control room can integrate with Schneider Electric OFS (OPC server) providing communication to Modicon PLC/PAC equipment such as Quantum, M340 and Premium ranges. High bandwidth communication is required between the central control room and the remote process automation system in order to use this approach for collecting data.

ClearSCADA can access both located and unlocated variable data from Schneider Electric PACs/PLCs.

**Third party PLCs**

There are several approaches for ClearSCADA in a central control room to acquire data from a third party PLC at a process site:

- Using a native communication driver such as Modbus RTU, Modbus/TCP, DF1, S7 and so on
- Using a third party OPC server to communicate with the PLC
- Using an RTU device as described below
The ClearSCADA OPC-DA client supports the data types described in the OPC-DA 1.0, 2.0 and 3.0 specifications. The data that can be accessed in any particular PLC, in this case, is limited by the functionality of the third party OPC server.

As PLC protocols use a pure polling approach, medium or high bandwidth communication is required between the central control room and the process site in order to use a native driver or third party OPC approach to collecting data.

**PLC with RTU module in an automation process**

Some PLC device ranges have optional RTU protocol modules. Where such modules support open telemetry protocols such as DNP3 or IEC 60870-5, the process automation data becomes available in a way consistent with data from other remote telemetry sites.

For example, the Schneider Electric Modicon M340 PAC has an optional RTU module (NOR0200H). This provides an interface to a control application to a telemetry system with low bandwidth, discontinuous communication links, and where the communication channel is shared with other RTU devices. Schneider Electric water solution architectures describe a remote site architecture known as “R3” for very large multi-pump control systems using the M340 PAC with RTU module.

This approach of using an RTU module with a PLC provides a low cost, low bandwidth interface from a control application into a telemetry and remote SCADA system.

**Using a SCADAPack RTU with a PLC**

Central control room access to a process automation system can be provided by a SCADAPack or SCADAPack E smart RTU. DNP3 or IEC 60870-5 protocols are often used for remote SCADA communication, with Modbus or Modbus/TCP protocol used by the RTU to communicate with the PLC locally. (Other PLC communication protocols available in the RTUs may be used. SCADAPack and SCADAPack E support DF1 protocol, for example). The use of an RTU as the interface between a central control room and a PLC system is further described in the field architecture described in 6.5.2.

This type of interface is suitable where the communication link to a process site is low bandwidth, where the PLC does not have an RTU protocol module available, where an RTU module for the
PLC is prohibitively expensive, or in particular where the facilities of a full functioned smart RTU is required for management of the information provided by a process automation application.

6.3.2. Data from process SCADA

In some circumstances it may be desirable for a central control room system to extract data from a remote process SCADA system rather than from the process automation PLC. This may be applicable where processed data is available in the process SCADA, or where historical or other tabular data provided by the remote process SCADA is desired at the central system.

There are several ways this can be achieved.

**OPC to process SCADA server**

OPC-DA is a recommended connectivity solution between Schneider Electric’s ClearSCADA remote SCADA and Vijeo Citect process SCADA solutions.

OPC provides an open connectivity solution between process control software systems. The most common OPC interchange standard for current value data is OPC-DA. It provides a tag browser interface for identification of data, and relies on COM or DCOM communication as the transport mechanism.

OPC XML-DA is similar to OPC-DA for interchange of current value data, using XML and web services transport. This can ease inter-system configuration and security deployment.

In a remote connection between a central control room remote SCADA and a process SCADA system, this architecture using OPC depends on a reliable IT network connection, with applicable security settings.

In a typical multi-site architecture, a central ClearSCADA system would operate as an OPC client. Process SCADA software would operate as an OPC server.

**ODBC / SQL to process SCADA server**

ODBC/SQL is one of a number of database connectivity solutions that can be used in multi-site architecture.

The central control room SCADA would typically be an ODBC/SQL client. The process SCADA software would be an ODBC/SQL server and may present real-time and/or historical data through its ODBC/SQL interface when the central control requests data.

In the case of the process SCADA server presenting real-time data via ODBC/SQL, a central ClearSCADA system can utilize its ODBC client to directly interrogate the process SCADA database and represent it as current data in the central control room SCADA database.

Transferring historical data into a central system typically requires a customized approach as a result of specific system implementation differences in historical database organization. There are
ways to address a solution for historical data, for example using a custom external historical transfer application, or using the ClearSCADA ODBC client to extract data from the process SCADA database with custom ClearSCADA logic to organize and insert data into the ClearSCADA historian.

This architecture using ODBC/SQL depends on a reliable IT network connection, with applicable security settings. Similar technology such as OLE/DB could also be used.

In general, this approach is complex for a tightly integrated central control room and process site solution, in particular if historical data integration is required. Other alternatives, as described throughout this section, should be considered if possible.

Process SCADA server as a DNP3 / IEC 60870-5 slave

Remote SCADA protocols such as DNP3 or IEC 60870-5 can be used to connect a central ClearSCADA system to process SCADA systems, if the process SCADA can present its data as if it were a slave device with these protocols.

For example, ClearSCADA can provide functionality of “DNP3 slave” and “IEC 60870-5 slave” with emulation as an RTU device. Any data from the ClearSCADA object database, regardless of how it is collected by ClearSCADA, can be represented through one of these telemetry protocols. ClearSCADA supports operation as a slave device with permanent remote links, non-permanent remote links and connection-on-demand links between the remote ClearSCADA server and the central SCADA system.

In summary, a remote ClearSCADA system on a process site can be a “slave” to a central ClearSCADA system.

Using the buffered, time-stamped event reporting capability of DNP3 or IEC 60870-5 protocols, ClearSCADA RTU slave components can provide a simple and reliable way to integrate historical, alarm and current value data from a remotely located process automation system into a central system without the need for customized historical data transfer.

This architecture can be used over business network infrastructure, but is also suitable where the link between the remote process automation system and central system is:

- Using discontinuous communications (PSTN, radio link, cellular IP, and so on),
- Has low bandwidth or is not an IP network

6.3.3. Multiple large process automation systems

Each of the techniques described above typically provides a subset of important operational information from a process to a central control room. Where an organization owns multiple large process systems and a central control room system, it can become difficult to maintain duplicate configuration and operational data sets for the separate process and central systems.
A solution to the challenge for multiple large process and central systems is provided by the ClearSCADA multiple server set architecture, where ViewX display clients can concurrently connect to multiple ClearSCADA databases.

When ClearSCADA is deployed as both a process SCADA platform and a centralized remote SCADA platform, both types of systems can be operated and managed together in a seamless, single environment. This affords major operational benefits and opportunities:

- Process sites can be operated remotely and transparently from a central control room
- The central control system and other process sites can be operated remotely and transparently from a process site
- A single logon can apply security access restrictions across all operational areas

This architecture provides a highly integrated solution, but with the benefit of distributed robustness. The central system and each process system are deployed with their own ClearSCADA database and server set, but these are seamlessly combined for operational display and management through the ViewX display clients including:

- Combined alarm lists
- Combined mimic displays
- Combined trend displays
- System navigation

Each ViewX display client can support integrated connection with up to 64 ClearSCADA server sets.

This architecture requires higher capacity IT communication links, compared with other remote multi-site solutions described above, in order to provide operational links between remote process systems and the central system.

Using ClearSCADA in combined remote and process architectures as shown in Figure 53 provides an integrated solution for operations and maintenance of remote and process SCADA systems.

Figure 53 depicts a color associated with the database for each SCADA server system. The remote SCADA is shown with a red database, Process #1 SCADA as a green database and Process #2 SCADA a yellow database.
When using ClearSCADA as solution for the servers and clients in this architecture, each display client in the system can optionally be a client to any of the SCADA servers, as indicated by the colors on the display clients. In this example, an operator client at the Process #1 site can visualize the Process #1 SCADA server database (green). A second operator client can visualize both Process #1 and Process #2 SCADA server databases (green and yellow). Similarly at Process #2 site, both Process #2 and Process #1 SCADA server databases can be visualized.

At the central operations center, an operator client can visualize the remote SCADA database (red). The second operator client can visualize the remote SCADA and both Process #1 and Process #2 SCADA databases. Similarly, engineering workstations at the central operations center, at the Process #1 site and at the Process #2 site can maintain SCADA database systems from any of the three locations.

The client/server combinations using ClearSCADA can support up to 64 separate connections to server database systems. Each of these connections can support redundancy server sets.

Figure 53: ClearSCADA multi-site architecture for remote SCADA and process sites
6.4. Remote communication network architecture

The following sections describe various architectures for communication solutions to answer the challenge of remote SCADA. A mix of private and public communication infrastructure is shown. Not all solutions will be applicable to all situations. This is an area of remote SCADA design that in particular requires careful consideration.

**Note:** Where a public infrastructure communication network (including Internet as well as other infrastructure) is used to interconnect parts of a remote SCADA system, careful attention should be paid to system reliability and security. It is generally accepted best practice not to use public infrastructure for critical applications and defense-in-depth security should be deployed.

6.4.1. Wide area wireless network

Trio radio solutions solve a number of challenges in wireless networks including ease of deployment, high reliability and ease of maintenance with integrated diagnostic information for on-going system support.

The Trio radio architecture provides collision avoidance in multi-point systems, ideal for DNP3, IEC 60870-5 and Modbus remote SCADA networks. This allows remote system maintenance as well as unsolicited reporting, peer-to-peer communications and multiple master communications to be managed concurrently across the same wireless network. Trio radios also support multiple communication protocols to run at the same time over the same radio link.

Serial and Ethernet radio variants, available in licensed and license-free models, are available in the Trio range. Also see 4.4. and 5.5. to help choose a remote communication network technology.

In general, serial communication is a simpler approach to communication where a single protocol provides the services necessary for remote SCADA communication. It is efficient, allowing optimization of communications to a large number of systems on the same communication link. Licensed narrowband radio systems with their inherent reliability often use serial communications to maximize communication efficiency.

Ethernet wireless communication is well suited to applications where IP connectivity is a critical part of the communications or SCADA solution. Multiple protocols (including native Ethernet or encapsulated serial over Ethernet) and multiple applications are possible, although careful consideration of security, bandwidth and the management of unnecessary Ethernet network traffic must be considered.
Optimized wireless network (point-to-multipoint model)

The optimized wireless network architecture provides a level of functionality suitable for an entry level solution or a solution with basic functionality. A typical point-to-multipoint architecture for remote SCADA networks uses a radio as an entry point (sometimes called a base or access point) to communicate with multiple remote radios. This type of network is applicable to licensed and unlicensed radio systems.

This architecture suits applications when the entry point radio has good RF coverage to all the other remote radio sites. The entry point radio is the first radio connected to, or in a chain of connections between, the SCADA LAN and the remote communication network.

In a licensed radio network, the entry point radio is often a 19" rack mounted base type, providing higher transmit power and higher duty cycle, enhanced reliability and additional diagnostic information. In both licensed and license-free systems, the entry point radio is responsible for management of collision avoidance as it is the only device which can communicate to all others directly.

Diagnostics are available for each radio in a Trio system through a single connection to one of the radios. Typically a connection is made between the entry point radio and a serial port on the remote SCADA server. Alternatively, a diagnostics connection can be made from the entry point radio to a diagnostics host PC using the Trio eDiags feature, or using a SCADAPack E RTU serial port configured for a TCP service port.

Figure 54: Optimized wireless network (point-to-multipoint model)

Where an Ethernet wireless network is deployed, for example using Trio J-Series radios, the entry point radio can be connected directly to the SCADA LAN, although careful consideration needs to be given to the LAN traffic that will end up on the wireless network. In some cases, it may be necessary to use an external router.

Where a serial wireless network is deployed, for example using Trio E-Series or K-Series radios, the entry point radio can be connected directly to a serial port on the remote SCADA server, to a serial port on a terminal server, or to an RTU as a communication gateway (e.g. SCADAPack or...
SCADAPack E RTU). Where mixed Ethernet and serial communication is required, serial traffic can be encapsulated within TCP or UDP communications over IP and converted to serial using the embedded terminal server features of the Trio J or Ethernet E Series radios.

Wide area wireless network (point-to-multipoint with repeater)

This architecture utilizes a radio repeater (a remote radio as a bridge / access point). It is particularly useful where the entry point radio does not have good RF coverage to the rest of the system. Repeaters are typically located at a site of high elevation (water tank, mountain top and so on) which offers maximum RF coverage over the target area of remotes.

This type of architecture is suited to both licensed and license-free radio bands. The operation is the same as the point-to-multipoint network described above, although network latency will be longer as the repeater must first receive data before retransmitting it to other devices.

Figure 55: Optimized wireless network (repeater / bridge model)

In licensed applications, there is a significant benefit to using a full duplex capable radio when deployed as a repeater (bridge). The reason for this is that a full duplex radio is capable of receiving and transmitting at the same time. The repeater is also responsible for managing collision avoidance and if full duplex capable, can indicate to other remote radios when the channel is busy.

In license-free applications, multiple repeaters (bridges) can be deployed in a network to provide wide area coverage.
Wide area wireless network (hierarchical model)

You can design an integrated radio system to cover challenging terrain, and over very wide areas, with a radio backbone and/or RTU routers, Ethernet switches and so on.

In such systems, point-to-point links are commonly used for interlinking multiple point-to-multipoint systems. This type of architecture is well suited to licensed radio bands, particularly to systems using DNP3 protocol where SCADAPack E RTUs can route across a large number of wireless connections, reducing traffic on sub-networks through directed routing. Standard SCADAPack RTUs can be used to store-and-forward Modbus communications through two levels of network. RTUs make ideal telemetry protocol routers for distributed networks and SCADA LAN gateways as they have multiple ports, support telemetry protocol routing, and are collocated with other equipment that can benefit from power monitoring, physical security monitoring, backup battery monitoring and so on.

Trio radios also provide the ability to interlink systems using Trio radio equipment alone, supporting protocol forwarding without the use of RTU routers. This can be useful to IEC 60870-5-101 and Modbus communication which don’t inherently allow for protocol routing.

Figure 56: Wide area wireless network (hierarchical model)
6.4.2. Cellular IP network

Cellular IP communication relies on public infrastructure networks from a telecommunications provider.

**Note:** Where a public infrastructure communication network (including Internet as well as other infrastructure) is used to interconnect parts of a remote SCADA system, careful attention should be paid to system security. Best practice and defense-in-depth security should be deployed.

System availability requirements for your application should be carefully analyzed if you are considering using public infrastructure communication systems. For more information see 5.6.2.

**Cellular IP (small model)**

Cellular IP modems at each remote site can connect to an RTU device to provide communication connectivity for remote SCADA.

Serial or Ethernet interfaces are available; each may potentially be suitable for different RTU devices in different applications.

For example:

- SCADAPack E RTU supports both Ethernet and serial (PPP) cellular IP modems for remote SCADA IP connectivity, including dynamic IP
- Standard SCADAPack RTUs support Ethernet modems
- M340 PAC with RTU module supporting Ethernet, including PPPoE DSL modems and serial (PPP) cellular IP modems

In the case of serial PPP cellular IP modem connections, the SCADAPack E RTU can manage the configuration of the cellular modem through initialization strings, allowing installation and maintenance of the modem without complex configuration.

Cellular dynamic IP addresses for remote sites can also be managed by the SCADAPack E RTU, as long as the central modem has a static IP address. See Remote SCADA and cellular dynamic IP addressing in 5.6.2.

In the following small model architecture for cellular IP networks, the connection of the network to the SCADA LAN is by way of an entry point cellular IP modem, local to the control room systems.

This architecture is suitable where there are a small number of remote systems. The cellular IP modem is operating in a “1-to-many” topology and may be constrained to providing a total system throughput equivalent to that of one remote device. A large volume of data coming from the remote sites, or anticipated to come from the remote sites in abnormal operating conditions or where system expansion is expected, may exceed the capacity of the entry point modem to
receive the data from the cellular network (even if its communication interface is Ethernet). In this case, use the large model cellular architecture, below.

Where the entry point cellular modem provides a PPP serial connection, a device such as a SCADAPack E smart RTU can be used as a remote communication gateway, connecting to both the entry point cellular modem and the SCADA LAN.

Where security measures provided by the modem and telecommunications network are deemed sufficient (i.e. the network is not on the public Internet, the service includes VPN and so on), a connection may be made from the modem to a communication gateway RTU, or directly to the SCADA LAN. Otherwise, additional security equipment, such as a firewall, should be used.

![Cellular IP Network Diagram](image)

**Figure 57: Cellular IP network (small)**

**Cellular IP (large model)**

Similar to the cellular IP small model, cellular IP modems at each remote site can connect to an RTU device to provide communication connectivity for remote SCADA.

In this large model architecture for cellular IP networks, the connection of the network to the SCADA LAN is by way of a ‘backhaul link’ from the telecommunication provider’s network.

This a common architecture for medium to large systems and where volumes of data coming from remote sites can be anticipated to be higher under certain operational conditions, or where network data usage is expected to expand over time.

As described above, a SCADAPack E RTU can automatically configure a serial cellular modem, easing the installation and long term maintenance of the modem without independent complex configuration in the modem.
Cellular dynamic IP addresses at remote sites can also be managed by a SCADAPack E solution. See Remote SCADA and cellular dynamic IP addressing in 5.6.2.

The backhaul link is typically in the form of a business IT connection, and may provide VPN services to the remote cellular network. It may use communication links such as Frame-Relay, DSL, or may use existing physical business network links such as fiber optic. It may use existing equipment such as IT routers. Talk to your telecommunications provider and IT network administrator for the architecture best suited to your application.

![Cellular IP network (with backhaul)](image)

**Figure 58: Cellular IP network (with backhaul)**

**Remote SCADA and cellular dynamic IP addressing**

Where only dynamic IP addresses are available from a telecommunications provider for cellular IP communications (e.g. GPRS), the architecture shown in Figure 59 can be used. This solution uses DNP3 telemetry protocol with a SCADAPack E as a gateway RTU on the SCADA LAN, and SCADAPack E RTUs at remote sites.

A SCADAPack 300E can be used as a gateway for up to approximately 25 remote RTUs. A SCADAPack ES can be used for up to 90 remote RTUs. The architecture can be extended to operate with more additional gateway RTUs for a larger number of cellular IP remote RTUs.

(It may be possible to use DNP3 RTUs other than SCADAPack E devices at remote sites, however there are specific requirements that must be provided such as using DNP3/TCP and detecting a renegotiated IP address as a trigger to sending a DNP3 TCP Keep-alive message or unsolicited response).

The gateway RTU uses the SCADAPack E DNP3 network routing table features to dynamically track changes in each remote RTU’s IP address, updating the network table routing entry on behalf of communications between the RTU and master station. The remote RTUs and the
master station use a static IP address for the communication with the gateway RTU for all communication transactions.

Using this architecture it is possible to use the SCADAPack E gateway RTU to route cellular dynamic IP communication between:

- Redundant remote SCADA servers to remote sites
- Maintenance terminal(s) on the SCADA LAN to a remote site
- Maintenance terminal at remote sites to other remote sites
- Peer-to-peer communication between remote sites

Figure 59: Architecture for remote network using cellular dynamic IP addressing
6.4.3. **Landline / PSTN network**

Landline and PSTN communication rely on public infrastructure networks from a telecommunications provider.

**Note:** Where a public infrastructure communication network (including Internet as well as other infrastructure) is used to interconnect parts of a remote SCADA system, careful attention should be paid to system security. Best practice and defense-in-depth security should be deployed.

Availability requirements for the communication system should also be considered.

Where leased circuits are used, each modem at the remote SCADA master station may be used in a point-to-point link with one remote RTU, or used in a point-to-multipoint link with multiple RTUs on each link. Cellular communication cannot be used with leased circuits.

In the case of point-to-multipoint links, ClearSCADA can directly control the serial port hardware control lines of the modem as it transmits data to each remote RTU in turn. Typically no front-end communication processor is required, although care should be taken in the choice of terminal server or serial controller used such that it allows control of the serial port hardware control lines in real time.

SCADA server redundancy is often a consideration when arranging communication equipment such as modems. In this architecture it is common for two sets of modems to be installed, with tie-lines between the modems sets so that the duplicate modems share the same physical communication circuits. ClearSCADA arbitrates between the modems in this arrangement, typically with one set being active at a time.

![Figure 60: PSTN / cellular dial-up remote communication](image-url)

For PSTN connections, modems are provided at the remote SCADA master station to support out-going connections to remote sites (dial-out) and potentially in-coming connections initiated...
from the remote sites (dial-in). Cellular communication is compatible with this dial-up architecture by using the appropriate cellular modem (e.g. GSM modem).

Standard SCADAPack RTUs support this architecture when using Modbus protocol. SCADAPack E RTUs support this architecture when using DNP3 protocol.

In the case of PSTN links, ClearSCADA can directly control the serial port hardware control lines of the modem to ensure reliable modem communication. ClearSCADA directly dials the modem with knowledge of remote site phone numbers. No front-end communication processor is required, although care should be taken in the choice of terminal server or serial controller used such that it allows the serial port control lines to be managed.

6.4.4. High availability remote network

High availability remote network (using PSTN)

A combination of communication types can increase the availability of a remote communications network. It is common for critical remote sites to be provided with both a primary and a fall-back communication link.

In the following example, a wireless network based on Trio radios forms the primary communication link to all sites. Critical sites have a fallback link using PSTN. Both links are connected to the RTU to increase communication availability.

PSTN links can use a combination of telephone line and cellular dial-up as appropriate to the remote site installation.

ClearSCADA, for example, provides native support for primary and fallback communication links for remote SCADA when using DNP3 or Modbus protocols.
In the following example, a wireless network based on Trio IP radios forms the primary communication link to all sites. Critical sites have a fallback link using Cellular IP. This architecture provides a high level of independence between the IP links, while providing full remote communication capability through the use of IP on both the primary and fallback links.

The two independent links are connected directly to the RTU. In the case of a serial cellular IP modem, the SCADAPack E RTU provides automatic configuration of the modem.

The operational cost of this architecture is low due to the use of private wireless infrastructure as the primary communication link.

ClearSCADA provides primary and fallback communication links as a native feature when using IP communication with DNP3, IEC 60870-5 and Modbus protocols.
6.4.5. Remote communication network links to diversely located servers

To benefit from the availability and business continuity advantages of diversely located SCADA servers, systems must be designed such that loss of the communication link from a main server to the remote communication network should not affect communication between a standby server and the remote communication network. To achieve increased availability, there should be no communication link dependencies between the two server systems and the remote communication network.

It is common for IP networks to interconnect SCADA servers and remote communication networks, particularly when the SCADA servers are located in enterprise data centers or utilize business network connections. Careful attention should be given to the IP network infrastructure design that links the remote communication network to the servers to ensure there are no common modes of failure between the networks.

Further, the IP network communication infrastructure used for linking the main / standby servers should be independent of the links from all the main and standby SCADA servers to the remote communication networks.

Where multiple communication links are provided to a remote site for high availability of the remote communication system, all sets of remote communication links must be available to all main, standby and triple standby server locations. As described above, all the remote communication links must operate independently from each other, and be independent from all the links used for inter-server connections.
6.5. Remote site architecture

The following sections describe architectures for remote sites, showing how RTUs integrate with field equipment for common remote SCADA solutions.

Particular field implementation requirements vary according to the industry segment and specific application. Schneider Electric water solution architectures, for example, describe a remote site architecture known as “R2” using SCADAPack E RTUs and other field devices. This section shows architectures consistent with those described for “R2” solutions.

Adapt these architectures according to application requirements.

6.5.1. Field equipment using physical I/O

RTUs include physical input and output (I/O) connections to field equipment.

Signals received by an RTU on inputs can be reported directly (unprocessed) to the remote SCADA master station. Inputs can also be utilized by RTU user logic in combination with other inputs and data to derive information (through calculation or accumulation). RTU inputs comprise:

- Digital inputs (on-off state such as a valve open or closed, a motor running or stopped, represented, for example, through the presence or absence of a 24VDC input signal)
- Analog inputs (value of a continuous quantity such as a flow or a level, represented, for example, through a 4-20mA output signal)
- Counter inputs (counting discrete quantities such as volume from flow meter pulses, provided by a contact closure or an electrical impulse)

User written RTU logic and commands directly received from the remote SCADA master station can be used to directly control outputs. RTU outputs comprise:

- Digital outputs (on-off state to open or close a valve, start or stop a motor, represented, for example, through pulsing or latching a relay)
- Analog outputs (a continuously variable quantity to adjust, for example, a motor speed or adjust the position of a valve; provided through a 4-20mA output signal, for example)

In compact RTUs such as the SCADAPack and SCADAPack E smart RTU, I/O is integrated with the RTU in the same device as the processor unit, power supply and, in some cases, remote communication device. This provides a cost effective and highly functional RTU, with low power consumption and small footprint. The I/O on a compact RTU can be expanded through the installation of optional I/O modules. I/O on expansion modules operate in the same way as I/O integrated in the compact RTU device.
In modular devices such as the M340 PAC, the processor unit, power supply, I/O, communication port and additional RTU module units are provided as separate plug-in modules. These modules are assembled individually onto a mounting plate. This provides flexibility in device configuration.

An RTU can provide an interface for digital, analog and counter inputs, including derived data, to a remote SCADA master station, and accept controls for data from a remote SCADA master station using protocols such as DNP3, IEC 60870-5 and Modbus. Changes in data can be time-stamped when using event-driven telemetry protocols such as DNP3 and IEC 60870-5.

The RTU connects to a communication device providing access to the remote communication network. This connection to a serial port or Ethernet port on the RTU is dependent on the remote communication equipment and remote network type.

A local configuration and maintenance terminal can be connected to the RTU for configuration, logic configuration, diagnostics, and so on. Many RTU devices support USB for easy connection to a local maintenance terminal. Serial and Ethernet interfaces can also be used for local configuration and maintenance.

![Figure 63: SCADAPack smart RTU with physically connected field I/O](image)

### 6.5.2 Field equipment using physical I/O and data connections

In addition to field equipment connection through physical I/O as described in the previous section, smart RTUs include rich communication capabilities for interacting with smart field devices through data connections. The following data interfaces are provided by Schneider Electric smart RTUs and network equipment for data connection to external devices:

- Multiple RS232 / RS485 serial ports on SCADAPack and SCADAPack E smart RTU
- Ethernet port on SCADAPack, SCADAPack E, NOR0200H RTU module for M340, M340 processor (dependent on processor model), M340 Ethernet module
- Serial port on M340 processor (dependent on model), NOR0200H RTU module
Dual Ethernet ports on SCADAPack ES smart RTU

Managed Ethernet ports using ConneXium Ethernet managed switches

CANopen fieldbus port on M340 PAC processor (dependent on processor model)

Many field devices with data interfaces communicate using a Modbus family protocol. Users should carefully examine the protocols supported by field devices to ensure compatibility with the RTU. Aspects of data communication should be checked for compatibility including:

- Physical interface and cabling (check if RS232 hardware handshaking is required. Check if RS485 connections - especially if over long distances- require isolation or biasing. Check that the Ethernet cabling is correct)

- Protocol type (check that the RTU expected to be the master or the slave device)

- Specific protocol format (e.g. “Modbus” isn’t a generic protocol. Modbus RTU, Modbus ASCII, Modbus/TCP, Modbus RTU in TCP, Modbus/UDP are all different in important ways. Check which variant of Modbus is actually required)

- Data types required (check if data is to be exchanged as packed binary bits in an analog register, as 16-bit signed integers, 32-bit unsigned integers, 32-bit floating point format. Check that both the RTU and the field device support all required types)

- Data address ranges (check that both the RTU and field device support the device addressing and data addressing requirements)

See protocol and interface information in 4.5.2. for SCADAPack Smart RTU, SCADAPack E Smart RTU and M340 PAC with additional RTU module.

Example field devices that can interface with an RTU are shown in Figure 50. In practice, a wide range of devices can interact with an RTU for integration with remote SCADA.
In general, the RTU and field devices exchange data locally. The data an RTU receives from a field device can be processed locally by a logic sequence for calculations and for local control decisions. The data can also be presented through the telemetry protocol, taking advantage of the RTU’s integration with the remote SCADA facilities that would not normally be available for field device data. For example, constantly changing process data from a local instrument can have a deviation and alarm limits applied by the RTU and have its data available for RTU event reporting to the remote SCADA; Changes in the process data can be buffered if the communications link to the remote site is lost. When communication is restored, the history of changes can be automatically integrated into the SCADA historical database. A process data problem can cause the RTU to generate an alarm with accurate time-stamping. If the alarm is sufficiently critical, the RTU can generate the event and immediately generate an unsolicited response to send it to the master station.

The following table describes example field devices and how they can be used to interact with an RTU. It includes field devices shown in Figure 64 (?) and throughout this document.
### Field device connections to a smart RTU

<table>
<thead>
<tr>
<th>Field device</th>
<th>Application examples</th>
<th>Physical interface</th>
<th>Protocol used by RTU</th>
<th>Protocol used by field device</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simple sensor</td>
<td>Pressure, flow, level, temperature, switch, ...</td>
<td>I/O, 4-20mA</td>
<td>Modbus RTU master, Modbus/UDP client, Modbus/TCP client</td>
<td>Modbus RTU slave, Modbus/UDP server, Modbus/TCP server</td>
</tr>
<tr>
<td>Intelligent sensor</td>
<td>SCADAPack multi-variable transmitter, SCADAPack flow computer, pressure sensor, flow meter, level sensor, ...</td>
<td>RS485, RS232 or Ethernet</td>
<td>Modbus RTU master or Modbus/TCP client</td>
<td>Modbus RTU slave or Modbus/TCP server</td>
</tr>
<tr>
<td>Motor starter</td>
<td>Altivar ATV variable speed drive, soft-starter</td>
<td>RS485 or Ethernet</td>
<td>Modbus RTU master or Modbus/TCP client</td>
<td>Modbus RTU slave or Modbus/TCP server</td>
</tr>
<tr>
<td>Wireless sensor network</td>
<td>Accutech wireless instrument base radio (remote pressure, flow, level sensors)</td>
<td>RS485</td>
<td>Modbus RTU master</td>
<td>Modbus RTU slave</td>
</tr>
<tr>
<td>HMI</td>
<td>Magelis HMI local display</td>
<td>Ethernet or RS232</td>
<td>Modbus/TCP server</td>
<td>Modbus/TCP client</td>
</tr>
<tr>
<td>Gas chromatograph</td>
<td>Pipeline flow calculation</td>
<td>Ethernet or RS485</td>
<td>Modbus/TCP client</td>
<td>Modbus/TCP server</td>
</tr>
<tr>
<td>Power meter</td>
<td>Ion power meter, energy management monitoring</td>
<td>Ethernet, RS232 or RS485</td>
<td>DNP3 master</td>
<td>DNP3 slave</td>
</tr>
<tr>
<td>GSM modem</td>
<td>SMS alarm dialer</td>
<td>RS232</td>
<td>Custom ASCII</td>
<td>Hayes command set</td>
</tr>
</tbody>
</table>

### 6.5.3. Highly available, security-enabled remote site

#### Improving remote communication availability

At critical remote sites, an alternate (backup) communication path between the control room and remote RTU can improve remote communication availability. For example, a primary digital remote radio network could be augmented by a cellular IP link, PSTN connection and so on. Other combinations are supported as described in 5.6.5. A key architectural consideration in achieving improved availability is the installation of primary and backup links that are highly independent. There should be no common modes of failure in the final system design. Consider the use of independent power supplies, separate the communication link entry points into the remote site, and ensure there are no external shared dependencies (e.g. telecommunications provider infrastructure).

Consideration could be given to separating an inter-site communication link (for peer-to-peer communication) from the remote communication network to the control room. This may be advantageous where the remote communication network is complex such as when it is provided.
by a telecommunications carrier and where inter-site control reliability is more important than communication with the control room. In many cases, such as when using digital remote radio networks, inter-site communication and control room communication can share the same reliable remote communication infrastructure.

Figure 65: SCADAPack smart RTU in highly available, security-enabled architecture

Telemetry protocol security

For remote network communication using DNP3, the SCADAPack E Secure Authentication option or AGA12-2 Encryption option can enhance remote security as described in 5.8.7. These architectures provide solutions for secure local and remote configuration as well as remote SCADA communication.

Trio digital remote radio network solutions offer on-air AES encryption for transmitted data (subject to country availability).

In the architecture shown in Figure 65, telemetry protocol security options can enhance security for remote communication, backup communication, peer-to-peer communication and local access links.
Remote site network security

Remote site Ethernet networks can be secure using Schneider Electric’s PlantStruxure architectures. In particular, the ConneXium Managed Ethernet Switch and ConneXium Industrial Firewall product ranges can provide security solutions for simple through complex remote site networks.

6.5.4. Example remote site architectures

The following architectures are defined in Schneider Electric’s Water & Wastewater solutions remote pumping station reference architectures. These provide examples of designs using Schneider Electric products, and include architectures for telemetry and remote SCADA.

Each of the architectures includes a metering device, motor starters and drives. The energy meter provides performance analytics. This includes enhanced operation optimization through the ability to integrate with water network management and advanced process control applications.

The interconnection of the RTU / PAC equipment with motor starters and drives allows the aggregation of operational performance data with energy management data, enabling business and enterprise applications to optimize energy usage.

“R2” remote water station architectures

The “R2 Optimized” architecture is suitable for monitoring and control of simple assets and plant such as water tanks, value control stations, storm basins, ground water wells and basic pumping / lifting / boosting stations. It uses a SCADAPack E RTU to provide coordination of site monitoring, control and remote communication.
The “R2 Advanced” architecture is suitable for monitoring and control of more complex water pumping stations and wastewater lifting station sites. This would typically involve up to five pumps with additional I/O for condition monitoring, smart motor starters, variable frequency drive controllers and so on. A higher capability SCADAPack E RTU is often used, supporting communication with several smart devices at the control site. Some site designs may include a backup control system such as simple level control interlocks with the starter electrical panel, or may use a simple PLC.

“R3” large autonomous water station architectures

The “R3” architectures are suitable for complex control of large autonomous stations such as complex water pumping stations (e.g. six or more pumps of varying sizes) and additional auxiliary functions at those stations (e.g. backup generator control).

The centralized architecture provides in-rack I/O to suit stations using a central I/O wiring design. The distributed architecture provides multiple I/O racks to suit stations using a distributed I/O wiring design.
Figure 67: M340 PAC with RTU module in “R3” centralized and distributed large autonomous sites

For more information on application architectures, refer to detailed Schneider Electric System Technical Note (STN) and Tested Validated Documented Architecture (TVDA) documentation.
## 7. Appendix

The following table describes the acronyms and defines the specific terms used in this document.

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AGA12</td>
<td>A standard telemetry protocol definition providing encryption and other security services for telemetry protocols (e.g. DNP3). Originally developed for the American Gas Association by the Gas Technology Institute. Adopted by the IEEE as standard IEEE 1711</td>
</tr>
<tr>
<td>Authentication (security)</td>
<td>A security mechanism establishing confirmation of the identity of two devices interchanging information with each other. For example, DNP3 provides secure authentication services using the IEC 62351-5 standard</td>
</tr>
<tr>
<td>Balanced (SCADA protocol)</td>
<td>Terminology used in IEC protocols to describe a communication architecture where either a master station or outstation may initiate transmission at any time. Balanced communication is only supported between two interconnected devices (physically or logically). For example IEC 60870-5-101 protocol supports balanced mode when two serial devices are directly interconnected, but not when the link is shared by more than two devices. Unbalanced transmission is used in this case. IEC 60870-5-104 protocol supports only balanced mode IP communication (does not support unbalanced mode). DNP3 provides a hybrid of balanced and unbalanced operation</td>
</tr>
<tr>
<td>Base (radio)</td>
<td>A communication device typically located centrally within a radio network to provide a wide area of radio path coverage. Usually transmits at a higher power level than remote radios and is optimized for high transmission duty cycle. Hot-standby base equipment increases system availability</td>
</tr>
<tr>
<td>CANopen</td>
<td>Controller Area Network fieldbus standard for interconnecting field devices</td>
</tr>
<tr>
<td>ChannelShare™</td>
<td>Trio wireless network collision avoidance features permitting devices across multiple radios to initiate communication at the same time. Allows a shared Trio radio network to support multiple masters as well as unsolicited reporting from multiple devices at the same time</td>
</tr>
<tr>
<td>COS Change of State</td>
<td>The generation of an event as a result of a point changing state (e.g. a binary point state change from Off to On, or where a point quality changes)</td>
</tr>
<tr>
<td>COV Change of Value</td>
<td>A change in analog point value. A significant or interesting change may result in the generation of an event. A significant change may be a specific deviation from a previous value. An interesting change may be a value exceeding an analog limit</td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Compact RTU</td>
<td>A highly functional remote terminal unit in a single device package that combines smart RTU functionality, internal and expandable physical I/O, integrated communication interfaces, and with control logic capability, typically using IEC 61131-3 languages for control logic. Also see RTU</td>
</tr>
<tr>
<td>Configurator</td>
<td>Software tool providing a configuration interface for communication to a local or possibly remote device for the purpose of setting device behavior, commissioning, maintaining and/or diagnosing the device</td>
</tr>
<tr>
<td>Critical infrastructure</td>
<td>Assets essential for the functioning of society and the economy. E.g. electrical generation, transmission and distribution, water treatment and distribution, gas and oil production, transportation and distribution</td>
</tr>
<tr>
<td>Cybersecurity (SCADA)</td>
<td>See Security (SCADA)</td>
</tr>
<tr>
<td>Data concentrator</td>
<td>The collection of data in an intermediate device known as a Data Concentrator or Sub-master, from remote RTUs or other smart devices (e.g. IED devices). The data concentrator presents the data from multiple downstream devices to an upstream master station or other data concentrator as a single device</td>
</tr>
<tr>
<td>Data concentrator</td>
<td>A device collecting data from, and managing multiple RTU devices (in a similar way to a Master Station), and collating the information using the functionality of an RTU. (A data concentrator is also known as a sub-master). Typically the data collected from multiple downstream devices (e.g. RTUs) is presented to an upstream master as a single RTU. It preserves the remote information content such as point quality and time-stamped events, and manages communication with the downstream devices</td>
</tr>
<tr>
<td>DCS</td>
<td>Distributed Control System</td>
</tr>
<tr>
<td>Deadband</td>
<td>An amount by which a value change is ignored. Value deadbands are commonly associated with analog points and their alarm limits, such that small variations in the analog value above and below the alarm limit do not cause successive alarms. Similarly, time deadbands dampen successive alarms within a given time period</td>
</tr>
<tr>
<td>Defense-in-depth</td>
<td>A multi-layered approach to securing a system. Also see definition of Security (SCADA)</td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Deviation</td>
<td>The change in the value of an analog point value. A change greater than or equal to a particular absolute or percentage deviation may be considered “interesting,” resulting in the generation of an event. A particular change in value may be considered “interesting” when it changes by a significant amount in a short period of time. Alternatively, changes in values of the same point may also be interesting when changing by a smaller amount but over a longer period of time. Capturing these types of changes as events uses integrating deviations</td>
</tr>
<tr>
<td>DSL</td>
<td>Digital Subscriber Line. Wide area communication technology provided by telecommunications carriers for medium to high speed data communication, typically as a Wide Area IP Network</td>
</tr>
<tr>
<td>DMZ</td>
<td>De-militarized zone. An IT term used to describe a small network segment inserted as a “neutral zone,” providing security isolation between networks that have different purposes (e.g. between SCADA network and enterprise network; between a company network and public network)</td>
</tr>
<tr>
<td>DNP3</td>
<td>Distributed Network Protocol. An open standard telemetry protocol widely adopted in the Electrical and Water industries in many geographic areas, including across the Americas, Australia, China, some parts of SE Asia and South Africa. Also used in other sectors such as Renewable Energy, Mining, Environmental. Also known as IEEE standard IEEE 1815</td>
</tr>
<tr>
<td>Dynamic IP (cellular)</td>
<td>Where a telecommunications carrier providing a cellular IP communication service does NOT guarantee that a device will be allocated the same (static) IP address upon subsequent connections. Further, some telecommunications carriers will periodically disconnect links to devices and force different IP addresses to be allocated</td>
</tr>
<tr>
<td>EcoStruxure Web Services (EWS)</td>
<td>Schneider Electric’s Web Services standard interface (based on SOAP/XML) allowing enterprise applications to easily exchange data. Supported by ClearSCADA as part of Schneider Electric’s EcoStruxure solution architecture</td>
</tr>
<tr>
<td>EDGE</td>
<td>Enhanced Data GSM Evolution. A cellular communication standard providing data services on GSM networks</td>
</tr>
<tr>
<td>EFM</td>
<td>Electronic Flow Measurement (for gas measurement applications)</td>
</tr>
<tr>
<td>Encryption (security)</td>
<td>A security mechanism that obscures the content of messages between two devices in order to hide the information being exchanged. E.g. AGA12-2 can provide encryption services for telemetry protocols</td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Event logging</td>
<td>Where a device records important and interesting changes (events) in data that it is monitoring, storing the events in an archive that can be retrieved at a later time. Event logging is part of the key functionality supported for telemetry communication</td>
</tr>
<tr>
<td>Fallback link</td>
<td>A secondary communication link to a remote site, used if the primary link to the site becomes inoperable</td>
</tr>
<tr>
<td>Field devices</td>
<td>Instrumentation and equipment at a remote site, typically connected to a smart RTU device for monitoring and control</td>
</tr>
<tr>
<td>Firewall</td>
<td>A device or software component that examines incoming and outgoing communication between devices, permitting recognized data to pass, blocking unexpected data</td>
</tr>
<tr>
<td>Gas Modbus</td>
<td>Also known as ENRON Modbus, an adaptation of Modbus RTU (but not compatible) for supporting Electronic Flow Measurement for gas applications</td>
</tr>
<tr>
<td>Gateway RTU</td>
<td>An RTU based device often used in conjunction with a master station to handle specialty communication requirements for a remote communication network. For example as a security gateway to provide encryption services, or as an interface to a dynamic IP cellular network</td>
</tr>
<tr>
<td>GPRS</td>
<td>General Packet Radio Services provided by a telecommunications carrier for cellular IP data communication over GSM networks. Telecommunications carriers may offer various combinations of VPN services, static IP or dynamic IP features on their networks depending upon the access plan structure</td>
</tr>
<tr>
<td>GSM</td>
<td>Global System for Mobile communication. The technology at the core of many cellular telephone and cellular data networks</td>
</tr>
<tr>
<td>Host (SCADA)</td>
<td>See definition for Master Station</td>
</tr>
<tr>
<td>HSPA</td>
<td>High Speed Packet Access. A 3G cellular communication technology operating on a GSM network providing data services. Incorporates HSDPA (downlink) protocol. Modem devices supporting HSPA often support HSDPA networks</td>
</tr>
<tr>
<td>IEC 60870-5</td>
<td>A suite of standards defining an open telemetry protocol framework. This framework suite forms the basis for specific protocols for RTU communication in the power sector. The protocols include IEC 60870-5-101 and IEC 60870-5-104 for RTU, widely adopted by electrical utilities in Europe. These protocols are also used in other sectors, such as Water, and in other geographies including some parts of the Middle East, South East Asia and South America. IEC 60870-5-103 is also part of this family of protocols, specifically optimized for communication with electrical protection equipment</td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>IEC 61131-3</td>
<td>Open standard logic programming languages for automation controllers. This standard is defined and promoted by the PLCopen organization, and is adopted by all major PLC and RTU manufacturers for process control logic. The logic programming languages defined by IEC 61131-3 are Ladder Diagram, Function Block Diagram, Structured Text, Sequential Function Chart and Instruction List. (Not all devices implement all languages)</td>
</tr>
<tr>
<td>IED</td>
<td>Intelligent Electronic Device. A general description of devices that support data communications. Popular terminology in the Electric sector for devices inside a substation that support data communication (e.g. protection relays)</td>
</tr>
<tr>
<td>Integrity poll</td>
<td>A telemetry protocol request from a master device requesting that an outstation respond with any buffered event data and the current value of all points it is monitoring</td>
</tr>
<tr>
<td>IP network</td>
<td>Internet Protocol network. In the context of telemetry and remote SCADA, Internet protocol services can carry telemetry over a diversity of remote communication network media (Ethernet data radio, DSL, cellular IP)</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology. IT Network or IT Infrastructure refers to business and enterprise computing communications, within which remote SCADA can integrate and operate</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network. Also see SCADA LAN</td>
</tr>
<tr>
<td>Landline</td>
<td>A generic term referring to a wired communication service provided by a telecommunications carrier. Includes dial-up connections (see PSTN, POTS), leased lines and so on. Typically requires a modem device approved for use on telecommunications carrier’s systems</td>
</tr>
<tr>
<td>Leased line</td>
<td>A specific type of analog landline circuit provided by a telecommunications carrier. Typically requires the use of approved external modem devices. May support multi-drop or point-to-point services. Typically low bandwidth and available over long distances</td>
</tr>
<tr>
<td>Level 2 subset</td>
<td>A subset of the full DNP3 specification providing data acquisition functions and basic data object formats, including events. At the time of writing this STN, conformance tests are published by the DNP User Group for slave device certification to DNP3 Level 2. This subset is supported by standard SCADAPack RTUs and many third party RTU products</td>
</tr>
<tr>
<td>Level 3 subset</td>
<td>A subset of the full DNP3 specification incorporating all Level 2 subset features and adding point-range read requests and expanded data objects including 32-bit integer controls. Supported by the M340 PAC’s additional RTU module</td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Level 4 subset</td>
<td>A subset of the full DNP3 specification incorporating all Level 3 subset features and adding expanded data acquisition functions, expanded data objects such as output event objects, floating point data types, device name-plate attributes, XML device profile. Supported by SCADAPack E RTUs and ClearSCADA master station software</td>
</tr>
<tr>
<td>LTE</td>
<td>Long Term Evolution. Cellular communication standard for high-speed data services on GSM networks</td>
</tr>
<tr>
<td>M2M</td>
<td>Machine-To-Machine. Automated communication between devices without human intervention</td>
</tr>
<tr>
<td>Master station</td>
<td>The equipment in a SCADA system responsible for collection of data from remote RTU devices. In remote SCADA, it provides the link between data collection (using a telemetry protocol) and the end user through visualization and storage of received data in current value and historical databases. It presents data using graphical displays, trend curves and event logs. The master station typically includes an alarm management facility for presentation, archive and analysis of operational problems, including redirection of alarms to maintenance and operations personnel. High availability of a master station is often achieved through the use of distributed standby master station servers</td>
</tr>
<tr>
<td>Metadata</td>
<td>Data describing attributes of information, separate from the information itself. For example, the value of a flow being measured may be represented in a numeric format such as a floating point value. If a description of the format of the flow is included along with the value of the flow (e.g. this value is a floating point value), the format is said to be metadata</td>
</tr>
<tr>
<td>Modular RTU</td>
<td>A remote terminal unit device made up of multiple device modules typically plugged in to a base or rack. Device modules are typically chosen by the user and interconnected in an arrangement suiting the user (e.g. power supply, CPU, I/O cards, communication cards). Typically using IEC 61131-3 languages for control logic. Also see RTU</td>
</tr>
<tr>
<td>Multi-drop</td>
<td>Describing multiple devices sharing the same communication link, where transmission from a master (for example) can be heard simultaneously by multiple RTU devices</td>
</tr>
<tr>
<td>Multi-master</td>
<td>See Multiple Master Support</td>
</tr>
<tr>
<td>Multi-site</td>
<td>A system architecture providing data consolidation where operation can occur from one of a number of independently run sites. For example, interconnected process SCADA systems and a remote SCADA system, allowing sites to be fully operated from multiple locations</td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Multiple master support</td>
<td>Where an RTU supports access to its data from multiple master stations. Some RTUs allow different sets of data to be accessible from different masters; others provide the same data to all masters. Where the RTU communication uses a telemetry protocol, the RTU supports independent event lists to each master. Also known as <em>multi-master</em> architecture</td>
</tr>
<tr>
<td>Multistream™</td>
<td>Trio wireless network feature simultaneously allowing multiple communication protocols to operate seamlessly over the same radio channel</td>
</tr>
<tr>
<td>NMS</td>
<td>Network Management System providing monitoring of IP network communication equipment (such as routers and radios) and computer infrastructure, typically using SNMP protocol. Remote SCADA can integrate with enterprise NMS systems, or provide similar functionality to NMS</td>
</tr>
<tr>
<td>OPC</td>
<td>Open connectivity standards for interchange of Process Control information</td>
</tr>
<tr>
<td>Optimized architecture</td>
<td>Description of a system or subsystem providing a level of functionality suitable for an entry level solution or a solution with basic functionality</td>
</tr>
<tr>
<td>Outstation</td>
<td>See definition for <em>RTU</em>. Be aware that in different geographies, different terms are used to refer to the same type of device</td>
</tr>
<tr>
<td>PAC</td>
<td>Process Automation Controller. Equivalent to a <em>PLC</em> in this document</td>
</tr>
<tr>
<td>Peer-to-peer</td>
<td>Two like devices initiating communication with each other. For example a SCADAPack E Smart RTU can initiate specific, efficient, DNP3 data exchanges with another RTU without requiring the data to pass through a separate master device (data concentrator, master station and so on)</td>
</tr>
<tr>
<td>Plant</td>
<td>A collection of industrial machinery and associated control equipment. In the context of this STN, it refers to both <em>remote site</em> assets and <em>process site</em> assets</td>
</tr>
<tr>
<td>PLC</td>
<td>Programmable Logic Controller</td>
</tr>
<tr>
<td>Point (remote SCADA)</td>
<td>An RTU and SCADA data structure representing a value or state, embedding functionality such as point quality and parameters defining functional operation: event generation, alarm reporting, scaling and so on. Provides a depth of functionality and information associated with a measured or calculated quantity in a remote SCADA device; in comparison, a simple <em>register</em> often found in basic PLC devices represents a raw value only. A point is often referenced by its data type (e.g. binary out, analog input) and its point number. It may also have an associated description field</td>
</tr>
<tr>
<td>Polling</td>
<td>The mechanism by which a master sequentially or periodically requests data from RTUs using a <em>telemetry protocol</em></td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>POTS</td>
<td>Plain Old Telephone System. See definition for PSTN</td>
</tr>
<tr>
<td>PPP</td>
<td>Point-to-Point Protocol. A TCP/IP standard for IP communication over serial links. Used in a variety of applications, including some cellular IP modems</td>
</tr>
<tr>
<td>PPPoE</td>
<td>Point-to-Point Protocol over Ethernet. Used in DSL and other IP modems</td>
</tr>
<tr>
<td>Process network</td>
<td>A communication network operating in a contained area, providing communication between industrial devices providing process automation</td>
</tr>
<tr>
<td>Process SCADA</td>
<td>The central server, client components, automation control and communication network equipment making up a system specializing in acquiring data from a local process automation system; typically in a contained area of hundreds of meters across or less</td>
</tr>
<tr>
<td>Process site</td>
<td>A physical location containing plant (equipment) controlled by a process automation system</td>
</tr>
<tr>
<td>Protocol</td>
<td>Common data language used between devices for exchanging information</td>
</tr>
<tr>
<td>PSTN</td>
<td>Public Switched Telephone Network. PSTN service is provided by a telecommunications carrier (most commonly for human telephone conversations). Telemetry communication using PSTN typically requires the use of externally approved modems and is used with devices (such as RTUs) with connect on-demand capability</td>
</tr>
<tr>
<td>Register</td>
<td>A simple container (e.g. a 16-bit word) to represent a measured or calculated quantity in a PLC device. A register may represent a value or multiple discrete states. Multiple registers can be combined for different formats (e.g. 2x 16-bit registers to represent a 32-bit floating point value). A register may be associated with a simple tag name.</td>
</tr>
<tr>
<td>Remote SCADA</td>
<td>The central server and client components that interface with a remote communication infrastructure and field equipment as a solution for data acquisition using telemetry from a distributed remote system; typically in a widely dispersed area of thousands of square kilometers</td>
</tr>
<tr>
<td>Remote site</td>
<td>A physical location at which field devices are monitoring and controlling plant equipment and are interconnected with a smart RTU device. The RTU device communicates, using a remote communication network, to a remote SCADA master station</td>
</tr>
<tr>
<td>Repeater</td>
<td>Receives information and resends the information to other devices</td>
</tr>
<tr>
<td>Repeater (radio)</td>
<td>Wireless device that receives an “upstream” transmission and retransmits, extending the coverage of the radio system for “downstream” devices</td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>RBE</td>
<td>Literally meaning the creation of a report (data item) from an exception (data change). In DNP3 and IEC 60870-5 protocols, this means the generation and storage of event data in an RTU. <em>Report By Exception</em> is NOT a definition of how event data is transmitted (e.g. through polling from a master). Do not confuse this definition with the definition of <em>Unsolicited Response</em></td>
</tr>
<tr>
<td>Router ( IP router)</td>
<td>A multi-port device dedicated to managing message communications in an IP network through configuration rules and configuration interchange with other IP router</td>
</tr>
<tr>
<td>Routing (telemetry)</td>
<td>Functionality provided by an RTU device that directs telemetry protocol messages between communication ports, based on configured rules. Used in hierarchical remote networks when the telemetry protocol supports source and destination addressing (e.g. DNP3)</td>
</tr>
<tr>
<td>RTU</td>
<td>Remote Terminal Unit (also known as an <em>outstation</em> or <em>telemetry</em> device). Responsible for gathering and storing information at a remote site. Uses events to record time stamp and quality information, providing alarm management and communication with a master station using a telemetry protocol. Communication is optimized for widely dispersed, remote systems. An RTU typically includes physical I/O and multiple communication interfaces. Also see <em>Compact RTU, Modular RTU, Smart RTU</em></td>
</tr>
<tr>
<td>SCADA</td>
<td>Supervisory Control and Data Acquisition. Describes the equipment and infrastructure associated with the operation of industrial automation systems. See definitions for <em>process SCADA</em> and <em>remote SCADA</em></td>
</tr>
<tr>
<td>SCADA LAN</td>
<td>A local area network (typically Ethernet based) forming the communications infrastructure that interconnects master station servers to automation controller devices (e.g. PLCs) and to remote communication networks (e.g. radio, cellular IP, landline). May be separated from a business <em>LAN</em> by a <em>DMZ</em> network</td>
</tr>
<tr>
<td>SCADA system</td>
<td>A generic term sometimes referring to the <em>Master station</em>. More broadly this term refers to all parts of data gathering in an automation control system</td>
</tr>
<tr>
<td>Secure Authentication</td>
<td>Contraction for “DNP3 Secure Authentication”. See <em>Authentication</em></td>
</tr>
<tr>
<td>Security (SCADA)</td>
<td>A multi-layered (<em>defense-in-depth</em>) approach to protecting a system from unintended operation due to deliberate or accidental influence</td>
</tr>
<tr>
<td>Security gateway (SCADA)</td>
<td>A gateway RTU device that provides specific security services between a <em>master station</em> and <em>remote site</em> RTUs</td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SIM card</td>
<td>Subscriber Identity Module. Supplied by a telecommunications provider to activate cellular communication equipment (e.g. telephone handset, smart phone, cellular modem)</td>
</tr>
<tr>
<td>Smart RTU</td>
<td>A remote terminal unit that provides a high level of functionality through configuration rather than requiring logic programming. Typically includes a wide range of communication options and the ability to integrate data from a number of peripheral devices. The native functionality provided by a smart RTU can typically be extended by the user through control logic</td>
</tr>
<tr>
<td>SOAP / XML</td>
<td>Simple Object Access Protocol using Extended Mark-up Language. Often used as part of a web services protocol suite for external applications to query data from a web server. ClearSCADA provides SOAP/XML access to its databases</td>
</tr>
<tr>
<td>Spontaneous transmission</td>
<td>See Unsolicited Response</td>
</tr>
<tr>
<td>STN</td>
<td>System Technical Note. See the start of this document for more information.</td>
</tr>
<tr>
<td>Store-and-forward</td>
<td>The delivery of a data message by a device, retransmitted so that another device can receive the message. A simple (and limited) form of Routing. Also see Repeater</td>
</tr>
<tr>
<td>Sub-master</td>
<td>See definition of Data Concentrator</td>
</tr>
<tr>
<td>Tag</td>
<td>A named data item, often associated with a register in a PLC device</td>
</tr>
<tr>
<td>Telemetry</td>
<td>Conceptually: “remote measurement” Physically: refers to the components dealing with the data generation and communication aspects of a distributed remote system</td>
</tr>
<tr>
<td>Telemetry protocol</td>
<td>The “language” between widely separated devices. Typically characterized by event driven information, optimized for non-permanent or connect on-demand, low bandwidth, and long range remote communication networks, including serial lines, landline and IP networks. Examples: DNP3 and IEC 60870-5 open protocols. Many telemetry protocols are single vendor proprietary protocols, some based on industrial protocols with vendor specific extensions to adapt them for remote communication, e.g. Modbus</td>
</tr>
<tr>
<td>Terminal server</td>
<td>A device that provides serial communication ports for software application to access across a LAN. Some telemetry applications use terminal servers that support modern control-line hand-shaking, operating as if they were serial ports permanently installed inside a PC or computer server</td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Unbalanced</strong> (SCADA protocol)</td>
<td>Terminology used in IEC protocols to describe a communication architecture where an outstation will only send a response to a master station when specifically requested. The outstation must not initiate transmission at any other time. For example, IEC 60870-5-101 protocol must be operated in unbalanced mode where two or more outstations and a master station communicate on the same remote communication link. Also see Balanced</td>
</tr>
<tr>
<td>Unsolicited response (Unsolicited reporting)</td>
<td>Spontaneous transmission from an RTU without a request from a master. The data transmitted in an Unsolicited Response is typically in the form of events (previously generated and stored from an RTU’s Report By Exception mechanism)</td>
</tr>
<tr>
<td>UTC</td>
<td>Universal Coordinated Time. The global time standard independent of time zone and daylight savings time adjustment. Historically known as GMT (Greenwich Mean Time). Time zones are specified as differences from UTC. E.g. UTC-5:00, UTC+10:00</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network. A connection (sometimes referred to as a tunnel) over an IT or telecommunication network that can provide authentication and encryption services for securing communication between devices</td>
</tr>
<tr>
<td>VSAT</td>
<td>Very Small Aperture Terminal. A two-way satellite ground station with a small dish antenna. VSATs typically provide narrowband data transmission when used for remote SCADA communication</td>
</tr>
<tr>
<td>VSD</td>
<td>Variable Speed Drive. A device that controls the speed of a motor, typically by varying the frequency of the power to the motor while monitoring and adapting to the power characteristics and providing protection for the motor and the application. Schneider Electric’s Altivar range of variable speed drives are examples of VSD control devices. Also known as VFD (variable frequency drive)</td>
</tr>
<tr>
<td><strong>Wide Area Network (WAN)</strong></td>
<td>Data communication network between distributed sites. Used in business computer networks to interconnect LANs at widely separated locations. In process automation, Wide Area Network describes an extension of a process network to nearby equipment, for example using Wi-Fi. This is not the same as a telemetry communication link. In remote SCADA, a Wide Area Network links together distributed LANs, for example a process network to a central operations control center network</td>
</tr>
</tbody>
</table>

Table 12: glossary