WHITE PAPER

SCADA Systems

CONTENTS

EXECUTIVE SUMMARY

With the wide range of RTU (Remote Terminal Units) and PLC (Programmable Logic Controllers) currently on the market, SCADA system engineers and decision makers face several challenges. Which classes of units provide the optimal functionality, expandability, and cost effectiveness for a given SCADA application? What type of unit will serve the mission not just today, but years into the future?

As implemented, RTUs and PLCs serve overlapping application niches and share some design details. To combat industry confusion, the discussion that follows provides a background of RTU and PLC units, and compares the various technical aspects for specifying the units including environmental ruggedness, modularity and scalability, and CPU performance. With remote applications for PLCs and RTUs continuing to expand, the discussion also helps the reader understand crucial remote system communication requirements including store and forward, report by exception, support for multiple protocols, and two-way communication with acknowledgements.

COMPLEX PROCESSES DEMAND SYSTEM-LEVEL INTELLIGENCE

Many industrial and infrastructure-scale enterprises depend on equipment located at multiple sites dispersed over a large geographical area. A vast majority of large infrastructure and industrial-scale ventures use Supervisory Control and Data Acquisition (SCADA) systems. According to Newton-Evans, the power utility industry alone uses SCADA at more than 50% of their installations .

SCADA systems provide monitoring, control, and automation functions that allow the enterprise to improve operational reliability, reduce costs through eased work force requirements, enhance overall Quality of Service (QoS), or meet expected QoS or other key performance factors as well as boost employee and customer safety.

Some key examples of SCADA applications include:

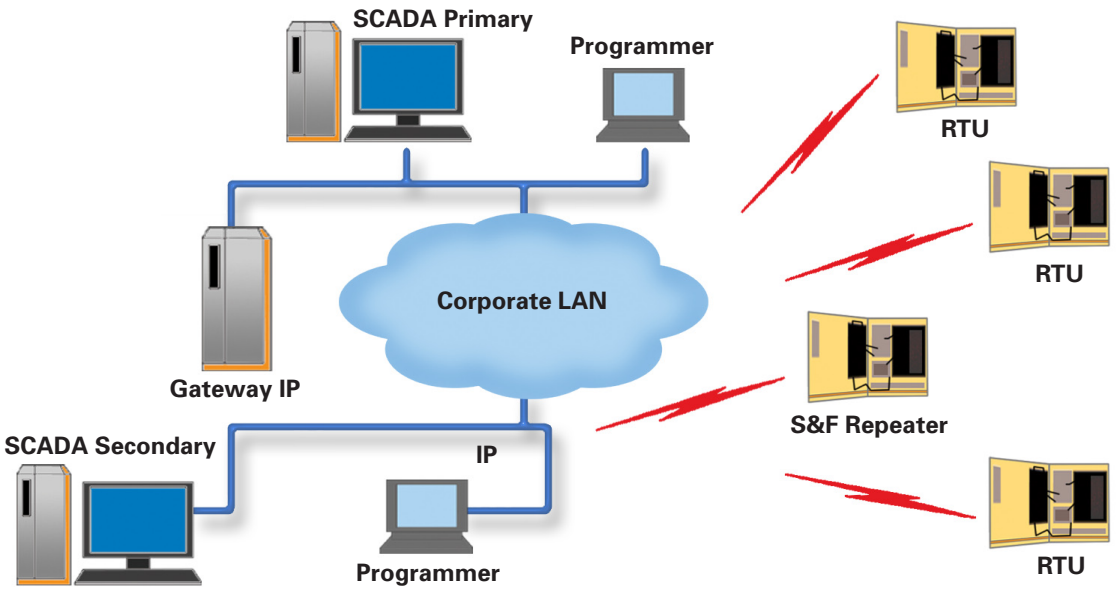
Public or Private Infrastructure:

- Water treatment and distribution
- Waste water collection and treatment
- Electrical power transmission and distribution
- Oil and gas pipeline monitoring and control

Industrial Processes (continuous, batch, or repetitive):

- Remote monitoring and control of oil and gas production, pumping, and storage at refineries from both offshore platforms and onshore wells
- Electrical power distribution from nuclear, gas-fired, coal, or renewable resources

In SCADA systems, RTUs and PLCs perform the majority of on-site control. The RTU or PLC acquires the site data, which includes meter readings, pressure, voltage, or other equipment status, then performs local control and transfers the data to the central SCADA system. However, when comparing and specifying a solution for challenging SCADA environments, RTU and PLC-based systems are not equal.



PLC Systems are Sub-Optimal for Complex SCADA Systems

Originally designed to replace relay logic, PLCs acquire analog and/or digital data through input modules, and execute a program loop while scanning the inputs and taking actions based on these inputs. PLCs perform well in sequential logic control applications with high discrete I/O data counts, but suffer from overly specialized design, which results in limited CPU performance, inadequate communication flexibility, and lack of easy scalability when it comes to adding future requirements other than I/O.

With the rapid expansion of remote site monitoring and control, three critical industry business trends have recently come into focus:

• **System performance and intelligence** – Process automation improves efficiency, plant safety, and reduces labor costs. However, complex processes like AGA gas flow calculations and high-resolution event capture in electric utility applications require very high performance and system-level intelligence. The reality is that even high-performance PLCs cannot meet all these expectations.

• **Communication flexibility** – Redundant communication links between remote systems and the central SCADA application form the basis of a reliable, secure, and safe enterprise. Power routing automation in electric applications, water distribution, warning systems, and oil and gas processes all require unique communication mediums including slow dial-up phone lines, medium speed RF, and broadband wired/wireless IP.

• **Configurability and reduced costs** – Although process monitoring and control are well defined and understood within many industries, the quest for flexibility and reduced Total Cost of Ownership (TCO) remains challenging. In the past, proprietary PLC units customized with third party components filled the niche, but suffered from lack of configurability and higher maintenance costs than fully integrated units. Today, businesses look for complete modular off-the shelf systems that yield high configurability with a significant improvement in TCO.

At the technical level, several requirements currently influence the SCADA specification process:

• **Local intelligence and processing** – High processing throughput, 32 bit CPUs with expanded memory for user applications and logging with support for highly complex control routines.

• **High-speed communication ports** – Monitoring large numbers of events requires systems that support multiple RS232/485 connections running at 230/460 kb/s and multiple Ethernet ports with 10/100 Mb/s capability.

• **High-density, fast, and highly accurate I/O modules** Hardware that implements 12.5 kHz input counters with 16-bit analog inputs and 14-bit analog outputs for improved accuracy.

• **Broadband wireless and wired IP communications** Recent innovations in IP devices demands reliable connectivity to local IEDs (Intelligent Electronic Devices) as well as emerging communication network standards.

• **Strict adherence** to open standard industry protocols including Modbus, DNP3, and DF-1 on serial and TCP/IP ports

• **Robust protocols** for support of mixed communication environments.

• **Protection of critical infrastructure** – Enhanced security such as password-protected programming, over the air encryption, authentication, and IP firewall capability.

RTUS PROVIDE SUPERIOR INTELLIGENCE, COMMUNICATIONS, AND FLEXIBILITY

Over the past decade, RTUs and PLCs have slowly progressed toward a common design and usage point. Still, primary markets determine the amount of change that systems can accommodate. In practice, the typical PLC usage model revolves around localized fast control of discrete variables. RTU usage focuses on remote monitoring with control, but with a higher demand for application communications and protocol flexibility. As a result, RTU designs tend to have greater CPU horsepower, programming flexibility and broader communication support than PLC systems.

Like a PLC, the RTU functions at the remote location wherever a SCADA system needs equipment monitoring or control. The optimal RTU system is modular—integrating the two-way data acquisition interface for process equipment control, and the interface to the communication subsystem. Modular RTUs and PLCs contain separate CPU, I/O, and communication modules, and support the addition of new modules through a common backplane.

When specifying SCADA system hardware, there are several critical areas to consider when comparing RTUs to PLCs. The following sections detail each area.

Rugged and Reliable Hardware Construction

Unlike PLCs, modular high performance RTUs include additional hardware features, power supplies with multiple AC/DC voltage rails, diagnostic displays, and provide support for integrated battery backup. Furthermore, RTUs must withstand the harsh environmental conditions encountered at offshore drilling platforms, arctic power stations, and other installations that require NEMA4/IP65 enclosure options.

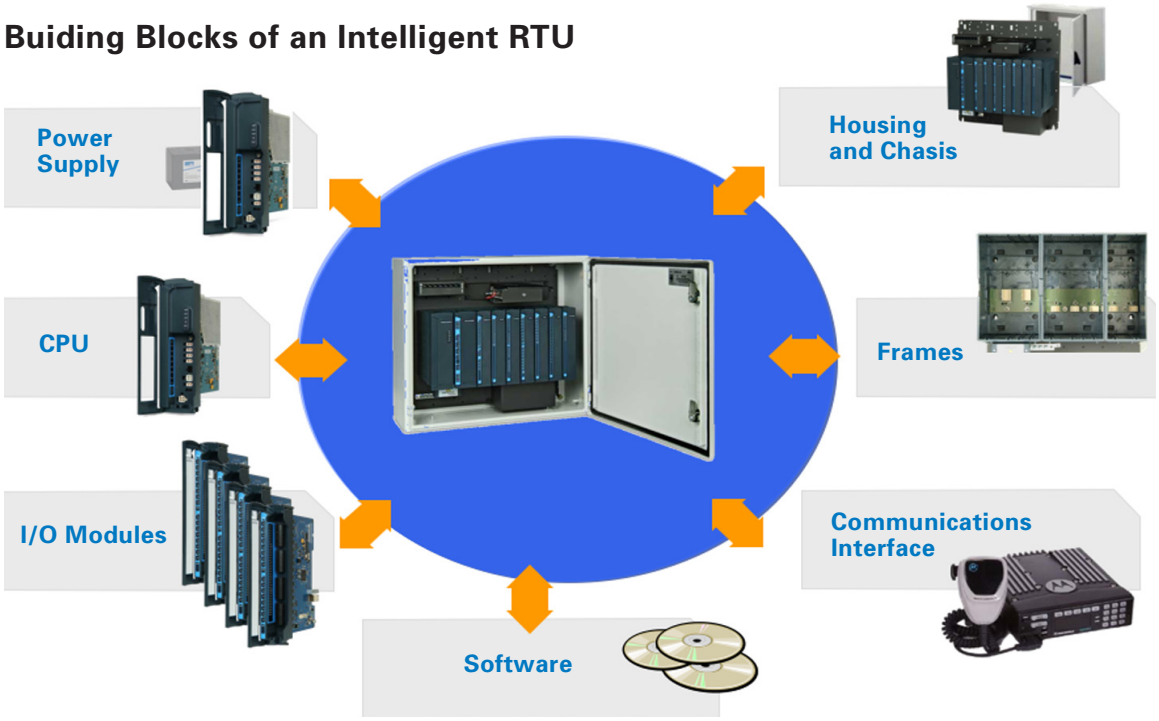
Key hardware specifications include:

• Modularity – RTU systems that use a modular approach enable flexible CPU, I/O, and radio/modem configurations. As a result, RTU modules provide mission-driven configurations and enable quick expansion as needs change.

• Intelligent power management, battery backup and optimized temperature compensated battery charging for overcharging and discharging protection. Some provide accurate remaining battery life to permit alarm or shut down procedures.

• Temperature and hazardous environment hardening:
  – Operating temperature: - 40 ºC to +70 ºC (-40 ºF to 158 ºF)
  – Operating humidity: 5% to 95% RH @ 50 ºC without condensation
  – Mechanical vibrations: Per EIA/TIA 603 Base-station, Sine 0.07 mm @ 10 to 30 Hz, 0.035 mm @ 30-60 Hz
  – Operating altitude: - 400 meter to + 4000 meter (-1312 ft to + 13120 ft)
  – Input isolation: 2.5 kV DC/AC between input and module logic
  – Overload and short circuit protection: Constant current limit with automatic recovery
  – Over-voltage protection

Buiding Blocks of an Intelligent RTU



Extensive Programming and Performance Capabilities

PLCs commonly contain limited intelligence, while older units reflect obsolete CPU technology, lack performance, and cannot scale when task size or functional requirements increase. When specifying a SCADA system, analyze the following key architectural building blocks while considering their affect on overall performance:

• **CPU** – RTUs require high processing capability to manage complex control tasks efficiently. For example, RTUs that contain a 200 MHz, 500 Million Instructions per Second (MIPS) CPU with multiple communication port support are optimal for performing simultaneous communications, networking, and control tasks.

• **Ladder and C source code** – Support for legacy, current, and future software applications and upgrades.

• **Scan times** – High processing power, I/O counts, and data rates translate directly into high scan rates. RTUs with high scan rates in the order of 1-ms SOE (Sequence of Events) resolution helps enable rapid respond to changing conditions at the remote site.

• **Real Time Operating System (RTOS)** – PLCs generally employ a proprietary OS architecture, while some RTUs use inefficient non-RTOS architectures. Because RTOS kernels use a highly optimized, efficient data model requiring minimal source code, RTUs built with RTOS benefit from faster task processing, reduced memory requirements, and lower risk of failure due to overly complex code.

Broad Communication and Protocol Support

While adequate in situations where system communication requirements are minimal, PLCs suffer from a lack of communication flexibility—only the larger and more expensive units can function both in a peer-to-peer and as the master controller. PLCs perform local processing tasks well, but lack the capability for handling newer system communication requirements or multiple protocols to connect with IEDs. Support for wireless IP stands out as another key issue when specifying a SCADA system.

To enable high SCADA communication reliability, redundancy, and flexibility make sure the system supports the following:

• **Time synchronization** – Ensure that the unit can time sync to the required accuracy. The electrical power industry requires sub-millisecond accuracy, which is not achievable without fast processors and an accurate time signal from a GPS receiver.

• **Store and forward** – Allows easy extension of radio networks without additional, expensive RF equipment; this adds redundancy, fault tolerance, and improves overall system reliability.

• **Dual link communications** – Improves system redundancy through full two-way messaging with acknowledgements on both links; also allows the data to travel "through" the RTU and communication medium simultaneously. For example, from IP to trunking radio, thus enabling easy system extension.

• **Alternate links** – Equipping the unit with multiple links increases the likelihood that communications reach their destination. For example, if path 1 fails, use path 2, or path 3.

• **Dual mode operation** – Make sure the unit can operate and easily switch between master/slave and peer-to-peer operation. In a master/slave system, every message must go through the SCADA master, thus creating a single point of failure. RTUs with dual mode operation significantly improve overall system reliability.

• **Data rates** – The higher the data rate, the faster the unit can acquire and act upon information from high I/O count modules and scale with SCADA system complexity.

• **Two-way radio operation** – Supporting multiple radio types and spectrums provides flexibility, especially in areas with high RF (Radio Frequency) interference:
  – Mobile/portable two-way radio
  – Analog/digital trunking
  – MAS 900 MHz
  – Broadband (WLAN, Canopy™, iNet900, etc)
  – Cellular modem (GPRS)

• **Report by exception** – Enables fast reporting of alarm conditions, yet minimizes channel use because the system only reports when necessary.

• **Wide range** of CPU protocols and programming interfaces:
  – MDLC and MDLC over IP
  – Modbus RTU on serial and TCP/IP
  – DNP 3.0 on serial and IP
  – IEC 60870
  – DF1 (Allen Bradley)
  – Any protocol implemented in the application program for serial ports (RS-232/485) and Ethernet ports (TCP/IP).

Local Control and High Capacity

For large monitoring and control tasks, SCADA systems require sufficient hardware and software capacity to perform their mission efficiently. While control loops and multiple protocol support can consume large amounts of system resources, intelligent hardware must also have enough resources to perform historical analysis and take predictive action if a system failure occurs. PLC systems with extensive control and capacity resources for logging historical data tend to be highly specialized—and expensive.

• **PID (Proportional Integral Derivative)** – Designers size various classes of PLC systems based upon the number of PID loops they can support within a specified time. The more loops a system supports, the faster and more expensive the processor/PLC.

• **SOE (Sequence of Events recording)** – Because most PLC designers optimize the unit to execute control routines not monitor them, PLCs generally lack SOE capabilities. RTUs, however, contain detailed support for SOE monitoring. High performance RTUs can log thousands of events time tagged to 1-ms.

• **Data logging** – To perform event data logging, systems require large amounts of available program and or user memory. Large PLCs tend to support data logging, but at a great expense in memory and price. When specifying a system, ensure that sufficient program memory exists for the target application.

• **I/O types and sizing** – When compared to an RTU, PLCs generally contain smaller I/O counts per module with overall lower density, which may require larger I/O racks to support needed capacity. For serial and/or IP links to another IED, make sure that the system contains sufficient hardware connections and programming flexibility to retrieve status and alarm information from other devices.

Ease of Maintenance and Upgradability

Because PLC-centric solutions contain limited configurability and program expandability, combining multiple functions into a single unit presents a major challenge. This limitation makes long-term SCADA system maintenance and scalability costly when compared to RTUs. Be sure to consider the needs of the overall system in two-five years, not just expanded I/O or a few new module slots. Furthermore, verify that the system can support future additions or changes in design and communication requirements.

To achieve optimal system scalability and lowered TCO, make sure the remote unit supports:

• Remote programming through wired/wireless IP networks and other communication mediums

• Remote downloads of applications, enabling rapid, secure configuration and upgrades of software code:
  – Site configuration IP configuration tables
  – Network configuration data
  – Phone book and modem setup files (STM files)
  – User programs (ladder and C) and user data

• Remote "safe" download of unit firmware allowing for upgrades without having to establish a local connection.

• High storage capacity (FLASH, DRAM, SRAM) for adding new programs, functions and increased user data storage

• Module hot swapping, which eliminates the need to power down the system to replace modules

Scalability of Security

Many PLC solutions perform well in a specialized functionality set, but lack the flexibility to add new capabilities for protecting infrastructure—such as remote security monitoring and access. Adding security enhancements to a PLC frequently requires the use of expensive ancillary hardware. In contrast, modular RTUs enable rapid scalability of a wide range of current and emerging security applications.

Monitoring and control are only two aspects of optimizing and protecting infrastructure. With today's expanding homeland security requirements, consider the following when specifying a SCADA system:

• **Support for multiple passwords at multiple abstraction levels** – Allows for compartmentalization of application software and SCADA hardware access control

• **Hardware IP firewalls** – Hides the unit's wireless/wired IP address

• **Support for currently available encryption** – Most PLC and RTU systems do not meet Data Encryption Standard (DES) and Advanced Encryption Standard (AES) requirements. New RTU systems under development use both a DES and AES compliant encryption routine.

• **Over the air and over the wire authentication** – All incoming packets verified and authenticated as valid, preventing unauthorized access by rogue programs.

• **Adding authorization to security routines** – Grants/restricts permissions to users and devices based upon user/device name and system access level.

• **Maintaining a sign-in and activity log** – Even though a system provides encryption or firewall protection, the unit must keep track of all access related activities autonomously.

HIGH PERFORMANCE RTUS MEET THE PROCESS CONTROL AND MONITORING CHALLENGE

SCADA systems built with the latest RTU technologies can deliver the optimal reliability, efficiency, and cost-effectiveness that today's complex infrastructure and industrial processes require. When specifying a SCADA system, be sure to investigate not only the current business and technical needs of the application, but the long-term scalability and TCO of the overall solution. Just as important, consider all aspects of the system, including performance, capacity, communications, ruggedness, and security.

Feature	High Performance RTU	PLC
Temperature	-40° to +70° C	-20° to +60° C
CPU word size – clock rate	32 bit – 200 MHz	16/32 bit - 50-100 MHz
RAM/Total memory	4 MB/32 MB	32 KB/256 KB
On-board serial/Ethernet ports	2/2/other options	Typically 1 of each
Remote application upload	Yes	No
Remote software diagnostics	Yes	No
Remote firmware download	Yes	No
Encryption support	Yes	No
Integrated radio support	Yes	No
Store and forward standard feature	Yes	No
Report by exception mode	Yes	No
Integrated power supply options with battery charging	Yes	No

MOTOROLA

Motorola, Inc. • 1301 East Algonquin Road • Schaumburg, IL 60196 U.S.A. • www.motorola.com/governmentandenterprise