RTU Basics

Remote Terminal Units in Industrial Control Systems

OT Security Learning Series

Document 080 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction

Information

A Remote Terminal Unit (RTU) is a microprocessor-controlled device that interfaces with physical equipment at remote locations and communicates with a central SCADA system. RTUs are essential components in utilities, oil and gas, water treatment, and other industries where monitoring and control must occur across geographically distributed sites.

RTUs serve as the eyes and ears of SCADA systems in remote locations. They collect data from sensors, execute control commands from the central system, and often operate autonomously when communication is lost. Understanding RTU architecture and operation is fundamental to securing distributed industrial infrastructure.

2 What is an RTU?

An RTU is a ruggedized, standalone device designed to:

- **Acquire Data** – Read values from sensors, meters, and field instruments
- **Execute Control** – Operate switches, valves, and other actuators
- **Communicate** – Transmit data to and receive commands from SCADA masters
- **Store Data** – Buffer readings when communication is unavailable
- **Process Locally** – Perform basic logic and calculations at the remote site

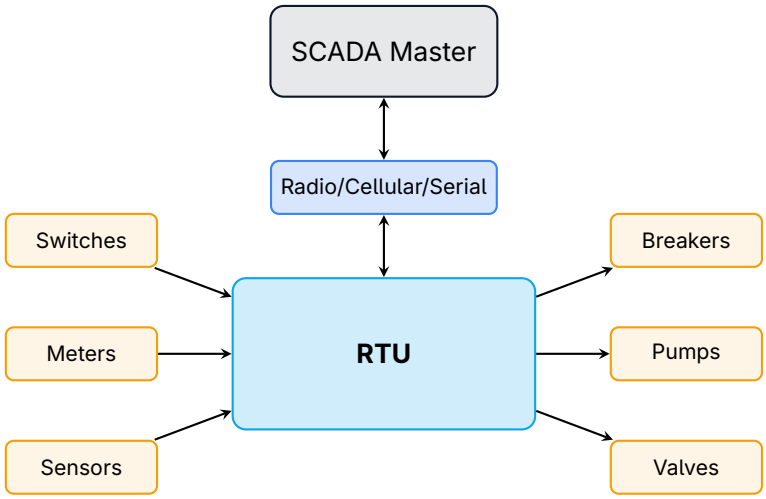

Figure 1: RTU in a typical SCADA architecture

3 RTU vs PLC

While RTUs and PLCs both interface with industrial processes, they serve different purposes:

Characteristic	RTU	PLC
Primary Purpose	Remote monitoring and telemetry	Local process control
Location	Geographically distributed sites	Within a plant or facility
Communication	Long-distance (radio, cellular, satellite)	Local networks (Ethernet, serial)
Autonomy	High – operates during comm loss	Moderate – usually networked
I/O Density	Lower, distributed I/O	Higher, concentrated I/O
Environment	Extreme outdoor conditions	Typically indoor, controlled
Scan Rate	Slower (seconds to minutes)	Fast (milliseconds)
Programming	Often simpler logic	Complex ladder/function block

Table 1: Key differences between RTUs and PLCs

Tip

Modern devices increasingly blur the RTU/PLC distinction. Many contemporary RTUs include PLC-like programming capabilities, while some PLCs support remote telemetry protocols. The term "RTU" often indicates the device's role in a distributed SCADA architecture rather than strict hardware differences.

4 RTU Architecture

4.1 Hardware Components

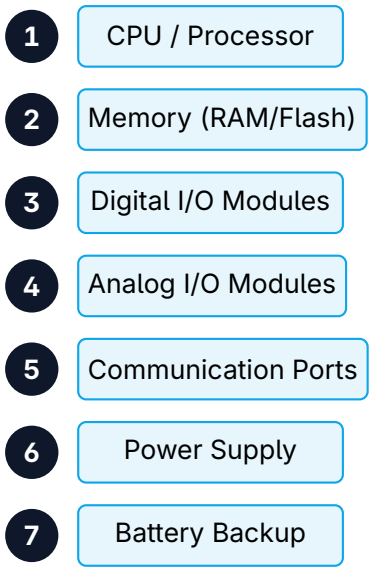

Figure 2: Core RTU hardware components

4.2 Input/Output Types

I/O Type	Signal	Examples
Digital Input	On/Off status	Valve position, pump running, alarm state
Digital Output	On/Off control	Start/stop pump, open/close valve
Analog Input	4-20mA, 0-10V	Temperature, pressure, flow, level
Analog Output	4-20mA, 0-10V	Setpoint adjustment, variable speed
Pulse/Counter	Pulse counting	Flow totalizer, energy meter

Table 2: Common RTU I/O types and applications

5 Communication Protocols

RTUs communicate using protocols designed for reliable telemetry over various media:

5.1 Common Protocols

- **DNP3** – Distributed Network Protocol, dominant in utilities
- **Modbus** – Simple, widely supported, RTU and TCP variants
- **IEC 60870-5-101/104** – International standard for telecontrol
- **IEC 61850** – Modern standard for substation automation

5.2 Communication Media

Medium	Typical Use	Considerations
Licensed Radio	Utilities, critical infrastructure	Reliable, dedicated spectrum
Cellular (4G/5G)	Wide-area, mobile sites	Coverage dependent, carrier costs
Satellite	Remote/offshore locations	High latency, expensive
Serial Leased Line	Legacy installations	Being phased out
Ethernet/IP	Modern installations	Requires network infrastructure

Table 3: RTU communication media options

6 Typical Applications

6.1 Electric Utilities

- Substation monitoring and control
- Distribution automation
- Capacitor bank switching
- Fault detection and isolation

6.2 Oil and Gas

- Pipeline monitoring (pressure, flow, leak detection)
- Well site automation
- Tank farm level monitoring
- Compressor station control

6.3 Water and Wastewater

- Pump station control
- Reservoir level monitoring
- Treatment plant remote I/O
- Distribution system pressure monitoring

7 Security Considerations

Critical

RTUs present significant security challenges due to their remote locations, legacy protocols, and often limited computational resources. Many RTUs were deployed before cybersecurity was a concern and lack basic security features.

7.1 Common Vulnerabilities

- **No Authentication** – Many protocols (Modbus, older DNP3) lack authentication
- **Cleartext Communication** – Data transmitted without encryption
- **Physical Access** – Remote sites may have weak physical security
- **Default Credentials** – Factory passwords often unchanged
- **Legacy Firmware** – Difficult or impossible to update
- **Insecure Remote Access** – Dial-up modems, unsecured cellular connections

7.2 Security Measures

Measure	Implementation
Protocol Security	DNP3 Secure Authentication, IEC 62351
Encryption	VPN tunnels, TLS for IP-based communication
Access Control	Strong passwords, disable unused ports
Physical Security	Locked enclosures, tamper detection
Monitoring	Log communications, detect anomalies
Network Segmentation	Separate RTU network from corporate IT

Table 4: RTU security measures

Key Point

When deploying new RTUs, select devices that support modern security features like DNP3 Secure Authentication, TLS, and role-based access control. For legacy devices, implement compensating controls such as VPN tunnels and network monitoring.

8 Summary

Key Takeaways

- **Definition:** RTUs are ruggedized devices that interface with field equipment at remote locations and communicate with central SCADA systems
- **vs PLCs:** RTUs emphasize remote telemetry and autonomous operation; PLCs emphasize local process control with fast scan rates
- **Components:** CPU, memory, digital/analog I/O, communication ports, power supply with battery backup
- **Protocols:** DNP3, Modbus, IEC 60870-5 are common; communication via radio, cellular, satellite, or IP networks
- **Applications:** Widely used in utilities, oil and gas, water/wastewater for distributed monitoring and control
- **Security:** Legacy RTUs often lack security features; implement protocol security, encryption, access control, and monitoring

9 Further Reading

Standards

- **IEEE 1815 (DNP3)** – Standard for electric power systems communications
  https://standards.ieee.org/standard/1815-2012.html
- **IEC 60870-5** – Telecontrol equipment and systems
  https://webstore.iec.ch/publication/3750

Resources

- **CISA ICS Security** – Industrial Control Systems resources
  https://www.cisa.gov/topics/industrial-control-systems
- **NIST SP 800-82** – Guide to ICS Security
  https://csrc.nist.gov/pubs/sp/800/82/r3/final

Books

- Bailey & Wright – *Practical SCADA for Industry* (Newnes)
- Boyer – *SCADA: Supervisory Control and Data Acquisition* (ISA)

Part of the OT Security Learning Series