HMI and SCADA Fundamentals

Understanding operator interfaces and supervisory control systems

OT Security Learning Series

Document 030 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction

Information

Human-Machine Interfaces (HMIs) and Supervisory Control and Data Acquisition (SCADA) systems form the critical bridge between human operators and industrial processes. Understanding these systems is essential for securing operational technology environments.

HMIs and SCADA systems serve as the "eyes and hands" of operators in industrial environments. While PLCs and RTUs execute control logic at the field level, HMIs and SCADA provide the visualization, monitoring, and high-level control capabilities that enable operators to oversee complex processes.

Key distinctions:

- **HMI** – Local operator interface for a specific process or machine
- **SCADA** – Distributed system for monitoring and controlling geographically dispersed assets

2 Human-Machine Interface (HMI)

An HMI is a device or software application that presents process data to operators and accepts control inputs. HMIs range from simple panel displays to sophisticated touchscreen workstations.

2.1 HMI Components

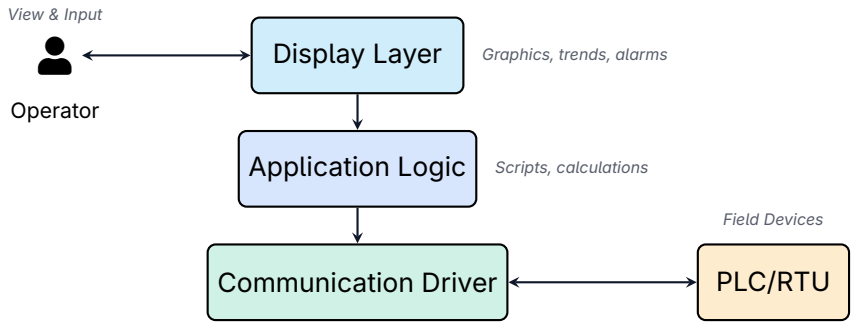

Figure 1: HMI Software Architecture

2.2 HMI Functions

- **Process Visualization** – Graphical representation of equipment, flows, and status
- **Alarm Management** – Display and acknowledgment of abnormal conditions
- **Trend Display** – Historical and real-time data charts

- **Control Interface** – Buttons, setpoint entry, mode selection
- **Data Logging** – Recording process values for analysis

2.3 HMI Types

Type	Description	Use Case
Panel HMI	Dedicated hardware with touchscreen	Machine-level control
PC-based HMI	Software on Windows/Linux PC	Complex processes
Web HMI	Browser-based interface	Remote monitoring
Mobile HMI	Tablet/smartphone apps	Field operations

Table 1: Common HMI Types

3 SCADA Systems

SCADA systems extend beyond local HMIs to provide centralized monitoring and control of distributed infrastructure. They are essential for utilities, pipelines, and other geographically dispersed operations.

3.1 SCADA Architecture

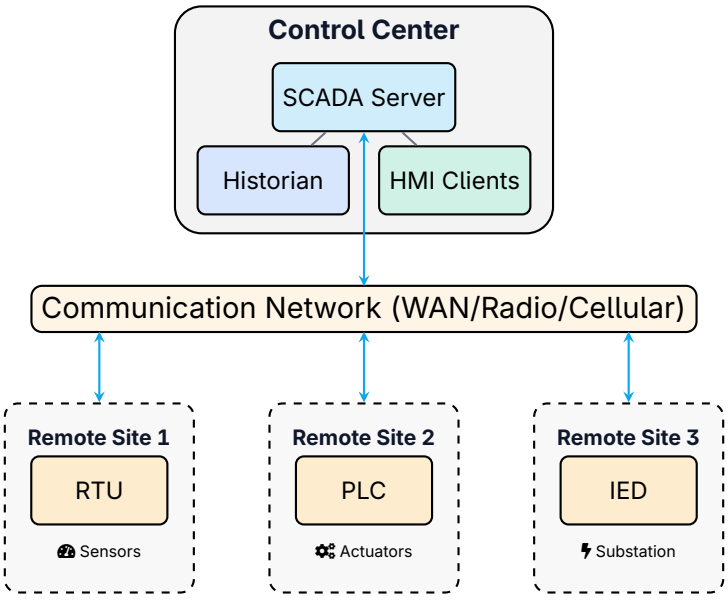

Figure 2: Typical SCADA System Architecture

3.2 SCADA Components

Core SCADA Components

- **Master Terminal Unit (MTU)** – Central SCADA server that polls remote sites
- **Remote Terminal Unit (RTU)** – Field device that collects data and executes commands
- **Communication Infrastructure** – Network connecting MTU to RTUs
- **HMI Workstations** – Operator interface displays
- **Historian** – Database for long-term data storage and analysis

3.3 SCADA vs DCS

Aspect	SCADA	DCS
Geography	Wide area, distributed	Single site, localized
Control	Supervisory (high-level)	Continuous process control
Communication	WAN, radio, cellular	High-speed LAN
Latency tolerance	Seconds to minutes	Milliseconds
Typical industries	Utilities, pipelines, water	Chemical, refining, power gen

Table 2: SCADA vs DCS Comparison

4 Communication Protocols

HMI and SCADA systems use various protocols to communicate with field devices:

Protocol	Common Use	Security
Modbus TCP/RTU	Legacy HMI-PLC communication	LOW None
DNP3	SCADA for utilities	MEDIUM Optional auth
IEC 61850	Substation automation	MEDIUM TLS capable
OPC DA/UA	HMI to multiple PLCs	HIGH UA has built-in
IEC 60870-5-104	Power grid SCADA	MEDIUM Optional auth

Table 3: Common HMI/SCADA Protocols

5 Security Considerations

Critical

HMI and SCADA systems are prime targets for attackers because compromising them provides direct control over physical processes. Many legacy systems were designed without security considerations and remain vulnerable.

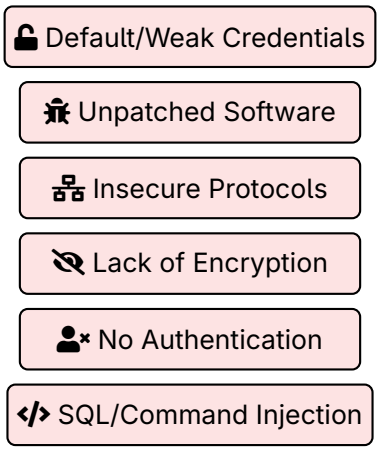

Figure 3: Common HMI/SCADA Vulnerabilities

5.1 Common Vulnerabilities

5.2 Attack Vectors

- **Network-based attacks** – Exploiting exposed SCADA servers or HMIs on corporate networks
- **Protocol manipulation** – Injecting malicious commands via insecure protocols
- **Social engineering** – Targeting operators with phishing to gain HMI access
- **Supply chain** – Compromising HMI software updates or vendor remote access
- **Insider threats** – Malicious or negligent actions by authorized users

5.3 Real-World Incidents

Warning

Notable HMI/SCADA attacks:

- **Ukraine 2015/2016** – Attackers used HMI access to open breakers, causing blackouts
- **Oldsmar 2021** – Attacker accessed water treatment HMI via remote access, attempted to poison water supply
- **Colonial Pipeline 2021** – While ransomware hit IT, SCADA was shut down as precaution

6 Security Best Practices

6.1 Access Control

- Implement role-based access control (RBAC) for all HMI users
- Require strong, unique passwords and enforce regular rotation

- Use multi-factor authentication for remote access
- Disable or remove default accounts
- Log all operator actions with timestamps

6.2 Network Security

- Isolate HMI/SCADA networks from corporate IT (network segmentation)
- Use firewalls between zones with strict rule sets
- Deploy intrusion detection systems (IDS) tuned for OT protocols
- Encrypt communications where possible (TLS, VPN)
- Disable unnecessary services and ports on HMI workstations

6.3 System Hardening

Key Point

Key hardening measures:

- Apply security patches after thorough testing
- Use application whitelisting on HMI workstations
- Disable USB ports and removable media where not needed
- Configure host-based firewalls
- Remove unnecessary software and services

7 Summary

Key Takeaways

- **HMIs** provide local operator interfaces for visualization and control of industrial processes
- **SCADA systems** enable centralized monitoring of geographically distributed assets
- Both systems sit at **Purdue Level 2** and are critical for process oversight
- Legacy systems often lack basic security controls like authentication and encryption
- Security requires **defense in depth**: access control, network segmentation, hardening, and monitoring
- Compromised HMI/SCADA can lead to **direct physical consequences**

8 Further Reading

Standards and Guidelines

- **NIST SP 800-82 Rev. 3** – Guide to OT Security
  https://csrc.nist.gov/pubs/sp/800/82/r3/final
- **IEC 62443-3-3** – System security requirements and security levels
  https://webstore.iec.ch/publication/7033
- **ISA-TR62443-2-3** – Patch management in IACS environments
  https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

Resources

- **CISA ICS Advisories** – Vulnerability alerts for SCADA/HMI products
  https://www.cisa.gov/news-events/cybersecurity-advisories
- **SANS ICS Resources** – Industrial control system security materials
  https://www.sans.org/industrial-control-systems-security/

Books

- Bailey, D. & Wright, E. – *Practical SCADA for Industry* (Newnes)
- Knapp, E. & Langill, J. – *Industrial Network Security* (Syngress)

Part of the OT Security Learning Series