OT Terminology and Glossary

Essential terms, acronyms, and concepts for OT security professionals

OT Security Learning Series

Document 050 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction

Information

Operational Technology (OT) has its own vocabulary distinct from IT. Understanding these terms is essential for effective communication between security teams, engineers, and operators in industrial environments.

This glossary provides definitions for common terms encountered in OT security, organized by category for easy reference.

2 System Types

Core OT Systems

SCADA
: *Supervisory Control and Data Acquisition* – System for remote monitoring and control of distributed assets (pipelines, power grids, water systems)

DCS
: *Distributed Control System* – Integrated control system for continuous processes (refineries, chemical plants, power generation)

PLC
: *Programmable Logic Controller* – Ruggedized computer for automating industrial processes and machinery

RTU
: *Remote Terminal Unit* – Field device that interfaces with sensors/actuators and communicates with SCADA

IED
: *Intelligent Electronic Device* – Smart device in power systems (protective relays, meters)

HMI
: *Human-Machine Interface* – Operator interface for monitoring and controlling industrial processes

SIS
: *Safety Instrumented System* – Independent system designed to bring processes to safe state

3 Network and Communication

3.1 Network Terms

OT Network
: Network connecting industrial control systems, isolated from corporate IT

Air Gap
: Physical isolation of a network with no connection to other networks

DMZ
: *Demilitarized Zone* – Network segment between IT and OT for controlled data exchange

Conduit
: Communication path between security zones (IEC 62443 term)

Zone Grouping of assets with common security requirements (IEC 62443 term)

Fieldbus
Industrial network connecting field devices to controllers

Backhaul
Communication link from remote sites to central control

3.2 Protocols

Protocol	Full Name	Use Case
Modbus	–	Register-based comms
DNP3	Distributed Network Protocol	SCADA, utilities
OPC UA	Open Platform Communications UA	Industrial interop
EtherNet/IP	EtherNet Industrial Protocol	Rockwell systems
PROFINET	Process Field Net	Siemens environments
BACnet	Building Automation Control	Building automation
IEC 61850	–	Substation automation
HART	Highway Addressable Remote Transducer	Smart instruments

Table 1: Common Industrial Protocols

4 Hardware Components

4.1 Field Devices

Sensor
Device that measures physical parameters (temperature, pressure, flow, level)

Transmitter
Sensor with built-in signal conditioning and communication

Actuator
Device that performs physical action (valve, motor, relay)

VFD/VSD
Variable Frequency/Speed Drive – Controls motor speed

I/O Module
Interface between controller and field devices (inputs/outputs)

Marshalling Cabinet
Enclosure where field wiring terminates before connecting to I/O

4.2 Control Equipment

Controller
Device executing control logic (PLC, DCS controller, RTU)

Safety Controller
PLC certified for safety functions (SIL-rated)

PAC *Programmable Automation Controller* – Advanced PLC with PC-like features

Engineering Workstation
PC used to program and configure controllers

Historian
Server that collects and stores time-series process data

OPC Server
Software that translates between industrial protocols and OPC

5 Programming and Logic

IEC 61131-3 Programming Languages

Ladder Logic (LD)
Graphical language resembling electrical relay diagrams

Function Block Diagram (FBD)
Graphical language using interconnected function blocks

Structured Text (ST)
Text-based language similar to Pascal

Instruction List (IL)
Low-level assembly-like language (deprecated)

Sequential Function Chart (SFC)
Graphical language for sequential processes

5.1 Control Concepts

Scan Cycle
Time for PLC to read inputs, execute logic, update outputs

Tag Named data point representing a process variable

Setpoint
Target value for a controlled variable

PID *Proportional-Integral-Derivative* – Common control algorithm

Interlock
Logic that prevents unsafe operations

Permissive
Condition that must be true before an action is allowed

6 Safety Terms

Warning

Safety systems use specific terminology defined in IEC 61511 and IEC 61508. Precise understanding is critical as these systems protect human life.

SIF *Safety Instrumented Function* – Specific safety action (sensor + logic + actuator)

SIL *Safety Integrity Level* – Risk reduction capability (SIL 1-4)

PFD *Probability of Failure on Demand* – Likelihood SIF fails when needed

BPCS *Basic Process Control System* – Normal process control (not safety)

ESD *Emergency Shutdown* – System or action to stop process safely

F&G *Fire and Gas* – Detection system for fires and gas releases

HAZOP
Hazard and Operability Study – Risk assessment methodology

LOPA *Layer of Protection Analysis* – Method to determine required SIL

7 Security Terms

7.1 Standards and Frameworks

IEC 62443
International standard series for industrial cybersecurity

NIST 800-82
US guide to OT security

NERC CIP
North American electric grid security standards

SL *Security Level* – IEC 62443 security capability rating (SL 1-4)

SAL *Security Assurance Level* – Development rigor level

7.2 Security Concepts

Defense in Depth
Multiple security layers to protect assets

Least Privilege
Minimum access rights needed for a task

Segmentation
Dividing networks into isolated zones

Allowlisting
Permitting only approved applications/traffic

OT IDS Intrusion detection system designed for industrial protocols

Asset Inventory
Comprehensive list of all OT devices and software

8 Operational Terms

Availability
: System uptime and operational readiness

Downtime
: Period when system is not operational

Maintenance Window
: Scheduled time for system updates/changes

MOC *Management of Change* – Formal process for system modifications

FAT *Factory Acceptance Test* – Testing at vendor before delivery

SAT *Site Acceptance Test* – Testing after installation at site

Commissioning
: Process of verifying and starting up new systems

Brownfield
: Existing facility with legacy systems

Greenfield
: New facility built from scratch

9 Industry-Specific Terms

9.1 Process Industries

Batch Process
: Production in discrete quantities (pharmaceuticals, food)

Continuous Process
: Uninterrupted production flow (refining, chemicals)

Recipe Set of parameters and steps for batch production

Unit Operation
: Single processing step (mixing, heating, filtering)

9.2 Utilities and Infrastructure

DERMS
: *Distributed Energy Resource Management System*

AMI *Advanced Metering Infrastructure* – Smart meter network

Substation
: Facility for transforming voltage levels in power grid

WWTP
: *Wastewater Treatment Plant*

WTP *Water Treatment Plant*

10 Summary

Key Categories

- **Systems** – SCADA, DCS, PLC, RTU, HMI, SIS
- **Networks** – DMZ, fieldbus, zones and conduits
- **Protocols** – Modbus, DNP3, OPC UA, EtherNet/IP
- **Safety** – SIF, SIL, PFD, ESD, HAZOP
- **Security** – IEC 62443, defense in depth, segmentation
- **Operations** – MOC, FAT/SAT, maintenance windows

11 Further Reading

Standards

- **IEC 62443 Series** – Industrial cybersecurity terminology
  https://webstore.iec.ch/publication/7029
- **IEC 61131-3** – PLC programming languages
  https://webstore.iec.ch/publication/4552

Resources

- **CISA – ICS Glossary**
  https://www.cisa.gov/topics/industrial-control-systems
- **ISA – Automation Terms**
  https://www.isa.org/

Books

- Boyer, S. – *SCADA: Supervisory Control and Data Acquisition* (ISA)
- Knapp, E. & Langill, J. – *Industrial Network Security* (Syngress)

Part of the OT Security Learning Series