ACCESS CONTROL
Assignment of access to assets based on user roles and attributes

ACTIVE DIRECTORY
Central identity store federated into OT to enforce role-based access, time-bound accounts, and auditability.

ACTUATOR
Devices that convert control signals into Physical Actions

ADC
Converts an analog process signal into a digital value the controller can interpret.

AMI
Advanced Metering Infrastructure.)Enables two-way communication between smart meters and utilities for metering, control, and data analysis

AMR
Automatic Metering Reading. One-way or limited two-way communication systems used to collect consumption data from utility meters.

ADVANCED PROCESS CONTROL (APC)
Model-based or multivariable control algorithms that run above basic PID loops to optimise quality/throughput.

AIR GAP
Physical Isolation between OT and IT Networks.

AIC TRIAD
Availability, Integrity, and Confidentiality — reordered from CIA to reflect OT priorities.

A

Operational Technology (OT) and OT Security Glossary

OT SECURITY HUDDLE

ALARM ANNUNCIATOR PANEL
Dedicated panel or HMI view presenting critical alarms in a conspicuous format

ALARM MANAGEMENT
Framework to configure, prioritize, and handle alarms

ALARM SERVER
SCADA/DCS service that aggregates, timestamps, and routes alarms to HMIs, historians, or paging systems.

ALARM SUPRESSION
Suppresses non-critical alarms to reduce operator overload.

ANALOG INPUT / ANALOG OUTPUT (AI/AO)
I/O channels on a PLC or remote rack that handle real-world analog signals

ANALOG SENSOR
Field device that returns a continuous-value signal (e.g., 4-20 mA temperature probe) to the control system

ANOMALY DETECTION
Behaviour-based detection of deviations from normal OT traffic/operations

APPLICATION SERVER (SCADA)
Hosts the supervisory application, graphics, trending, and basic historian functions for a process area.

APPLICATION WHITELISTING
Endpoint security control permitting only vetted executables—widely recommended for Level 3 Windows assets.

ASSESSMENT (SECURITY RISK)
Evaluation of threats, vulnerabilities, and potential impacts using contextual risk scoring models (e.g., SLAs, risk matrices).

ASSET INVENTORY
Framework to configure, prioritize, and handle alarms

AUTO/MANUAL STATION
Local switch or HMI element that lets operators toggle a control loop between automatic and manual modes

AUTOMATION CONTROLLER (PAC/IPC)
Industrial PC or programmable automation controller combining PLC determinism with PC-grade processing.

AUTOMATION SYSTEM
Includes SCADA, DCS, and PLC-based setups used to automate industrial operations.

ATTACK SURFACE
All points in a system that are exposed to possible intrusion. Reduction is key to resilience.

ATTACK VECTOR
Method or path used by an attacker to gain unauthorized access (e.g., USB drop, phishing, protocol abuse).

AUDIT TRAIL
Logged sequence of system activities used for monitoring, forensics, and compliance. Often stored in SIEM.

AUTHENTICATION
Verifying user/device identity (e.g., MFA, certificate-based login). OT systems may use centralized or local auth.

AUTHORIZATION
Determines permitted actions for authenticated users. Often implemented via Role-Based Access Control (RBAC).

AVAILABILITY
Ensuring system uptime and process continuity. Often prioritized over confidentiality in OT.