Professional Certificate in Operational Technology Engineer (United Kingdom)

Cybersecurity Fundamentals

Access Control – mechanisms that restrict who can view or use resources. Related terms: authentication, authorization, role-based access control (RBAC). Example: A SCADA workstation requires a user to log in with a password before any engineering functions are available. Challenge: Balancing strict controls with the need for rapid response in emergency situations.

Advanced Persistent Threat (APT) – a prolonged, targeted cyber-attack where an intruder remains undetected to achieve strategic objectives. Related terms: zero-day exploit, command-and-control (C2), threat actor. Example: An APT group infiltrates an oil-and-gas control network to exfiltrate production data over months. Challenge: Detecting low-and-slow activity that blends with normal OT traffic.

Authentication – process of verifying the identity of a user, device, or system. Related terms: multi-factor authentication (MFA), password policy, digital certificate. Example: An operator uses a smart card plus PIN to access a PLC programming interface. Challenge: Implementing MFA without impeding time-critical operations.

Authorization – granting or denying access rights to resources after authentication. Related terms: access control list (ACL), privilege escalation, least privilege. Example: A maintenance engineer receives read-only rights to sensor data but cannot modify control logic. Challenge: Maintaining accurate permission matrices as staff roles evolve.

Availability – ensuring that OT services and data are accessible when needed. Related terms: redundancy, disaster recovery, service-level agreement (SLA). Example: A redundant PLC pair provides seamless failover if the primary controller fails. Challenge: Protecting availability while defending against denial-of-service attacks.

Baseline Configuration – a documented, approved set of system settings used as a reference for security compliance. Related terms: hardening, configuration drift, audit. Example: A firewall rule set that permits only required protocols between engineering workstations and RTUs. Challenge: Keeping the baseline current amid frequent firmware updates.

Biometric Authentication – use of physiological traits such as fingerprint or iris for identity verification. Related terms: multifactor authentication, spoofing, liveness detection. Example: A control room door unlocks only after a fingerprint scan matches an authorized operator. Challenge: Ensuring reliability in harsh industrial environments.

Black-Box Testing – security testing where the tester has no prior knowledge of the system internals. Related terms: penetration testing, vulnerability scanning, red teaming. Example: A pen-tester attempts to breach a PLC network without architecture diagrams. Challenge: Limited visibility may miss subtle configuration weaknesses.

Botnet – a network of compromised devices controlled remotely to perform coordinated attacks. Related terms: command-and-control (C2), malware, distributed denial-of-service (DDoS). Example: Infected HMIs are enlisted to flood a utility's public portal, disrupting customer access. Challenge: Detecting compromised OT assets that exhibit normal operational behavior.

Bridge (Network) – a device that connects two LAN segments, forwarding traffic based on MAC addresses. Related terms: switch, router, segmentation. Example: A Ethernet bridge links a legacy serial network to a modern IP subnet without altering protocols. Challenge: Ensuring the bridge does not become a conduit for lateral movement.

Certificate Authority (CA) – trusted entity that issues digital certificates for authentication and encryption. Related terms: PKI, TLS/SSL, revocation list. Example: A SCADA server presents a certificate signed by the plant's internal CA to prove its identity to remote HMI clients. Challenge: Managing certificate lifecycles across heterogeneous OT devices.

Change Management – formal process for requesting, reviewing, approving, and documenting modifications to OT systems. Related terms: configuration control, versioning, risk assessment. Example: Before upgrading a PLC firmware, a change request is logged, reviewed by the safety team, and scheduled during a maintenance window. Challenge: Balancing the need for rapid patches with rigorous approval procedures.

Chroot Jail – a security mechanism that isolates a process to a specific directory subtree. Related terms: containerization, sandbox, least privilege. Example: A legacy data logger runs inside a chroot jail to limit its access to the file system. Challenge: Ensuring the jail does not inadvertently expose privileged binaries.

Cipher Suite – a set of algorithms that provide encryption, integrity, and authentication for secure communications. Related terms: TLS, SSL, cryptographic protocol. Example: A DNP3 Secure Authentication implementation selects AES-256-GCM as its cipher suite. Challenge: Selecting suites compatible with constrained OT devices while maintaining strong security.

Compliance – adherence to legal, regulatory, or industry standards governing security. Related terms: ISO 27001, NIS Directive, GDPR. Example: A UK water utility must demonstrate compliance with the NIS 2 regulations concerning critical infrastructure. Challenge: Mapping technical controls to high-level regulatory language.

Compromise Assessment – systematic evaluation to determine if an OT environment has been breached. Related terms: incident response, forensics, indicator of compromise (IOC). Example: After a ransomware alert, the security team conducts a compromise assessment on the control network to locate malicious binaries. Challenge: Performing deep analysis without disrupting real-time processes.

Confidentiality – ensuring that information is disclosed only to authorized entities. Related terms: encryption, access control, data classification. Example: Proprietary process parameters are encrypted at rest on the historian server. Challenge: Protecting data while maintaining low latency for control loops.

Control System Cybersecurity (CSCY) – discipline focused on protecting industrial control systems from

cyber threats. Related terms: OT security, ICS hardening, risk management. Example: A CSCY program implements network segmentation, intrusion detection, and patch management for a petrochemical plant. Challenge: Integrating CSCY practices with existing safety and operational standards.

Credential Dumping – extraction of password hashes or tokens from memory or storage. Related terms: LSASS, privilege escalation, password cracking. Example: An attacker uses a tool to dump Windows administrator hashes from a supervisory workstation. Challenge: Detecting dumping activity on systems that rarely produce logs.

Cross-Site Scripting (XSS) – web vulnerability where malicious scripts are injected into trusted pages. Related terms: web application firewall (WAF), input validation, client-side attack. Example: A HMI web portal fails to sanitize user input, allowing an attacker to execute JavaScript in the browser of another operator. Challenge: Many OT HMIs are built on legacy web stacks with limited patching.

Cyber-Physical System (CPS) – integration of computation, networking, and physical processes. Related terms: IoT, OT, digital twin. Example: A smart grid uses sensors, controllers, and communication links to balance supply and demand in real time. Challenge: Securing the cyber layer without compromising the timing constraints of the physical layer.

Data Diodes – hardware devices that enforce unidirectional data flow, preventing return traffic. Related terms: air gap, one-way gateway, network segmentation. Example: A historian receives telemetry from field devices through a data diode, ensuring that no commands can travel back. Challenge: Configuring monitoring and management channels that still respect the one-way restriction.

Defense-in-Depth – layered security approach that combines multiple controls to protect assets. Related terms: perimeter security, host hardening, application security. Example: A refinery employs firewalls, intrusion detection systems, host hardening, and user training to defend its control network. Challenge: Avoiding unnecessary complexity that can obscure visibility.

Deception Technology – use of decoys, honeypots, and fake assets to lure attackers and gather intelligence. Related terms: honeynet, threat hunting, indicator of attack (IOA). Example: A simulated PLC with fake registers is deployed in a DMZ to detect lateral movement attempts. Challenge: Ensuring decoys do not interfere with legitimate traffic or safety functions.

Denial-of-Service (DoS) – attack that exhausts resources, rendering a system unavailable. Related terms: DDoS, bandwidth saturation, service disruption. Example: An attacker floods a SCADA server with malformed packets, causing the control interface to freeze. Challenge: Distinguishing malicious traffic from legitimate bursts caused by process spikes.

Digital Twin – virtual replica of a physical asset used for simulation, monitoring, and analysis. Related terms: CPS, model-based engineering, predictive maintenance. Example: A digital twin of a turbine is synchronized with real-time sensor data to predict failures. Challenge: Securing the twin’s data feed to prevent manipulation of the physical system.

Disaster Recovery (DR) – strategy for restoring IT/OT services after a catastrophic event. Related terms:

business continuity, backup, RPO/RTO. Example: A backup of the control system configuration is stored off-site and can be restored within four hours after a fire. Challenge: Testing DR plans without interrupting production.

DMZ (Demilitarized Zone) – network segment that isolates external-facing services from internal OT networks. Related terms: perimeter firewall, segmentation, jump host. Example: A Historian web interface resides in a DMZ, allowing remote engineers to view trends without direct access to the control network. Challenge: Configuring strict rules to prevent DMZ compromise from propagating inward.

DNS Spoofing – attack that corrupts DNS responses to redirect traffic to malicious destinations. Related terms: cache poisoning, man-in-the-middle (MITM), secure DNS (DNSSEC). Example: An attacker modifies the DNS entry for a firmware update server, causing devices to download a trojanized image. Challenge: Many OT devices rely on static DNS entries that are difficult to update.

Domain-Based Security – approach that groups assets by logical or functional domains for tailored controls. Related terms: security zones, risk segmentation, policy enforcement. Example: A “process control” domain has stricter authentication than a “monitoring” domain. Challenge: Maintaining clear boundaries as systems interconnect for Industry 4.0 Initiatives.

Edge Computing – processing data close to the source rather than in a central data center. Related terms: fog computing, latency, distributed architecture. Example: A PLC performs local analytics on vibration data to trigger an alarm before sending summary data to the cloud. Challenge: Ensuring edge nodes are patched and monitored despite limited management interfaces.

Endpoint Detection and Response (EDR) – tools that monitor, detect, and respond to threats on individual devices. Related terms: host-based IDS, forensics, behavioral analytics. Example: An EDR agent on an engineering workstation records process creation events to flag suspicious script execution. Challenge: Deploying agents on legacy OT equipment with constrained resources.

Encryption – transformation of data into unreadable form using algorithms and keys. Related terms: cipher, key management, TLS. Example: TLS is used to secure MQTT messages sent from field sensors to a central broker. Challenge: Selecting encryption that meets performance constraints of real-time control loops.

Enterprise Risk Management (ERM) – systematic process for identifying, assessing, and mitigating risks across an organization. Related terms: risk register, ISO 31000, risk appetite. Example: A utility incorporates OT cyber-risk assessments into its overall ERM framework to align with corporate governance. Challenge: Translating technical vulnerabilities into business-level risk metrics.

Exfiltration – unauthorized transfer of data from a target system to an external location. Related terms: data leakage, command-and-control (C2), staging. Example: Malware compresses PLC program files and uploads them to a remote server via an outbound HTTPS connection. Challenge: Monitoring outbound traffic in environments where external communication is limited but essential.

Fail-Safe – design principle where a system defaults to a safe state in the event of a failure. Related terms: fail-secure, redundancy, safe-state. Example: If a valve controller loses power, it automatically closes to

prevent over-pressure. Challenge: Ensuring security controls (e.G., Authentication) do not inadvertently prevent safe-state activation.

Firewall – network security device that filters traffic based on predefined rules. Related terms: stateful inspection, packet filtering, network segmentation. Example: A next-generation firewall blocks all inbound traffic to the control network except for specific SCADA protocols from authorized management stations. Challenge: Correctly mapping industrial protocol ports to avoid accidental blockage of critical traffic.

Forward Secrecy – cryptographic property that ensures session keys cannot be derived from long-term keys. Related terms: Diffie-Hellman, key exchange, TLS. Example: A TLS configuration that uses ECDHE provides forward secrecy for encrypted telemetry streams. Challenge: Some legacy OT devices only support static RSA key exchange, lacking forward secrecy.

Fuzz Testing – automated technique that supplies random or malformed inputs to discover vulnerabilities. Related terms: software testing, buffer overflow, security assessment. Example: A fuzzer targets the Modbus TCP stack of a PLC to uncover parsing errors. Challenge: Ensuring that fuzzing does not disrupt live processes or safety functions.

Hardened Operating System – OS configuration that removes unnecessary services and applies security patches. Related terms: minimal install, security baseline, system hardening. Example: A PLC runs a hardened Linux kernel with only the Modbus daemon enabled. Challenge: Maintaining hardening while supporting vendor-specific drivers required for field I/O.

Incident Response (IR) – coordinated approach to detect, contain, eradicate, and recover from security events. Related terms: playbook, forensics, post-mortem. Example: An IR team follows a predefined playbook to isolate a compromised engineering workstation, collect volatile memory, and restore from a known-good image. Challenge: Executing IR steps without halting critical production processes.

Industrial Control System (ICS) – integrated hardware and software that monitors and controls industrial processes. Related terms: SCADA, PLC, DCS. Example: A water treatment plant uses a DCS to manage pump sequencing, valve positions, and chemical dosing. Challenge: Protecting legacy components that were not designed with security in mind.

Industrial Internet of Things (IIoT) – networked sensors, actuators, and devices that enable data-driven operation of industrial assets. Related terms: edge computing, cloud integration, digital transformation. Example: Smart meters transmit consumption data over MQTT to a utility's analytics platform. Challenge: Integrating heterogeneous devices while maintaining a consistent security posture.

Intrusion Detection System (IDS) – technology that monitors network or host activity for signs of malicious behavior. Related terms: signature-based, anomaly-based, alerting. Example: A network IDS flags an unexpected Modbus "Write Multiple Registers" command originating from a workstation that normally only reads data. Challenge: Tuning IDS thresholds to reduce false positives that could lead to alarm fatigue.

IP Whitelisting – security method that permits traffic only from explicitly allowed IP addresses. Related terms: access control list (ACL), network segmentation, firewall rule. Example: Only the IP of the central

historian is allowed to connect to the PLC's configuration port. Challenge: Managing dynamic IP allocations in environments with DHCP or mobile devices.

Key Management – processes and tools for generating, storing, rotating, and revoking cryptographic keys. Related terms: PKI, HSM, certificate lifecycle. Example: An HSM stores AES keys used to encrypt archived process data, with automatic rotation every 90 days. Challenge: Integrating key management with devices that lack native support for secure storage.

Kill Chain – model describing the stages of a cyber attack from reconnaissance to objective. Related terms: MITRE ATT&CK, threat hunting, defense-in-depth. Example: An attacker follows the kill chain by first scanning for open ports, then exploiting a PLC firmware vulnerability, and finally exfiltrating data. Challenge: Breaking the chain early requires proactive detection at each stage.

Least Privilege – principle that users and processes receive only the access necessary to perform their functions. Related terms: role-based access control (RBAC), privilege escalation, access review. Example: A contractor's account can view sensor trends but cannot modify control parameters. Challenge: Regularly reviewing privileges as job responsibilities evolve.

Logical Segmentation – division of a network into separate zones using virtual LANs (VLANs) or software-defined networking. Related terms: DMZ, firewall, micro-segmentation. Example: The engineering workstations reside in VLAN 10, while field devices are placed in VLAN 20, with strict inter-VLAN ACLs. Challenge: Ensuring segmentation does not interfere with time-sensitive control traffic.

Malware – malicious software designed to disrupt, damage, or gain unauthorized access to systems. Related terms: ransomware, trojan, rootkit. Example: A ransomware variant encrypts PLC configuration files, demanding payment to restore operation. Challenge: Limited visibility into proprietary file systems that may hide malware artifacts.

Man-in-the-Middle (MITM) – attack where the adversary intercepts and possibly alters communications between two parties. Related terms: packet injection, SSL stripping, session hijacking. Example: An attacker positions a rogue device on the control network to modify Modbus commands before they reach a valve controller. Challenge: Detecting subtle timing changes or packet modifications in high-throughput environments.

Man-In-The-Browser (MITB) – attack that injects malicious code into a web browser to capture credentials or alter displayed data. Related terms: web shell, phishing, browser hijack. Example: An operator's HMI web client is compromised, allowing the attacker to change set-points displayed on the screen. Challenge: Many industrial browsers lack modern security extensions.

Micro-Segmentation – granular network segmentation that isolates workloads at the host or application level. Related terms: software-defined perimeter, zero-trust, policy enforcement point. Example: Each PLC is assigned a unique security policy that only permits communication from its designated supervisory system. Challenge: Creating and maintaining hundreds of policies without overwhelming administrators.

MITRE ATT&CK® for OT – knowledge base of adversary tactics and techniques specific to operational

technology. Related terms: kill chain, threat modeling, security controls. Example: The “Manipulation of PLC Logic” technique is mapped to detection controls such as configuration integrity monitoring. Challenge: Aligning ATT&CK mappings with existing security tooling that may be IT-centric.

Network Time Protocol (NTP) – protocol for synchronizing clocks of computer systems over packet networks. Related terms: time drift, chrony, security. Example: PLCs use NTP to timestamp events, enabling accurate forensic analysis after an incident. Challenge: NTP can be abused for amplification attacks if not properly secured.

Network Topology – physical and logical arrangement of network nodes and links. Related terms: bus, star, ring. Example: A ring topology provides redundancy for critical communication between master and slave devices. Challenge: Documenting topology accurately to support impact analysis during change management.

Non-Repudiation – assurance that a party cannot deny the authenticity of a transaction they performed. Related terms: digital signature, audit log, integrity. Example: A signed command to open a valve provides evidence that the authorized operator initiated the action. Challenge: Storing signatures in tamper-proof logs while respecting limited storage on embedded devices.

Obfuscation – technique that makes code or data harder to analyze, often used by malware. Related terms: packer, encryption, anti-analysis. Example: A malicious DLL uses code obfuscation to hide its payload from static analysis tools. Challenge: Distinguishing legitimate code obfuscation (e.G., For intellectual property protection) from malicious intent.

Off-The-Shelf (OTS) Software – commercially available software not specifically designed for OT environments. Related terms: COTS, vendor support, compatibility. Example: A generic Windows workstation runs a third-party HMI client. Challenge: Ensuring OTS software receives timely security updates while maintaining operational continuity.

One-Way Authentication – process where only one party verifies the identity of the other, common in client-server models. Related terms: server authentication, mutual TLS, certificate validation. Example: An HMI validates the server certificate of a PLC, but the PLC does not verify the HMI’s identity. Challenge: Unilateral trust can be exploited if the client is compromised.

Open-Source Software (OSS) – software whose source code is publicly available for inspection, modification, and distribution. Related terms: community support, vulnerability disclosure, license compliance. Example: An open-source MQTT broker is used to aggregate sensor data. Challenge: Tracking OSS dependencies to ensure patches are applied promptly.

Operational Technology (OT) – hardware and software that monitors and controls physical devices, processes, and events. Related terms: ICS, SCADA, process automation. Example: A series of PLCs managing a gas compression station constitute the OT layer. Challenge: Integrating OT security with existing IT governance frameworks.

Patch Management – systematic process for acquiring, testing, and deploying software updates. Related

terms: vulnerability remediation, change control, rollback. Example: A monthly maintenance window is used to apply vendor-released firmware patches to all field devices. Challenge: Balancing the need for rapid patching against the risk of introducing instability into live control loops.

Phishing – social engineering technique that attempts to trick recipients into revealing credentials or installing malware. Related terms: spear phishing, credential harvesting, email spoofing. Example: An engineer receives an email appearing to be from the vendor, containing a link to a malicious DLL. Challenge: Training OT staff to recognize sophisticated, industry-specific phishing attempts.

Physical Security – measures that protect equipment and facilities from unauthorized physical access. Related terms: access control, surveillance, tamper-evident seals. Example: A locked cabinet houses the primary network switch for the control zone. Challenge: Coordinating physical and logical security to avoid gaps where an attacker could bypass network controls.

PLC (Programmable Logic Controller) – industrial computer that executes control logic to manage machinery and processes. Related terms: ladder logic, firmware, IO modules. Example: A PLC reads sensor inputs, runs a control algorithm, and drives actuator outputs for a conveyor system. Challenge: Securing the PLC against unauthorized code changes while preserving deterministic execution.

Port Scanning – technique used to discover open network ports on a target device. Related terms: network reconnaissance, Nmap, service enumeration. Example: A security analyst runs a scan to identify which Modbus ports are exposed on the field network. Challenge: Scanning can disrupt time-critical traffic if not performed carefully.

Privileged Access Management (PAM) – controls that secure, monitor, and audit accounts with elevated rights. Related terms: password vault, session recording, just-in-time access. Example: An admin uses a PAM solution to retrieve a one-time password for a PLC before applying a firmware update. Challenge: Integrating PAM with legacy devices that lack API support.

Protocol Anomaly Detection – monitoring technique that flags deviations from expected protocol behavior. Related terms: behavioral analytics, IDS, baseline profiling. Example: A DNP3 master sends a “Write” command to a slave that normally only receives “Read” requests, triggering an alert. Challenge: Defining normal protocol patterns in environments with mixed vendor implementations.

Public Key Infrastructure (PKI) – framework for managing digital certificates and public-key encryption. Related terms: certificate authority (CA), CRL, TLS. Example: Each HMI receives a client certificate from the plant PKI to authenticate to the historian. Challenge: Provisioning and renewing certificates on devices with limited UI.

Q-Rating (IEC 61850) – security rating that assesses the resilience of communication devices against cyber attacks. Related terms: IEC 62443, security level (SL), risk assessment. Example: A substation relay is evaluated to meet a Q-Rating of 4, indicating strong resistance to network-based threats. Challenge: Achieving high Q-Ratings while maintaining compatibility with legacy field equipment.

Ransomware – malicious software that encrypts data and demands payment for decryption. Related terms:

crypto-locker, extortion, backup strategy. Example: A ransomware variant encrypts the configuration files of a DCS, preventing operators from changing set-points. Challenge: Restoring from backups without violating safety integrity during the recovery window.

Remote Access VPN – secure tunnel that enables authorized users to connect to internal networks from external locations. Related terms: two-factor authentication, split tunneling, network segmentation. Example: An off-site engineer uses a VPN to access the plant's engineering workstation for a scheduled update. Challenge: Ensuring VPN traffic is inspected and does not bypass segmentation controls.

Replay Attack – attempt to resend captured network packets to repeat a previously performed action. Related terms: nonce, timestamp, integrity check. Example: An attacker replays a valid "open valve" command captured earlier, causing unintended operation. Challenge: Implementing anti-replay mechanisms in protocols that lack built-in sequence numbers.

Risk Assessment – process of identifying, evaluating, and prioritizing risks to determine appropriate mitigation strategies. Related terms: threat modeling, impact analysis, risk matrix. Example: A risk assessment identifies the loss of confidentiality of process parameters as a moderate risk, prompting encryption at rest. Challenge: Quantifying impact on safety and production continuity.

Safety-Integrated Security (SIS) – approach that aligns safety and security controls to protect both people and assets. Related terms: IEC 61508, IEC 62443, risk reduction. Example: A safety-instrumented system (SIS) includes authentication checks before allowing a manual override. Challenge: Avoiding conflicts where security measures unintentionally inhibit safety functions.

Secure Boot – hardware-based process that verifies the integrity of firmware before execution. Related terms: trusted platform module (TPM), code signing, root of trust. Example: A PLC's bootloader checks a digital signature on the firmware image, refusing to load tampered code. Challenge: Managing keys across a large fleet of devices with limited management interfaces.

Security Information and Event Management (SIEM) – platform that aggregates, correlates, and analyzes log data from multiple sources. Related terms: log collection, correlation rules, alerting. Example: A SIEM correlates a failed login on a workstation with a simultaneous outbound connection to a known C2 server. Challenge: Normalizing logs from proprietary OT protocols that lack standard syslog output.

Security Operations Center (SOC) – centralized team responsible for monitoring, detection, and response to security incidents. Related terms: threat hunting, incident response, playbooks. Example: The SOC receives an alert from an IDS about anomalous Modbus traffic and initiates a containment workflow. Challenge: Staffing the SOC with expertise in both IT and OT domains.

Security Level (SL) – defined set of security requirements from IEC 62443, ranging from SL-1 (basic) to SL-4 (advanced). Related terms: risk assessment, defense-in-depth, Q-Rating. Example: A critical substation is required to meet SL-3, mandating strong authentication and encryption for all external connections. Challenge: Achieving higher SLs without impairing real-time control performance.

Secure Firmware Update – process that ensures firmware is authentic, integrity-checked, and applied safely.

Related terms: code signing, rollback protection, OTA (over-the-air). Example: A PLC receives a signed firmware image via a secure OTA channel, verifies the signature, and writes it to a protected partition. Challenge: Handling devices that lack built-in secure update mechanisms.

Segmentation – practice of dividing a network into zones to limit the spread of threats. Related terms: DMZ, VLAN, firewall. Example: The control network is segmented from the corporate IT network by a firewall that permits only specific management protocols. Challenge: Maintaining necessary communication paths for engineering while preventing unauthorized lateral movement.

Secure Shell (SSH) – cryptographic network protocol for secure remote login and command execution. Related terms: public key authentication, port forwarding, hardening. Example: An engineer uses SSH with key-based authentication to access a PLC's console for troubleshooting. Challenge: Ensuring SSH is disabled on devices where it is not required to reduce attack surface.

Supply Chain Attack – compromise of hardware or software components during manufacturing, distribution, or update. Related terms: software trojan, hardware backdoor, trusted supplier. Example: A compromised firmware image is inserted into a PLC during a vendor's third-party assembly process. Challenge: Verifying provenance of components in a global supply network.

Threat Intelligence – information about adversaries, tactics, techniques, and indicators that helps organizations anticipate attacks. Related terms: IOC, CTI, feed. Example: A feed provides hashes of known OT-targeted malware, which are used to update detection signatures. Challenge: Correlating generic threat intel with the specific asset inventory of an OT environment.

Threat Modeling – systematic analysis of potential threats to determine where security controls are needed. Related terms: attack trees, STRIDE, risk assessment. Example: A threat model identifies "unauthorized PLC reprogramming" as a high-impact scenario, leading to the implementation of code signing. Challenge: Capturing complex interactions between physical processes and cyber assets.

Time-Based One-Time Password (TOTP) – algorithm that generates a short-lived password based on a shared secret and the current time. Related terms: MFA, Google Authenticator, HOTP. Example: A field engineer uses a TOTP token on a mobile device to authenticate to a remote HMI. Challenge: Ensuring device clocks remain synchronized to avoid login failures.

Transport Layer Security (TLS) – cryptographic protocol that provides privacy and data integrity between communicating applications. Related terms: handshake, cipher suite, certificate. Example: An MQTT broker enforces TLS 1.2 For all client connections, encrypting telemetry data in transit.