2 Fundamentals of OT Systems Introduction

Topics

- Key Components of OT Systems
- Architecture and Design Principles of OT Networks and Systems
    - Hierarchy
    - Modularity
    - Determinism
    - Resiliency
    - Security
- Key OT Protocols

Key Components of OT Systems

Hardware

- **Sensors**
  - Monitor physical properties like temperature or pressure
- **Actuators**
  - Take instructions, usually from a PLC
  - Carry out physical actions like opening a valve or starting a motor
- **Programmable Logic Controllers (PLCs)**
  - The brains of the OT system
  - Process data from sensors and send commands to actuators
- **Networking Equipment**
  - Routers, switches, cables, etc.

Software

- **Operating Systems**
  - Manage the hardware resources of a device
  - Provide services for software applications
- **Applications**
  - Programs that carry out specific tasks
- **Firmware**
  - Low-level software that controls a device's hardware

Control Systems

- **Supervisory Control and Data Acquisition (SCADA) Systems**
  - High-level control system
  - Allows operators to monitor and control industrial processes remotely
- **Distributed Control Systems (DCS)**
  - Autonomously manages complex processes across a large facility
  - Distributes control functions across various subsystems
  - For greater efficiency and reliability

Architecture and Design Principles of OT Networks and Systems

Hierarchy

- At the top are enterprise-level systems, such as
  - **Enterprise Resource Planning (ERP)** systems
  - Link the operations on the factory flood with broader business goals
- Beneath that tier are **SCADA** systems
  - Managing industrial processes
- Middle layers contain control systems
  - **PLCs (Programmable Logic Controllers)** or
  - **DCS (Distributed Control Systems)**
- At the lowest level are field devices
  - Sensors and actuators

Purdue Model

- Level 6: The Security Management Layer
    - Implement security policies
    - Risk management
    - Incident response
    - Compliance
- Level 4/5: The Enterprise Business Systems Layer
    - ERP systems
- Level 3.5: The Demilitarized Zone (DMZ)
    - A buffer between internal and external networks, for security

Purdue Model

- Level 3: The Site Manufacturing Operations Layer
  - Work orders, schedules, etc.
- Level 2: The Area Supervisory Layer
  - SCADA
- Level 1: The Controller Layer
  - PLCs
- Level 0: The Physical Layer
  - Sensors and actuators that drive production systems

Modularity

- System uses distinct, independent modules
- Provides flexibility, scalability, and efficiency
- Advantage
  - Cost-effective: can upgrade or replace individual modules
- Disadvantage
  - Security: more modules increases attack surface

Determinism

- If a condition repeats, the same action will result
- Provides improved coordination, predictability, and performance
- Advantages
    - Performance and Reliability
- Disadvantage
    - Flexibility Trade-off
    - A highly deterministic system can be less flexible
    - Cannot adapt to changes or unexpected events

Resiliency

- The OT system's ability to maintain operations and quickly recover from adverse conditions or disruptions
  - Hardware failures, power outages, cyberattacks, etc.
- Resilience strategies
  - Processes to identify and isolate issues, implement fixes or workarounds, and validate that the system is functioning correctly
- Disadvantage
  - Increased costs, for
    - Redundant hardware
    - Managing and maintaining a more complex system
    - Disaster recovery planning

Security

- Protecting **Confidentiality**, **Integrity**, and **Availability**
- Prevent unauthorized access
- Risk management, monitoring, updates
- Key element
  - Incident Response Planning
- Challenge
  - Complexity

Key OT Protocols

Modbus, OPC, and DNP3

- **Modbus**
  - Old and simple, easy to implement
- **OPC (OLE for Process Control)**
  - Standard for data exchange in the OT world
  - Allows different hardware and software to communicate effectively
  - OPC UA (Unified Architecture)
    - Is popular, with platform independence and robust security features
- **DNP3 (Distributed Network Protocol)**
  - Robust and flexible
  - Popular in utilities sector

Ethernet/IP and PROFINET

- **Ethernet/IP**
  - A member of the DeviceNet family
  - Uses Ethernet infrastructure
- **PROFINET**
  - An extension of the popular PROFIBUS fieldbus system
  - High-speed and flexible architecture for industrial Ethernet

Kahoot!

Ch 2