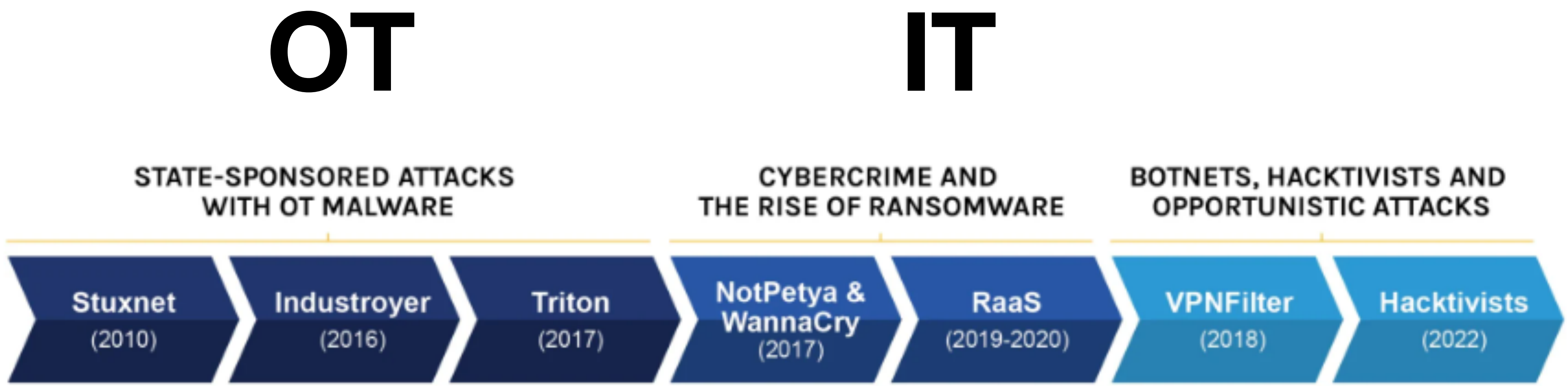
Securing Critical Infrastructure

Sam Bowne
April 28, 2025

History of Critical Infrastructure Security



- From https://www.forescout.com/blog/since-stuxnet-a-brief-history-of-critical-infrastructure-attacks/

1 Understanding Operational Technology

Operational Technology (OT)

- Technology that interacts with the physical world
- Hardware, software, and systems
  - That monitor, control, and optimize real-world processes
  - In industries including
    - Manufacturing
    - Transportation
    - Energy
    - Healthcare
    - And more

Topics

- Differentiating OT from IT
- Network Infrastructure for OT systems
- Protocols: The Traffic Rules of OT Communication
- Hierarchical Network Architecture: Organizing Chaos
- Network Performance - The Need for Speed and Precision
- Robustness and Reliability: Weathering the Storm
- Applications of OT in Industries

Differentiating OT from IT

OT v. IT

- OT
  - Concerned with the operation of physical processes
  - Like manufacturing, power generation, etc.
  - Drives machinery, controlling pressure, temperature, etc.
- IT
  - Computers, software, networks and systems
  - For processing and distributing data
  - Supports data analysis, decision making, communication, etc.

OT v. IT

- OT
  - Located on the plant floor
  - Direct control and management of industrial operations
- IT
  - Office-based
  - Computing and communication technologies, such as
  - Databases, email, enterprise resource planning systems

IT/OT Convergence

- Integrating the two domains can lead to
  - Improved efficiency, productivity, and decision-making
- IT Priorities
  - Confidentiality, Integrity, Availability
- OT Priorities
  - Safety, Reliability, Productivity

Network Infrastructure for OT Systems

Infrastructure

- Hardware and software
- That facilitates communication between OT components
  - Sensors, actuators, control systems, etc.
- Networks may be small and localized
  - Or multi-site networks spanning entire facilities
  - Or even geographical regions

Protocols

- Rules that define how data is sent over the network
- Traditional OT Protocols
  - **Modbus**
  - **Profibus**
  - **DNP3**
- Designed for reliability and real-time communication
- Prioritizing operational continuity over data security

Convergence

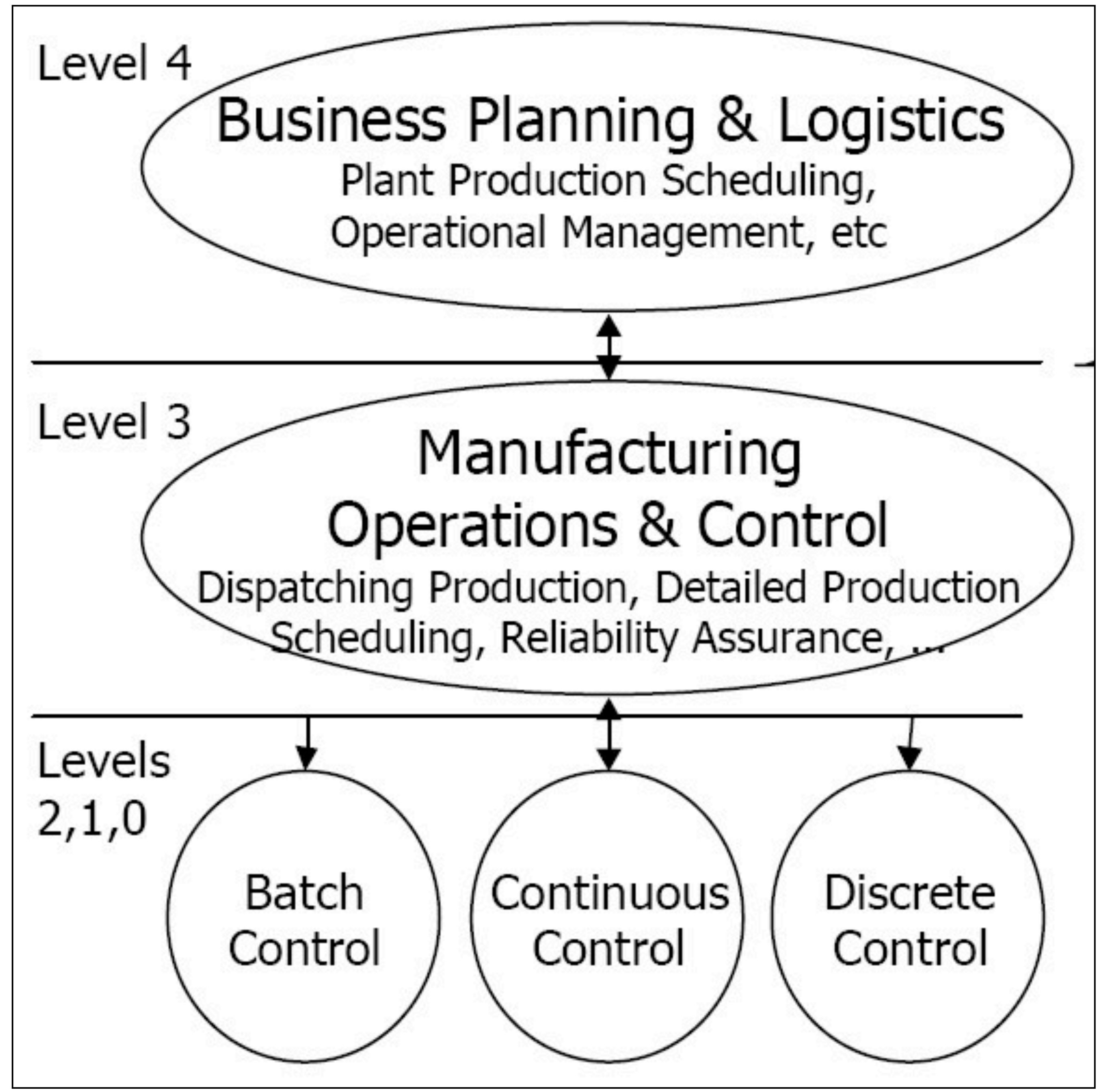
- TCP/IP is becoming prevalent in OT systems
- Benefits
  - Interoperability
  - Advanced data management capabilities
- Risks
  - Exposes OT systems to cyber-attacks

OT Network Architecture

- Hierarchical, with layers for:
  - Enterprise systems
  - Control systems
  - Field devices
- Factors to consider:
  - Determinism (actions occur at set, predictable times)
  - Latency (time between an instruction and data transfer)
  - Jitter (variation in latency)

Purdue Enterprise Reference Architecture (PERA)

- From Wikipedia



Protocols: The Traffic Rules of OT Communication

Protocols

- **Modbus**, **Profibus**, and **DNP3**
  - Provide real-time, reliable communications
  - Lightweight and simplistic
  - Require little computational power
  - Suited for resource-limited industrial settings

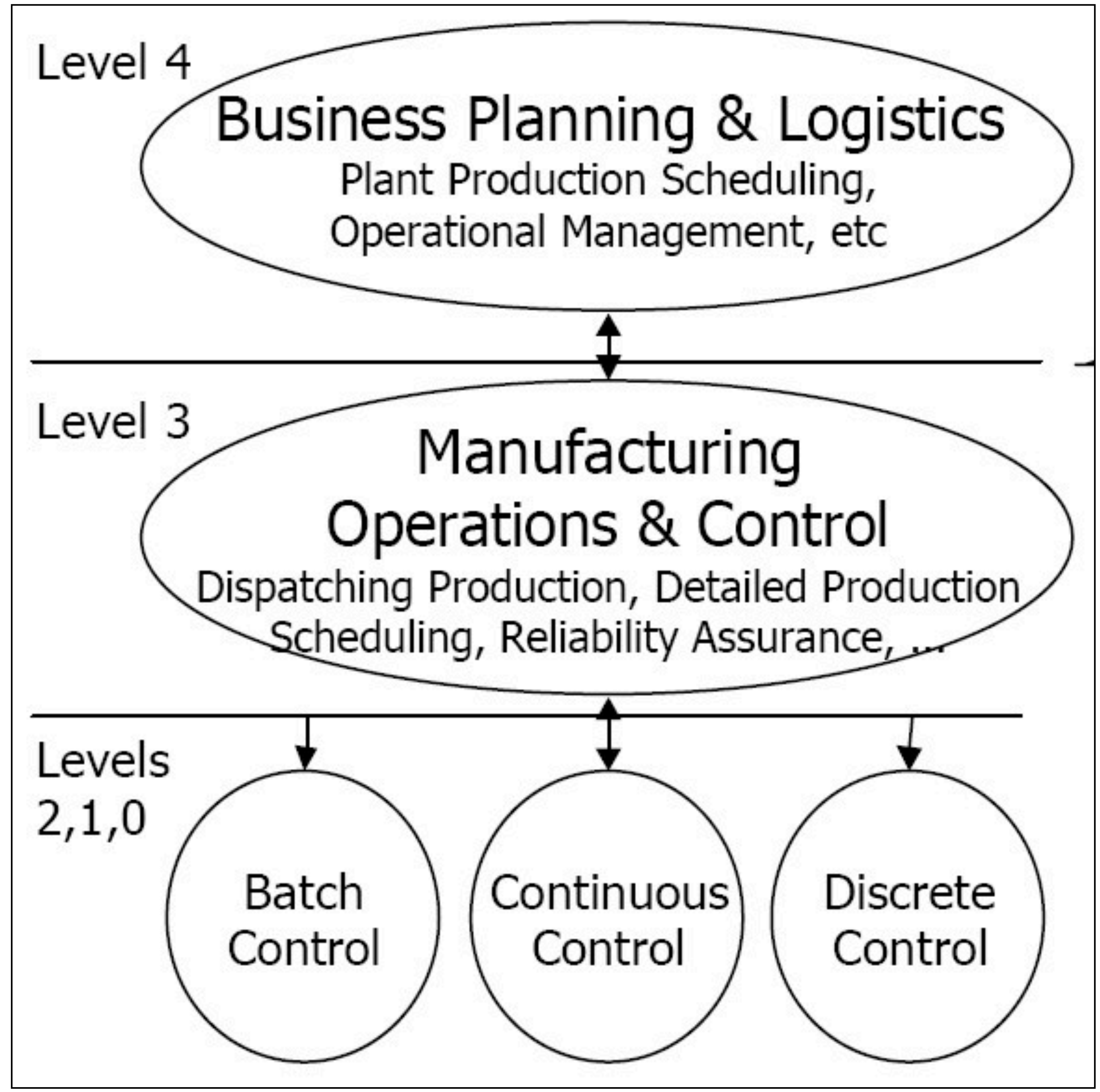
Comparing Protocols

- **Modbus**
  - Old and simple, from 1979
  - Easy deployment, rapid communication
- **Profibus**
  - A bit more complex
  - Greater data capacity
  - Can network an extensive range of automation devices
- **DNP3**
  - Most robust
  - Common in utilities, where telemetry data and control commands need to be reliably handled

Hierarchical Network Architecture: Organizing Chaos

Purdue Enterprise Reference Architecture (PERA)

- Top level
  - Enterprise systems
  - Data servers and managerial workstations
  - Data analysis, process optimization, and oversight of the entire operation
- Middle level
  - Control systems
- Lower levels
  - Sensors and actuators
  - Interact directly with physical processes



Network Performance - The Need for Speed and Precision

OT Network Requirements

- Real-time control (determinism)
- Latency
  - Lower latency means faster data transfer
- Jitter
  - Variation in latency
  - Must be minimized

Robustness and Reliability: Weathering the Storm

Planning for Contingencies

- OT systems operate in harsh environments
  - Power plant, oil rig, factory floor
- Plan for contingencies, such as
  - Equipment failure
  - Electromagnetic interference
  - Extreme environmental conditions
  - Physical tampering

Redundancy and Diversity

- Redundancy
  - Backup systems take over in case of failure
- Diversity
  - In components and technologies
  - Reduce common points of failure

Applications of OT in Industries

OT in Manufacturing

- Automates production processes
- Improves quality control
- Facilitates predictive maintenance
  - With Artificial Intelligence (AI) and Machine Learning (M L)
- Fully automated production line

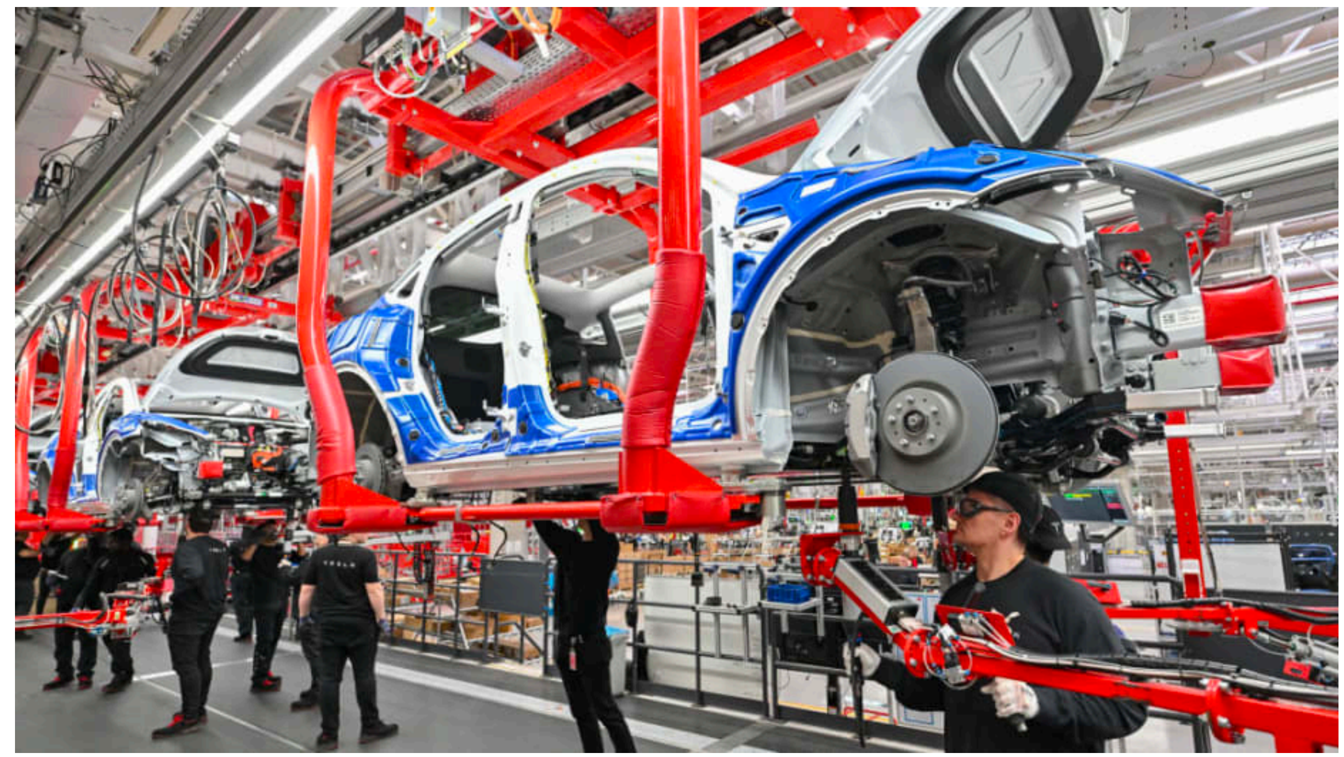


Image from https://www.cnbc.com/2023/07/24/tesla-to-discuss-factory-plan-for-new-24000-car-with-india-commerce-minister-says-report.html

Energy and Transportation

- Energy and Utilities
  - OT helps manage the generation and distribution of electricity
  - In a nuclear power plant, OT monitors and controls temperature and pressure
  - Adjusts the angle of turbine blades in a wind farm
- Transportation
  - Traffic management systems
    - Sensors monitor traffic flow and adjust signal timing
  - Control systems in railways and airports

Oil and Healthcare

- Oil and Gas
  - OT monitors and controls drilling operations
  - Manages pipeline flows
  - Detects leaks
  - Reduces the need for humans in harsh environments
- Healthcare
  - Manages HVAC in hospitals
  - Automated devices for patient care
    - Like infusion pumps that deliver doses of medicine at predetermined intervals

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

3 Integration of IT and OT Introduction

Topics

- Benefits of IT-OT Convergence
- Challenges and Considerations

Benefits of IT-OT Convergence

Enhanced Visibility and Decision-Making

- Data from sensors can be displayed on user-friendly dashboards
- Alerts can be sent for dangerous situations

- Image from https://periclesgroup.substack.com/p/how-homer-simpson-and-hippies-have

Benefits of Convergence

- **Increased Efficiency and Productivity**
  - Monitoring vehicles with GPS can improve fuel efficiency
- **Improved Agility and Innovation**
  - If the price of a mineral drops, production of it could be decreased
- **Better Risk Management and Cybersecurity**
  - Data from many sensors could detect unusual activity
  - Such as a cyberattack or malfunction

Challenges and Considerations

Challenges and Considerations

- **Cultural Differences**
  - OT team wants to maintain operation and reach production targets
  - IT team might prioritize protecting data integrity and IT security protocols
  - Training should help harmonize the teams
- **Technological Compatibility**
  - OT systems often use old technology, which is incompatible with modern IT gear
  - Upgrading OT devices may be difficult or costly
  - Middleware is a common solution

Challenges and Considerations

- **Security Concerns**
  - IT threats like malware may impact OT on a converged network
  - Defenses like firewalls, IDS, and access control can help
  - Awareness training and incident response plans are also needed
- **Data Overload**
  - OT devices may produce a lot of data, overwhelming IT log analysis systems
  - Data analytics and machine learning can help
  - This data may raise security and privacy concerns

Challenges and Considerations

- **Regulatory Compliance**
  - Local, regional, and international regulations about
  - Occupational safety, environmental sustainability, data privacy, and more