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

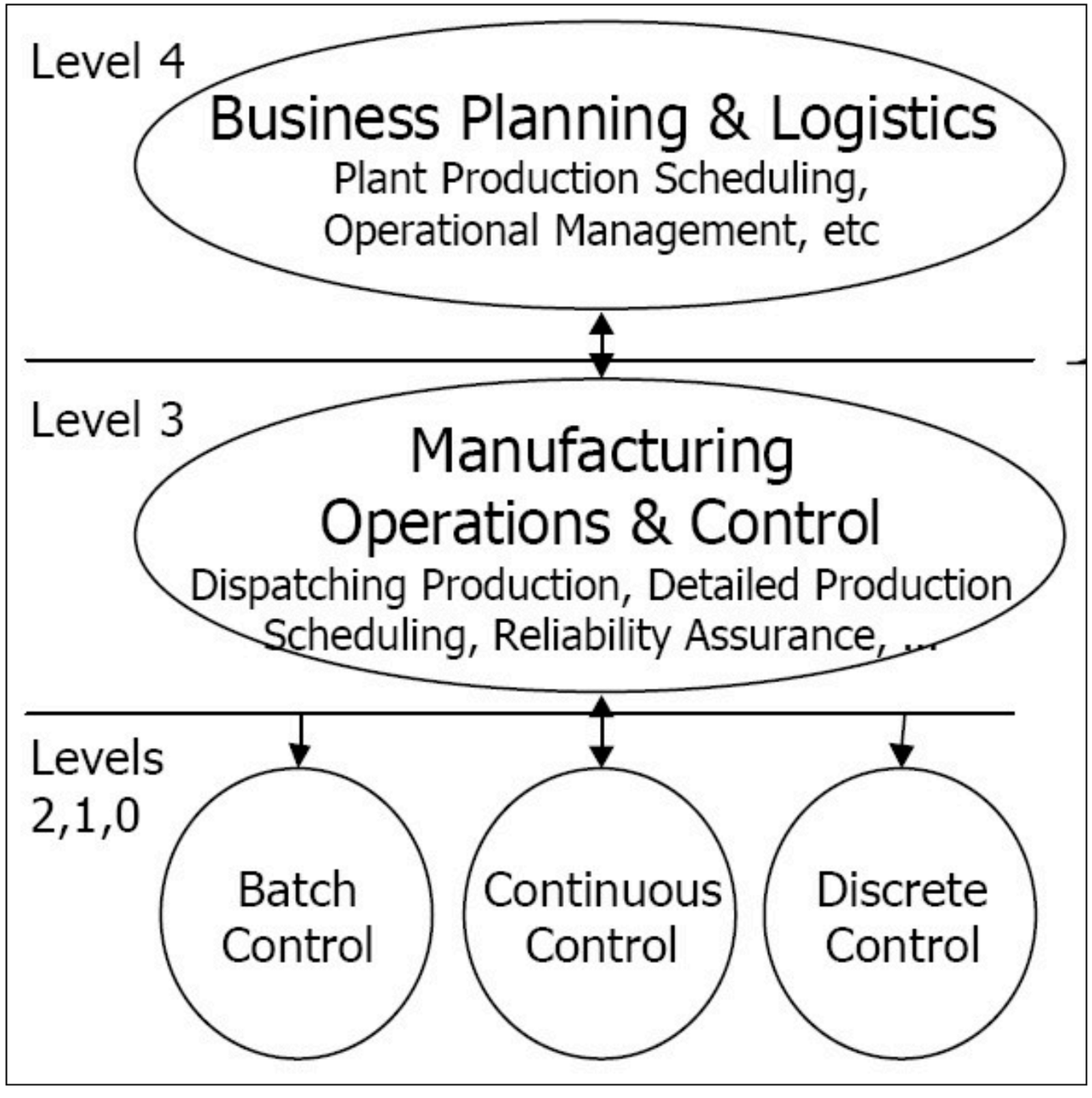
- TCP/IP is becoming prevalent in OT systems
- Benefits
  - Interoperability
  - Advanced data management capabilities
- Risks
  - Exposes OT systems to cyber-attacks

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

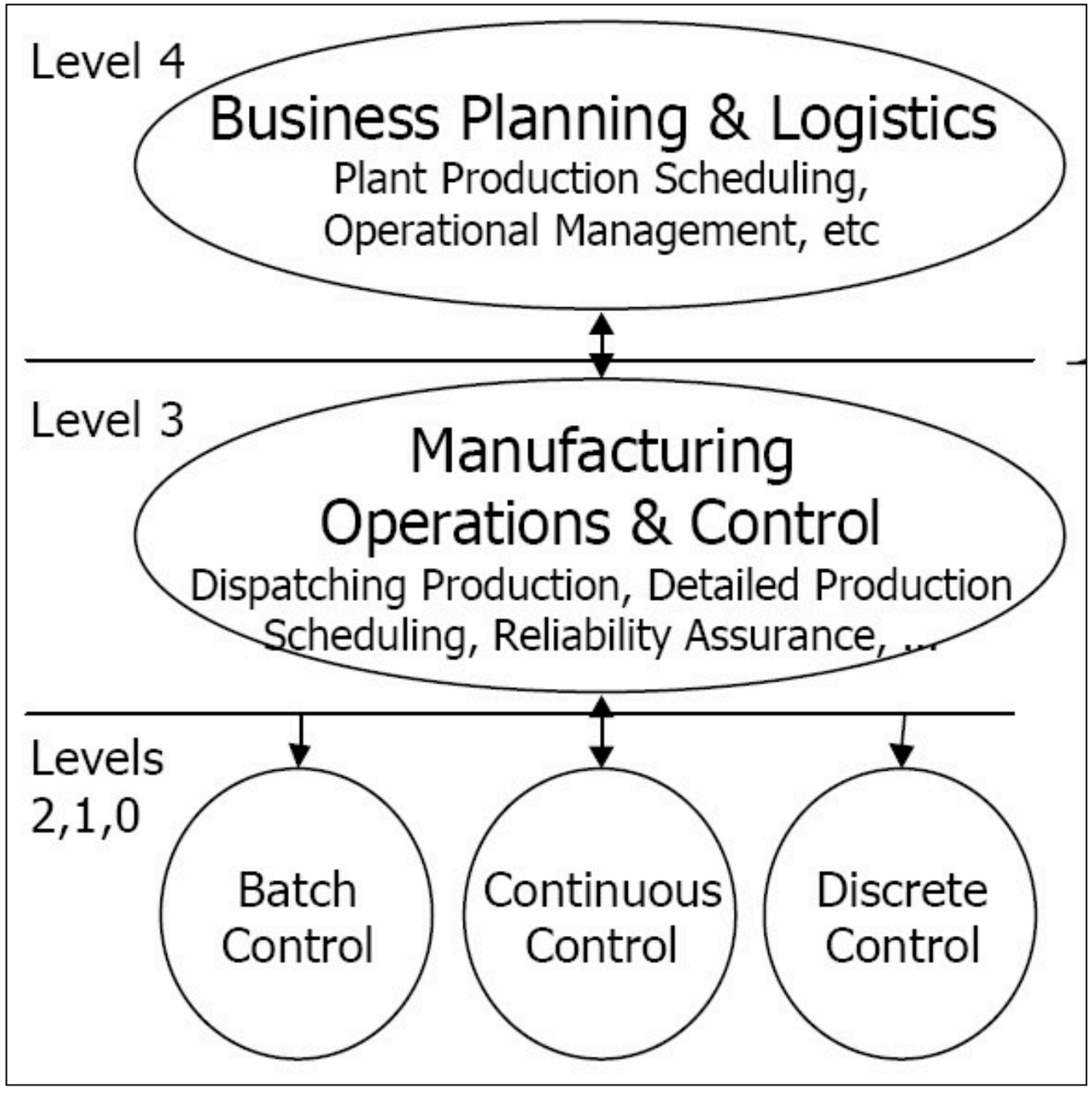
Comparing Protocols

- **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

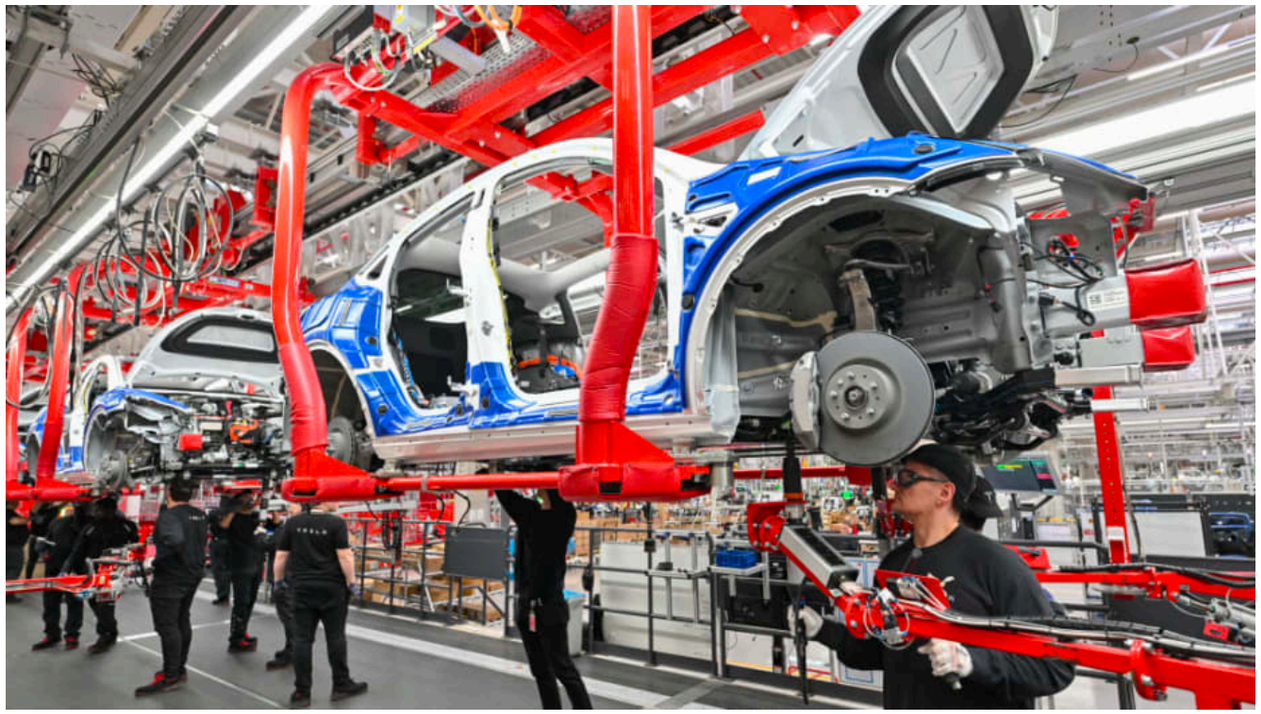


Image from https://www.cnbc.com/2023/07/24/tesla-to-discuss-factory-plan-for-new-24000-car-with-india-commerce-minister-says-report.html

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

Ch 1