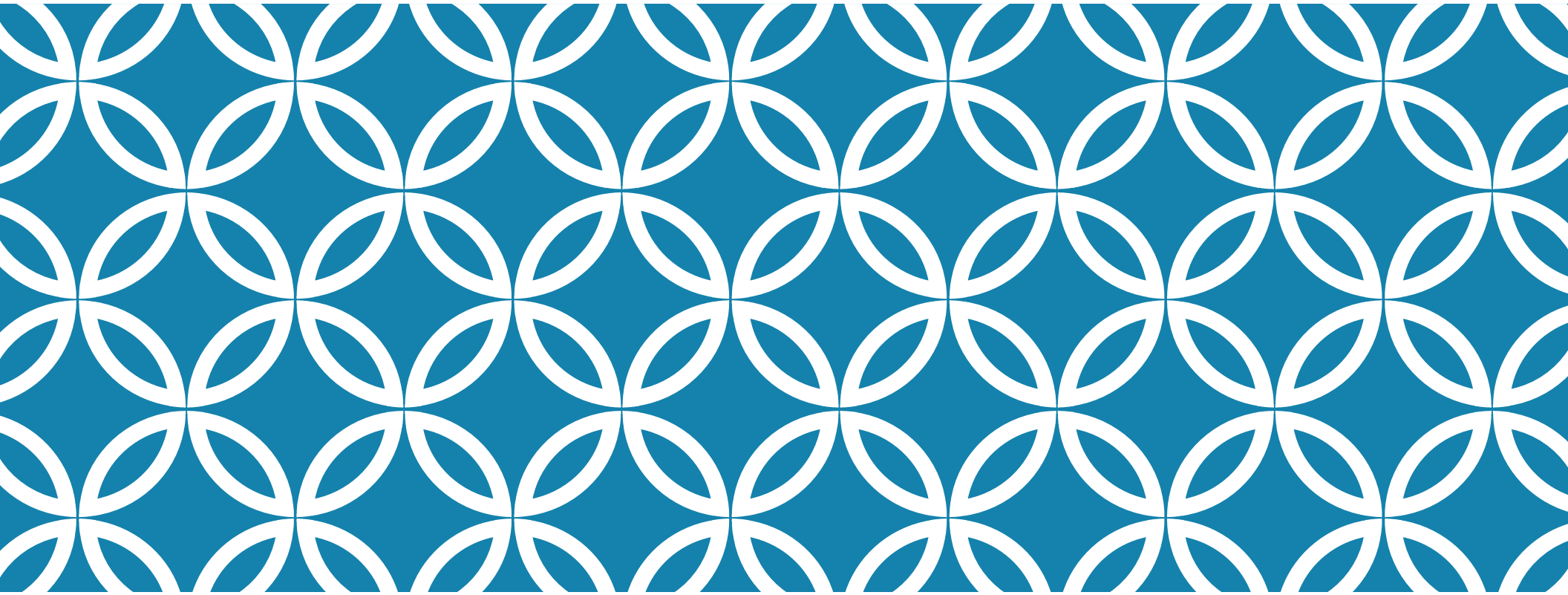


SCADA ARCHITECTURE

SCADA SYSTEM ARCHITECTURE - COMPONENTS

1. **Operator:** Human operator who monitors the SCADA system and performs supervisory control functions for the remote plant operations.

2. **Human machine interface (HMI)**: Presents data to the operator and provides for control inputs in a variety of formats, including graphics, schematics, windows, pull-down menus, touch-screens, and so on.

SCADA SYSTEM ARCHITECTURE - COMPONENTS

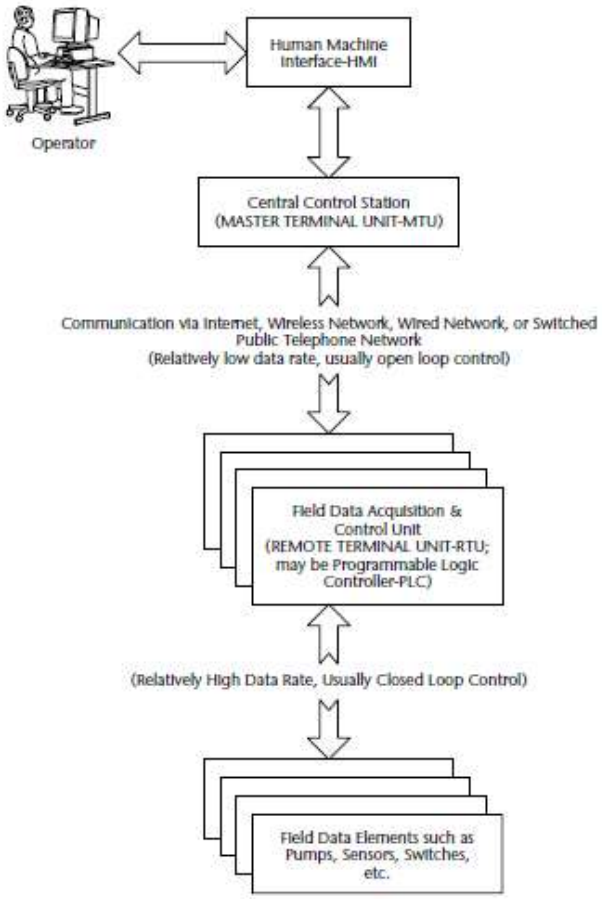
3.Master terminal unit (MTU): Equivalent to a master unit in a master/slave architecture. The MTU presents data to the operator through the HMI, gathers data from the distant site, and transmits control signals to the remote site. The transmission rate of data between the MTU and the remote site is relatively low and the control method is usually open loop because of possible time delays or data flow interruptions.

4.Communications means: Communication method between the MTU and remote controllers. Communication can be through the Internet, wireless or wired networks, or the switched public telephone network.

SCADA SYSTEM ARCHITECTURE - COMPONENTS

5. Remote terminal unit (RTU): Functions as a slave in the master/slave architecture. Sends control signals to the device under control, acquires data from these devices, and transmits the data to the MTU. An RTU may be a PLC. The data rate between the RTU and controlled device is relatively high and the control method is usually closed loop.

TYPICAL SCADA SYSTEMS ARCHITECTURE



TYPICAL SCADA SYSTEM ARCHITECTURE

SCADA architecture comprises two levels: a master or client level at the supervisory control center and a slave or data server level that interacts with the processes under control.

SCADA software components:

SCADA master/client

- Human machine interface
- Alarm handling
- Event and log monitoring
- Special applications
- ActiveX or Java controls

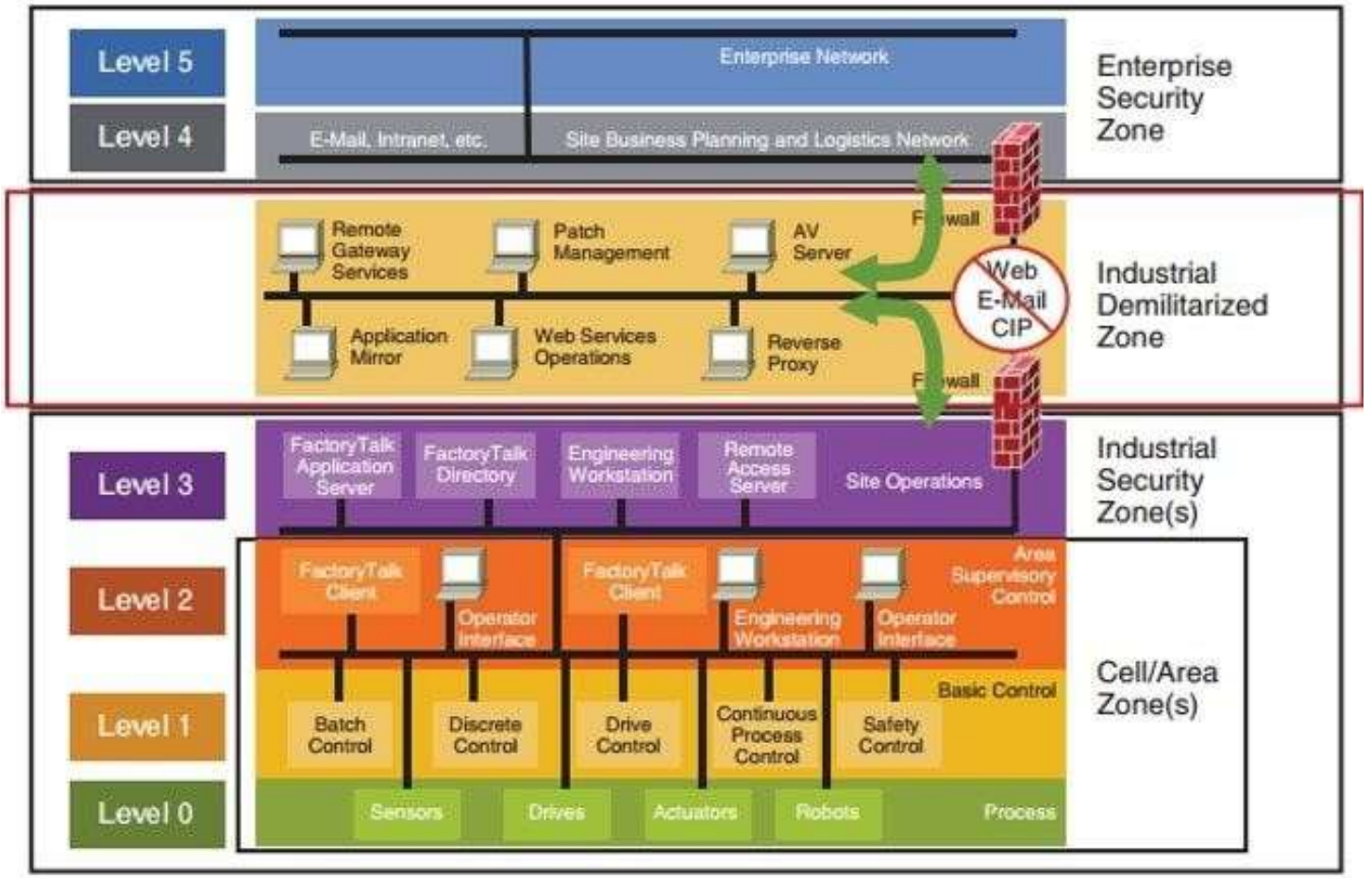
TYPICAL SCADA SYSTEM ARCHITECTURE

SCADA software components:

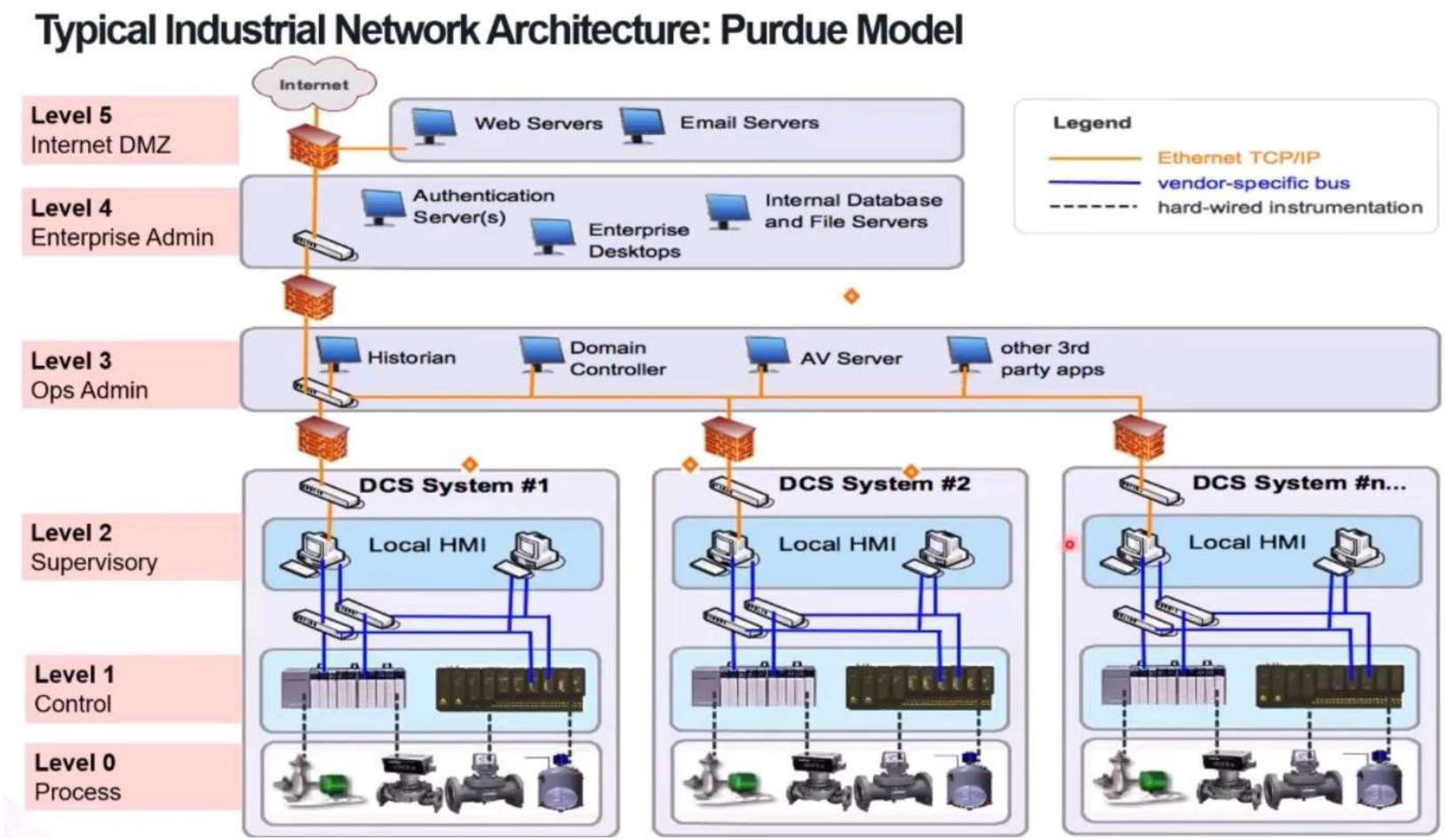
SCADA slave/data server

- Human machine interface
- Real-time system manager
- Data processing applications
- Report generator
- Alarm handling
- Drivers and interfaces to control components
- Spreadsheet
- Data logging
- Archiving
- Charting and trending

SCADA SYSTEM ARCHITECTURE



SCADA SYSTEM ARCHITECTURE



SCADA SYSTEM ARCHITECTURE – PURDUE MODEL

- The Purdue Enterprise Reference Architecture (PERA) reference model for enterprise architecture was developed in the 1990's by Theodore J. Williams and members of the Industry-Purdue University Consortium for Computer Integrated Manufacturing.
- This model was adopted by ISA-99 (now ISA/IEC 62443), among other industrial security standards, and used as a key concept for ICS network segmentation.
- The Purdue Reference Model, or just "Purdue Model" as it is now called in ICS communities, is widely used to describe the major interdependencies and interworking between all the major components in a major ICS and is a good place to start when trying to understand any OT environment.

SCADA SYSTEM ARCHITECTURE – PURDUE MODEL – ENFORCEMENT ZONE

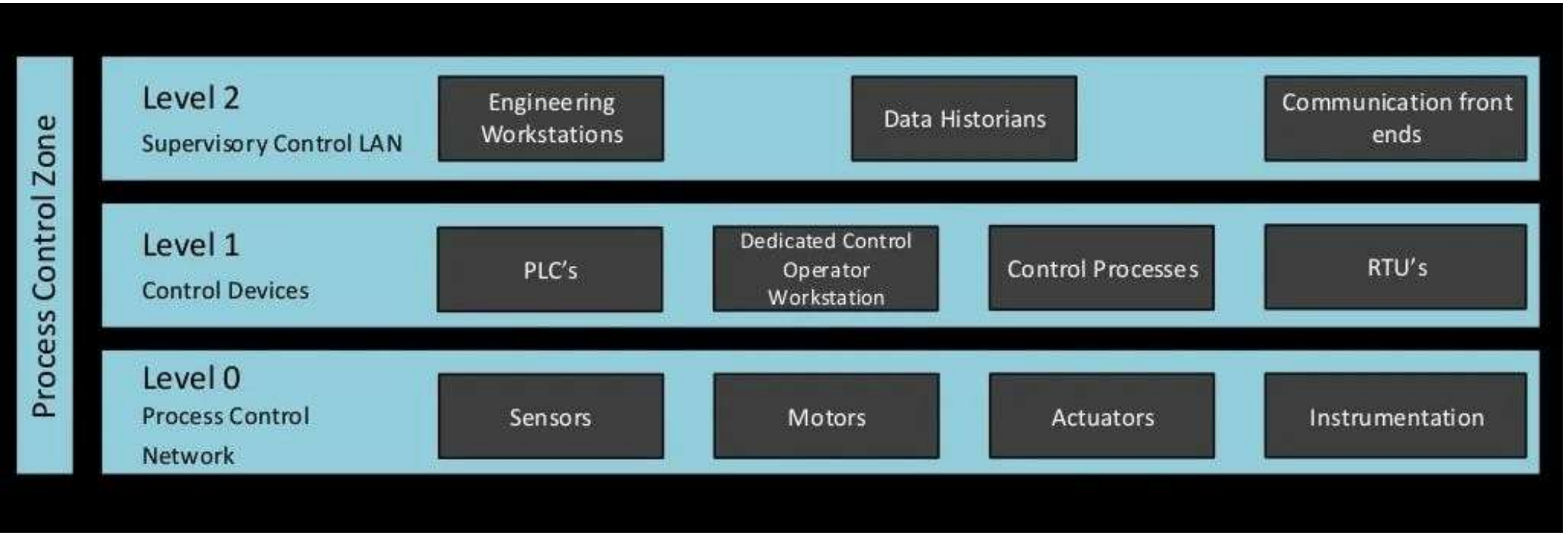
SCADA SYSTEM ARCHITECTURE – PURDUE MODEL – SAFETY ZONE

Safety Valve

Safety PLC

Safety Gear

SCADA SYSTEM ARCHITECTURE – PURDUE MODEL – PROCESS CONTROL ZONE



SCADA SYSTEM ARCHITECTURE – PURDUE MODEL – PROCESS CONTROL ZONE

SCADA SYSTEM ARCHITECTURE – PURDUE MODEL – PROCESS CONTROL ZONE

PLC - Programmable Logic Controller

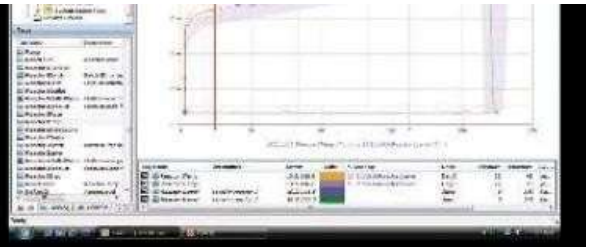
RTU - Remote Terminal Unit

Dedicated Operator Workstation

Level 1 Control Devices	PLC's	Dedicated Control Operator Workstation	Control Processes	RTU's

SCADA SYSTEM ARCHITECTURE – PURDUE MODEL – PROCESS CONTROL ZONE

HMI Panel



Data Historian

Control Room

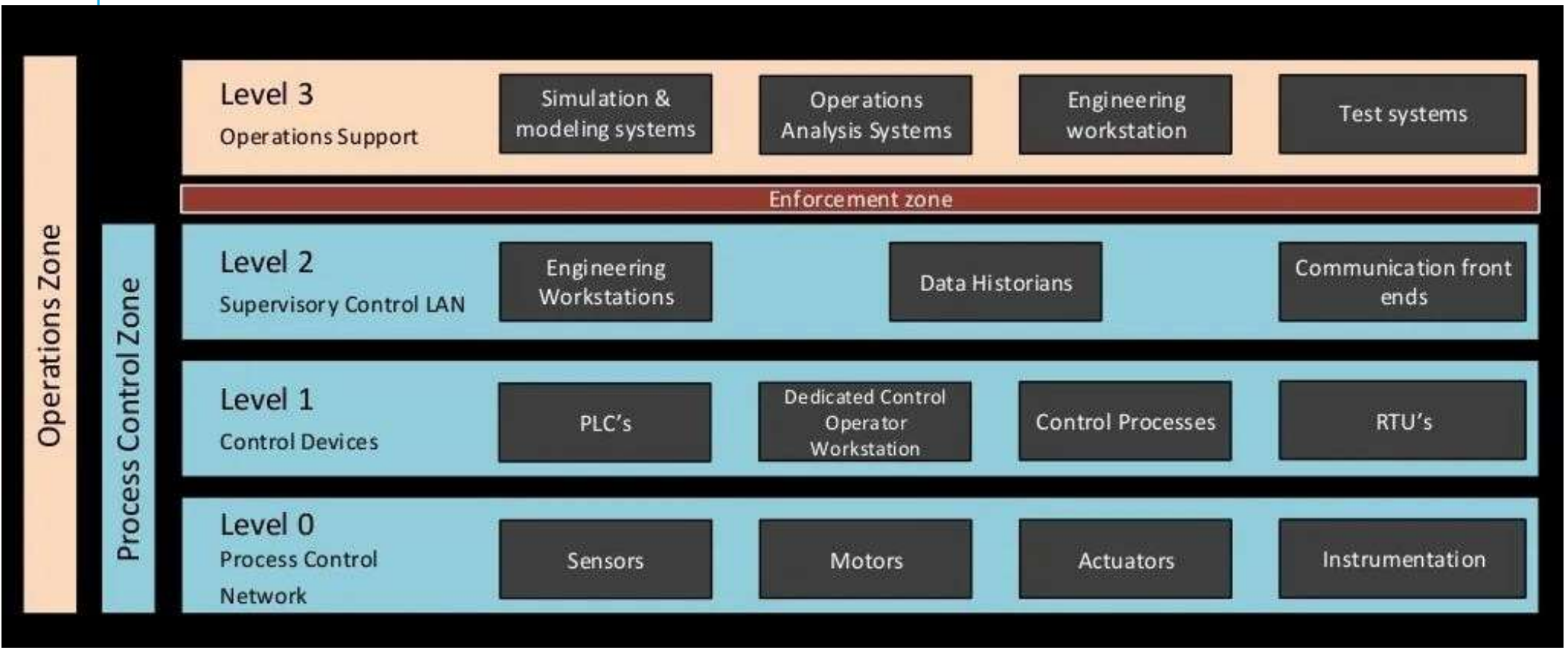
Level 2
Supervisory Control LAN

Engineering Workstations

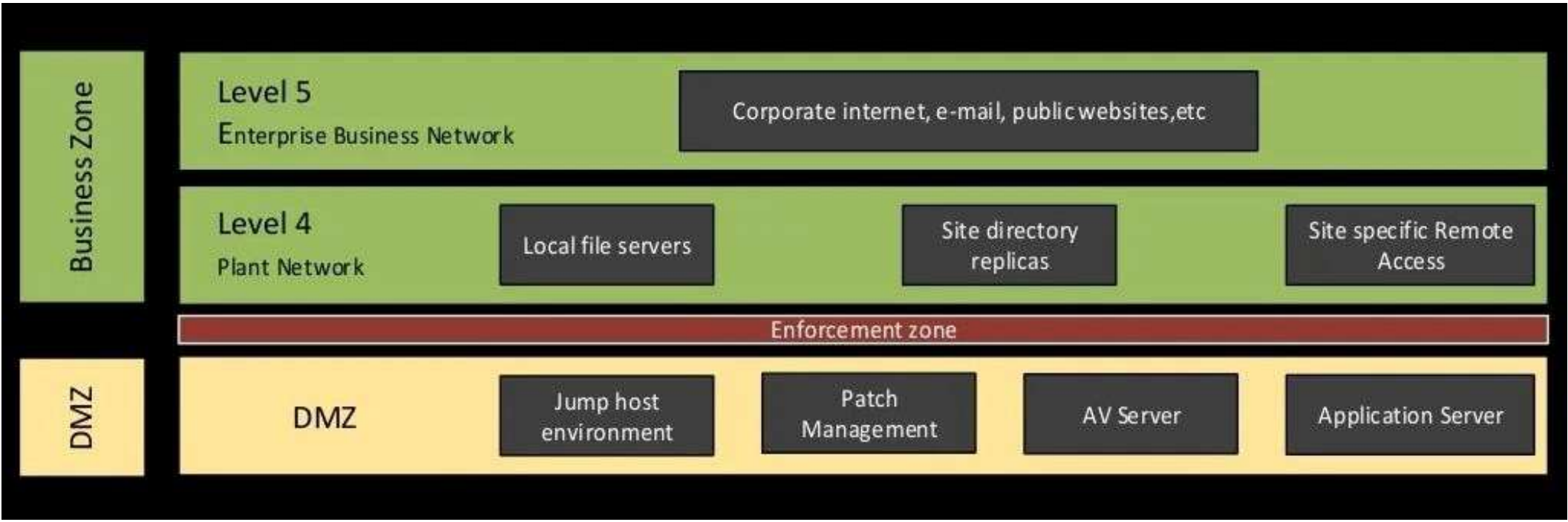
Data Historians

Communication front ends

SCADA SYSTEM ARCHITECTURE – PURDUE MODEL – OPERATIONS ZONE



SCADA SYSTEM ARCHITECTURE – PURDUE MODEL – DMZ & BUSINESS ZONE



SCADA SYSTEM ARCHITECTURE – PURDUE MODEL – LEVEL 5 ENTERPRISE ZONE

- The Enterprise Zone is where the supply chain is managed. ERP systems such as SAP and JD Edwards are used to understand and respond to supply and demand.

- These systems take data from all the subordinate systems, often across multiple sites or an enterprise, to look at overall supply, production, and demand to manage work orders.

- ICSs are rarely connected directly to this level, but there is a clear demand for accurate and timely information from the various OT networks and ICS components.

SCADA SYSTEM ARCHITECTURE – PURDUE MODEL – LEVEL 4 SITE BUSINESS PLANNING AND LOGISTICS

- Level 5 usually exists at a corporate or multisite headquarters, Level 4 represents the IT systems used at each site, plant, or facility to control the operation of the local facility.

- This level takes orders from Level 5 and monitors the performance at lower levels to understand the state of operations, performance against the production schedule, management of problems at the local plant, and updating enterprise systems at Level 5.

SCADA SYSTEM ARCHITECTURE – PURDUE MODEL – LEVEL 3.5 ICS-DEMILITARIZED ZONE

- The ICS-Demilitarized Zone (ICS-DMZ) is the layer for sharing information between IT and OT.
- This is a more modern construct, driven by standards efforts such as NIST Cybersecurity Framework, NIST 800-82, NERC CIP, and ISA-62443.
- Commonly present in the ICS-DMZ are replication servers, patch Management servers, engineering workstations, and configuration/change management systems
- The purpose of the DMZ is to provide a secure exchange of IT information without exposing critical components in lower layers directly to attack.

SCADA SYSTEM ARCHITECTURE – PURDUE MODEL – LEVEL 3 SITE MANUFACTURING AND OPERATIONS CONTROL

- While Levels 5 and 4 exist solely on the IT side of the network, with the DMZ being the filling in the Oreo cookie, so to speak, Levels 3 and below define and comprise the systems on the OT side of the network.

- Level 3 typically contains SCADA's supervisory aspect, DCS view and control access, or the control rooms with view and monitoring functions for the rest of the OT network.

- This is the primary layer for operator-level interaction with the system, with operators viewing and monitoring process events and trends, responding to alarms and events, managing uptime and availability of the process with functions such as work order maintenance, and ensuring product quality.

SCADA SYSTEM ARCHITECTURE – PURDUE MODEL – LEVEL 2 AREA SUPERVISORY CONTROL

- Level 2 has many of the same functions as Level 3, but this level is where process cell or line-level functions primarily exist for local control over individual areas of a process.
- This level is distinguished by being the level where actual ICSs start to appear, such as PLCs and Variable Frequency Drives (VFDs).
- However, the main systems at this level include HMIs. Within this level, you see a local view of live process events and operator-level process interaction through HMI panels and automated control of the process through these logic-driven components.

SCADA SYSTEM ARCHITECTURE – PURDUE MODEL – LEVEL 1 BASIC CONTROL

- Although some PLCs, VFDs, and the like exist at Level 2, this is the primary location for such equipment.
- This level compromises what is known as the Basic Process Control Systems, or BPCSs.
- BPCS is a generic term applying to nonsafety-related control systems in which the following functions are performed and managed:
  - BPCSs control the process within configurable limits (known as set points).

SCADA SYSTEM ARCHITECTURE – PURDUE MODEL – LEVEL 1 BASIC CONTROL

- BPCS is a generic term applying to nonsafety-related control systems in which the following functions are performed and managed:
  - BPCSs provide live data to HMIs for operator-level interaction with the process.
  - Operators interact with the set points and logic of the BPCS at this level to optimize the plant operations.
  - Process-level alarms and events are managed and responded to at this level. Level 2 depends on information from Levels 3 and above for schedule, monitoring alarms, and providing feedback on how to manage the process.
  - BPCSs also include sensors, actuators, relays, and other components that measure and report process values to PLCs, DCSs, SCADA, and other components in Levels 1-5.

SCADA SYSTEM ARCHITECTURE – PURDUE MODEL – LEVEL 0 PROCESS

- Also known as the Equipment Under Control (EUC) level, this is where the physical equipment that is being controlled by Level 1is located.
- These include drives, motors, valves, and other components that comprise the actual process.
- The integrity of Level 0 is paramount to safe and efficient operations, as this is where the actual physics of the process are manipulated. If the BPCS and the EUC fail to operate properly, or the information about the process state is inaccurate, then the BPCS or operators are unable to accurately respond to process conditions.

SCADA SYSTEM ARCHITECTURE – PURDUE MODEL – LEVEL 0 PROCESS

- Also known as the Equipment Under Control (EUC) level, this is where the physical equipment that is being controlled by Level 1is located.
- These include drives, motors, valves, and other components that comprise the actual process.
- The integrity of Level 0 is paramount to safe and efficient operations, as this is where the actual physics of the process are manipulated. If the BPCS and the EUC fail to operate properly, or the information about the process state is inaccurate, then the BPCS or operators are unable to accurately respond to process conditions.