ICS / OT Architecture & Network Fundamentals

Operational Technology · Industrial Control Systems

● LIVE · CTX_LOADED
REV 2026.05 · v1.0
SCOPE · OFFENSIVE PREP

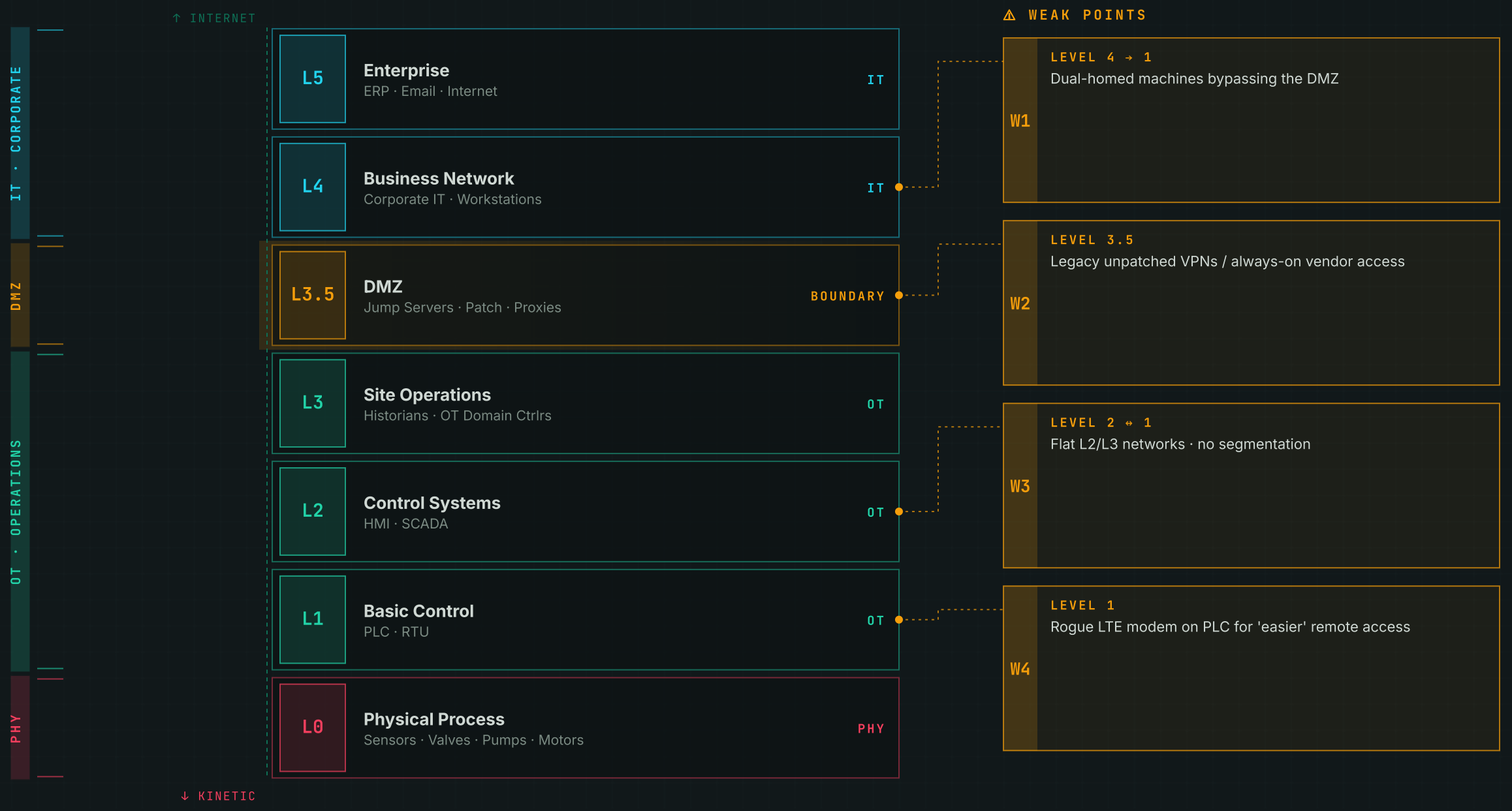
01

WHAT IT IS
The framework governing how industrial systems communicate, operate, and are isolated from corporate networks (IT).

WHY IT MATTERS
A breach in OT translates to kinetic impact — physical damage, environmental disaster, or loss of life.

WHERE
Manufacturing floors, power grids, water treatment facilities, offshore oil rigs.

§02 Purdue Model + IEC 62443 · zones · conduits · weak points



IT · L4-5 | DMZ · L3.5 | OT · L1-3 | Physical · L0

Industrial protocols (Modbus / DNP3 / CIP) ship without auth or encryption · routability ≈ control

§03 Attack Surface · where IT becomes OT

IT/OT Convergence	Compromise IT workstation → dump creds → lateral move through poorly-segmented OT DMZ.
Vendor Remote Access	Third-party maintenance with overly permissive, always-on access to L2/L3 assets.
Insecure Protocols	Modbus / DNP3 / CIP lack auth & encryption — if you can route to it, you can control it.

KILL CHAIN

01 Phishing (IT) → 02 Privilege Escalation → 03 Pivot to OT DMZ → 04 Compromise Engineering Workstation → 05 Send malicious logic to PLC

§04 MITRE ATT&CK · ICS · techniques most-used in OT compromise

T0866	**Exploitation of Remote Services**	Abusing RDP / VNC on HMIs.
T0889	**Modify Parameter**	Change setpoints on HMI — override temp limit → equipment failure.
T0836	**Modify Control Logic**	Push malicious ladder logic to PLC — change physical process behavior.

§05 Detection & Monitoring · signals · why active scans break OT

- ◉ **Cross-boundary traffic**
  Connections across IT ↔ OT boundary, esp. L4 IP → L1 PLC direct.
- ◉ **Abnormal PLC programming**
  STOP commands, logic uploads, downloads outside maintenance windows.
- ◉ **Why IT tools fail**
  Active scans crash fragile OT devices. Use passive taps (SPAN/Mirror) parsing industrial protocols.

§06 Mitigation & Hardening · what to actually deploy

- \+ **Zones & Conduits**
  IEC 62443 — group assets by security req (Zones); restrict comms to defined paths (Conduits).
- \+ **Secure Access**
  Zero-trust network access for vendors. Kill broad legacy VPNs.
- \+ **Jump Host Hardening**
  MFA on all jump boxes. Disable RDP copy/paste & drive mapping IT→OT.

§07 Red Team · offensive · what actually works

01 Living off the land — native engineering tools on compromised workstations are enough to manipulate processes.

02 Easy wins: cleartext passwords in vendor docs; rogue LTE modems plugged into PLCs by engineers.

03 Once inside, you rarely need exploits.

§08 Blue Team · defensive · what most teams miss

01 Don't over-focus on patching PLCs — uptime requirements make it brutal.

02 Highest impact: strict ingress/egress filtering at L3.5 DMZ.

03 If IT is ransomwared, OT must sever ties and operate autonomously.

§09 Quick Commands · passive only on production OT

```
› wireshark -Y 'modbus' ⟶ Filter Modbus TCP traffic
› grassmarlin --passive ⟶ Passive OT network mapping
› malcolm ingest pcap/ ⟶ Visualize OT traffic, no active scans
› nmap --script s7-info -sT ⟶ Use ONLY in lab — can crash live PLCs
```

§10 Memory Hooks · commit these to muscle memory

HOOK
Purdue
5=IT · 3=OT Servers · 2=HMI · 1=PLC · 0=Physics

HOOK
AIC not CIA
Availability > Integrity > Confidentiality. Uptime is king.

HOOK
IEC 62443
Gold standard. Remember: Zones & Conduits.