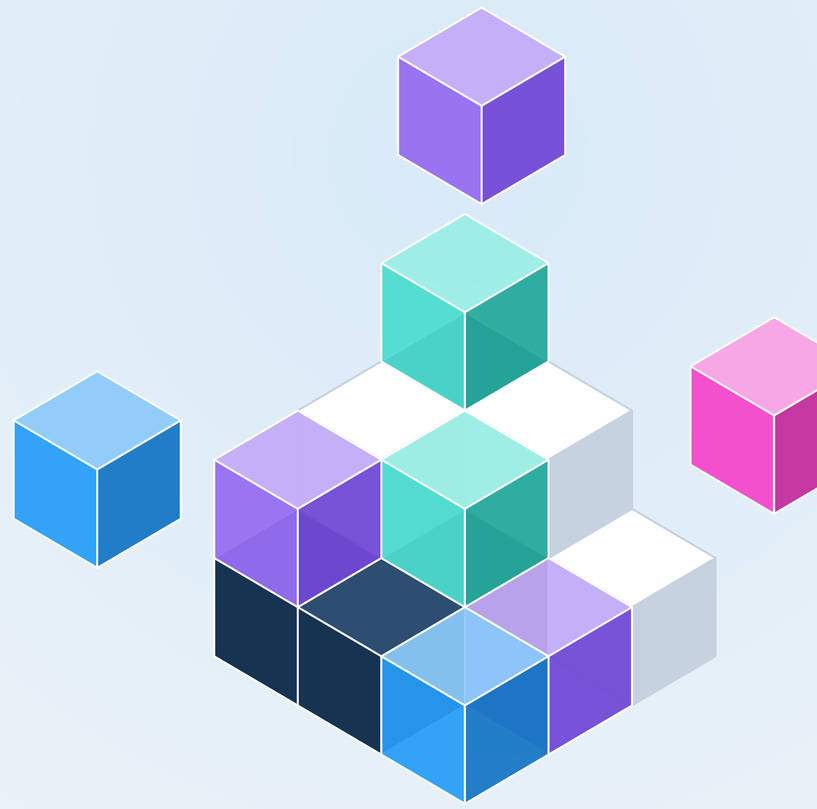
DIGITAL OPERATIONS

Cybersecurity for Industrial Operations

Industrial cybersecurity protects production systems with several layers of defense, separating IT and OT, controlling access and preparing to detect and recover from incidents.



01 THE CORE MODEL

DEFENSE IN DEPTH · LAYERED PROTECTION

LAYER 1	**Policies and people**	Training, access rules, incident plan
LAYER 2	**Perimeter**	Firewall between IT and OT, demilitarized zone
LAYER 3	**Network zones**	Segmented cells and conduits, IEC 62443
LAYER 4	**Endpoints**	Hardened PCs and HMIs, patch management
LAYER 5	**Control systems**	PLCs, safety systems, offline backups

DETECT AND RESPOND

PROTECT

IT/OT zones

Separate office and production networks, with controlled conduits between them.

Least privilege

Users and remote access get only the rights they need, when they need them.

Incident response

A tested plan to detect, isolate, recover and learn.

02 PROTECT AND RECOVER

Assume a breach will happen; plan to contain it and recover.

PERIMETER ONLY — DEFENSE IN DEPTH

PERIMETER-ONLY SECURITY

- − Flat network behind one firewall
- − Shared passwords on machines
- − No tested backups of PLC programs

DEFENSE IN DEPTH

- + Segmented zones contain an attack
- + Personal accounts, controlled remote access
- + Offline backups and recovery drills

03 WORKED EXAMPLE

REMOTE SERVICE ACCESS FOR MACHINE BUILDERS · ILLUSTRATIVE

RISK	→	CONTROL	→	ACCESS	→	RECOVERY
Open vendor VPN		**Jump server**		**On request, logged**		**Offline PLC backups**
always on, shared login		in the DMZ		personal accounts		tested every quarter

04 MANAGEMENT TAKEAWAYS

01 — Know your OT assets

You cannot protect machines and PLCs you have not listed.

02 — Segment the network

Zones stop one infection from stopping the whole plant.

03 — Practice recovery

Run drills to restore production from backups.

05 COMMON MISTAKE

LIMITATION

Treating OT like office IT

Patching and scanning production systems without planning can stop a line. Coordinate with operations.