FACTORYHELM SECURE OT PROGRAMME

Secure OT: start here

How to secure the OT that AI runs on, meet NIS2 and answer customer questionnaires with the files in this programme

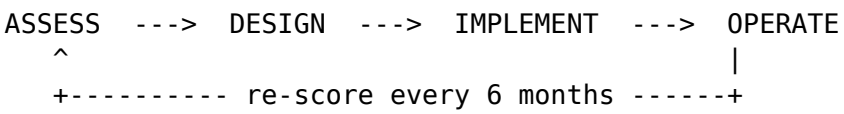
v1.1 (November 2026) | Worked example: Northbridge Components (fictional worked example)

Why this programme

Ransomware, open supplier access and flat networks are what stop plants, and NIS2 now makes management accountable for OT security. Customers pass the same requirements down their supply chain. This programme follows IEC 62443 and NIS2 in the order a lean team can do them: know your assets, zone them, control access, prepare for incidents and show the evidence.

The method on one page

Phase	What you do
1. Assess	Inventory assets and vulnerabilities; zone the plant; set target security levels; check NIS2 scope.
2. Design	Write the cybersecurity requirements; approve policy, procedures and the remote access standard.
3. Implement	Close SR gaps by priority; route all remote access through the broker; run the roadmap.
4. Operate	Triage vulnerabilities monthly, exercise incident playbooks, report NIS2 incidents on time, answer customers.



The files, in the order to use them

#	File	Phase	Who	Effort
1	OT Asset Inventory and Vulnerability Workbook (Excel)	Assess	Controls engineering per plant	2-4 days per plant
2	IEC 62443 Zones, Conduits and Risk Workbook (Excel)	Assess	OT Security Lead	2-3 days per plant
3	IEC 62443-3-3 System Requirements Gap Checklist (Excel)	Assess	OT Security Lead + integrator	1 day per critical zone
4	NIS2 and CRA Readiness Workbook (Excel)	Assess	CISO + Legal	1 day
5	Cybersecurity Requirements Specification (Word)	Design	OT Security Lead	2 days per critical line
6	OT Security Policy and Core Procedures (Word)	Design	OT Security Lead; MD approves	2 days
7	OT Secure Remote Access Standard and	Design	OT Security Lead	1 day

Remote access register, pre-filled for three plants

From OT Remote Access Register (Excel), sheet "Connection Register". Worked example: Northbridge Components (fictional), three plants: Chemnitz (DE), Plzen (CZ), Greenville (US).

Connection Register

Every remote path into OT. Risk score and rating are calculated. | FactoryHelm OT Remote Access Kit | factoryhelm.com | v1.1 (November 2026)

Conn ID	Plant	Supplier / user group	Assets reached	Zone / Purdue level	Method	MFA (Y/N)	Recorded (Y/N)	Always-on (Y/N)	Approval per session (Y/N)	Reaches L1-L2 directly (Y/N)	Business owner	Last used	Last reviewed	Risk score (calc)	Rating (calc)	Review due (calc)	Action
RA-01	Chemnitz (DE)	VisionEdge (AI vision)	Weld line W2 vision IPC	Z-CELL-W2 / L2	Jump host (DMZ, MFA, recorded)	Y	Y	N	Y	N	Production Manager W	2026-11-03	2026-10-01	0	Low	Due 2026-12-31	
RA-02	Chemnitz (DE)	RoboWeld GmbH (robot OEM)	Robot controllers W1-W3	Z-CELL-W / L1	4G/5G router on machine	N	N	Y	N	Y	Maintenance Lead	2026-09-18		13	Critical	Never reviewed	Remove router; move to jump host (Q1 2027 shutdown)
RA-03	Chemnitz (DE)	Historian vendor	Site historian	Z-SITE / L3	Vendor cloud portal via DMZ broker	Y	Y	N	Y	N	OT Engineer	2026-10-22	2026-10-01	1	Low	Due 2026-12-31	
RA-04	Chemnitz (DE)	Press OEM	Press line P1 PLC + HMI	Z-CELL-P / L1	Remote desktop tool (TeamViewer etc.)	N	N	N	N	Y	Maintenance Lead	2026-06-02		10	Critical	Never reviewed	Uninstall tool; issue jump host account
RA-05	Plzen (CZ)	Integrator (MES)	MES servers	Z-SITE / L3	Site-to-site VPN	Y	N	Y	N	N	IT Plant Lead	2026-11-10	2026-07-15	8	High	Overdue	Add session recording; turn tunnel on per request
RA-06	Plzen (CZ)	Compressor OEM	Compressor controllers	Z-UTIL / L1	4G/5G router on machine	N	N	Y	N	Y	Facilities			13	Critical	Never reviewed	Unknown until walk-down; disconnect SIM
RA-07	Plzen (CZ)	CNC OEM	CNC cell C4	Z-CELL-C / L2	Vendor cloud portal via DMZ broker	Y	Y	N	Y	N	Production Manager C	2026-08-30	2026-10-01	1	Low	Due 2026-12-31	
RA-08	Greenville (US)	Furnace OEM	Heat treat furnace PLC	Z-CELL-HT / L1	Client VPN to OT	Y	N	N	Y	Y	Plant Engineer	2026-10-05	2026-08-20	6	High	Due 2026-11-19	Route via jump host; stop direct L1 reach
RA-09	Greenville (US)	PdM analytics vendor	Vibration gateway	Z-DMZ / L3.5	Vendor cloud portal via DMZ broker	Y	Y	Y	N	N	Reliability Engineer	2026-11-14	2026-09-01	4	Medium	Due 2026-12-01	Data push only; confirm no inbound
RA-10	Group / Corporate	Internal OT engineers (on call)	All plants via jump host	DMZ / L3.5	Jump host (DMZ, MFA, recorded)	Y	Y	N	N	N	OT Security Lead	2026-11-15	2026-10-01	1	Low	Due 2026-12-31	
RA-11	Chemnitz (DE)	Drives supplier	Line W drives	Z-CELL-W / L1	Direct inbound port	N	N	Y	N	Y	Maintenance Lead			13	Critical	Never reviewed	Found in firewall review: close port 5900 now