Common OT Network Ports

Reference for ICS/SCADA firewall rules, traffic baselining and asset discovery. Ports are TCP unless noted.

Industrial Protocols

Port	Protocol / Service	Used For
502	Modbus TCP	Read/write PLC registers and coils; also carries Schneider UMAS
802	Modbus TCP Security	Modbus over TLS
20000 TCP/UDP	DNP3	SCADA master to RTU/outstation telemetry (common in water and electric)
19999	DNP3 Secure (TLS)	Secure DNP3
2404	IEC 60870-5-104	Telecontrol, mostly European utilities
102	ISO-TSAP	Siemens S7comm, IEC 61850 MMS, ICCP/TASE.2
44818 TCP/UDP	EtherNet/IP (CIP)	Explicit messaging to Rockwell/Allen-Bradley PLCs
2222 UDP	EtherNet/IP	Implicit (Class 1) real-time I/O
2221	EtherNet/IP Secure	CIP over TLS
34962–34964	PROFINET	Siemens and other PROFINET devices (RT traffic is Layer 2)
4840	OPC UA	Vendor-neutral data exchange, HMI/historian to PLC
135 + dynamic	OPC DA / DCOM	Legacy OPC Classic (difficult to firewall)
47808 UDP	BACnet/IP	Building automation, HVAC
1911 / 4911	Niagara Fox	Tridium building management (4911 is TLS)
18245 / 18246 UDP	GE SRTP / EGD	GE PLC programming and data exchange
9600 UDP	Omron FINS	Omron PLC communications
5006 / 5007	MELSEC	Mitsubishi PLCs
1962	PCWorx	Phoenix Contact PLCs
20547	ProConOS	KW-Software runtime (Phoenix Contact and others)
1217 / 2455	CODESYS	CODESYS runtime programming
789	Red Lion Crimson	Red Lion HMIs and data stations
4000	ROC Plus	Emerson flow computers and RTUs
5094 TCP/UDP	HART-IP	Field instrument configuration and diagnostics
1089–1091	Foundation Fieldbus HSE	Process field devices
1883 / 8883	MQTT (Sparkplug B)	Edge-to-SCADA publish/subscribe (8883 is TLS)

SCADA, HMI and Historians

Port	Protocol / Service	Used For
14000	GE Proficy Historian	Collector to historian archiver; client queries

Port	Protocol / Service	Used For
135 + dynamic	DCOM (iFIX/OPC collectors)	iFIX and OPC collector to historian
2010	iFIX networking	SCADA node to iClient/View node
8088 / 8043	Ignition Gateway	Inductive Automation HTTP/HTTPS
5413	Wonderware SuiteLink	AVEVA/Wonderware I/O servers
5450	PI Data Archive	AVEVA/OSIsoft PI historian
1433	Microsoft SQL Server	Historians, alarm and event databases

Supporting IT Services Common in OT

Port	Protocol / Service	Used For
21 / 69 UDP	FTP / TFTP	Firmware and configuration transfers (cleartext)
22 / 23	SSH / Telnet	Device management; Telnet still common on legacy gear
80 / 443	HTTP / HTTPS	Device web interfaces, thin-client HMIs
123 UDP	NTP	Time sync for logs and sequence-of-events
319 / 320 UDP	PTP (IEEE 1588)	Precision time for substations and motion control
161 / 162 UDP	SNMP	Switch and device monitoring, traps
514 UDP	Syslog	Log forwarding to SIEM/collector
3389	RDP	Engineering workstation and HMI remote access
5900	VNC	HMI panel remote viewing

Notes

IEC 61850 GOOSE and Sampled Values, and PROFINET RT, run at Layer 2 with no IP port, so port-based firewall rules will not see them.

DCOM (port 135) hands off to dynamic high ports. Restrict the DCOM port range on iFIX, OPC and collector hosts, or the firewall rule ends up wide open.

Vendors can reconfigure many of these defaults. Validate against actual traffic captures before writing rules.