Making a Career in OT / ICS / SCADA Security

Protect the systems that run the physical world.

AUTHOR	Babashaheer
VERSION	1.0
DATE	April 2026
SERIES	Cybersecurity Career Series — Document 11 of 12
AUDIENCE	Engineers and security professionals entering the OT/ICS security field

Contents

Digitally signed by Baba Shaheer Gutappa
Date: 2026.04.25 10:24:10 +01'00'

1. What Is OT / ICS / SCADA Security?

Every time you turn on a light, fill your car with petrol, turn on a tap or board a train, you are depending on Operational Technology — physical systems controlled by computers. Power grids, water treatment plants, oil pipelines, gas distribution networks, manufacturing lines, railway signalling systems, hospital equipment — all are controlled by industrial computers that were designed decades ago with no thought given to cybersecurity.

OT/ICS/SCADA security is the discipline of protecting these systems from cyberattack. It is one of the most consequential and fastest-growing specialisms in cybersecurity — because an attack on a power grid or water treatment plant does not just cost money. It can injure or kill people, cause environmental disasters and destabilise critical national infrastructure.

OT security is where cybersecurity meets the physical world.
A breach in IT loses data. A breach in OT can shut down a hospital, contaminate a water supply or cause an explosion at a refinery.

Level	Typical UK Salary	Common Roles
Junior	£35,000 – £52,000	OT Security Analyst, ICS Security Consultant (junior), CNI Security Analyst
Mid	£55,000 – £80,000	OT/ICS Security Engineer, SCADA Security Specialist, OT Penetration Tester
Senior	£80,000 – £110,000+	Lead OT Security Architect, Head of ICS Security, CNI Security Lead
Specialist	£700 – £1,200/day	Independent OT Security Consultant, ICS Penetration Test Lead

Table 1: UK salary ranges for OT/ICS security roles (CW Jobs, 2024)

2. Key Terminology — OT, ICS, SCADA, DCS, PLC, RTU

OT/ICS security has its own dense vocabulary. Understanding these terms is the first step — they describe real physical systems, not abstract concepts.

Term	Full Name	What It Is	Where You Find It
OT	Operational Technology	Hardware and software that monitors and controls physical processes — distinct from IT which processes information	Any industrial environment: energy, manufacturing, transport, water
ICS	Industrial Control System	The umbrella term for all systems used to control industrial processes — includes SCADA, DCS, PLCs and RTUs	Power plants, refineries, factories, utilities
SCADA	Supervisory Control and Data Acquisition	Centralised system that monitors and controls geographically dispersed assets — reads sensor data and sends commands	Water networks, gas pipelines, electricity distribution, railways
DCS	Distributed Control System	Control system for continuous processes where control is distributed across multiple controllers in a plant	Chemical plants, oil refineries, power stations — processes that run continuously
PLC	Programmable Logic Controller	Rugged industrial computer that directly controls physical equipment — reads inputs (sensors) and drives outputs (valves, motors)	Factory floors, pumping stations, any automated physical process
RTU	Remote Terminal Unit	Similar to PLC but designed for geographically remote locations with limited communications — reports status and receives commands	Remote pipeline monitoring, substations, weather stations
HMI	Human-Machine Interface	The screen and controls that a human operator uses to monitor and interact with the industrial process	Control rooms, engineering workstations
Historian	Process Historian	Database server that records all process data over time — used for analysis, compliance and troubleshooting	Typically at Level 3 of the Purdue Model

Table 2: Key OT/ICS terminology every security professional must know

3. The Purdue Model — How OT Networks Are Structured

The Purdue Enterprise Reference Architecture (PERA) — commonly called the Purdue Model — is the standard framework for understanding how industrial control system networks are structured. It defines five levels, from the physical process at the bottom to enterprise business systems at the top. Every OT security professional must understand it intimately — it is the map of the environment you protect.

The Purdue Model — OT/ICS Network Architecture

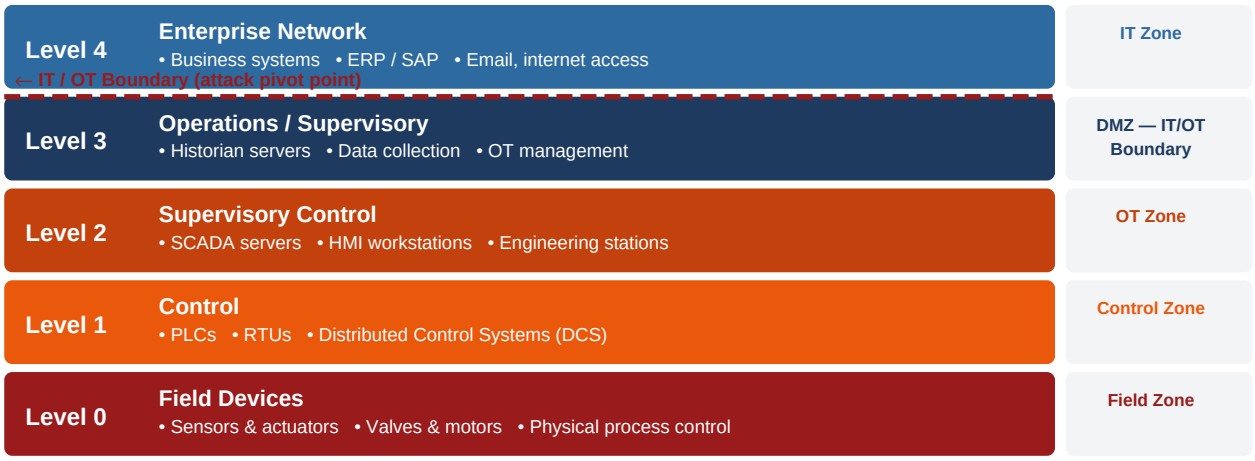


Figure 1: The Purdue Model. The red dashed line marks the IT/OT boundary — the most critical security boundary in any industrial environment.

The IT/OT boundary is where most OT attacks cross over.
Attackers compromise IT systems first, then pivot through the Historian or engineering workstations to reach PLCs and physical process control.

4. Why OT Security Is Fundamentally Different from IT Security

The single most important thing to understand about OT security is that you cannot apply IT security practices directly to OT environments. The constraints are completely different — and ignoring this is how OT security projects fail and how well-meaning IT security professionals cause production outages.

	IT Security	OT / ICS Security
Primary concern	Confidentiality, then integrity, then availability (CIA)	Availability first, then integrity — confidentiality is secondary
Patching	Patch regularly — monthly or faster	Cannot patch — patches require testing, planned downtime, vendor approval. Some systems cannot be patched at all.
Availability	Systems can be rebooted, backed up, restored	Systems run 24/7/365 — many cannot be restarted without shutting down physical processes
Antivirus	Standard deployment	Often cannot run on OT devices — insufficient CPU/RAM, may break industrial software
Encryption	TLS everywhere, standard practice	Many OT protocols (Modbus, DNP3, Profibus) have no encryption support — adding it can break timing requirements
Lifespan	3–7 years, regular replacement	10–30 years is normal. Some SCADA systems run Windows XP or older — no patches available
Incident response	Isolate, investigate, restore from backup	Isolating a PLC may shut down a power plant. 'Turn it off and on again' is not an option
Vulnerability scanning	Scan everything regularly	Aggressive scanning can crash OT devices — some PLCs hang or reboot when port-scanned

Table 3: IT security vs OT/ICS security — the fundamental differences

Typical OT Attack Path

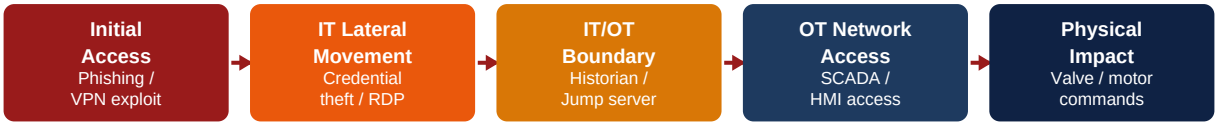


Figure 2: Typical OT attack path — initial access via IT, pivot through IT/OT boundary, reach physical control.

5. The Threat Landscape — Who Attacks OT and Why

OT attacks are carried out by nation-state actors, cybercriminals and, less commonly, hacktivists and insiders. The motivations and capabilities differ significantly — understanding who is targeting critical infrastructure and why shapes how you defend it.

Actor	Motivation	OT Attack Goal	Notable Examples
Nation-state (Russia, China, Iran, North Korea)	Geopolitical — espionage, pre-positioning for conflict, sabotage	Persistent access to CNI for intelligence gathering and potential future disruption	Sandworm (Ukraine power grid 2015/2016), Triton/TRISIS (Saudi Aramco 2017)
Ransomware groups	Financial — ransom payment	Often IT-focused but OT is collateral damage when IT/OT are connected	Colonial Pipeline (2021) — fuel supply disrupted across US East Coast
Hacktivist groups	Political/ideological — disruption and embarrassment	Operational disruption, public attention	Attacks on water utilities in US and Israel (2023–2024)
Insider threats	Financial gain, grievance, coercion	Sabotage — insider has direct access to PLCs and process control	Numerous documented cases in water, manufacturing and energy sectors
Nation-state pre-positioning	Strategic — prepare for wartime disruption	Dormant access to critical infrastructure, ready to activate	Volt Typhoon (Chinese pre-positioning in US CNI, 2024)

Table 4: Threat actors targeting OT/ICS — motivation and goals

6. Landmark OT Attacks — Learning from Real Incidents

The history of OT cyberattacks is short but alarming. Each major incident revealed new capabilities and shifted the entire field's understanding of what is possible. Every OT security professional must know these cases.

Incident	Year	Target	What Happened	Significance
Stuxnet	2010	Iranian uranium enrichment (Natanz)	US/Israeli malware destroyed ~1,000 centrifuges by manipulating PLC speed while showing normal readings to operators	First confirmed nation-state cyberweapon causing physical destruction. Proved ICS attacks were real.
Ukraine Power Grid	2015	Ukrainian electricity distribution	BlackEnergy malware + coordinated attack cut power to ~225,000 customers for hours	First confirmed cyberattack causing a power outage. Attackers operated circuit breakers remotely.
Ukraine Power Grid 2	2016	Ukrainian transmission substation	INDUSTROYER/Crashoverride malware designed to speak native ICS protocols (IEC 104, IEC 61850)	First malware specifically designed for ICS protocols — not adapted IT malware.
Triton / TRISIS	2017	Saudi Aramco petrochemical plant	Targeted Triconex Safety Instrumented Systems — designed to disable safety shutdowns	Attacked safety systems. If successful, could have caused explosion and casualties.
Colonial Pipeline	2021	US fuel pipeline operator	DarkSide ransomware hit IT systems — Colonial shut down OT as precaution	Ransomware causing OT shutdown. Fuel shortages across US East Coast. $4.4M ransom paid.
Oldsmar Water Plant	2021	Florida water treatment facility	Attacker remotely accessed HMI and increased sodium hydroxide to 111x safe level	Showed that small utilities with minimal security are soft targets for OT attacks.

Table 5: Landmark OT/ICS cyberattacks — each one changed the field

7. Core OT Security Principles and Frameworks

OT security has its own set of frameworks and standards that acknowledge the unique constraints of industrial environments. Applying IT frameworks directly to OT without adaptation leads to broken systems and failed projects.

Key OT security principles

- **Network segmentation first:** The single most effective OT security control is strict network segmentation — air gaps or DMZs between IT and OT, and between OT zones. This limits attacker movement even if one zone is compromised.
- **Passive monitoring, not active scanning:** Because aggressive scans can crash OT devices, monitoring in OT environments is passive — capturing and analysing network traffic without sending probes. Tools like Claroty, Dragos and Nozomi work this way.
- **Asset inventory is the foundation:** You cannot protect what you cannot see. Building a complete inventory of every OT device — vendor, model, firmware version, network connections — is the first step in every OT security programme.
- **Zero Trust for remote access:** Remote access to OT systems (used by vendors, engineers and operators) is a major attack vector. Every remote session must be authenticated, recorded and terminated when complete. Jump servers with MFA are the standard.
- **Incident response must preserve operations:** OT incident response plans must account for the fact that shutting down systems may cause greater harm than the attack itself. Response procedures must be developed with operational engineers.
- **Vendor and supply chain risk:** OT vendors routinely require remote access to maintain equipment. This access must be controlled, monitored and time-limited. Supply chain attacks (Stuxnet was delivered via USB by a contractor) are a real vector.

Framework / Standard	Published By	Scope	Mandatory?
IEC 62443	IEC (International Electrotechnical Commission)	The most comprehensive international standard for ICS cybersecurity — covers risk assessment, system design, component requirements	Voluntary globally; required by contract in many critical sectors
NIST SP 800-82	NIST	Guide to ICS security — covers SCADA, DCS, PLC environments with IT/OT convergence guidance	Mandatory for US federal agencies; widely adopted globally as best practice
NCSC CAF — Cyber Assessment Framework	UK NCSC	UK framework for critical national infrastructure operators — 14 principles across 4 objectives	Mandatory for UK CNI operators regulated under NIS Regulations

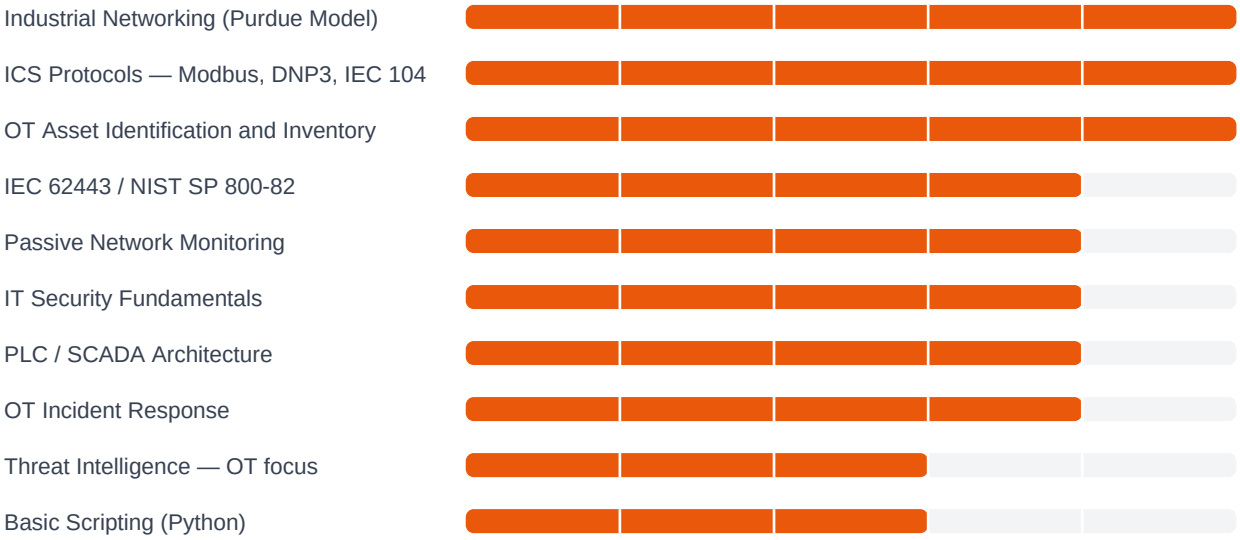
Framework / Standard	Published By	Scope	Mandatory?
NERC CIP	North American Electric Reliability Corporation	Mandatory cybersecurity standards for electricity sector in North America	Mandatory for US/Canadian electricity sector — fines up to $1M/day
ISA/IEC 62443	ISA	Practitioner-focused OT security standards — widely referenced in engineering projects	De facto standard for industrial automation cybersecurity worldwide

Table 6: Key OT/ICS security frameworks and standards

8. Core Skills and Tools

OT security requires a hybrid skill set that most IT security professionals do not have. You need enough engineering knowledge to understand what PLCs and SCADA systems actually do — and enough security knowledge to know how to protect them without breaking them.

Skills expected at mid-level OT security engineer:



Tool / Platform	Category	What It Does	Cost
Claroty	OT Asset Visibility / IDS	Passive monitoring of OT networks. Auto-discovers all OT assets, detects anomalies, maps communications.	Commercial
Dragos	OT Threat Detection	OT-specific threat detection platform. Includes threat intelligence on ICS-focused threat groups.	Commercial
Nozomi Networks	OT/IoT Visibility	Passive asset discovery and anomaly detection across OT and IoT. Strong for mixed IT/OT environments.	Commercial
Claroty / Tenable OT	Vulnerability Management	OT-aware vulnerability assessment without aggressive scanning that could crash devices.	Commercial
Wireshark + OT dissectors	Protocol Analysis	Wireshark with plugins for Modbus, DNP3, EtherNet/IP, PROFINET — read industrial protocol traffic.	Free
ScadaFence	OT Network Monitoring	Passive OT monitoring focused on manufacturing and energy environments.	Commercial
OpenPLC Runtime	Lab / Learning	Open-source PLC simulator. Run ladder logic on a Raspberry Pi. Essential for OT security labs.	Free
GRFICS	ICS Simulation	Graphical Realism Framework for ICS — free simulation environment for practising OT attacks and defence.	Free

Tool / Platform	Category	What It Does	Cost
S7 Comm Scanner / PLCScan	OT Scanning	Discover Siemens S7 and other PLC devices on a network — used in OT pen testing.	Free

Table 7: Core tools for OT/ICS security professionals

9. Career Paths in OT / ICS Security

OT security is a niche with a chronic shortage of qualified professionals. The combination of engineering knowledge and security expertise is rare. This means salaries are high, demand is growing fast and experienced professionals are genuinely scarce. Good entry paths include IT security with OT specialisation, or engineering with security overlay.

Role	What You Do	Where You Work	UK Salary
OT/ICS Security Analyst	Monitor OT networks using passive tools. Triage anomalies. Maintain asset inventory.	Energy, utilities, manufacturing	£35k–£52k
OT Security Engineer	Implement OT security controls — segmentation, monitoring, remote access security, patching programme.	CNI operators, oil & gas, power	£55k–£75k
ICS Penetration Tester	Test OT/ICS environments for vulnerabilities — safely, without crashing production systems.	Specialist consultancies, NCSC	£60k–£90k
OT Security Architect	Design OT security architectures — Purdue model implementation, IT/OT boundary design, Zero Trust for OT.	Large energy companies, consulting	£75k–£100k
CNI Security Specialist	Advise on and implement security for critical national infrastructure — regulated environment.	Government, NCSC, CNI operators	£70k–£95k
OT Security Consultant	Independent advisory and assessment across multiple industrial clients.	Self-employed, specialist firms	£700–£1,200/day

Table 8: Career paths in OT/ICS security (Reed, 2024; CW Jobs, 2024)

10. The Learning Roadmap

Most OT security professionals come from one of two backgrounds: IT security professionals who learn the OT side, or engineers (electrical, chemical, mechanical) who learn the security side. Both paths work — the hybrid knowledge is what makes the role scarce and well-paid.

1. **Understand industrial systems — what they control and how**
   Read NIST SP 800-82 (free PDF). Watch YouTube videos on how PLCs work, what SCADA systems do, how a power grid or water treatment plant operates. You must understand the physical process before you can secure it. 2–3 weeks.

2. **Learn the Purdue Model deeply**
   Draw the Purdue Model from memory. Understand what sits at each level, what protocols cross each boundary, and why the IT/OT boundary is the critical security point. Read the ICS-CERT resources on ics-cert.us-cert.gov. 1 week.

3. **Study ICS protocols**
   Learn what Modbus, DNP3, IEC 104 and EtherNet/IP are, what they do, and why their lack of authentication is a security problem. Wireshark with OT dissectors lets you analyse real protocol traffic in a lab. 2–3 weeks.

4. **Build an OT lab**
   Install OpenPLC Runtime on a Raspberry Pi (free). Simulate a simple process. Use GRFICS (free, open-source ICS simulation). Practice Modbus commands. Even a basic lab gives you hands-on experience no certification replicates. 2–3 weeks.

5. **Study IEC 62443**
   Read the IEC 62443 standard overview (ISA publishes good summaries). Understand the four security levels, the zone and conduit model, and what a security requirements specification looks like. This is the dominant framework in OT security engagements. 2–3 weeks.

6. **Take the SANS ICS curriculum**
   ICS410 (ICS/SCADA Security Essentials) is the entry-level SANS OT course. It is expensive but the most complete structured learning available. The Dragos Year in Review reports and CISA ICS advisories are free alternatives. Ongoing.

7. **Get GICSP certified**
   The Global Industrial Cyber Security Professional (GICSP) from GIAC is the most widely recognised OT security certification. It validates both ICS knowledge and security expertise. Pairs well with CompTIA Security+.

8. **Apply for OT security roles**
   CNI operators (National Grid, Thames Water, Network Rail, NHS), oil & gas companies, NCSC, specialist OT security consultancies (Dragos, Claroty, Applied Risk, Resilience). Your OT lab and GICSP make you a genuine candidate.

Timeline: 12–18 months from IT security background to first OT security role.
From engineering background adding security: 9–14 months.
The scarcity of qualified OT security professionals means demand far exceeds supply.

11. Certifications That Matter

Certification	Level	Provider	Focus	Why It Matters
CompTIA Security+	Beginner	CompTIA	Broad IT security foundations	Baseline before OT specialisation. Required by some CNI employers.
GICSP — Global Industrial Cyber Security Professional	Mid	GIAC / SANS	ICS/OT security — Purdue model, OT protocols, risk assessment, incident response	The most widely recognised OT security certification. Validates both OT knowledge and security expertise.
ICS410 — ICS/SCADA Security Essentials	Mid	SANS	Comprehensive OT security training — the course that leads to GICSP	The gold-standard OT security course. Expensive but comprehensive.
ICS515 — ICS Visibility, Detection and Response	Mid–Senior	SANS / Dragos	OT threat hunting, network monitoring, incident response in ICS environments	Advanced OT operations training. Highly regarded by CNI operators and government.
CSSA — Certified SCADA Security Architect	Mid	IACRB	SCADA security architecture and risk assessment	Vendor-neutral SCADA-specific certification. Less well-known than GICSP but respected.
IEC 62443 Cybersecurity Certificate	Mid	ISA / Exida	IEC 62443 standard — the dominant OT security framework	Demonstrates specific knowledge of the dominant regulatory and contractual standard in OT.
CISM / CISSP	Senior	ISACA / ISC2	Security management — applied to OT context	For OT security managers and leads. Combines with OT-specific knowledge for senior roles.

Table 9: Certifications for OT/ICS security professionals

12. Case Study — A Water Treatment Plant Attack

> This fictional case study is based on the documented 2021 Oldsmar, Florida water treatment attack.
> It illustrates the unique challenges of OT incident detection and response.

The Organisation

Westfield Water Services operates a water treatment facility serving 12,000 residents. Their SCADA system controls chlorine and sodium hydroxide dosing — chemicals that purify water but are dangerous at elevated concentrations. The system is managed remotely using TeamViewer by the facility's single IT engineer. There is no OT security programme and no network segmentation.

14:05 — Unexpected remote cursor movement

Operator notices the mouse moving on its own

A plant operator is monitoring the SCADA HMI screen when she notices the mouse cursor begin moving by itself. A remote session has connected — she can see it in the TeamViewer notification. She assumes it is the IT engineer doing maintenance.

The cursor navigates to the sodium hydroxide dosing control and changes the setpoint from 111 parts per million to 11,100 — one hundred times the safe limit. The operator immediately changes it back and calls the IT engineer.

The investigation and root cause

What the investigation found

The TeamViewer software was using a shared password across all staff — never changed since installation three years prior. No MFA. No access logging. No network segmentation between the internet-facing IT systems and the OT HMI.

The attacker had internet-direct access to the SCADA HMI. There was no firewall between the public internet and the

What should have prevented this

- **Network segmentation:** The HMI should never be directly reachable from the internet. A jump server with MFA in a DMZ is the minimum — preferably a one-way data diode
- **Remote access control:** TeamViewer should have required MFA, used unique credentials per user, logged all sessions, and required a second person to approve connections
- **Process safety backup:** Chemical dosing systems should have independent safety interlocks (Safety Instrumented Systems) that prevent dangerous setpoints regardless of software commands
- **Monitoring and alerting:** Any setpoint change beyond ±10% of normal operating range should trigger an immediate alert to the operator and supervisor
- **Regular assessment:** Even a basic OT security assessment would have flagged direct internet exposure of the HMI as a critical finding

The attack nearly poisoned the water supply of 12,000 people.

It was stopped only because an alert operator was watching the screen at the right moment.

Without that operator: contaminated water would have reached homes within hours.

13. Breaking In — Getting Your First Role

OT security has a supply shortage of qualified people. This makes it one of the more accessible senior specialisms for people with the right combination of background — but you need to demonstrate credibly that you understand both the operational environment and the security challenges.

Build visible evidence of OT security knowledge

- **OpenPLC lab:** Build a Raspberry Pi PLC lab. Write a simple ladder logic programme. Run a Modbus client against it. Scan it with nmap. Document what breaks and what you learn. This is genuinely rare hands-on evidence
- **GRFICS simulation:** GRFICS is a free OT simulation environment — it simulates a chemical plant process with a real HMI. Practice attack and defence in a safe environment. Write up your findings
- **ICS-CERT advisories:** Read and annotate ICS-CERT/CISA ICS advisories — explain what the vulnerability is, why it matters in an OT context, and what the mitigation requires. Demonstrates OT security thinking
- **Incident analysis write-ups:** Take a public OT incident (Colonial Pipeline, Ukraine power grid) and write a structured analysis — attack path, impact, what controls would have prevented it. This is exactly what OT security consultants produce
- **IEC 62443 self-study:** Document your study of IEC 62443 — even a structured blog post explaining the zone and conduit model demonstrates framework knowledge

Where to Look	Notes
CyberSecurityJobs.com	Search 'OT security', 'ICS security', 'SCADA security analyst'
LinkedIn	OT security is a small community — connect directly with practitioners at Dragos, Claroty, Nozomi, Applied Risk
Energy sector (National Grid, BP, Shell, Thames Water, EDF)	Major CNI operators hire OT security engineers directly — often prefer candidates with engineering backgrounds
NCSC / DSIT / Cabinet Office	UK government OT/CNI security roles — require SC or DV clearance
OT specialist consultancies (Dragos, Applied Risk, Cybikon, Adelard)	Specialist OT security firms — best for developing deep expertise quickly across multiple sectors
Defence primes (BAE Systems, Leonardo, Leidos, QinetiQ)	OT security for defence infrastructure — clearance usually required

Table 10: Where to find OT/ICS security roles

Interview questions to prepare for

- Explain the Purdue Model and why the IT/OT boundary is the most critical security point.
- Why can you not simply apply IT security practices to OT environments?
- What is a PLC and how does it differ from a standard server? What security implications does this create?
- Walk me through how an attacker would move from an IT network into an OT environment.

- What is passive monitoring and why is it preferred over active scanning in OT environments?
- A plant operator reports their HMI cursor moving on its own. What is your first response?
- What is IEC 62443 and what is the zone and conduit model?
- How would you approach securing remote vendor access to a SCADA system?

The best OT security interview answer:
"Here is my OpenPLC lab setup. Here is what I found when I tried to attack it."
Hands-on lab evidence in a field where few candidates have any is a major differentiator.

14. References

1. CISA (2024) *ICS-CERT Advisories and Industrial Control Systems Security Resources.* Available at: https://www.cisa.gov/topics/industrial-control-systems [Accessed: 10 April 2026].

2. CW Jobs (2024) *Technology Salary Survey 2024.* Available at: https://www.cwjobs.co.uk/salary-checker [Accessed: 10 April 2026].

3. Dragos (2024) *Year in Review: ICS/OT Cybersecurity.* Available at: https://www.dragos.com/year-in-review/ [Accessed: 11 April 2026].

4. GIAC (2024) *GICSP — Global Industrial Cyber Security Professional.* Available at: https://www.giac.org/certifications/global-industrial-cyber-security-professional-gicsp/ [Accessed: 11 April 2026].

5. IEC (2022) *IEC 62443: Security for Industrial Automation and Control Systems.* Geneva: International Electrotechnical Commission.

6. ISA (2024) *ISA/IEC 62443 Standards.* Available at: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards [Accessed: 12 April 2026].

7. Langner, R. (2011) *Stuxnet: Dissecting a Cyberwarfare Weapon.* IEEE Security & Privacy, 9(3), pp.49–51.

8. Lee, R., Assante, M. and Conway, T. (2016) *Analysis of the Cyber Attack on the Ukrainian Power Grid.* E-ISAC / SANS ICS. Available at: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf [Accessed: 12 April 2026].

9. NCSC (2024) *Cyber Assessment Framework.* National Cyber Security Centre. Available at: https://www.ncsc.gov.uk/collection/caf [Accessed: 13 April 2026].

10. NIST (2023) *SP 800-82 Rev. 3: Guide to Operational Technology (OT) Security.* Available at: https://doi.org/10.6028/NIST.SP.800-82r3 [Accessed: 13 April 2026].

11. OpenPLC Project (2024) *OpenPLC Runtime — Open Source PLC.* Available at: https://openplcproject.com [Accessed: 14 April 2026].

12. Reed (2024) *Cybersecurity Salary Guide UK 2024.* Available at: https://www.reed.co.uk/career-advice/cybersecurity-salary [Accessed: 14 April 2026].

13. Slowik, J. (2019) *TRITON: The First ICS Cyberattack on Safety Instrumented Systems.* Dragos. Available at: https://www.dragos.com/resource/trisis-crashoverride-industroyer/ [Accessed: 14 April 2026].

Document prepared by **Babashaheer**. Version 1.0 — April 2026. Cybersecurity Career Series — Document 11 of 12.