



SELF-PACED CERTIFICATION FOR AUTOMATION ENGINEERS · OTCS-201

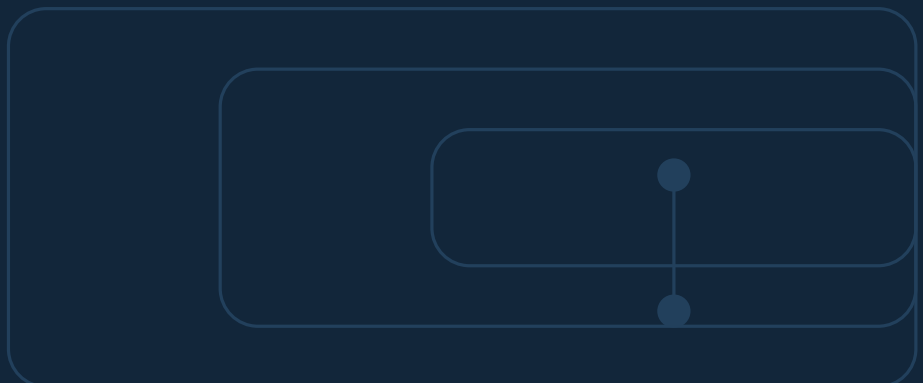
The cyber passport every automation tender asks for

The OT Security Passport answers the cyber clauses in today's tenders and customer audits: zones and conduits, IEC 62443, secure remote access, hardened controllers, a secured supervisory layer, governed edge and cloud. Online, self-paced, assessed unit by unit, and it ends in a QR-verifiable certificate.

OTCS-201

Industrial Cybersecurity Essentials for Engineers

13 units · about 4 hours · 65-question final ·
launch offer to 2 Oct 2026: ₹7,999 **₹3,999** incl.
GST



Built by an automation company, not a content studio

WonderSys has delivered PLC, SCADA and DCS projects for two decades. The academy exists because the people we commission plants with are the people we could not hire ready-made. Everything in this course is what our own engineers are required to know before they go to site.

WonderSys Automation

- Schneider Electric Resource and Digitalization Partner; AVEVA Resource Partner.
- Control-system design, panel building, PLC, SCADA, DCS and safety-system integration across steel, power, water, process and public-sector manufacturing and research establishments.
- Assessed above target in our principal's 2026 partner cyber-maturity assessment: the disciplines in this course are the ones we run ourselves.
- Our engineers answer tender pre-qualification questionnaires, customer audits and FAT/SAT clauses every month.

WonderSys Academy

- Hands-on training on real industrial panels: Siemens, Allen Bradley, Schneider Electric, ABB, Mitsubishi, Delta, Omron. Never simulations, never stock imagery.
- 500+ engineers trained; instruction in six languages; placement assistance with system integrators and OEM partners.
- Faculty who commission plants for a living and teach between projects.
- Certificates issued by our own LMS, verifiable by QR code, valid two years.

NEED OF THE HOUR

Why this subject, and why now

Cyber clauses are now in the tender, not the appendix.

Utilities, steel, refineries and pharma now ask the system integrator, not only the OEM, for IEC 62443 alignment, secure remote access, patch and backup discipline and an incident plan. In India, CERT-In's reporting rules and the DPDP Act add legal duties on top. An engineer who cannot answer these questions costs their employer the bid.

The controller has become a network device.

Modern PLCs ship with certificates, role-based access, 802.1X and encrypted protocols. Edge gateways and cloud historians are attached to plants that were air-gapped five years ago. Programming a controller now includes securing it.

Customers audit the contractor, not just the product.

Remote-access logs, credential handover, backup evidence and a first-hour incident plan are asked for at FAT, SAT and every annual review. The engineer on site is the one who has to produce them.

Employers hire for the whole job.

The gap between a fresh graduate and a billable engineer is largely discipline: cyber, documentation and conduct. Closing it is the fastest route to placement and to the next salary band.

Industry expectation versus what engineers bring

Tender clauses are only the visible part. The expectation runs through pre-qualification, site entry, conduct, documentation, audits and handover. Each row is a place we have watched capable engineers fall short, and the unit that closes it.

Where	What industry expects	What most engineers bring	Closed by
Pre-qualification, tender	IEC 62443 role clarity, a security plan, evidence of secure development and remote-access practice.	Buzzwords copied from the standard; no evidence trail.	OTCS 3, 10
Design review	A zone-and-conduit drawing, Purdue placement, a path-based risk assessment.	A flat network and a single VLAN; risk treated as an IT matter.	OTCS 2, 4, 7
Remote support	Requested, approved, brokered, authenticated, logged and time-boxed sessions.	TeamViewer on a laptop with a shared password.	OTCS 5, 8
Configuring the controller	Certificates, roles, port lock-down and encrypted protocols on M580, ControlLogix, S7-1500.	Default credentials, everything enabled, project file on a USB stick.	OTCS 6, 11
Supervisory layer	Directory-tied security modes, secured and verified writes, encrypted platform traffic, galaxy backup.	One shared operator login; no audit of who changed what.	OTCS 12
Edge, IIoT and cloud	Outbound-only conduits, six shared-responsibility questions answered, CERT-In and DPDP obligations known.	A gateway with inbound rules "because the vendor needed it".	OTCS 13
When something goes wrong	Incident first-hour actions, near-miss reporting, recovery from verified backups.	Silence, then improvisation.	OTCS 9; ISRS 9
Statutory and customer audits	Factories Act duties, contractor obligations, documentation that survives an audit.	Unaware of the law; documents assembled after the fact.	ISRS 7; OTCS 10
Conduct on a customer site	Professional handover, credentials returned, escalation done properly, customer confidence kept.	Good engineering undone by poor site behaviour.	ISRS 10; OTCS 8

OUTCOME OF THE LEARNING

What changes after the passport

- You can answer a tender's cyber clauses with evidence, not adjectives.
- You can draw any plant as zones and conduits and defend the drawing in a design review.
- You can read a controller or SCADA security datasheet from any vendor and map it back to the standard.
- You can design, run and audit a remote-access session a customer will sign off.
- You know the first hour of an incident and what to restore from.
- You carry a QR-verifiable OT Security Passport a customer can check before they let you connect.

Industrial Cybersecurity Essentials for Engineers

Answer the cyber clauses that now appear in every automation tender.

Who it is for

Automation, control, commissioning and service engineers; system integrators answering pre-qualification questionnaires; plant engineers managing vendors.

What you will be able to do

- Draw a plant as zones and conduits, place any device on the Purdue model and explain security levels.
- Read the IEC 62443 family and know which part applies to you as a service provider (2-4).
- Run a one-workshop, path-based risk assessment a customer will pay for.
- Design and audit remote access: requested, approved, brokered, authenticated, logged, time-boxed.
- Apply media, workstation, patching and backup discipline; segment and harden switches and controllers.
- Handle credentials and handover; act correctly in the first hour of an incident; pass a customer audit.
- Read any controller's security datasheet (Schneider M580, Rockwell ControlLogix, Siemens S7-1500) and map certificates, roles, 802.1X and encrypted protocols back to the standard.
- Secure the supervisory layer (AVEVA System Platform as the worked example, with FactoryTalk View and WinCC): directory-tied security modes, secured and verified writes, encrypted platform traffic, galaxy backup.
- Govern edge gateways, wireless, vendor skids and cloud services as outbound-only conduits, with CERT-In and DPDP obligations for plants in India.

The 13 units

- | | |
|--|--|
| 1 Cyber IS safety: the OT threat landscape | 8 Identity, accounts and project credentials |
| 2 Zones, conduits and levels | 9 Detection, response and recovery |
| 3 The IEC 62443 family, practically | 10 The contractor's cyber obligations |
| 4 Threats, vulnerabilities and risk assessment | 11 Securing a real controller: M580, ControlLogix, S7-1500 |
| 5 Secure remote access and vendor management | 12 Securing the supervisory layer: AVEVA System Platform |
| 6 Media, workstations and patching | 13 Edge, IIoT and the cloud |
| 7 Segmentation and hardening in practice | |

How it works

Narrated video with animated cutaways and a downloadable transcript for every unit; about 2 h 20 min of video, about 4 hours of guided learning with the quizzes. 70% on each unit quiz unlocks the next, unlimited retakes. 75% on the 65-question final earns the OT Security Passport, verifiable by QR code and valid two years.

LAUNCH OFFER · ENDS 2 OCTOBER 2026



₹7,999 ₹3,999
incl. GST · lifetime access · list price
₹7,999 from 3 October 2026

Scan to enrol, or visit
academy.wondersysautomation.com/courses/ot-cybersecurity

Aligned to IEC 62443, NIST SP 800-82 and NIST CSF 2.0. Teaches the principles in our own words; it is not a certification against IEC 62443 itself. Product names belong to their owners; WonderSys is a Schneider Electric Resource and Digitalization Partner and an AVEVA Resource Partner.

Enrolling takes a minute. Pay once on the academy site (UPI, card or net banking through Razorpay). Your LMS login is created automatically and emailed to you the moment payment succeeds; the first unit is open immediately.

Talk to us.

Prakash D S, WonderSys Academy,
Bengaluru
+91 99025 88448
prakash@wondersysautomation.com
wondersysacademy.com