

Dispense — Penetration Testing in Ambiente Industriale (OT e IoT)

Oct 31, 2026 · @Vincenzo Calabrò

Dispense del modulo avanzato di Cyber Security dedicato al penetration testing dei sistemi cyber-fisici. In ambiente industriale la **safety** viene prima di qualsiasi vulnerabilità trovata, e questo ridisegna metodo, strumenti ed etica rispetto al pentest IT tradizionale.

1. Introduzione e obiettivi formativi

Il corso forma professionisti capaci di valutare la sicurezza di infrastrutture cyber-fisiche — reti OT (Operational Technology) e dispositivi IoT industriali — senza mai comprometterne la continuità operativa o l'incolumità delle persone. Non è un corso di pentest IT applicato alle fabbriche: è una disciplina con regole proprie.

Al termine del percorso lo studente è in grado di:

- Descrivere l'architettura di un sistema di controllo industriale (ICS) e collocarne i componenti nel Modello Purdue.
- Riconoscere e analizzare i principali protocolli industriali e il loro traffico di rete.
- Valutare la superficie d'attacco di un dispositivo embedded su firmware, hardware e canale radio.
- Pianificare e condurre un assessment OT-aware, privilegiando tecniche non invasive e rispettando un vincolo di safety esplicito.
- Mappare i risultati su framework riconosciuti (MITRE ATT&CK for ICS) e redigere un report professionale con risk scoring cyber-fisico.
- Inquadrare l'attività nel contesto normativo (IEC 62443, NIST SP 800-82, NIS2) e legale.

Prerequisiti: basi di networking (TCP/IP), sistemi operativi e sicurezza IT. Non si assume alcuna conoscenza pregressa di automazione industriale: PLC, SCADA, DCS, HMI e RTU vengono introdotti dai fondamentali.

2. OT e IT: perché cambiano le regole

Nell'IT tradizionale la priorità segue la triade Riservatezza → Integrità → Disponibilità (CIA). In ambiente OT l'ordine si ribalta: prima la **safety** (incolumità e integrità del processo fisico), poi la **disponibilità** (la linea non si ferma), poi l'integrità e infine la riservatezza. Questa inversione spiega ogni scelta metodologica del corso.

La conseguenza pratica più importante riguarda l'invasività: una scansione di rete o un fuzzing che nel mondo IT sono di norma innocui, su un PLC datato possono provocare un fault e fermare — o danneggiare — un impianto. Da qui la preferenza sistematica per approcci passivi e per ambienti di test isolati dalla produzione.

Dimensione	IT tradizionale	OT / Industriale
Priorità	Riservatezza dei dati	Safety e continuità del processo
Ciclo di vita	3-5 anni	15-30 anni, legacy diffuso
Patching	Frequente, automatizzato	Raro, in finestre di fermo pianificate
Vincolo temporale	Best-effort	Real-time, deterministico
Scansione attiva	Di norma innocua	Può fermare o danneggiare l'impianto
Riavvio di un nodo	Operazione ordinaria	Può interrompere un processo critico

Trasferire meccanicamente tecniche e strumenti IT in ambito OT espone l'impianto a rischi concreti, ed è la ragione per cui il metodo descritto nei capitoli successivi è diverso.

3. Architetture industriali e Modello Purdue

I componenti fondamentali di un ICS sono: il **PLC** (Programmable Logic Controller), che esegue la logica di automazione; l'**HMI** (Human-Machine Interface), con cui l'operatore supervisiona il processo; la **RTU** (Remote Terminal Unit), per siti distribuiti; i sistemi **SCADA** (supervisione e acquisizione dati) e **DCS** (controllo distribuito); e l'**historian**, che archivia le serie storiche di processo.

Il Modello Purdue organizza questi componenti in livelli, dalla gestione d'impresa fino al processo fisico. Serve a ragionare su dove un attaccante può arrivare e dove il pentester può operare: l'intrusione quasi sempre parte dall'IT e la domanda è quanto in profondità riesca a spingersi.

Livello	Zona	Contenuto tipico	Rilevanza per il pentest
L4-L5	Enterprise / IT	ERP, posta, dominio	Punto d'ingresso più comune
L3.5	DMZ industriale	Broker, proxy, jump host	Confine critico: regge la segregazione?
L3	Operations / SCADA	Historian, server di supervisione	Pivot verso il controllo

Livello	Zona	Contenuto tipico	Rilevanza per il pentest
L2	Supervisione d'area	HMI, workstation di controllo	Interazione diretta con il processo
L1	Controllo	PLC, RTU, controllori	Logica che muove gli attuatori
L0	Processo fisico	Sensori e attuatori	Qui l'impatto è reale e cinetico

IEC 62443 formalizza questa segmentazione con i concetti di **zona** (gruppo di asset con requisiti di sicurezza omogenei) e **conduit** (canale di comunicazione controllato tra zone). A ogni zona si assegna un **Security Level** (SL 1-4) in base alla capacità avversaria da cui deve proteggersi. La tenuta dei conduit, specie attorno alla DMZ industriale (L3.5), è spesso il primo oggetto di verifica di un assessment.

4. Protocolli industriali e analisi del traffico

Molti protocolli OT nascono per reti fisicamente isolate e sono quindi *insecure by design*: privi di autenticazione e cifratura, trattano come legittimo chiunque parli sul bus. Sul filo, un comando lecito e uno ostile sono indistinguibili. Per questo l'analisi del traffico è al tempo stesso il primo passo e il più sicuro: si ascolta senza iniettare nulla.

Protocollo	Ambito tipico	Nota di sicurezza
Modbus/TCP	Automazione di fabbrica	Nessuna autenticazione nativa
S7comm	PLC Siemens	Autenticazione debole nelle versioni storiche
PROFINET	Automazione real-time	Esposto su rete di campo
EtherNet/IP · CIP	Automazione (Rockwell)	Comandi non autenticati
DNP3	Energia e utilities	Secure Authentication opzionale, spesso non attiva
IEC 60870-5-104	Telecontrollo elettrico	Nessuna sicurezza nativa
IEC 61850	Sottostazioni elettriche	GOOSE/SV sensibili a spoofing
BACnet	Building automation	Controlli d'accesso limitati
OPC-UA	Convergenza IT/OT, IIoT	Sicurezza nativa (se configurata)

Protocollo	Ambito tipico	Nota di sicurezza
MQTT · CoAP	IIoT, telemetria	Sicurezza demandata al TLS sottostante

OPC-UA è l'eccezione moderna: integra autenticazione, firma e cifratura, purché il profilo di sicurezza sia abilitato. In laboratorio il lavoro parte sempre dalla dissezione del traffico con Wireshark e dissector dedicati, imparando a riconoscere i *function code* e le anomalie, su cattura passiva o testbed isolato — mai con injection su sistemi in esercizio.

5. Sicurezza IoT ed embedded

L'IoT industriale aggiunge hardware economico, aggiornato di rado e spesso progettato con poca attenzione alla sicurezza. La sua superficie d'attacco si legge su tre piani complementari.

Firmware. Estrazione e unpacking dell'immagine (binwalk), ricerca di credenziali e chiavi hardcoded, analisi di configurazioni e certificati, reverse engineering statico del binario (Ghidra). Le credenziali cablate nel firmware restano uno dei difetti più comuni e gravi.

Hardware. I progettisti lasciano spesso attive porte di debug sul circuito, mai disabilitate in produzione: interfacce seriali (UART), di debug del processore (JTAG) e di memoria (SPI). Permettono dump della memoria, accesso a console di boot e, talvolta, il bypass dell'avvio sicuro.

Radio. I protocolli wireless introducono canali intercettabili e meccanismi di pairing talvolta deboli: BLE, Zigbee, LoRaWAN, Wi-Fi. L'analisi riguarda la gestione delle chiavi di sessione, la robustezza dell'accoppiamento e la riservatezza del canale.

Vincolo didattico invariabile: ogni tecnica si esercita esclusivamente su dispositivi di proprietà del laboratorio, acquistati a questo scopo, e mai su apparati di un cliente in esercizio.

6. Metodologia di penetration testing OT-aware

La sequenza resta quella classica del pentest, ma pesata sulla safety: è una rampa di invasività crescente in cui ogni passo in avanti richiede autorizzazione esplicita, ambiente controllato e criteri di arresto definiti *prima*.

1. **Scoping e Rules of Engagement.** Si definiscono perimetro, asset inclusi ed esclusi, finestre temporali, referenti e — soprattutto — i criteri di stop: quando interrompere immediatamente se un sistema mostra instabilità.
2. **Ricognizione passiva.** OSINT e ricerca di dispositivi esposti (Shodan, Censys) senza toccarli; ascolto del traffico di rete per mappare asset e protocolli.

3. **Threat modeling.** Costruzione della mappa degli asset, dei percorsi d'attacco plausibili e della loro valutazione d'impatto sul processo fisico.
4. **Validazione controllata.** Verifica mirata delle ipotesi, preferibilmente su sistema replica o in finestra di fermo concordata; l'attivo si introduce solo qui e solo con autorizzazione.
5. **Reporting e remediation.** Traduzione dei risultati in rischio cyber-fisico, con priorità e piano di rientro allineato a IEC 62443.

La differenza rispetto all'IT è sostanziale: qui non si lancia un exploit per vedere cosa succede. Ogni azione attiva è preceduta da threat modeling e da una decisione consapevole, idealmente su un ambiente che non sia la produzione.

7. MITRE ATT&CK for ICS

ATT&CK for ICS è la controparte industriale della matrice ATT&CK Enterprise: un linguaggio comune per descrivere le tattiche e le tecniche avversarie nei sistemi di controllo. Serve a pianificare il test, a strutturare il report (ogni finding mappato a una tecnica) e a dialogare con il difensore.

Le prime tattiche assomigliano a quelle IT (accesso iniziale, esecuzione, persistenza, movimento laterale), ma le ultime sono peculiari dell'OT:

- **Inhibit Response Function** — disattivare allarmi e funzioni di sicurezza, cioè neutralizzare le barriere che dovrebbero fermare un incidente.
- **Impair Process Control** — manipolare setpoint, parametri e comandi per alterare il processo.
- **Impact** — l'effetto finale sul mondo fisico: perdita di controllo, perdita di sicurezza, manipolazione o danno.

La differenza chiave rispetto all'IT: l'obiettivo avversario non è esfiltrare dati, ma agire sul processo fisico. Nel report, mappare ogni passo alla tecnica corrispondente permette al committente di leggere la catena completa dell'attacco e di capire quali contromisure la spezzano.

8. Il laboratorio sicuro

Non si impara il pentest OT su un impianto vero. Si costruisce un *testbed* riproducibile e isolato dalla produzione, dove ogni errore costa zero. Il laboratorio replica il comportamento del processo, non il suo valore produttivo: libertà totale di sbagliare, impatto reale nullo.

Tre componenti ricorrenti:

- **Simulazione di processo.** PLC virtuali o didattici, simulatori di processo fisico e HMI software permettono di osservare cosa accade a una valvola, un motore o una temperatura quando si invia un certo comando — senza conseguenze reali.
- **Honeypot e monitoraggio.** Honeypot ICS (ad esempio Conpot, che emula un sistema SCADA) per studiare le tecniche avversarie, e sonde passive per imparare a riconoscere il traffico anomalo.
- **Isolamento.** Rete di laboratorio segregata, nessun ponte verso ambienti reali e snapshot delle macchine per ripartire da uno stato pulito dopo ogni esercitazione.

Il testbed è il cuore pratico del corso: le tecniche aggressive che altrove sarebbero irresponsabili qui diventano didattica, proprio perché l'ambiente è una replica controllata.

9. Standard e quadro normativo

Gli standard non sono contorno: definiscono cosa un assessment deve verificare e come tradurne i risultati in requisiti di conformità.

- **IEC 62443** — lo standard di riferimento per la sicurezza degli IACS (Industrial Automation and Control Systems). Introduce zone, conduit e Security Level, e ripartisce i requisiti tra asset owner, integratori di sistema e produttori di componenti.
- **NIST SP 800-82** — guida alla sicurezza degli OT: architetture, contromisure e, aspetto prezioso, indicazioni su come condurre assessment senza impattare il processo.
- **Direttiva NIS2** — quadro europeo che estende gli obblighi di cybersecurity a più settori critici, con responsabilità della dirigenza e obblighi di notifica degli incidenti. È il motore che rende queste pratiche un dovere e non solo una buona abitudine.

Sul piano **legale**, va ricordato che ogni attività è lecita solo su sistemi di proprietà o con mandato scritto. In Italia l'accesso non autorizzato a sistemi informatici e telematici è reato (art. 615-ter c.p.), e condotte collegate (danneggiamento, intercettazione) hanno rilievo penale autonomo. Le Rules of Engagement non sono formalità: sono la base giuridica dell'intervento. *Questo inquadramento è a scopo didattico e non costituisce consulenza legale.*

10. Casi di studio

Tre attacchi hanno dimostrato l'impatto cyber-fisico del software ostile. Li studiamo da difensori: cosa è stato colpito, come, e cosa avrebbe potuto fermarli.

Attacco	Anno	Bersaglio	Lezione difensiva
Stuxnet	2010	Centrifughe di arricchimento	Logica PLC manipolata mentre gli operatori vedevano valori normali: il salto dal digitale al danno meccanico
Industroyer	2016	Rete elettrica	Malware che parla nativamente i protocolli elettrici (IEC 60870-5-104, IEC 61850) per aprire gli interruttori
Triton / TRISIS	2017	Safety Instrumented System	Attacco diretto all'ultima barriera di sicurezza che protegge le persone

In tutti e tre i casi l'obiettivo dell'attacco è il processo fisico, non i dati. Triton è il più grave sul piano concettuale: colpendo i Safety Instrumented System, prendeva di mira proprio i sistemi concepiti per prevenire incidenti e proteggere l'incolumità. Ogni caso diventa in aula una lezione concreta su cosa monitorare, cosa segmentare e dove i conduit devono reggere.

11. Safety e legalità: il principio non negoziabile

È il punto che distingue il pentest industriale da quello IT. Un finding in più non vale mai il rischio di fermare un impianto o di mettere in pericolo una persona. Tre pilastri vanno interiorizzati e ripetuti a ogni esercitazione.

1. **Autorizzazione.** Si opera solo su sistemi di proprietà o con mandato scritto. Scope e Rules of Engagement — compresi i criteri di stop — sono definiti prima di iniziare.
2. **Primo, non nuocere.** Preferenza sistematica per le tecniche passive. Nessun test invasivo in produzione senza ambiente replica o finestra di fermo concordata.
3. **Legalità.** Rispetto del quadro normativo (NIS2, IEC 62443) e penale sull'accesso abusivo ai sistemi.

Chi non fa proprio questo principio non è pronto a operare in OT, per quanto valido sul piano tecnico. La competenza offensiva serve a difendere; separata dalla responsabilità, diventa un rischio.

12. Struttura didattica, moduli e valutazione

Il corso si articola in sei moduli che ricalcano il percorso di queste dispense, dal fondamento concettuale al reporting, con peso crescente del laboratorio.

#	Modulo	Taglio	Ore
M1	Fondamenti OT/ICS e Modello Purdue	Teoria	1 T
M2	Protocolli industriali e analisi del traffico	Teoria + Lab	0,5 T + 1 L
M3	IoT ed embedded: firmware, hardware, radio	Lab	1,5 L
M4	Metodologia OT-aware e MITRE ATT&CK for ICS	Teoria + Lab	0,5 T + 1 L
M5	Testbed, honeypot e simulazione di processo	Lab	1,5 L
M6	Reporting, risk scoring cyber-fisico, IEC 62443	Teoria + Lab	1 L

Il corso vale 2 CFU, per un totale di 8 ore: 2 di teoria e 6 di laboratorio (T = teoria, L = laboratorio). La dotazione minima del laboratorio è un PC per postazione e un set di dispositivi IoT dedicati alle esercitazioni.

Valutazione (pesi indicativi, adattabili al regolamento):

- **Progetto di laboratorio — 40%.** Assessment completo su testbed, dalla ricognizione al piano di remediation.
- **Report professionale — 35%.** Qualità tecnica, risk scoring cyber-fisico e chiarezza per un destinatario non tecnico.
- **Prova orale — 25%.** Fondamenti, scelte metodologiche e padronanza del vincolo di safety.

La valutazione premia il metodo e la responsabilità, non il mero numero di vulnerabilità individuate.

13. Letture e risorse

Riferimenti per approfondire, da integrare con il materiale d'aula:

- **IEC 62443 (serie)** — sicurezza degli IACS: zone, conduit, Security Level.
- **NIST SP 800-82** — Guide to Operational Technology (OT) Security.
- **MITRE ATT&CK for ICS** — matrice di tattiche e tecniche avversarie per i sistemi di controllo.
- **Direttiva (UE) 2022/2555 (NIS2)** e relativo recepimento nazionale.
- Documentazione dei protocolli: specifiche Modbus, DNP3, OPC-UA, IEC 61850.
- Analisi tecniche pubbliche dei casi Stuxnet, Industroyer e Triton/TRISIS, a fini di studio difensivo.