// CORSO DI LAUREA MAGISTRALE · CYBER SECURITY

MODULO AVANZATO — ICS / OT / IoT

Penetration Testing in Ambiente Industriale

Valutare la sicurezza dei sistemi cyber-fisici — OT e IoT — senza mai compromettere la safety.

IEC 62443 | NIST SP 800-82 | MITRE ATT&CK for ICS | NIS2

// AGENDA

Percorso della lezione

01

Fondamenti OT/ICS

Componenti, IT vs OT, Modello Purdue

02

Superficie d’attacco

Protocolli, ricognizione, IoT ed embedded

03

Metodologia

Processo, MITRE, laboratorio, reporting

04

Quadro & safety

Standard, casi reali, principio etico-legale

Chiudiamo con sintesi, autovalutazione e indicazioni per l’esercitazione di laboratorio.

// OBIETTIVI

Al termine saprai...

- ✓ Collocare i componenti di un ICS nel Modello Purdue e leggere un percorso d’attacco attraverso i livelli
- ✓ Riconoscere e analizzare il traffico dei principali protocolli industriali
- ✓ Valutare la superficie d’attacco di un dispositivo embedded su firmware, hardware e radio
- ✓ Pianificare un assessment OT-aware e mapparlo su MITRE ATT&CK for ICS

I componenti di un ICS

Prima di attaccare o difendere, bisogna saper nominare le parti. Questo è il vocabolario minimo dell’automazione industriale.

Sigla	Nome	Funzione
PLC	Programmable Logic Controller	Esegue la logica di automazione in tempo reale
HMI	Human-Machine Interface	Pannello con cui l’operatore supervisiona
RTU	Remote Terminal Unit	Controllo di siti remoti e distribuiti
SCADA	Supervisory Control & Data Acquisition	Supervisione e raccolta dati su larga scala
DCS	Distributed Control System	Controllo distribuito di impianti di processo

Perché l’OT non è l’IT

Nel mondo industriale la priorità della triade si ribalta: non più **Riservatezza → Integrità → Disponibilità**, ma **Safety → Disponibilità → Integrità → Riservatezza**. Questo cambia ogni scelta di testing.

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, finestre di fermo pianificate
Vincolo temporale	Best-effort	Real-time, deterministico
Una scansione attiva	Innocua di norma	Può fermare o danneggiare l’impianto

01 — FONDAMENTI

Il Modello Purdue

La segmentazione a livelli (zone e conduit, IEC 62443) definisce dove un attaccante può arrivare e dove il pentester può operare. L’obiettivo difensivo è impedire il percorso dal dominio IT fino al processo fisico.

L4–5	**Enterprise / IT**	ERP, posta, dominio — tipico punto d’ingresso
L3.5	**DMZ industriale**	Il confine critico: dove si gioca la segregazione
L3	**Operations & SCADA**	Historian, server di supervisione
L1–2	**Controllo — PLC / HMI / RTU**	Logica di automazione, interfacce operatore

01 — FONDAMENTI

Un percorso d’attacco tipico

La maggior parte delle intrusioni OT non comincia in fabbrica, ma in ufficio. Ecco la catena che il pentest prova a ricostruire — e che la difesa deve spezzare.

L4-5	Phishing o VPN esposta → primo accesso nell’IT	⚠
L3.5	Conduit mal configurato → passaggio della DMZ industriale	⚠
L3	Historian o server SCADA → mappatura del processo	⚠
L1-0	Comando al PLC → impatto sul processo fisico	⚠

02 — SUPERFICIE D’ATTACCO

Protocolli industriali

Molti protocolli OT nascono senza autenticazione né cifratura: un comando legittimo e un comando ostile sono indistinguibili sul filo. Analizzarne il traffico è il primo passo passivo e sicuro.

Automazione di fabbrica

Modbus/TCP
S7comm (Siemens)
PROFINET
EtherNet/IP · CIP

Energia & utilities

DNP3
IEC 60870-5-104
IEC 61850 (sottostazioni)
BACnet (building)

Convergenza & IIoT

OPC-UA
MQTT
CoAP
AMQP

02 — SUPERFICIE D’ATTACCO

Anatomia di Modbus/TCP

Un caso emblematico di protocollo *insecure by design*: nessuna autenticazione, nessuna cifratura. Chi raggiunge la porta parla col dispositivo.

```
// struttura del frame (MBAP + PDU)

[Transaction ID] [Protocol ID] [Length] [Unit ID] [Function Code] [Data]
```

FC 03

Read Holding Registers

FC 06

Write Single Register

FC 05 / 16

Write Coils / Registers

02 — SUPERFICIE D’ATTACCO

Ricognizione senza toccare

In OT la prima regola è non generare rumore sull’impianto. La ricognizione passiva permette di sapere molto prima di inviare un solo pacchetto al target.

Motori di esposizione

Shodan e Censys indicizzano dispositivi OT raggiungibili da Internet: banner, protocolli, versioni — tutto senza interrogare direttamente il bersaglio.

OSINT

Documenti pubblici, offerte di lavoro, foto di impianto, repository: rivelano marche di PLC, fornitori e topologie senza alcun contatto tecnico.

Ascolto del traffico

Su una porta mirror, la cattura passiva mappa asset, protocolli e relazioni senza iniettare nulla nella rete di processo.

02 — SUPERFICIE D’ATTACCO

Dispositivi IoT & embedded

L’IoT industriale aggiunge hardware economico e aggiornato di rado: la superficie d’attacco va letta su tre piani — firmware, hardware, radio.

01 / FIRMWARE

Analisi del binario

Estrazione e unpacking, ricerca di credenziali e chiavi hardcoded, reverse engineering statico. Strumenti: binwalk, Ghidra.

02 / HARDWARE

Interfacce di debug

Accesso a porte seriali e di debug esposte sul circuito (UART, JTAG, SPI), dump della memoria, bypass dell’avvio.

03 / RADIO

Protocolli wireless

Superfici su BLE, Zigbee, LoRaWAN e Wi-Fi: pairing deboli, chiavi di sessione, intercettazione del canale.

02 — SUPERFICIE D’ATTACCO

Analisi del firmware

Un flusso di lavoro ripetibile per capire cosa gira dentro un dispositivo — da esercitare solo su hardware di laboratorio.

01	02	03	04
Acquisizione	**Unpacking**	**Ispezione**	**Reverse**
Download ufficiale o dump dalla memoria flash	binwalk: estrae filesystem e componenti	Credenziali, chiavi, certificati hardcoded	Ghidra: analisi statica dei binari chiave

DIFETTO N.1 Le credenziali hardcoded restano la vulnerabilità più ricorrente nei dispositivi embedded.

02 — SUPERFICIE D’ATTACCO

Interfacce hardware

Le porte di debug che i progettisti lasciano sul circuito sono spesso la via d’accesso più diretta — e la più trascurata in produzione.

Interfaccia	A cosa serve	Cosa consente
UART	Console seriale di sistema	Accesso alla shell e ai log di boot
JTAG	Debug del processore	Dump memoria, breakpoint, bypass del boot
SPI	Bus verso la memoria flash	Lettura diretta del firmware dal chip

La contromisura è disabilitare o proteggere queste interfacce in produzione: spesso restano attive per comodità di assistenza.
Esercitazione solo su hardware del laboratorio.

03 — METODOLOGIA

Un pentest OT-aware

La sequenza resta quella classica, ma pesata sulla safety: si parte sempre dal passivo e si sale di invasività solo con autorizzazione esplicita e ambiente controllato.

01	02	03	04	05
Scoping & RoE	**Ricognizione passiva**	**Threat modeling**	**Validazione controllata**	**Reporting & remediation**
Regole d’ingaggio, perimetro, finestre e criteri di stop.	OSINT, Shodan/Censys, ascolto del traffico di rete.	Mappatura asset, percorsi d’attacco, impatto sul processo.	Verifica mirata, su replica o in finestra concordata.	Rischio cyber-fisico, priorità, piano di rientro.

Threat modeling: un esempio

Scenario d’aula: impianto di trattamento acque con PLC che regola il dosaggio di un reagente. Modelliamo la minaccia prima di toccare qualunque cosa.

Elemento	Analisi
Asset critico	Setpoint di dosaggio del reagente nel PLC
Minaccia	Scrittura non autorizzata del setpoint via Modbus
Percorso	IT → DMZ debole → rete di controllo → PLC
Impatto	Qualità dell’acqua compromessa — rischio per la salute
Verifica	Solo su replica: confermare che il conduit sia attraversabile

03 — METODOLOGIA

MITRE ATT&CK for ICS

Un linguaggio comune per descrivere le tattiche avversarie nei sistemi di controllo: utile per pianificare il test, strutturare il report e dialogare con il difensore.

TA0108

Initial Access

TA0104

Execution

TA0110

Persistence

TA0109

Lateral Movement

TA0107

Inhibit Response Function

TA0105

Impact

03 — METODOLOGIA

Il laboratorio sicuro

Non si impara pentest OT su un impianto vero. Si costruisce un testbed riproducibile, isolato dalla produzione, dove ogni errore costa zero.

Simulazione di processo

PLC virtuali e didattici, simulatori di processo fisico, HMI software. Si osserva l’effetto di un comando senza alcuna conseguenza reale.

Honeypot & monitoraggio

Honeypot ICS (es. Conpot) 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, snapshot per ripartire pulito dopo ogni esercitazione.

03 — METODOLOGIA · HANDS-ON

Esercitazione guidata

Obiettivo: condurre una ricognizione completa su un testbed con PLC virtuale, dalla cattura passiva al threat model, senza alcuna azione invasiva.

STEP A

Mappare

Cattura passiva del traffico, identificazione di asset, protocolli e function code osservati.

STEP B

Modellare

Costruire il threat model: asset critico, percorso plausibile, impatto sul processo.

STEP C

Documentare

Bozza di report: finding, rischio cyber-fisico, raccomandazione di remediation.

03 — METODOLOGIA

Reporting e risk scoring

In ambito professionale un assessment vale quanto il documento che lo comunica. In OT il rischio non è solo tecnico: va pesato sull’impatto fisico e sulla safety.

Probabilità

Esposizione del conduit, facilità del percorso, competenza richiesta all’attaccante.

Impatto fisico

Effetto sul processo: fermo, danno all’impianto, conseguenze su ambiente e persone.

Safety

Un rischio che tocca l’incolumità pesa più di qualsiasi altro, a parità di probabilità.

Il report deve parlare a due pubblici: il tecnico che applica la remediation e il dirigente che decide le priorità. Chiarezza per entrambi è una competenza valutata.

03 — METODOLOGIA

Dalla vulnerabilità alla difesa

Trovare non basta: il valore sta nel piano di rientro. In OT la remediation ruota attorno a segmentazione e monitoraggio, perché il patching è spesso impraticabile.

- **Segmentazione** — zone e conduit IEC 62443, con Security Level adeguato a ogni area
- **Monitoraggio passivo** — rilevamento di anomalie sul traffico, senza perturbare il processo
- **Accessi e manutenzione** — controllo degli accessi remoti e dei fornitori

Standard e normative

IEC 62443	Lo standard di riferimento per la sicurezza degli IACS: zone, conduit, Security Level e requisiti per asset owner, integratori e produttori.
NIST 800-82	Guida alla sicurezza degli OT: architetture, contromisure e, soprattutto, come condurre assessment senza impattare il processo.
NIS2	Direttiva europea che estende gli obblighi di cybersecurity a più settori critici, con responsabilità e notifica degli incidenti.

04 — QUADRO & SAFETY

Casi di studio reali

Tre attacchi che hanno dimostrato l’impatto cyber-fisico. Li analizziamo a fini difensivi: cosa è stato colpito, come, e cosa avrebbe potuto fermarli.

Stuxnet

2010 · Centrifughe

Manipolazione occulta della logica PLC con falsificazione dei dati verso gli operatori. Il salto dal digitale al danno meccanico.

Industroyer

2016 · Rete elettrica

Malware che parla nativamente i protocolli di rete elettrica (IEC 60870-5-104, IEC 61850) per aprire gli interruttori.

Triton / TRISIS

2017 · Sistemi di sicurezza

Il bersaglio sono i Safety Instrumented System: colpire proprio l’ultima barriera che protegge le persone.

// PRINCIPIO NON NEGOZIABILE

La safety viene prima di qualsiasi finding

01 — Autorizzazione

Solo su sistemi di proprietà o con mandato scritto. Scope e regole d’ingaggio definiti prima di iniziare.

02 — Primo, non nuocere

Preferenza per il passivo. Nessun test invasivo in produzione senza replica o finestra concordata.

03 — Legalità

Rispetto di NIS2, IEC 62443 e del quadro penale sull’accesso abusivo ai sistemi.

// SINTESI

Cosa portare a casa

1. In OT la priorità è la **safety**: cambia metodo, strumenti ed etica rispetto al pentest IT

2. Molti protocolli industriali sono **insecure by design**: l’analisi passiva è potente e sicura

3. Si procede **dal passivo all’attivo**, con autorizzazione e criteri di stop definiti prima

4. Il risultato è **difensivo**: segmentazione, monitoraggio e un report che pesa l’impatto fisico

// VERIFICA

Domande di autovalutazione

Provate a rispondere prima di confrontarvi con le dispense. Se una domanda vi mette in difficoltà, sapete dove tornare.

Q1 Perché una scansione attiva innocua nell'IT può essere pericolosa in OT?

Q2 Cosa sono zone e conduit, e a quale livello Purdue si gioca la segregazione?

Q3 Perché l'analisi passiva del traffico è il primo passo di un pentest OT?

05 — STRUTTURA DIDATTICA

I moduli del corso

#	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

2 CFU · 8 ore totali (2 teoria + 6 laboratorio) · dotazione lab: PC + dispositivi IoT · T = teoria, L = laboratorio.

05 — STRUTTURA DIDATTICA

Come si viene valutati

40%

Progetto di laboratorio

Assessment completo su testbed, dalla ricognizione al piano di remediation.

35%

Report professionale

Qualità tecnica, risk scoring cyber-fisico e chiarezza per un destinatario non tecnico.

25%

Prova orale

Fondamenti, scelte metodologiche e padronanza del vincolo di safety.

La valutazione premia il metodo e la responsabilità, non solo il numero di vulnerabilità trovate. Percentuali indicative, adattabili al regolamento.

// APPENDICE

Glossario degli acronimi

ICS	Industrial Control System
PLC	Programmable Logic Controller
DCS	Distributed Control System
RTU	Remote Terminal Unit
SIS	Safety Instrumented System
SL	Security Level (IEC 62443)
OT	Operational Technology
SCADA	Supervisory Control & Data Acquisition
HMI	Human-Machine Interface
IIoT	Industrial Internet of Things
RoE	Rules of Engagement
OSINT	Open-Source Intelligence

// CHIUSURA

Difendere un impianto significa prima capire come lo si attacca — con responsabilità.

Dai fondamenti OT al reporting: un percorso in cui la competenza tecnica e la cultura della safety crescono insieme.

Domande & discussione | Prossimo passo: definire ore, CFU e dotazione del laboratorio

// DOCENTE

Vincenzo Calabrò

Computer Engineer · Cyber Security & Digital Forensics Analyst
Lecturer | Speaker | Trainer

INQUADRA PER APPROFONDIRE

vincenzocalabro.it

Materiali, profilo e contatti per domande, tesi e approfondimenti.