



CORSO DI CYBER SECURITY · MODULO INFRASTRUTTURE CRITICHE

Digital Forensics e Incident Response delle infrastrutture critiche

Convergenza IT/OT, modello di minaccia e paradigmi forensi per i sistemi ciber-fisici dell'energia

Vincenzo Calabrò · Ingegnere informatico, cyber security e digital forensics analyst

Obiettivi formativi e struttura della lezione

Al termine della lezione lo studente sarà in grado di

1. descrivere l'architettura di un'infrastruttura energetica moderna e la convergenza fra IT e OT, con riferimento al modello Purdue e a NIST SP 800-82;
2. analizzare la catena di compromissione di un sistema ciber-fisico, anche attraverso il caso dell'attacco alla rete elettrica ucraina del 23 dicembre 2015;
3. applicare la metodologia DFIR ai sistemi OT secondo NIST IR 8428, tenendo conto dei vincoli di disponibilità del processo e di safety;
4. valutare i paradigmi di forensic readiness, forensics by design, forensic predittiva e forensic as a service alla luce della letteratura e degli standard.

Articolazione della lezione

- I** Il contesto: architettura energetica e convergenza IT/OT
- II** Il modello di minaccia: livelli, vettori, caso ucraino, strumenti e quadro normativo
- III** Digital forensics e incident response in ambito OT
- IV** Forensic readiness ed evoluzione del paradigma forense

The background of the slide is a dark blue-grey color with a faint, abstract network pattern. This pattern consists of numerous small, light-blue dots connected by thin, light-blue lines, forming a complex web of interconnected nodes and edges. Some nodes are slightly larger or more prominent than others, and the overall structure suggests a distributed system or a complex network topology.

I

Il contesto: l'infrastruttura energetica come sistema ciber-fisico distribuito

Architettura, flussi di energia e di dati, convergenza IT/OT e priorità divergenti fra i due domini.

Architettura di un'infrastruttura energetica moderna



Il sistema è distribuito su un numero elevato di nodi, ciascuno dei quali costituisce un possibile punto di accesso per un attaccante (cfr. NIST SP 800-82 Rev. 3, 2023).

Flusso di energia, flusso di dati e convergenza IT/OT

⚡ **Flusso di energia:** generazione, accumulo, consumo

📊 **Flusso di dati:** sensori, acquisizione, analisi

Dominio IT

INFORMATION TECHNOLOGY

- Server, workstation, posta elettronica
- Sistemi ERP e applicativi gestionali
- Gestione delle identità e degli accessi
- VPN e accesso remoto

Zona di convergenza

COMPONENTI CONDIVISI

- Engineering workstation
- Dati di processo e historian
- Industrial Internet of Things (IIoT)
- Sensori e dispositivi connessi in rete

Dominio OT

OPERATIONAL TECHNOLOGY

- Sistemi SCADA
- Controllori logici programmabili (PLC)
- Reti industriali e RTU
- Sensori e attuatori di campo

La digitalizzazione dei processi industriali ha prodotto benefici nella gestione dei dati e, al tempo stesso, ha reso raggiungibili dalla rete aziendale componenti che in passato erano isolati (NIST SP 800-82 Rev. 3; IEC 62443-1-1).

Gerarchia delle priorità nei due domini

Sistemi IT

ORDINE DELLE PRIORITÀ

- 1** **Confidenzialità**
protezione dei dati da accessi non autorizzati
- 2** **Integrità**
correttezza e non alterazione delle informazioni
- 3** **Disponibilità**
può essere temporaneamente sacrificata nelle fasi di contenimento

Sistemi OT ed energetici

ORDINE DELLE PRIORITÀ

- 1** **Disponibilità**
continuità del processo di produzione e distribuzione
- 2** **Safety**
sicurezza delle persone, degli impianti e dell'ambiente
- 3** **Integrità e confidenzialità**
rilevanti, ma subordinate alla continuità operativa e alla safety

La differenza di priorità è documentata in NIST SP 800-82 Rev. 3 (2023) e nella serie IEC 62443; essa condiziona la strategia di risposta all'incidente, trattata nella terza parte della lezione.

II

Il modello di minaccia: livelli, vettori, strumenti e un caso documentato

Modello Purdue, catena di compromissione, caso ucraino del 2015, strumenti d'attacco e quadro normativo.

Il modello Purdue: la stratificazione dell'architettura

Livelli 4–5	Rete aziendale (IT)	Dominio IT, server di posta, ERP, workstation, accesso a Internet
Livello 3.5	Zona demilitarizzata (DMZ)	Servizi esposti, proxy, jump host, accesso VPN
Livello 3	Gestione delle operazioni	Server SCADA, engineering workstation, domain controller OT
Livello 2	Controllo di supervisione	Interfacce HMI per il monitoraggio e l’invio di comandi
Livello 1	Controllo di base	PLC e RTU (es. sottostazioni che inviano dati ai sistemi SCADA)
Livello 0	Processo fisico	Sensori intelligenti, trasformatori, interruttori di alta tensione

 Zona IT  Zona di confine  Zona OT

Fonti: Williams (1994); ISA-95; IEC 62443-3-2 (zone e condotti); NIST SP 800-82 Rev. 3 (architettura di rete).

Vettori di accesso iniziale e tempo di permanenza



Spear phishing

Messaggi mirati a figure con privilegi elevati, resi più efficaci dall'ingegneria sociale e dai contenuti sintetici.



Catena di fornitura

Compromissione di software, dispositivi o fornitori con accesso alla rete; la NIS2 (art. 21) ne impone la gestione del rischio.



Accesso remoto

VPN o credenziali di accesso remoto sottratte; dispositivi di rete non aggiornati sono il punto d'ingresso in diversi casi recenti.

TEMPO DI PERMANENZA

Fra l'accesso iniziale e l'impatto trascorrono spesso settimane o mesi, impiegati per esfiltrazione, ricognizione e selezione dei dispositivi. Nel caso ucraino del 2015 l'intrusione precedette l'attacco di diversi mesi (Lee, Assante e Conway, 2016).

CASO DOCUMENTATO: ARUP, 2024

Hong Kong: un dipendente ha autorizzato trasferimenti per circa 200 milioni di HKD (25 milioni di USD) dopo una videoconferenza con il direttore finanziario e colleghi riprodotti mediante deepfake (conferma della società, maggio 2024).

La catena di compromissione

1. Accesso iniziale

Initial Access

Primo punto d'appoggio nella rete aziendale (phishing, catena di fornitura, accesso remoto).

2. Movimento laterale

Lateral Movement

Escalation dei privilegi, raccolta di credenziali, attraversamento di DMZ e firewall.

3. Discovery

Discovery, Collection

Mappatura di asset e servizi per individuare i dispositivi industriali raggiungibili.

4. Accesso alla rete OT

Lateral Movement (rete OT)

Ingresso nella rete di controllo: SCADA, PLC, engineering workstation.

5. Azione OT

Impair Process Control

Comandi alla rete di campo, modifica di configurazioni, inibizione del ripristino.

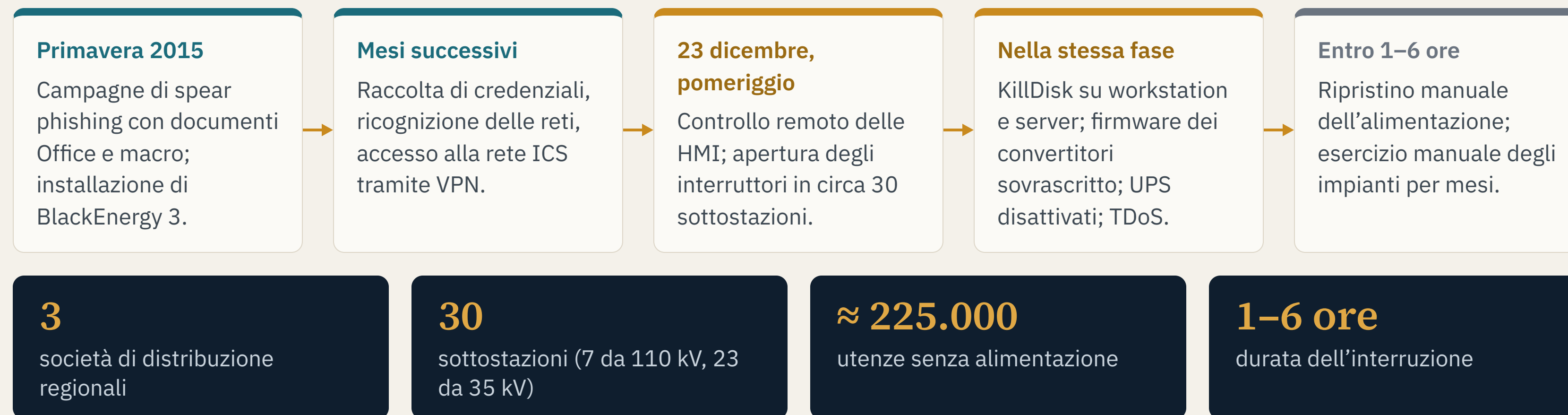
6. Impatto sul processo

Impact

Dal blocco della produzione alla modifica di parametri non immediatamente rilevabile.

La ricostruzione dell'intera sequenza è l'oggetto dell'analisi forense (NIST IR 8428); le tattiche indicate seguono la matrice MITRE ATT&CK for ICS.

Caso di studio: Ucraina, 23 dicembre 2015



Attribuzione pubblica al gruppo Sandworm, collegato ai servizi d'intelligence russi (incriminazione del Dipartimento di Giustizia statunitense, ottobre 2020). Fonti: Lee, Assante e Conway, SANS ICS/E-ISAC (2016); ICS-CERT, IR-ALERT-H-16-056-01 (2016).

Il caso ucraino letto sul modello Purdue

Fase	Tecnica osservata	Livello Purdue
1 · Accesso iniziale	Spear phishing con allegati Office e macro; installazione del malware BlackEnergy 3	Livelli 4–5 (rete aziendale)
2 · Movimento laterale	Raccolta di credenziali e ricognizione protratta per mesi	Livelli 4–5
3 · Attraversamento	Ingresso nella rete ICS tramite VPN legittima con credenziali sottratte	Livello 3.5 (DMZ)
4 · Azione OT	Controllo remoto delle interfacce HMI; apertura degli interruttori	Livelli 2–3
5 · Inibizione del ripristino	KillDisk; firmware dei convertitori seriale-Ethernet sovrascritto; UPS disattivati; TDoS al call center	Livelli 1–3
6 · Impatto fisico	Circa 225.000 utenze senza alimentazione per 1–6 ore; ripristino manuale	Livello 0 (processo)

La sequenza coincide con la catena di compromissione descritta nella slide precedente; le fasi 5 e 6 corrispondono alle tattiche Inhibit Response Function e Impact di MITRE ATT&CK for ICS. Fonti: Lee, Assante e Conway (2016); ICS-CERT (2016).

Strumenti d’attacco e protocolli bersaglio

FRAMEWORK D’ATTACCO SPECIFICO PER L’OT

PIPEDREAM / INCONTROLLER

Insieme di strumenti modulari reso pubblico nell’aprile 2022 (Dragos; Mandiant; CISA, Alert AA22-103A), concepito per individuare i dispositivi industriali in rete, assumerne il controllo e inviare comandi.

- Modularità: componenti selezionabili in funzione dell’architettura industriale
- Precondizione: un accesso alla rete IT o OT ottenuto con i vettori descritti
- Passaggio dal dominio informatico al processo fisico (sistema ciber-fisico)

Dispositivi e protocolli interessati

Bersaglio	Protocolli	Rilevanza
Server OPC UA	OPC UA	Interscambio dati fra PLC, RTU e SCADA
PLC Schneider Electric	Modbus, CODESYS	Protocolli privi di cifratura
PLC Omron	HTTP, FINS	Protocollo proprietario di messaggistica
Historian e SOE	Registri di processo	Manipolazione dei registri di evento

Molti protocolli industriali non prevedono autenticazione né cifratura. Per il settore elettrico la serie IEC 62351 definisce i meccanismi di sicurezza per IEC 61850 e IEC 60870-5; la loro adozione sui dispositivi esistenti è tuttavia graduale.

Altri casi documentati, 2023–2026

Maggio 2023

Danimarca, 22 operatori energetici

Compromissione simultanea attraverso una vulnerabilità dei firewall Zyxel (CVE-2023-28771) non corretta; rapporto SektorCERT, novembre 2023.

29 dic. 2025

Polonia, generazione distribuita

Almeno 30 impianti eolici e fotovoltaici e un impianto di cogenerazione; wiper su RTU, modem, router e switch; perdita del controllo remoto (CERT Polska, 2026).

Agosto 2026

Regno Unito, generatore

Generatore di piccola scala fermo per circa quattro giorni; attribuzione a gruppi legati all'Iran riportata dalla stampa, non confermata ufficialmente (agosto 2026).

11–12 ott. 2026

Francia, grande distribuzione

Alcune centinaia di punti vendita; controllori di refrigerazione Danfoss fuori supporto forzati a sbrinamento con set-point a 50 °C; indagine della Procura di Parigi.

Tre elementi ricorrenti: dispositivi di rete e controllori non aggiornati come punto d'ingresso, azione distruttiva sui componenti di campo, impatto fisico diretto. Il caso francese non riguarda il settore energetico, ma mostra la natura fisica delle conseguenze di un attacco OT.

Quadro normativo e standard di riferimento

DIRETTIVA (UE) 2022/2555

NIS2

Misure di gestione del rischio (art. 21), inclusa la catena di fornitura, e notifica degli incidenti (art. 23). Recepita con il D.Lgs. 4 settembre 2024, n. 138.

DIRETTIVA (UE) 2022/2557

CER

Resilienza fisica e organizzativa dei soggetti critici, a complemento della sicurezza informatica. Recepita con il D.Lgs. 4 settembre 2024, n. 134.

NIST, GIUGNO 2022

NIST IR 8428

DFIR Framework for Operational Technology: riferimento specifico per la digital forensics nei sistemi OT, adottato come traccia nella terza parte.

Ambito	Standard e linee guida
Sicurezza OT e settore elettrico	IEC 62443 (serie); IEC 62351 (sicurezza dei protocolli IEC 61850 e IEC 60870-5); ISO/IEC 27019:2017; NIST SP 800-82 Rev. 3 (2023)
Evidenze digitali e indagini	ISO/IEC 27037:2012; ISO/IEC 27041, 27042 e 27043:2015; NIST SP 800-86 (2006)
Gestione degli incidenti	ISO/IEC 27035-1 e 27035-2:2023; NIST SP 800-61 Rev. 3 (2025)

III

Digital forensics e incident response in ambito OT

Domande investigative, differenze rispetto all'IT e sequenza di risposta nel rispetto del processo.

Le domande investigative, livello per livello

Livello	Domanda investigativa	Fonti di evidenza
1 · Accesso iniziale (IT)	Chi ha ottenuto l’accesso e con quali credenziali?	Identità, Active Directory, MFA, log VPN
2 · Confine (DMZ)	Come è stato attraversato il confine IT/OT?	Log di firewall, DMZ e accessi remoti
3 · Operazioni (L3)	Da quale engineering workstation è partito il comando?	RAM e log della workstation; domain controller OT
4 · Supervisione (L2)	Quale comando è stato modificato e inviato?	SCADA, HMI, historian e registri SOE
5 · Controllo e campo (L1–L0)	Quale controller ha accettato il comando e con quale effetto?	PLC e RTU, configurazioni, firmware, dati di processo

Raccolta delle evidenze secondo ISO/IEC 27037 e NIST IR 8428; sui limiti dell’acquisizione dai dispositivi di campo: Ahmed et al. (2012), Van der Knijff (2014).

La risposta all'incidente nei due domini

SISTEMA IT COMPROMESSO

L'isolamento è una prima misura ammissibile

- Scollegamento dei sistemi compromessi, se necessario anche della connettività verso Internet.
- In questa fase la disponibilità passa in secondo piano rispetto all'integrità.
- Obiettivo: impedire movimento laterale e propagazione (NIST SP 800-61 Rev. 3).

SISTEMA OT COMPROMESSO

L'interruzione del processo non è la prima opzione

- Produzione e distribuzione devono proseguire; l'isolamento va valutato caso per caso.
- Un riavvio o un isolamento indiscriminato può compromettere processo e safety.
- Obiettivo: interventi mirati, concordati con l'ingegneria (NIST SP 800-82 Rev. 3; NIST IR 8428).

La diversa gerarchia delle priorità determina due strategie di contenimento: nell'IT si accetta la perdita temporanea di disponibilità; nell'OT la continuità del processo e la safety vincolano ogni intervento, che va pianificato prima dell'incidente.

Sequenza di risposta compatibile con il processo

FASE 1

Safety assessment

Verifica dello stato dell'impianto con l'ingegneria di processo: intervento di interlock e sistemi di sicurezza, variazioni anomale di potenza o tensione, condizioni di esercizio manuale.



FASE 2

Contenimento mirato

Revoca degli account compromessi e chiusura dei canali di accesso remoto individuati; nessun isolamento o riavvio indiscriminato dei dispositivi di campo.



FASE 3

Ripristino su baseline validata

Ripristino della configurazione di riferimento approvata (golden configuration), con verifica dell'integrità del firmware e possibilità di rollback.

La sequenza è coerente con le fasi di contenimento, eradicazione e ripristino di NIST SP 800-61 Rev. 3, adattate ai vincoli dell'OT (NIST IR 8428). Essa presuppone un'infrastruttura già predisposta: è l'oggetto della forensic readiness (Tan, 2001; Rowlingson, 2004).

IV

Forensic readiness ed evoluzione del paradigma forense

Prerequisiti, rilettura del caso ucraino, competenze, forensics by design, predittiva e as a service.

Forensic readiness: i prerequisiti dell'infrastruttura



Inventario contestuale

Ruolo di ogni dispositivo nel processo ed effetti di interrogazioni e riavvii (IEC 62443-2-1).



Logging centralizzato

Log completi, raccolti in un punto centrale, con retention definita e copia fuori banda.



Sincronizzazione temporale

Senza allineamento degli orologi la timeline non è ricostruibile (ISO/IEC 27037; NIST SP 800-86).



Configurazioni di riferimento

Golden configuration e versioni note del firmware; il downgrade a versioni vulnerabili è documentato.



Governance ed esercitazioni

Ruoli definiti prima dell'incidente e verificati con esercitazioni (ISO/IEC 27035-2; NIST SP 800-61).



Registro delle decisioni

Rischi valutati, alternative considerate e autorizzazioni, a supporto della catena di custodia.

Il concetto di forensic readiness è introdotto da Tan (2001) e sistematizzato da Rowlingson (2004) in dieci passi; Eden et al. (2016) ne propongono l'adattamento ai sistemi SCADA/ICS.

Il caso ucraino e i criteri della readiness

Fattori che hanno ostacolato analisi e ripristino

- KillDisk ha cancellato workstation e server, con perdita di log ed evidenze locali: necessità di logging centralizzato e copie fuori banda.
- Firmware dei convertitori seriale-Ethernet sovrascritto, dispositivi inutilizzabili: necessità di configurazioni di riferimento, versioning e ricambi.
- UPS disattivati e negazione del servizio telefonico: necessità di canali di comunicazione alternativi e di piani di continuità.
- Accesso VPN con credenziali valide e senza autenticazione a più fattori: necessità di gestione delle identità e di log degli accessi remoti.

Fattori che hanno consentito la risposta

- Possibilità di esercizio manuale delle sottostazioni: ripristino dell'alimentazione entro 1–6 ore, in coerenza con la priorità alla disponibilità e alla safety.
- Evidenze residue (e-mail di phishing, campioni di BlackEnergy e KillDisk, log di rete) sufficienti alla ricostruzione e all'attribuzione.
- Analisi condotta con enti esterni (SANS/E-ISAC, ICS-CERT) e condivisione pubblica dei risultati, come raccomandato da NIST SP 800-61 Rev. 3.
- Documentazione del caso divenuta riferimento per esercitazioni e per la progettazione della readiness negli operatori elettrici.

Le competenze coinvolte nella gestione dell'incidente

Digital forensics

Piano delle evidenze, catena di custodia, timeline degli eventi, relazione tecnica.

Ingegneria di processo

Conosce la logica dei PLC; interviene nel ripristino e valida le configurazioni.

Safety

Sicurezza delle persone, degli impianti e dell'ambiente in ogni decisione operativa.



Incidente OT

La gestione dell'incidente in ambito OT richiede il concorso simultaneo di competenze informatiche e industriali. NIST IR 8428 e ISO/IEC 27043 raccomandano ruoli e responsabilità definiti prima dell'evento e la registrazione delle decisioni.

SOC e CISO

Rilevazione, escalation, threat intelligence e coordinamento della risposta.

Esercizio e manutenzione

Opera sul campo; conosce processi, priorità e livelli di servizio.

Direzione e governance

Autorizza gli interventi, valuta rischi e alternative, mantiene il registro delle decisioni.

Dalla forensics reattiva alla forensics continuativa



Le fasi 1 e 2 sono consolidate nella letteratura e negli standard; le fasi 3, 4 e 5 sono proposte della pratica professionale e oggetto di ricerca, non ancora codificate in norme tecniche.

Forensics by design e catena di fornitura

DUE LIVELLI DI PREDISPOSIZIONE

Forensic readiness

L'organizzazione è pronta: audit abilitati, retention dei log, valutazione delle vulnerabilità, inventario e governance in essere (Rowlingson 2004).

Forensics by design

I requisiti forensi sono incorporati nella progettazione e nell'architettura dell'impianto e dei suoi componenti (Rahman et al. 2016), con effetti sulla rapidità della prevenzione e della risposta.

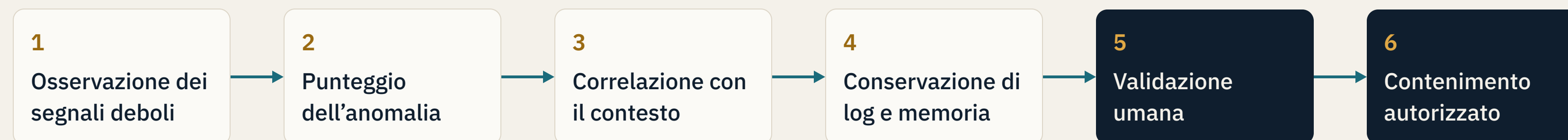
CLAUSOLE CONTRATTUALI PER I FORNITORI

Fornitori e gestori di dispositivi proprietari partecipano per contratto alla predisposizione forense (NIS2, art. 21, par. 2, lett. d; IEC 62443-2-4):

- ✓ Log degli accessi ai sistemi gestiti
- ✓ Clausola sugli incidenti di sicurezza
- ✓ Configurazioni e relativi backup
- ✓ Supporto del fornitore nella risposta
- ✓ Diritti di audit

Forensic predittiva e supervisione umana

Su un'infrastruttura predisposta, tecniche di analisi e di apprendimento automatico possono segnalare anomalie e avviare la conservazione delle evidenze prima della loro perdita.



FUNZIONI AFFIDATE ALL'ANALISI AUTOMATICA

Rilevazione di deviazioni, sequenze e relazioni anomale fra eventi singolarmente non significativi; attribuzione di un punteggio; avvio della conservazione delle evidenze volatili.

FUNZIONI RISERVATE ALL'OPERATORE

Valutazione del contesto, della safety e dell'impatto; autorizzazione del contenimento. Per i sistemi ad alto rischio il Regolamento (UE) 2024/1689 (art. 14) richiede una sorveglianza umana effettiva.

CONCLUSIONI

Conclusioni

- 1** Nei sistemi OT la gerarchia delle priorità (disponibilità, safety) determina modalità di risposta diverse da quelle dell'IT (NIST SP 800-82 Rev. 3; NIST IR 8428).
- 2** Il tempo di permanenza dell'attaccante, misurabile in mesi nei casi documentati (Ucraina 2015, Polonia 2025), è la finestra utile per intercettare gli eventi precursori.
- 3** La ricostruzione della catena di compromissione richiede inventario contestuale, log centralizzati, sincronizzazione temporale e configurazioni di riferimento (Rowlingson 2004).
- 4** La predisposizione forense deve estendersi alla catena di fornitura, come richiesto dall'art. 21 della NIS2 e dalla IEC 62443-2-4.
- 5** L'impiego dell'analisi automatica nella rilevazione precoce richiede la supervisione umana sulle decisioni di contenimento (Regolamento (UE) 2024/1689, art. 14).

CONCLUSIONI

Domande per la discussione ed esercitazione

Questioni aperte

1. In quali circostanze l'isolamento di un dispositivo OT è giustificato nonostante l'impatto sul processo, e chi è legittimato a decidere?
2. Quali evidenze volatili rischiano di andare perdute durante un safety assessment prolungato, e con quali strumenti possono essere conservate (ISO/IEC 27037)?
3. La forensic as a service è compatibile con i requisiti di catena di custodia e di riservatezza di un soggetto essenziale ai sensi della NIS2?
4. Con quali criteri valutare l'affidabilità di un'anomalia segnalata da un sistema automatico prima di autorizzare un intervento sul processo?

ESERCITAZIONE

Un gestore della distribuzione rileva una variazione anomala dei set-point in una sottostazione.

In gruppi, con i ruoli della slide sulle competenze, progettare:

- piano di acquisizione delle evidenze per livello Purdue;
- sequenza di risposta compatibile con il servizio;
- clausole contrattuali per il fornitore SCADA;
- registro delle decisioni condiviso.

RIFERIMENTI (1 DI 2)

Normativa e standard

NORMATIVA EUROPEA E NAZIONALE

Direttiva (UE) 2022/2555 (NIS2), 14 dicembre 2022; recepita con D.Lgs. 4 settembre 2024, n. 138.

Direttiva (UE) 2022/2557 (CER), 14 dicembre 2022; recepita con D.Lgs. 4 settembre 2024, n. 134.

Regolamento (UE) 2024/1689 (intelligenza artificiale), 13 giugno 2024, art. 14 e allegato III.

SICUREZZA OT E SETTORE ELETTRICO

IEC 62443 (serie), *Security for industrial automation and control systems*, parti 1-1, 2-1, 2-4, 3-2, 3-3.

IEC 62351 (serie), sicurezza dei dati e delle comunicazioni per i sistemi di gestione dell'energia elettrica.

ISO/IEC 27019:2017, *Information security controls for the energy utility industry*.

NIST SP 800-82 Rev. 3 (2023), *Guide to Operational Technology (OT) Security*.

EVIDENZE DIGITALI E INDAGINI

ISO/IEC 27037:2012, identificazione, raccolta, acquisizione e conservazione delle evidenze digitali.

ISO/IEC 27041, 27042 e 27043 (2015): idoneità dei metodi, analisi e interpretazione, processi di indagine.

NIST SP 800-86 (2006), *Guide to Integrating Forensic Techniques into Incident Response*.

NIST IR 8428 (2022), *Digital Forensics and Incident Response (DFIR) Framework for Operational Technology*.

GESTIONE DEGLI INCIDENTI E TASSONOMIE

ISO/IEC 27035-1:2023 e 27035-2:2023, *Information security incident management*.

NIST SP 800-61 Rev. 3 (2025), *Incident Response Recommendations and Considerations*.

MITRE ATT&CK for ICS, base di conoscenza delle tattiche e tecniche contro i sistemi di controllo industriale.

RIFERIMENTI (2 DI 2)

Letteratura scientifica e rapporti tecnici

LETTERATURA SCIENTIFICA

Williams T.J. (1994), The Purdue enterprise reference architecture, *Computers in Industry*, 24(2–3), 141–158.

Tan J. (2001), *Forensic Readiness*, @stake.

Rowlingson R. (2004), A Ten Step Process for Forensic Readiness, *International Journal of Digital Evidence*, 2(3).

Ahmed I., Obermeier S., Naedele M., Richard G.G. (2012), SCADA Systems: Challenges for Forensic Investigations, *IEEE Computer*, 45(12), 44–51.

Van der Knijff R.M. (2014), Control systems/SCADA forensics, what's the difference?, *Digital Investigation*, 11(3), 160–174.

Rahman N.H.A., Glisson W.B., Yang Y., Choo K.-K.R. (2016), Forensic-by-Design Framework for Cyber-Physical Cloud Systems, *IEEE Cloud Computing*, 3(1), 50–59.

Eden P. et al. (2016), Forensic Readiness for SCADA/ICS Incident Response, *4th International Symposium for ICS & SCADA Cyber Security Research*.

RAPPORTI TECNICI E FONTI SUI CASI

Lee R.M., Assante M.J., Conway T. (2016), *Analysis of the Cyber Attack on the Ukrainian Power Grid*, SANS ICS / E-ISAC, 18 marzo 2016.

ICS-CERT (2016), Alert IR-ALERT-H-16-056-01, *Cyber-Attack Against Ukrainian Critical Infrastructure*; US DoJ (2020), incriminazione di sei ufficiali del GRU.

Dragos (2022), *PIPEDREAM: CHERNOVITE's Emerging Malware Targeting Industrial Control Systems*; Mandiant (2022), *INCONTROLLER*; CISA (2022), Alert AA22-103A.

SektorCERT (2023), *The attack against Danish, critical infrastructure*, novembre 2023.

CERT Polska (2026), *Cyber Sabotage in the Energy Sector: Lessons from Poland's December 29 Attacks*; Dragos (2026), *Poland Power Grid Attack*.

Stampa: The Telegraph e The Register (ago. 2026) sul caso britannico; AFP, BFM TV, MacGeneration (ott. 2026) sul caso francese; SCMP (mag. 2024) su Arup.

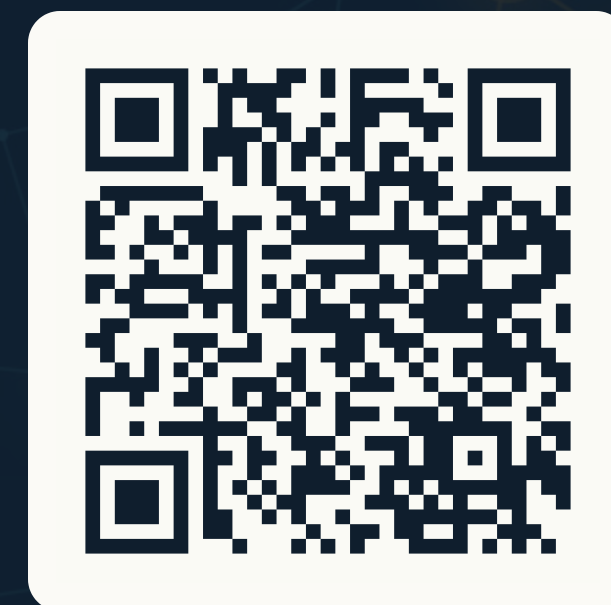


Grazie per l'attenzione

Vincenzo Calabrò

Ingegnere informatico · Cyber security e digital forensics
analyst · Docente e formatore

vincenzocalabro.it · linkedin.com/in/vincenzocalabro



Profilo LinkedIn