

Zero Trust selettivo negli ambienti **OT**

Il modello MATRIX:

un framework metodologico
per l'adozione selettiva dello
zero trust negli ambienti
Operational Technology

A cura di **Vincenzo Calabrò**

Indice

About the author	4
Abstract e Parole Chiave	5
01 Introduzione	6
1.1 Convergenza IT/OT e fine dell'air gap	7
1.2 L'erosione del modello perimetrale	7
1.3 Perché lo Zero Trust diventa necessario	8
1.4 Specificità OT: disponibilità, integrità e safety	8
1.5 Obiettivi e struttura del paper	9
02 Background e lavori correlati	11
2.1 Lo zero trust: dai perimetri alle identità	12
2.2 Anatomia degli ambienti Operational Technology	13
2.3 Perché i controlli EIT non si trasferiscono direttamente?	15
2.4 Lavori correlati	15
03 Il framework MATRIX	17
3.1 M - Caratterizzazione del contesto di missione e dei DAAS	19
3.2 A - Profilazione dell'idoneità degli asset	19
3.3 T - Modellazione delle minacce e della superficie d'attacco	21
3.4 R - Analisi del rischio e dei compromessi	22
3.5 I - Implementazione: la matrice di allocazione delle capability	23
3.6 X - Esecuzione, monitoraggio ed evoluzione della maturità	25

04	Validazione	26
4.1	Validazione illustrativa: le sottostazioni elettriche digitali	27
4.2	Validazione di copertura rispetto agli standard	29
4.3	Validazione comparativa	30
4.4	Validazione retrospettiva: l'attacco alla rete di distribuzione ucraina del 2015	31
4.5	Sintesi della validazione	33
05	Implicazioni	34
5.1	Pregi del framework MATRIX	35
5.2	Limiti e assunzioni	35
5.3	Generalizzabilità e adattabilità del modello	36
06	Conformità normativa	37
6.1	Il quadro regolatorio europeo e nazionale	38
6.2	Mappatura del framework agli obblighi	40
07	Conclusioni e sviluppi futuri	42
	Riferimenti bibliografici	44



**CYBER SECURITY &
DIGITAL FORENSICS**

Vincenzo Calabrò

Funzionario alla Sicurezza CIS · Ministero dell'Interno
Digital Forensics Analyst

È laureato in Ingegneria Informatica e in Sicurezza Informatica presso le Università di Roma La Sapienza e di Milano. Ha indirizzato la propria formazione nei settori della cyber security e della digital forensics, conseguendo i diplomi di perfezionamento in Data Protection e Data Governance, in Criminalità Informatica e Investigazioni Digitali e in Big Data e Artificial Intelligence. Ha inoltre ottenuto l'Advanced Cybersecurity Graduate Certificate alla School of Engineering della Stanford University e i Professional Certificate in Information Security; Incident Response Process; Digital Forensics; Cybersecurity Engineering and Software Assurance; Applied Data Science for Cybersecurity; Artificial Intelligence (AI) for Cybersecurity al Software Engineering Institute della Carnegie Mellon University.

Dal 1992 è nei ruoli del Ministero dell'Interno, ove ricopre l'incarico di Funzionario alla Sicurezza CIS: in tale veste contribuisce alla valutazione dei rischi cyber, all'implementazione delle misure di sicurezza e alla risoluzione di incidenti informatici. Offre altresì consulenza tecnica nel campo della digital forensics per l'Autorità giudiziaria, la Polizia giudiziaria e gli studi legali.

Una matrice per allocare la fiducia

La trasformazione digitale delle infrastrutture critiche ha eroso la tradizionale separazione tra le reti informatiche aziendali (Enterprise Information Technology, EIT) e i sistemi di automazione industriale (Operational Technology, OT), esponendo gli impianti progettati per operare in isolamento a minacce sempre più sofisticate. Il paradigma zero trust, basato sul principio "never trust, always verify", è diventato un punto di riferimento per la sicurezza dell'EIT, ma la sua applicazione diretta agli ambienti OT è ostacolata da differenze sostanziali in termini di architettura, vincoli di tempo reale e requisiti di sicurezza, nonché dalla presenza diffusa di tecnologie legacy. Questo studio propone MATRIX, un framework metodologico per l'adozione selettiva e mission-driven dei controlli zero trust in ambienti OT eterogenei. Il framework, suddiviso in sei fasi

(caratterizzazione del contesto di missione, profilazione dell'idoneità degli asset, modellazione delle minacce, analisi dei compromessi, implementazione tramite matrice di allocazione delle capacità ed esecuzione con evoluzione incrementale della maturità), collega in modo esplicito la comprensione dell'ambiente operativo alla selezione dei controlli tecnicamente sostenibili per ciascuna classe di asset. La metodologia integra i principi normativi consolidati (NIST SP 800-207, NIST SP 800-82r3, ISA/IEC 62443) e la letteratura scientifica più recente e viene illustrata mediante uno scenario applicativo relativo alle sottostazioni elettriche digitali. I risultati attesi includono la riduzione della superficie d'attacco, il contenimento del movimento laterale e la gestione esplicita del rischio residuo associato ai componenti non aggiornabili.

PAROLE CHIAVE

Zero Trust

Operational Technology

Infrastrutture critiche

Modello Purdue

NIST SP 800-207

NIST SP 800-82r3

ISA/IEC 62443

NIS2

Sottostazioni digitali

Rischio residuo

01

CAPITOLO 1

Introduzione

- 1.1 Convergenza IT/OT e fine dell'air gap
- 1.2 L'erosione del modello perimetrale
- 1.3 Perché lo Zero Trust diventa necessario
- 1.4 Specificità OT: disponibilità, integrità e safety
- 1.5 Obiettivi e struttura del paper



Introduzione

Dalla fine dell'air gap alla necessità, problematica, dello Zero Trust negli ambienti industriali

1.1 Convergenza IT/OT e fine dell'air gap

Per decenni, la sicurezza dei sistemi di controllo industriale si è basata su un presupposto rassicurante, ma fragile: l'isolamento fisico. Le reti che governano impianti energetici, sistemi idrici, processi manifatturieri e infrastrutture di trasporto erano concepite come enclavi separate, protette da un air gap rispetto al mondo esterno e alle reti aziendali.

Tale separazione, già imperfetta in passato, si è progressivamente dissolta sotto la spinta della trasformazione digitale e della convergenza tra Information Technology (IT) e Operational Technology (OT). L'esigenza di analisi dei dati in tempo reale, di manutenzione predittiva, di accesso remoto dei fornitori e di integrazione con i servizi cloud ha moltiplicato i punti di contatto tra i due domini, trasformando i sistemi, che un tempo erano opachi per l'attaccante, in bersagli raggiungibili.¹

1.2 L'erosione del modello perimetrale

Le conseguenze di questa esposizione non sono solo ipotesi accademiche. La scoperta di Stuxnet nel 2010 ha dimostrato che un'arma informatica può oltrepassare l'isolamento di un impianto e manipolare i controllori logici programmabili responsabili di un processo fisico, con conseguenze distruttive sul macchinario.²

Pochi anni dopo, l'attacco alla rete elettrica ucraina del dicembre 2015 provocò un'interruzione di corrente che coinvolse centinaia di migliaia di utenti, confermando la capacità degli avversari di colpire deliberatamente la distribuzione dell'energia.³ La successiva ondata di campagne di ransomware contro le infrastrutture critiche, culminata con episodi che hanno paralizzato la logistica di approvvigionamento del carburante, ha messo in luce come le motivazioni economiche e geopolitiche possano convergere sullo stesso obiettivo.

¹ Cloud Security Alliance, *Zero Trust Guidance for Critical Infrastructure*. Seattle, WA, USA: CSA Zero Trust Working Group, ott. 2024.

² R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Security & Privacy*, vol. 9, n. 3, pp. 49–51, 2011.

³ R. M. Lee, M. J. Assante e T. Conway, *Analysis of the Cyber Attack on the Ukrainian Power Grid*. Washington, DC, USA: E-ISAC e SANS Industrial Control Systems, 2016.

1.3 Perché lo Zero Trust diventa necessario

In risposta all'inadeguatezza delle difese perimetrali, è emerso così il paradigma zero trust, introdotto da Kindervag nel 2010 come superamento del modello "castello e fossato"⁴ e successivamente formalizzato dal National Institute of Standards and Technology nella Special Publication 800-207.⁵

Lo Zero Trust sposta il baricentro della sicurezza dal confine di rete alle risorse, alle identità e ai singoli flussi di accesso. Il suo principio fondamentale è che nessuna entità, che si tratti di un utente, di un dispositivo o di un servizio, debba godere di fiducia implicita solo in virtù della sua collocazione di rete; ogni richiesta di accesso deve essere autenticata, autorizzata e valutata dinamicamente prima e durante l'interazione con una risorsa.⁶

1.4 Specificità OT: disponibilità, integrità e safety

Il modello si è dimostrato efficace nei contesti EIT, in cui la mobilità degli

utenti, l'adozione del cloud e la diffusione di dispositivi personali avevano già reso obsoleto il concetto di perimetro. La sua applicazione agli ambienti OT, tuttavia, non è affatto immediata. I sistemi OT, infatti, ribaltano la gerarchia delle priorità in materia di sicurezza tipica dell'IT: se nell'IT prevale la riservatezza, nell'OT la gerarchia si capovolge a favore della disponibilità e dell'integrità, perché un'interruzione del processo fisico può tradursi in danni materiali, rischi per l'incolumità delle persone e interruzione di servizi essenziali.⁷ A ciò si aggiungono vincoli stringenti in termini di latenza, la necessità di un funzionamento continuo, l'uso di protocolli proprietari privi di autenticazione e la pervasiva presenza di dispositivi legacy progettati quando la connettività era un'eccezione e non la regola. Meccanismi che nell'IT si danno per scontati, come gli agenti software sugli endpoint, le scansioni antimalware e le frequenti riconfigurazioni delle policy, possono risultare semplicemente impraticabili su un relè di protezione che ha ancora decenni di servizio davanti a sé.

⁴ J. Kindervag, *Build Security Into Your Network's DNA: The Zero Trust Network Architecture*. Cambridge, MA, USA: Forrester Research, 2010.

⁵ S. Rose, O. Borchert, S. Mitchell e S. Connelly, *Zero Trust Architecture*, NIST Special Publication 800-207. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2020, doi: 10.6028/NIST.SP.800-207.

⁶ S. Rose, O. Borchert, S. Mitchell e S. Connelly, *Zero Trust Architecture*, NIST Special Publication 800-207. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2020, doi: 10.6028/NIST.SP.800-207.

⁷ K. Stouffer, M. Pease, C. Tang, T. Zimmerman, V. Pillitteri, S. Lightman, A. Hahn, S. Saravia, A. Sherule e M. Thompson, *Guide to Operational Technology (OT) Security*, NIST Special Publication 800-82r3. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2023, doi: 10.6028/NIST.SP.800-82r3.

Solo di recente la comunità tecnica e normativa ha colmato questo vuoto. La revisione 3 della NIST SP 800-82 ha ampliato il proprio ambito di applicazione, estendendolo dall'insieme ristretto dei sistemi di controllo industriale all'intera categoria dell'OT (Operational Technology) e aggiornando l'analisi delle minacce, delle vulnerabilità e delle contromisure.⁸ Nel mese di ottobre 2024, la Cloud Security Alliance ha pubblicato una guida dedicata all'applicazione dei principi Zero Trust alle infrastrutture critiche, organizzata attorno a un processo in cinque fasi.⁹ A livello europeo, l'Agenzia dell'Unione europea per la cibersicurezza (ENISA) ha elaborato una guida tecnica per l'attuazione delle misure di gestione del rischio previste dalla direttiva NIS2,¹⁰ mentre la ricerca del Software Engineering Institute sui sistemi OT ad alta criticità, nata per i sistemi di difesa con OT embedded ma di valenza generale, ha contribuito a tradurre i principi in pratica.^{11/12} Sul piano normativo, paralle-

lamente, l'entrata in vigore della direttiva NIS2 e del suo recepimento nazionale ha trasformato l'adozione di adeguate misure di sicurezza per l'OT da una buona pratica ingegneristica a un obbligo giuridico per gli operatori dei settori essenziali, tra cui il settore energetico.^{13/14}

1.5 Obiettivi e struttura del paper

Questi contributi forniscono principi solidi e, in alcuni casi, architetture di riferimento puntuali. Ciò che ancora manca è una metodologia strutturata e ripetibile che colleghi sistematicamente la comprensione dell'ambiente operativo alla selezione e all'allocazione granulare dei controlli Zero Trust, riconoscendo che in un impianto reale tali controlli non possono essere applicati in modo uniforme. La domanda fondamentale non è quale architettura Zero Trust adottare, ma quali capacità Zero Trust sono tecnicamente sostenibili per ciascuna classe di asset e con quale priorità rispetto alla missio-

⁸ K. Stouffer, M. Pease, C. Tang, T. Zimmerman, V. Pillitteri, S. Lightman, A. Hahn, S. Saravia, A. Sherule e M. Thompson, *Guide to Operational Technology (OT) Security*, NIST Special Publication 800-82r3. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2023, doi: 10.6028/NIST.SP.800-82r3.

⁹ Cloud Security Alliance, *Zero Trust Guidance for Critical Infrastructure*. Seattle, WA, USA: CSA Zero Trust Working Group, ott. 2024

¹⁰ Agenzia dell'Unione europea per la cibersicurezza (ENISA), *Technical Implementation Guidance on Cybersecurity Risk Management Measures*, v1.0. Atene, Grecia: ENISA, giugno 2025.

¹¹ C. J. Alberts, T. Morrow, R. Brown e C. M. Wallen, *Tailoring Security and Zero Trust Principles to Weapon System Environments*, Special Report. Pittsburgh, PA, USA: Software Engineering Institute, Carnegie Mellon University, 2025.

¹² R. Brown, "Implementing Zero Trust in Operational Technology: A Practical Case Study," *SEI Insights (blog)*, Software Engineering Institute, Carnegie Mellon University, 16 giugno 2026.

¹³ Parlamento europeo e Consiglio, *Direttiva (UE) 2022/2555 (NIS2), relativa a misure per un livello comune elevato di cibersicurezza nell'Unione*, 14 dicembre 2022. GU UE L 333.

¹⁴ *Decreto Legislativo 4 settembre 2024, n. 138*, recepimento della direttiva (UE) 2022/2555 (NIS2). Gazzetta Ufficiale della Repubblica Italiana, n. 230, 1° ottobre 2024.

ne. Questo lavoro affronta questa lacuna proponendo MATRIX, un framework metodologico per l'adozione selettiva e orientata alla missione dello Zero Trust negli ambienti OT. L'acronimo riassume le sei fasi del processo: "Mission context", "Asset suitability", "Threat surface", "Risk tradeoff", "Implementation" ed "Execution". Il framework si basa su una matrice che associa le capacità Zero Trust alle classi di asset, ponderata in base alla criticità della missione e vincolata dal profilo di idoneità tecnica.

Il testo è organizzato come segue. La Sezione 2 ricostruisce i fondamenti dello zero trust e le specificità degli ambienti OT, proponendo una rassegna critica della letteratura che motiva la necessità

di un framework. La Sezione 3 presenta MATRIX, descrivendone le sei fasi. La Sezione 4 ne illustra l'applicazione a uno scenario di sottostazioni elettriche digitali e ne conduce la validazione su standard, confronto e caso reale. La Sezione 5 ne illustra i pregi, i limiti e la generalizzabilità, la Sezione 6 lo colloca nel quadro normativo europeo e nazionale e ne illustra il contributo alla conformità, mentre la Sezione 7 ne trae le conclusioni e indica gli sviluppi futuri.

PRINCIPIO GUIDA

La domanda non è quale architettura Zero Trust adottare, ma quali capacità sono tecnicamente sostenibili per ciascuna classe di asset, e con quale priorità rispetto alla missione.

02

CAPITOLO 2

Background e lavori correlati

- 2.1 Lo zero trust: dai perimetri alle identità
- 2.2 Anatomia degli ambienti Operational Technology
- 2.3 Perché i controlli EIT non si trasferiscono direttamente?
- 2.4 Lavori correlati



Background e lavori correlati

Fondamenti dello Zero Trust, anatomia degli ambienti OT e limiti del trasferimento diretto dei controlli EIT

2.1 Lo zero trust: dai perimetri alle identità

Lo zero trust non è un prodotto o una tecnologia specifica, ma una strategia di sicurezza basata su un insieme di principi. La NIST SP 800-207 ne enuncia i principi fondamentali:

- tutte le risorse di dati e di calcolo sono trattate come tali, indipendentemente dalla loro posizione;
- ogni comunicazione è protetta, a prescindere dalla rete su cui transita;
- l'accesso alle singole risorse è concesso per sessione, sulla base del principio del privilegio minimo;
- le decisioni di accesso sono determinate da una policy dinamica che considera l'identità del richiedente, lo stato del dispositivo e altri

attributi comportamentali e ambientali;

- l'organizzazione monitora e misura costantemente l'integrità e la postura di sicurezza dei propri asset, applica e rivaluta in modo continuo l'autenticazione e l'autorizzazione e raccoglie quante più informazioni possibili sullo stato corrente, al fine di migliorare nel tempo la propria postura.¹⁵

Sul piano logico, questi principi si traducono in un'architettura in cui il piano di controllo e il piano dei dati sono nettamente separati. Il policy engine, il cuore decisionale del sistema, esegue un algoritmo di fiducia per concedere, negare o revocare l'accesso; il policy administrator instaura o interrompe il canale di comunicazione in base alla decisione presa; il policy enforcement point, collocato lungo il percorso tra il soggetto e la risorsa, applica materialmente l'esito.¹⁶

¹⁵ S. Rose, O. Borchert, S. Mitchell e S. Connelly, *Zero Trust Architecture*, NIST Special Publication 800-207. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2020, doi: 10.6028/NIST.SP.800-207.

¹⁶ S. Rose, O. Borchert, S. Mitchell e S. Connelly, *Zero Trust Architecture*, NIST Special Publication 800-207. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2020, doi: 10.6028/NIST.SP.800-207.

Il passaggio concettuale più rilevante consiste nello spostare il baricentro dei controlli dalla segmentazione basata su parametri di rete quali indirizzi, sottoreti e perimetri, verso l'identità di utenti, dispositivi e servizi, con politiche di autorizzazione costruite attorno ad attributi anziché a topologie.¹⁷ La letteratura ha contribuito a sistematizzare il campo: la rassegna di Syed et al. offre una tassonomia esaustiva delle architetture e delle componenti zero trust,¹⁸ mentre Fernandez e Brazhuk ne propongono un'analisi critica, mettendo in luce le ambiguità definitive e i nodi irrisolti nella traduzione dei principi in pratica.¹⁹ Bertino, da parte sua, invita a una valutazione misurata dei benefici effettivi, ricordando che lo zero trust non è una panacea ma una strategia il cui valore dipende dalla qualità dell'implementazione.²⁰

2.2 Anatomia degli ambienti Operational Technology

Per comprendere perché lo zero trust non può essere trasferito senza adatta-

menti nell'ambito OT, è necessario osservare la struttura tipica di un ambiente OT. Il modello architetturale dominante è il modello Purdue, derivato dalla Purdue Enterprise Reference Architecture, elaborata all'inizio degli anni Novanta da Williams e dal consorzio universitario sul Computer Integrated Manufacturing.²¹ Concepito originariamente per razionalizzare i flussi informativi negli impianti automatizzati, il modello è stato adottato dalla comunità della sicurezza, in quanto la gerarchia funzionale che descrive si presta a delimitare confini difensivi naturali.

La serie di standard ISA/IEC 62443 ha adottato questa stratificazione traducendola nei concetti di zone e conduits: raggruppamenti di sistemi con requisiti di sicurezza omogenei e canali di comunicazione controllati che li collegano e ciascuno associato a un livello di sicurezza target commisurato al rischio.²² La Figura 1 riassume questa organizzazione.

Ai livelli inferiori si trova il processo fisico (Livello 0), con i suoi sensori

¹⁷ S. Rose, O. Borchert, S. Mitchell e S. Connelly, *Zero Trust Architecture*, NIST Special Publication 800-207. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2020, doi: 10.6028/NIST.SP.800-207.

¹⁸ N. F. Syed, S. W. Shah, A. Shaghghi, A. Anwar, Z. Baig e R. Doss, "Zero trust architecture (ZTA): A comprehensive survey," *IEEE Access*, vol. 10, pp. 57143–57179, 2022.

¹⁹ E. B. Fernandez e A. Brazhuk, "A critical analysis of zero trust architecture (ZTA)," *Computer Standards & Interfaces*, vol. 89, art. 103832, 2024.

²⁰ E. Bertino, "Zero trust architecture: Does it help?," *IEEE Security & Privacy*, vol. 19, n. 5, pp. 95–96, 2021.

²¹ T. J. Williams, "The Purdue enterprise reference architecture," *Computers in Industry*, vol. 24, n. 2-3, pp. 141–158, 1994.

²² International Electrotechnical Commission, *IEC 62443: Security for Industrial Automation and Control Systems* (serie). Ginevra, Svizzera: IEC.

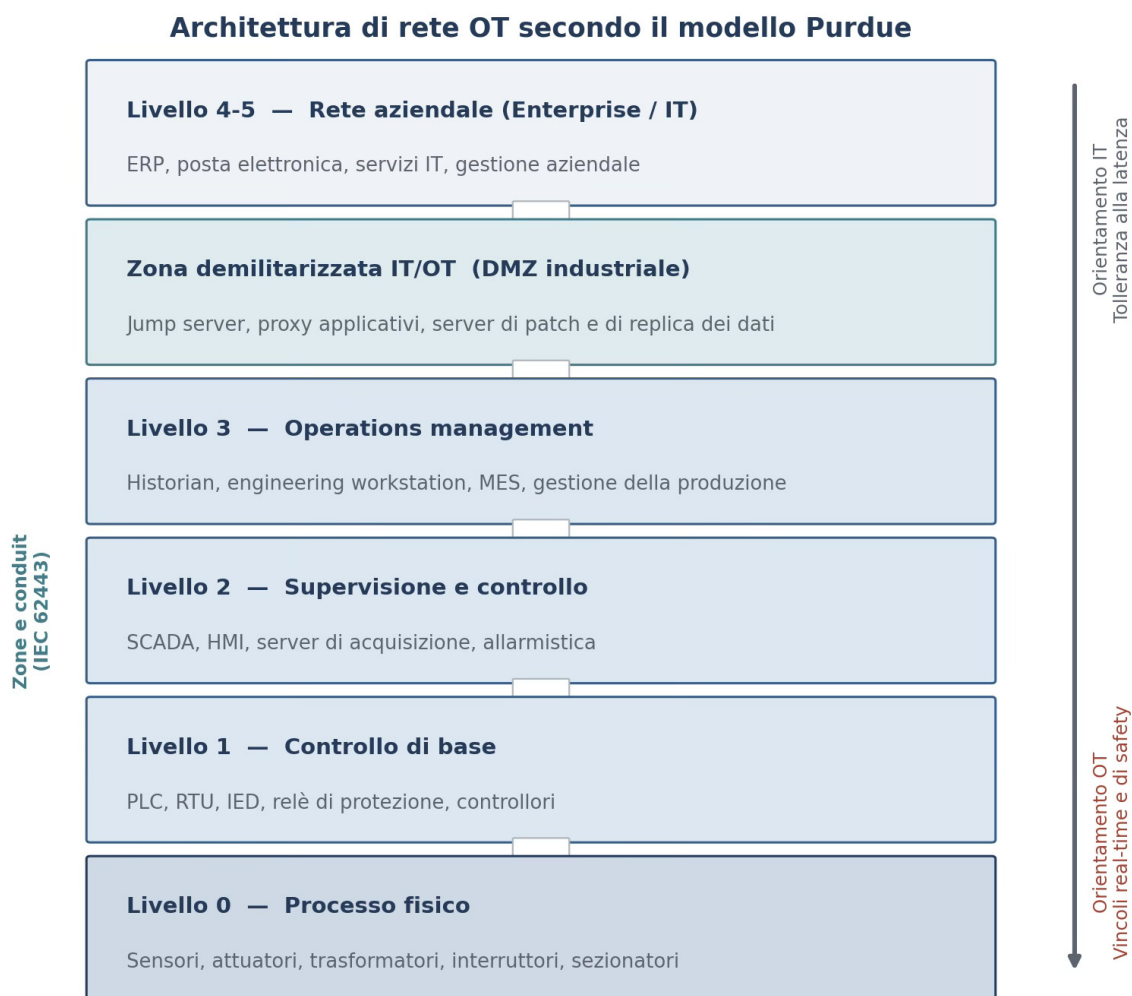


Figura 1. L'architettura di rete OT secondo il modello Purdue prevede i livelli funzionali, la zona demilitarizzata IT/OT e l'intensificarsi dei vincoli di tempo reale verso il processo fisico.

e attuatori, governato dai dispositivi di controllo di base (Livello 1), quali i controllori logici programmabili (PLC), le unità terminali remote (RTU), i dispositivi elettronici intelligenti (IED) e i relè di protezione. Il livello di supervisione (Livello 2) ospita i sistemi SCADA e le interfacce uomo-macchina (HMI), che consentono il monitoraggio e il comando, mentre il livello di operations management (Livello 3) raccoglie gli historian, le workstation per l'ingegneria e i sistemi di gestione

della produzione. Tra il dominio OT e la rete aziendale (livelli 4 e 5) si interpone, nelle architetture mature, una zona demilitarizzata industriale che media ogni scambio. Come evidenziato sul lato destro della figura, una caratteristica fondamentale è che i requisiti di tempo reale e di sicurezza aumentano scendendo verso il processo, mentre l'affinità con le tecnologie IT e, di conseguenza, la possibilità di riutilizzare i relativi controlli di sicurezza, aumenta risalendo verso l'alto.

2.3 Perché i controlli EIT non si trasferiscono direttamente?

Le ragioni dell'incompatibilità sono molteplici e si rafforzano a vicenda. In primo luogo, l'eterogeneità: un impianto OT è costituito da apparecchiature di generazioni e fornitori diversi, spesso governate da protocolli proprietari che non prevedono autenticazione e controlli di integrità. In secondo luogo, la disponibilità continua: molti processi non tollerano interruzioni e le finestre di manutenzione per aggiornamenti o riconfigurazioni sono rare e costose. Infine, la sensibilità alla latenza: l'introduzione di un controllo che aggiunga ritardo alla catena di comando può compromettere la funzione, pertanto ogni meccanismo zero trust deve dimostrare di non interferire con i vincoli temporali del processo.²³ A questi si aggiungono i limiti di calcolo, memoria ed energia dei dispositivi più datati che non dispongono del margine necessario per ospitare agenti software o funzioni crittografiche. Un filone di ricerca del Software Engineering Institute, sviluppato originariamente per i sistemi di difesa con OT embedded ma di valenza generale, ha condensato questi fattori in un insieme di attributi utili a valutare l'idoneità di un sistema ad accogliere le capacità zero trust: la configurabilità

dinamica, la flessibilità di progettazione o retrofit, i vincoli di dimensione, peso e potenza (size, weight and power, SWaP), la tolleranza alla latenza e il grado di centralità IT rispetto a OT.²⁴ Riprenderemo questi attributi nella sezione successiva come base per la fase di profilazione.

2.4 Lavori correlati

Sul fronte normativo e istituzionale, oltre alle già citate NIST SP 800-207 e 800-82r3, meritano attenzione alcuni documenti per il loro approccio metodologico. La guida della Cloud Security Alliance per le infrastrutture critiche suddivide l'adozione dello zero trust in cinque fasi: - definire la superficie da proteggere in termini di dati, applicazioni, asset e servizi; - mappare i flussi delle transazioni; - costruire l'architettura zero trust; - formulare le relative politiche; - monitorare e mantenere la rete.²⁵

A livello europeo, l'ENISA (Agenzia dell'Unione europea per la cybersicurezza) ha pubblicato una guida tecnica che traduce le misure di gestione del rischio della NIS2 in indicazioni operative, esempi di documentazione e mappature verso standard internazionali quali ISO/IEC 27001, il NIST Cybersecurity Framework e la serie IEC 62443, offrendo un riferimento direttamente utiliz-

²³ K. Stouffer, M. Pease, C. Tang, T. Zimmerman, V. Pillitteri, S. Lightman, A. Hahn, S. Saravia, A. Sherule e M. Thompson, *Guide to Operational Technology (OT) Security*, NIST Special Publication 800-82r3. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2023, doi: 10.6028/NIST.SP.800-82r3.

²⁴ C. J. Alberts, T. Morrow, R. Brown e C. M. Wallen, *Tailoring Security and Zero Trust Principles to Weapon System Environments*, Special Report. Pittsburgh, PA, USA: Software Engineering Institute, Carnegie Mellon University, 2025.

²⁵ Cloud Security Alliance, *Zero Trust Guidance for Critical Infrastructure*. Seattle, WA, USA: CSA Zero Trust Working Group, ott. 2024.

zabile dalle organizzazioni dell'Unione.²⁶ La ricerca accademica ha affrontato il problema da angolazioni complementari. Feng e Hu propongono un'architettura zero trust per i sistemi cyber-fisici industriali, mostrando come i principi possano essere riformulati tenendo conto dell'accoppiamento tra computazione e processo fisico.²⁷ Zanasi, Russo e Colajanni hanno elaborato un'architettura zero trust flessibile per le infrastrutture industriali basate su Industrial IoT, con l'obiettivo esplicito di adattare l'applicazione delle regole alla diversità dei dispositivi.²⁸ Federici, Martintoni e Senni si concentrano in particolare sull'accesso remoto alle infrastrutture IIoT, proponendo un'architettura a due livelli di controllo conforme al modello zero trust.²⁹ Per quanto riguarda la transizione, Phiayura e Teerakanok delineano un framework di migrazione verso lo zero trust, sebbene orientato principalmente ai contesti IT.³⁰

Da questa analisi emerge un quadro coerente, ma incompleto. Le linee guida istituzionali forniscono processi di alto livello validi, ma volutamente generici, mentre i contributi accademici offrono architetture e meccanismi puntuali, spesso validati su scenari circoscritti o su sistemi relativamente moderni. Resta scoperto lo spazio intermedio: una metodologia che, a partire da una comprensione mission-centrica dell'ambiente, conduca in modo tracciabile alla selezione dei controlli effettivamente sostenibili per ogni classe di asset, integri esplicitamente l'analisi dei compromessi tra sicurezza e continuità operativa e gestisca il rischio residuo dei componenti non adeguabili. È questo lo spazio che MATRIX intende occupare, non in alternativa, ma in complemento agli schemi esistenti, dei quali assume e perfeziona i passaggi.

VINCOLI OT

Latenza stringente, disponibilità continua, eterogeneità dei protocolli, margini di calcolo e memoria ridotti (SWaP) e requisiti di safety restringono lo spazio dei controlli applicabili.

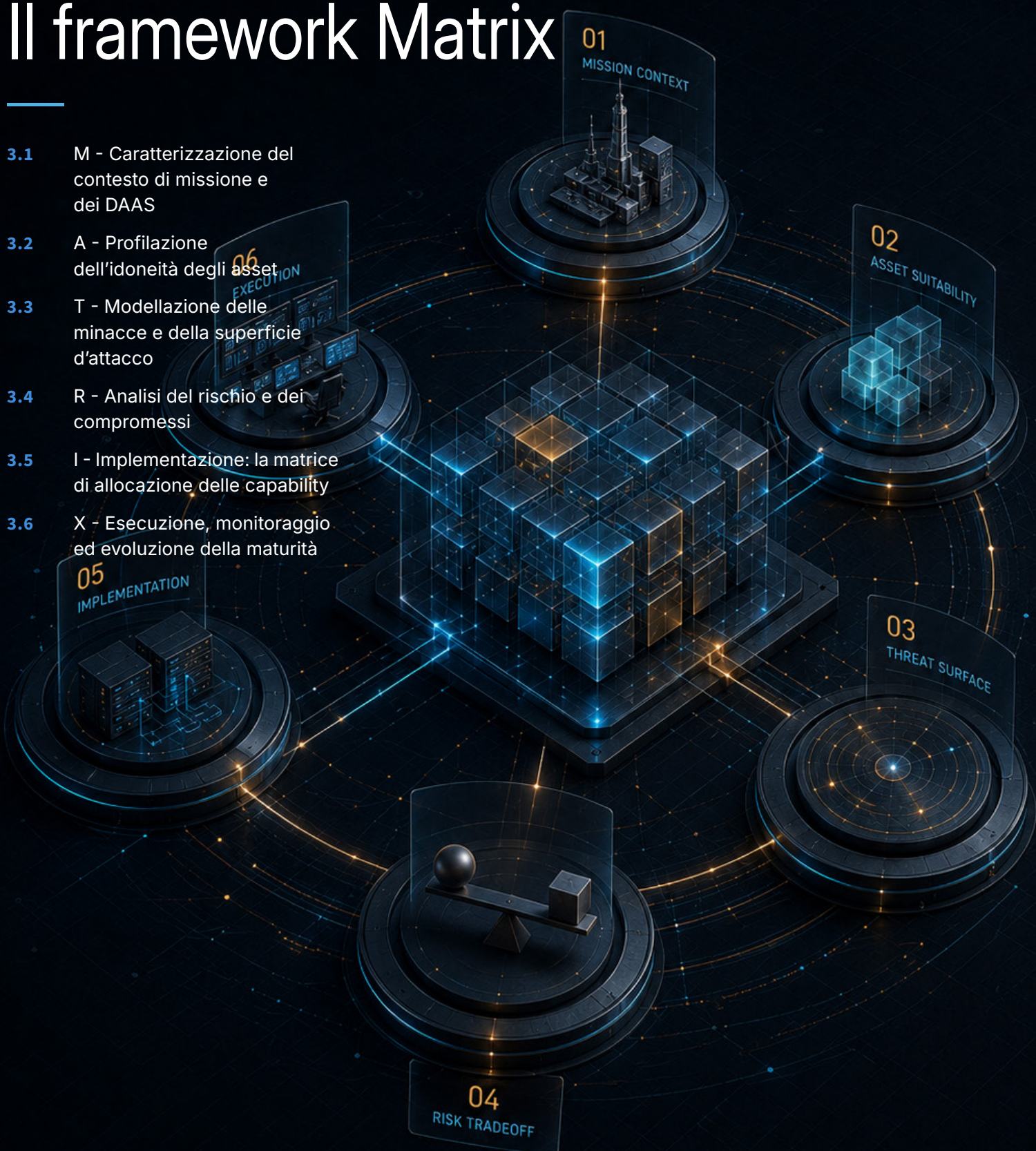
- ²⁶ Agenzia dell'Unione europea per la cibersicurezza (ENISA), *Technical Implementation Guidance on Cybersecurity Risk Management Measures*, v1.0. Atene, Grecia: ENISA, giugno 2025.
- ²⁷ X. Feng e S. Hu, "Cyber-physical zero trust architecture for industrial cyber-physical systems," *IEEE Transactions on Industrial Cyber-Physical Systems*, vol. 1, pp. 394–405, 2023.
- ²⁸ C. Zanasi, S. Russo e M. Colajanni, "Flexible zero trust architecture for the cybersecurity of industrial IoT infrastructures," *Ad Hoc Networks*, vol. 156, art. 103414, 2024, doi: 10.1016/j.adhoc.2024.103414.
- ²⁹ F. Federici, D. Martintoni e V. Senni, "A zero-trust architecture for remote access in industrial IoT infrastructures," *Electronics*, vol. 12, n. 3, art. 566, 2023, doi: 10.3390/electronics12030566.
- ³⁰ P. Phiayura e S. Teerakanok, "A comprehensive framework for migrating to zero trust architecture," *IEEE Access*, vol. 11, pp. 19487–19511, 2023.

03

CAPITOLO 3

Il framework Matrix

- 3.1 M - Caratterizzazione del contesto di missione e dei DAAS
- 3.2 A - Profilazione dell'idoneità degli asset
- 3.3 T - Modellazione delle minacce e della superficie d'attacco
- 3.4 R - Analisi del rischio e dei compromessi
- 3.5 I - Implementazione: la matrice di allocazione delle capability
- 3.6 X - Esecuzione, monitoraggio ed evoluzione della maturità



Il framework MATRIX

Le sei fasi che legano la comprensione della missione alla selezione dei controlli tecnicamente sostenibili

MATRIX si basa su tre principi guida:

1. L'orientamento alla missione: la sicurezza non è un fine in sé, ma uno strumento al servi-

zio della capacità del sistema di svolgere la propria funzione in modo sicuro e affidabile. Ne consegue che le misure di protezione devono essere ca-

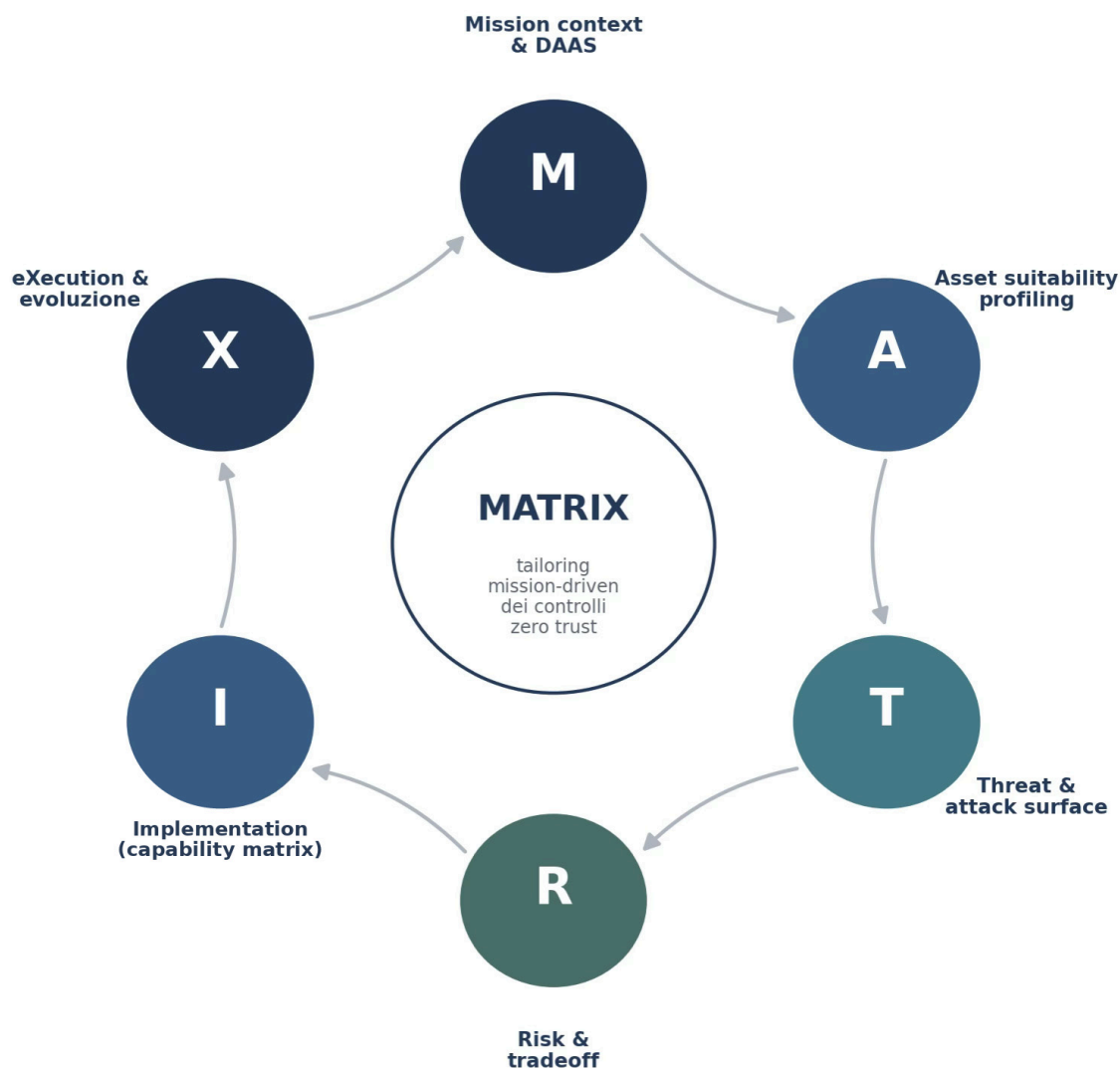


Figura 2. Le sei fasi del framework MATRIX, organizzate come ciclo iterativo attorno alla matrice di allocazione delle capability.

librate sul valore che ciascun asset riveste per la missione;

2. L'applicabilità differenziata: in un ambiente eterogeneo, non esiste una configurazione zero trust valida per l'intero impianto e i singoli componenti del modello devono essere scomposti e allocati dove è tecnicamente possibile;
3. La natura iterativa è legata al ciclo di vita: l'adozione dello Zero Trust non è un progetto a termine, ma un processo continuo che deve essere rivalutato in base all'evoluzione delle tecnologie, delle minacce e delle risorse disponibili.

La Figura 2 rappresenta le sei fasi del framework come un ciclo che alimenta e aggiorna l'artefatto centrale: la matrice di allocazione delle capacità.

3.1 M - Caratterizzazione del contesto di missione e dei DAAS

La prima fase stabilisce il perché del sistema prima ancora del come proteggerlo. Si tratta di ricostruire la missione attraverso i mission thread, ossia le sequenze di attività e processi che descrivono come il sistema consegue i propri obiettivi, e di individuare gli scenari e le modalità operative in cui esso funziona. In un sistema di distribuzione elettrica, ad esempio, la missione consiste nel trasformare, regolare e distribuire energia tra le fonti di ge-

nerazione e gli utilizzatori finali in modo sicuro e continuo; gli scenari rilevanti comprendono la regolazione della tensione, la gestione della distribuzione del carico e la protezione contro i guasti. All'interno di questi thread si identificano i DAAS - dati, applicazioni, asset e servizi - che ne costituiscono gli abilitatori. Questa caratterizzazione non ha valore puramente descrittivo: definisce le conseguenze potenziali di un attacco, fornendo il metro con cui, nelle fasi successive, si peseranno le minacce e si priorizzeranno i controlli. Senza questo radicamento, la selezione delle capability rischierebbe di ottimizzare la sicurezza di asset marginali trascurando quelli da cui dipende la continuità del servizio.

OUTPUT DELLA FASE

Mappa dei DAAS e delle conseguenze potenziali di un attacco.

3.2 A - Profilazione dell'idoneità degli asset

La seconda fase risponde a una domanda spesso elusa: quanto un determinato asset è in grado di accogliere capability zero trust? La profilazione valuta ciascuna classe di asset rispetto ai cinque attributi richiamati nella Sezione 2.3. La configurabilità dinamica misura la possibilità di modificare in tempi prossimi al reale relazioni di fiducia, flussi e politiche di accesso. La flessibilità di retrofit esprime

la capacità del sistema di accogliere modifiche progettuali o adeguamenti senza stravolgimenti architetturali. Il margine SWaP indica la disponibilità di risorse di calcolo, memoria ed energia eccedenti rispetto alla funzione primaria. La tolleranza alla latenza quantifica quanto ritardo il sistema possa assorbire senza violare i propri requisiti prestazionali. La centratura IT, infine, segnala quanto un componente OT sia IT-like e dunque permeabile al riuso dei controlli di sicurezza informatica tradizionali.

Attribuendo a ciascun attributo un punteggio su scala ordinale si ottiene un profilo di idoneità per classe di asset, rappresentabile come in Figura 3. Il confronto è illuminante: una HMI costruita su piattaforma Windows e un server SCADA presentano profili ampi, compatibili con l'installazione di agenti, l'autenticazione a più fattori e una gestione granulare degli accessi; un IED legacy, governato da protocolli proprietari e privo di gestione dell'identità, mostra un profilo compreso su ogni asse e non può ospitare controlli on-device. Il profilo non è un giudi-

Profilo di idoneità per classe di asset

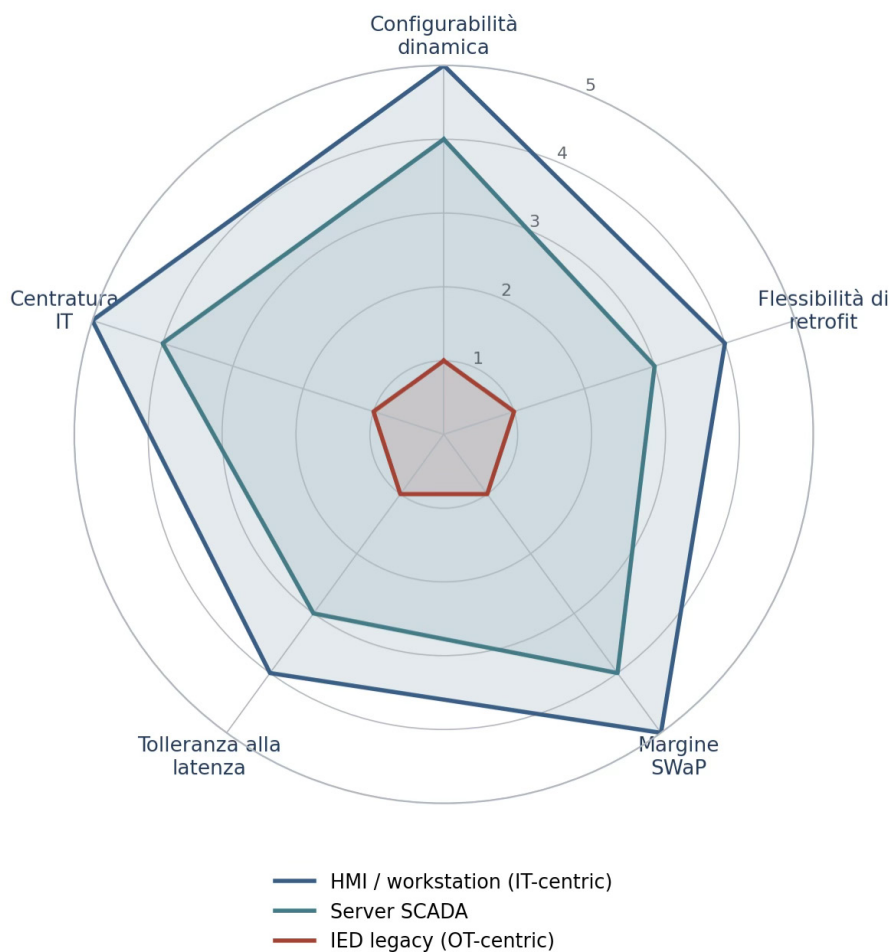


Figura 3. Profilo di idoneità di tre classi di asset rispetto ai cinque attributi che ne determinano la capacità di accogliere controlli zero trust.

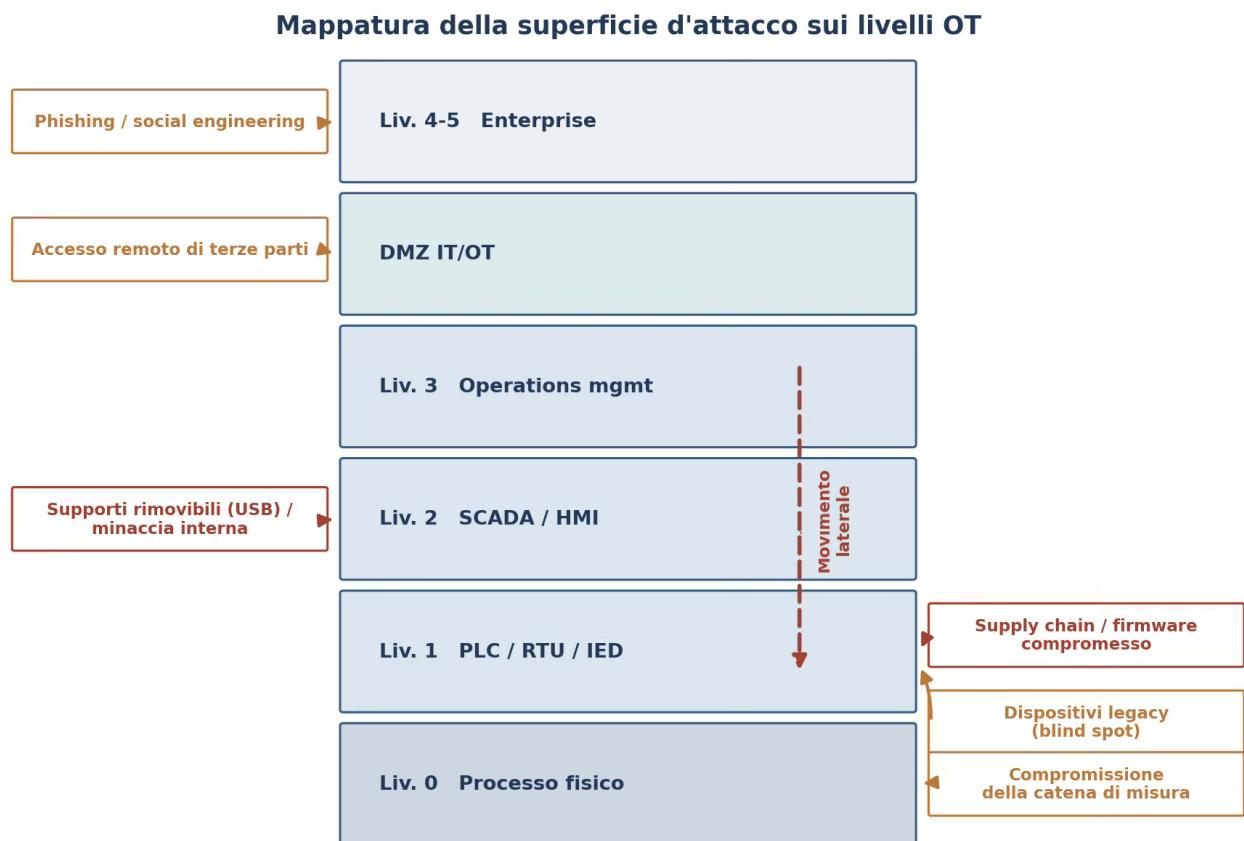


Figura 4. Mappatura della superficie d'attacco di un ambiente OT sui livelli del modello Purdue e principali vettori di compromissione.

zio definitivo sull'asset, bensì una mappa dei vincoli che orienterà l'allocazione: dove l'idoneità è alta, il controllo potrà risiedere sul dispositivo; dove è bassa, occorrerà ricorrere a meccanismi esterni o compensativi.

OUTPUT DELLA FASE

Profilo di idoneità per ciascuna classe di asset.

3.3 T - Modellazione delle minacce e della superficie d'attacco

La terza fase costruisce il quadro avversariale specifico del sistema. Muovendo dai cataloghi di minaccia consolidati - che per le infrastrutture critiche comprendono advanced persistent threat, ransomware, minaccia interna, vulnerabilità della supply chain e fragilità dei sistemi legacy^{31/32} - si conduce una mappatura puntuale dei punti di

³¹ Cloud Security Alliance, *Zero Trust Guidance for Critical Infrastructure*. Seattle, WA, USA: CSA Zero Trust Working Group, ott. 2024.

³² K. Stouffer, M. Pease, C. Tang, T. Zimmerman, V. Pillitteri, S. Lightman, A. Hahn, S. Saravia, A. Sherule e M. Thompson, *Guide to Operational Technology (OT) Security*, NIST Special Publication 800-82r3. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2023, doi: 10.6028/NIST.SP.800-82r3.

ingresso lungo i livelli dell'architettura. Le rilevazioni periodiche dell'ENISA confermano, per le infrastrutture critiche europee, la centralità delle minacce alla disponibilità, del ransomware e degli attacchi alla catena di fornitura, spesso favoriti da reti scarsamente segmentate e da infrastrutture obsolete.³³ L'esercizio, sintetizzato in Figura 4, smentisce l'illusione dell'isolamento: anche un impianto considerato segregato è raggiungibile attraverso l'accesso remoto dei fornitori, gli aggiornamenti firmware, i supporti rimovibili collegati alle workstation, i dispositivi già presenti all'interno del perimetro e le compromissioni introdotte lungo la catena di fornitura. Il movimento laterale, in particolare, mostra come un singolo punto di compromissione possa propagarsi tra apparati e attraverso i livelli se la difesa si affida unicamente alla segmentazione e ai controlli di confine.

La modellazione delle minacce va condotta in dialogo con la caratterizzazione di missione: non tutte le minacce hanno lo stesso peso, e la loro rilevanza si misura sulle conseguenze che produrrebbero sui mission thread identificati nella prima fase. Un attacco capace di alterare i segnali inviati ai dispositivi di protezione, ad esempio, è più grave di un'esfiltrazione di dati storici, perché incide direttamente sulla funzione fisica del sistema.

OUTPUT DELLA FASE

Mappa della superficie di attacco e dei vettori di compromissione.

3.4 R - Analisi del rischio e dei compromessi

La quarta fase affronta il nodo che più nettamente distingue l'OT dall'EIT: il compromesso tra sicurezza e continuità operativa. Lo spazio dei compromessi (tradeoff space) è l'insieme delle soluzioni ammissibili che bilanciano requisiti in tensione tra loro - la protezione da un lato, la disponibilità, la safety, le prestazioni e i costi dall'altro. Un controllo che riduca il rischio informatico ma introduca latenza inaccettabile, o che richieda finestre di fermo impianto incompatibili con il servizio, non è una soluzione ma un nuovo problema. L'analisi consiste perciò nel valutare, per ogni controllo candidato, non solo la riduzione di rischio che apporta ma anche gli effetti collaterali che genera sulle altre dimensioni del sistema.

Il risultato è una prioritizzazione: combinando la criticità di missione di ciascun asset (dalla fase M), il suo profilo di idoneità (dalla fase A) e la sua esposizione alle minacce (dalla fase T), si ottiene una graduatoria che indica dove l'inve-

³³ Agenzia dell'Unione europea per la cibersicurezza (ENISA), *ENISA Threat Landscape 2024*. Atene, Grecia: ENISA, settembre 2024, doi: 10.2824/0710888.

stimento in controlli zero trust produce il massimo beneficio a parità di impatto operativo. Questa graduatoria non è statica: lo spazio dei compromessi muta nel tempo al variare delle tecnologie disponibili, dei vincoli di budget e del panorama delle minacce, e va perciò riesaminato periodicamente. La quarta fase, in sostanza, trasforma la conoscenza accumulata nelle tre precedenti in criteri di decisione espliciti e difendibili.

OUTPUT DELLA FASE

Prioritizzazione dei controlli nello spazio dei compromessi.

3.5 I - Implementazione: la matrice di allocazione delle capability

La quinta fase produce l'artefatto che dà nome al framework. La matrice di allocazione incrocia, sulle righe, le classi di asset individuate e profilate e, sulle colonne, le capability zero trust che si intende dispiegare - tra cui la gestione dell'identità e l'autenticazione a più fattori, la microsegmentation, l'autorizzazione continua basata su policy, la protezione crittografica e i controlli di integrità, la verifica della postura dei dispositivi e il monitoraggio con registrazione centralizzata. Ogni cella esprime non un semplice sì/no, ma la modalità con cui la capability

Tabella 1. Esempio illustrativo di matrice di allocazione delle capability zero trust per classe di asset.

Classe di asset	Identità & MFA	Microsegmentation	Autorizz. continua	Crittografia & integrità	Postura dispositivo	Monitoraggio & logging
HMI/workstation (IT-centric)	Nativo	Nativo	Nativo	Nativo	Nativo	Nativo
Server SCADA	Nativo	Nativo	Nativo	Nativo	Nativo	Nativo
IED moderno (Liv. 1)	Intermed.	Nativo	Intermed.	Nativo	Intermed.	Nativo
IED/RTU legacy	Intermed.	Intermed.	Intermed.	Intermed.	-	Intermed.
Dispositivi di campo (Liv. 0)	-	Compens.	-	-	-	Compens.

Legenda: Nativo = applicazione del controllo sul dispositivo; Intermed. = enforcement mediato da un layer intermedio; Compens. = controllo compensativo esterno; - = non praticabile. I valori hanno carattere esemplificativo e vanno determinati caso per caso mediante le fasi A e R del framework.

può essere realizzata su quella classe di asset, secondo quattro esiti possibili: applicazione nativa sul dispositivo, applicazione mediata da un layer intermediario, controllo compensativo esterno, oppure non praticabilità. La Tabella 1 ne offre un esempio illustrativo.

La logica sottostante deriva direttamente dal profilo di idoneità. Per gli asset a centratura IT e ampio margine - HMI e server - la maggior parte delle capability è applicabile nativamente. Per i dispositivi a bassa idoneità - gli IED legacy - l'enforcement non può risiedere sul dispositivo e deve essere delegato: un layer intermediario può offrire un'interfaccia standardizzata verso protocolli e apparati eterogenei, fungendo da punto di applicazione

delle politiche e garantendo l'interoperabilità fino a quando la segnalazione digitale moderna non sarà dispiegata. Là dove nemmeno questa mediazione è possibile, si ricorre a controlli compensativi - segmentazione rigorosa, monitoraggio passivo del traffico, restrizione fisica degli accessi - e si registra esplicitamente il rischio residuo. La matrice rende così trasparente, asset per asset e capability per capability, ciò che è stato protetto, come, e ciò che resta scoperto.

OUTPUT DELLA FASE

Matrice di allocazione delle capability.

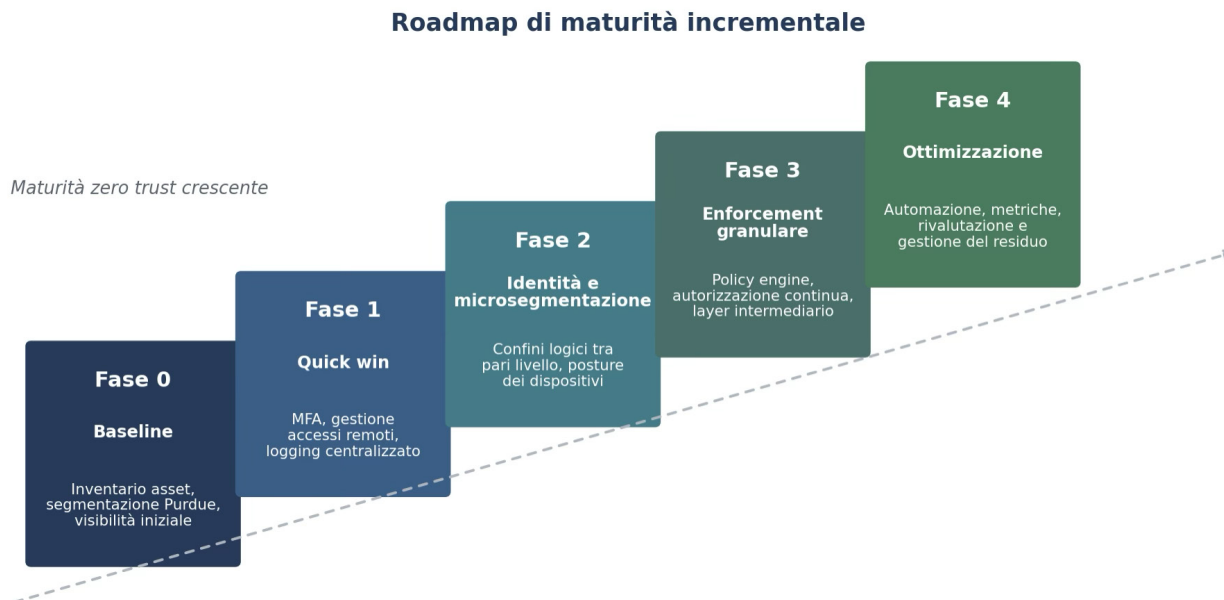


Figura 5. Roadmap di maturità incrementale per l'adozione progressiva delle capability zero trust.

3.6 X - Esecuzione, monitoraggio ed evoluzione della maturità

L'ultima fase trasforma la matrice in un programma di attuazione. Coerentemente con il principio della natura iterativa, MATRIX non prevede un dispiegamento simultaneo di tutti i controlli, ma una progressione per stadi di maturità, più sostenibile sul piano organizzativo e tecnico. Una roadmap tipica, illustrata in Figura 5, muove da una fase di baseline - inventario degli asset, segmentazione secondo il modello Purdue, acquisizione di visibilità - verso interventi a basso impatto e alto ritorno quali l'autenticazione a più fattori e la gestione centralizzata degli accessi remoti; prosegue con l'introduzione di confini logici tra apparati di pari livello e della verifica della postura dei dispositivi; approda all'enforcement granulare mediante policy engine e autorizzazione continua e, infine, alla fase di ottimizzazione, automazione e misurazione.

Il monitoraggio continuo non è un'appendice ma la condizione che rende lo zero trust uno stato dinamico anziché una configurazione congelata: l'ispezione e la registrazione di tutto il traffico alimentano la rivalutazione periodica delle decisioni prese nelle fasi precedenti, riattivando il ciclo. In questo quadro va gestito, con onestà metodologica, il rischio residuo. Alcuni impianti e dispositivi legacy potrebbero non essere ragionevolmente

adeguabili allo zero trust; le organizzazioni che li mantengono in servizio devono contabilizzare il rischio che ne deriva e decidere, su base informata, se e quando sostituirli. Riconoscere questo limite non è una debolezza del framework, ma una sua componente: MATRIX non promette una protezione totale, bensì una protezione consapevole, tracciabile e proporzionata.

PRINCIPIO GUIDA

MATRIX non promette una protezione totale, bensì una protezione consapevole, tracciabile e proporzionata.

RISCHIO RESIDUO

Alcuni dispositivi legacy non sono ragionevolmente adeguabili: il rischio che ne deriva va contabilizzato in modo esplicito, non rimosso.

04

CAPITOLO 4

Validazione

- 4.1 Validazione illustrativa: le sottostazioni elettriche digitali
- 4.2 Validazione di copertura rispetto agli standard
- 4.3 Validazione comparativa
- 4.4 Validazione retrospettiva: l'attacco alla rete di distribuzione ucraina del 2015
- 4.5 Sintesi della validazione



Validazione

Lo scenario NovaGrid è una validazione articolata su standard, confronto e incidente reale documentato

La validazione del framework adotta un approccio multimetodo articolato su tre componenti complementari: una validazione di copertura rispetto agli standard di riferimento, una validazione comparativa rispetto agli schemi esistenti e una validazione retrospettiva condotta su un incidente reale e documentato. Lo scenario illustrativo delle sottostazioni digitali, descritto nel seguito, fornisce il sostrato a cui le tre componenti fanno riferimento.

4.1 Validazione illustrativa: le sottostazioni elettriche digitali

Per mostrare il framework all'opera consideriamo uno scenario applicativo relativo a un ipotetico operatore di distribuzione, qui denominato NovaGrid, che gestisce un parco di sottostazioni elettriche digitali. Una sottostazione svolge la funzione di abbassare i livelli di alta tensione provenienti dalla rete di trasmissione per alimentare i circuiti di distribuzione locale, regolando la fornitura in risposta alla domanda di abitazioni e piccole utenze. I sistemi di automazione di NovaGrid comunicano con

IED, relè e altri apparati; un'interfaccia uomo-macchina di tipo web supporta gli operatori nel monitoraggio e nel comando locale e remoto, mentre un sistema SCADA fornisce la vista d'insieme sulla stabilità della rete e sulle manovre.

L'infrastruttura è il risultato di una stratificazione storica: accanto a un sistema SCADA moderno convivono apparati legacy che governano un centinaio di sottostazioni secondarie tramite protocolli proprietari non integrabili con il sistema di monitoraggio centrale, e la cui sostituzione integrale non è, allo stato, una priorità sostenibile per ragioni di costo e di affidabilità. Lo scenario è volutamente analogo, nelle sue caratteristiche tecniche, ai casi discussi nella letteratura recente sul tema,³⁴ ma i dettagli e le scelte qui presentati sono originali e funzionali alla sola illustrazione del metodo.

Applicando la fase M, NovaGrid ricostruisce i propri mission thread attorno alla trasformazione, regolazione e distribuzione dell'energia, identificando come DAAS critici i segnali di comando

³⁴ R. Brown, "Implementing Zero Trust in Operational Technology: A Practical Case Study," *SEI Insights* (blog), Software Engineering Institute, Carnegie Mellon University, 16 giugno 2026.

verso i dispositivi di protezione, i dati di telemetria del sistema SCADA e i servizi di automazione delle manovre. La caratterizzazione evidenzia che la conseguenza più grave non è la perdita di riservatezza dei dati, ma la perdita di integrità o disponibilità del comando: un'alterazione dei segnali inviati ai relè potrebbe compromettere la protezione del sistema e la continuità della fornitura.

Nella fase A, NovaGrid profila le proprie classi di asset. Le HMI su piattaforma Windows e i server SCADA mostrano un'idoneità elevata e uniforme, compatibile con controlli on-device. Gli IED moderni nelle sottostazioni primarie presentano un'idoneità intermedia. Gli apparati legacy delle sottostazioni secondarie, privi di gestione dell'identità e di controlli di accesso granulari, esibiscono un'idoneità minima e dovranno affidarsi a meccanismi esterni di enforcement.

La fase T conduce alla mappatura della superficie d'attacco. NovaGrid riconosce di essere esposta soprattutto a tre delle categorie di minaccia canoniche: la minaccia interna, le vulnerabilità della supply chain e gli attori di tipo nation-state, con il ransomware come minaccia trasversale ad alto impatto, aggravata dalle fragilità dell'infrastruttura legacy. La mappatura individua punti di ingresso che vanno dall'accesso remoto dei fornitori agli aggiornamenti firmware, dai supporti rimovibili collegati alle workstation ai

dispositivi legacy che costituiscono altrettanti blind spot. Particolare attenzione è riservata al rischio di manomissione in transito degli apparati - relè e controllori - durante la consegna dai fornitori, dove la discontinuità di visibilità nella logistica dell'ultimo miglio apre un varco di fiducia sfruttabile.

Nella fase R, NovaGrid pondera i controlli candidati rispetto ai vincoli operativi. La verifica riguarda, ad esempio, se l'introduzione di software antimalware o di scansioni in tempo reale interferisca con i processi critici dell'automazione, e se i controlli granulari desiderati - tali da impedire che un dispositivo compromesso di Livello 2 possa interagire con un controllore di Livello 1 senza superare verifiche di identità e autorizzazione in tempo reale - siano sostenibili sui diversi apparati. L'analisi conferma che ciò che è praticabile sulle sottostazioni primarie non lo è sulle secondarie, dove i protocolli legacy non supportano controlli di accesso granulari né gestione dell'identità.

La fase I consolida queste valutazioni nella matrice di allocazione (cfr. Tabella 1). Per HMI e server SCADA, NovaGrid prevede l'applicazione nativa dell'autenticazione a più fattori, della verifica della postura e del monitoraggio; tra apparati di pari livello impone confini logici e controlli di accesso stringenti per ostacolare il movimento laterale; per le connessioni remo-

te di terze parti adotta una gestione centralizzata e sicura, valutando ogni tentativo di autenticazione al SCADA rispetto al policy engine. Per gli IED legacy, l'enforcement è delegato a un layer intermediario che offre un'interfaccia standardizzata verso i diversi protocolli e dispositivi, assicurando l'interoperabilità in attesa del dispiegamento della segnalazione digitale moderna nelle sottostazioni secondarie e della loro integrazione nell'architettura zero trust.

Infine, nella fase X, NovaGrid colloca questi interventi lungo una roadmap di maturità (cfr. Figura 5), partendo dalla messa in sicurezza degli asset a più alto rischio - engineering workstation, workstation operatore, historian - con controlli on-device, e procedendo per stadi successivi. L'organizzazione valuta che l'onere amministrativo e la complessità tecnica introdotti rientrino in soglie di rischio operativo accettabili, e riconosce esplicitamente che alcune sottostazioni secondarie potrebbero non essere adeguabili nel breve periodo, contabilizzandone il rischio residuo. Il risultato non è un impianto a prova di attacco, ma un sistema in cui la superficie d'attacco è ridotta, il movimento laterale è osta-

colato, gli accessi critici sono verificati con continuità e ciò che resta scoperto è noto e monitorato.

4.2 Validazione di copertura rispetto agli standard

Il primo criterio di adeguatezza di un framework di selezione dei controlli è la sua completezza: le sei fasi devono generare, nel loro insieme, gli artefatti e le attività che gli standard di settore prescrivono, senza lasciare scoperti requisiti essenziali.

La Tabella 2 mappa ciascuna fase di MATRIX sui corrispondenti requisiti della NIST SP 800-82r3,³⁵ della serie ISA/IEC 62443³⁶ e dell'articolo 24 del decreto di recepimento della NIS2.³⁷ La mappatura mostra che le fasi del framework coprono l'intero ciclo prescritto dalle tre fonti, dalla identificazione del contesto e degli asset fino al monitoraggio continuo e alla gestione del rischio residuo.

L'esercizio non rivela lacune di copertura. La specificità di MATRIX rispetto alle tre fonti non risiede dunque nell'aggiunta di requisiti nuovi, ma nel meccanismo, assente negli standard, che vincola la selezione di ciascun controllo all'ido-

³⁵ K. Stouffer, M. Pease, C. Tang, T. Zimmerman, V. Pillitteri, S. Lightman, A. Hahn, S. Saravia, A. Sherule e M. Thompson, *Guide to Operational Technology (OT) Security*, NIST Special Publication 800-82r3. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2023, doi: 10.6028/NIST.SP.800-82r3.

³⁶ International Electrotechnical Commission, IEC 62443: *Security for Industrial Automation and Control Systems* (serie). Ginevra, Svizzera: IEC.

³⁷ *Decreto Legislativo 4 settembre 2024, n. 138*, recepimento della direttiva (UE) 2022/2555 (NIS2). Gazzetta Ufficiale della Repubblica Italiana, n. 230, 1° ottobre 2024.

Tabella 2. Mappatura di copertura delle fasi di MATRIX sui requisiti degli standard di riferimento.

Fase MATRIX	NIST SP 800-82r3	ISA/IEC 62443	Art. 24 D.Lgs. 138/2024
M, contesto di missione e DAAS	Identificazione di sistema e impatto; categorizzazione	Definizione del system under consideration e delle zone	Analisi del rischio orientata all'impatto
A, idoneità degli asset	Inventario e caratterizzazione degli asset OT	Assegnazione dei security level target per zona	Gestione e proporzionalità delle misure
T, superficie d'attacco	Analisi di minacce e vulnerabilità	Identificazione di threat e conduit esposti	Gestione delle vulnerabilità e della supply chain
R, rischio e compromessi	Valutazione e trattamento del rischio	Riconciliazione tra security level target e raggiunto	Selezione di misure adeguate e proporzionate
I, matrice di allocazione	Selezione e implementazione delle contromisure	Realizzazione dei requisiti di sicurezza per zona	Controllo accessi, MFA, crittografia, segmentazione
X, esecuzione ed evoluzione	Monitoraggio, manutenzione e miglioramento continuo	Gestione del ciclo di vita della sicurezza	Continuità operativa, gestione e notifica incidenti

neità tecnica dell'asset e alla criticità di missione, rendendo esplicita la logica di allocazione differenziata.

4.3 Validazione comparativa

La seconda componente confronta MATRIX con i due schemi metodologici a esso più prossimi: il processo in cinque fasi della Cloud Security Alliance per le infrastrutture

critiche³⁸ e l'approccio del Software Engineering Institute alla mappatura dei principi zero trust su ambienti a vincoli stringenti.³⁹

Il confronto è condotto rispetto a cinque criteri rilevanti per l'adozione in ambito OT, sintetizzati nella Tabella 3.

Il confronto evidenzia che MATRIX eredita dal SEI la centralità dei compromessi e l'idea di profilazione dell'idoneità, ma le

³⁸ Cloud Security Alliance, *Zero Trust Guidance for Critical Infrastructure*. Seattle, WA, USA: CSA Zero Trust Working Group, ott. 2024.

³⁹ C. J. Alberts, T. Morrow, R. Brown e C. M. Wallen, *Tailoring Security and Zero Trust Principles to Weapon System Environments*, Special Report. Pittsburgh, PA, USA: Software Engineering Institute, Carnegie Mellon University, 2025.

Tabella 3. Confronto strutturato tra MATRIX e gli schemi metodologici esistenti.

Criterio	CSA cinque fasi	SEI principi e tradeoff	MATRIX
Orientamento alla missione	Implicito	Parziale	Esplicito, fase M
Profilazione dell'idoneità degli asset	Assente	Presente, set di attributi	Presente e integrata nella selezione
Analisi esplicita dei compromessi	Limitata	Centrale	Centrale, fase R
Allocazione differenziata dei controlli	Assente	Concettuale	Operativa, matrice di allocazione
Tracciabilità documentale per la conformità	Bassa	Media	Alta, artefatto matriciale

traduce in un artefatto operativo, la matrice di allocazione, che né il processo CSA né il lavoro SEI rendono esplicito. Il valore distintivo si concentra quindi nella capacità di produrre, asset per asset e capability per capability, una traccia decisionale comunicabile e verificabile.

4.4 Validazione retrospettiva: l'attacco alla rete di distribuzione ucraina del 2015

La componente più stringente applica il framework, a posteriori, a un inci-

dente reale e ampiamente documentato, così da verificare se le sue fasi avrebbero condotto alla selezione di controlli pertinenti rispetto ai vettori effettivamente sfruttati. Il caso scelto è l'attacco del 23 dicembre 2015 alle società di distribuzione elettrica ucraine, che provocò un'interruzione di alimentazione per circa 225.000 utenze e la cui ricostruzione forense è disponibile nella relazione E-ISAC e SANS.⁴⁰ La scelta è motivata da due ragioni: l'incidente colpì un ambiente di sottostazioni di distribuzione, omologo allo

⁴⁰ R. M. Lee, M. J. Assante e T. Conway, *Analysis of the Cyber Attack on the Ukrainian Power Grid*. Washington, DC, USA: E-ISAC e SANS Industrial Control Systems, 2016.

Tabella 4. Applicazione retrospettiva di MATRIX alla catena di attacco del 2015.

Passo dell'attacco	Fase MATRIX	Capability di contenimento
Spear phishing con macro su workstation corporate, impianto di BlackEnergy 3	T, A	Verifica della postura del dispositivo; segmentazione IT e OT
Ricognizione prolungata e raccolta di credenziali, assenza di autenticazione forte	A, I	Identità e autenticazione a più fattori; monitoraggio centralizzato
Accesso remoto ai sistemi SCADA tramite credenziali legittime	I	Autorizzazione continua basata su policy; gestione sicura degli accessi remoti di terze parti
Apertura manuale degli interruttori da HMI compromesse	M, I	Microsegmentazione tra livelli; verifica dell'identità sui comandi verso il Livello 1
Sovrascrittura del firmware dei convertitori seriale-Ethernet delle sottostazioni	A, R	Controlli compensativi e gestione del rischio residuo sugli asset non aggiornabili
Cancellazione delle workstation con KillDisk e perdita di visibilità	X	Monitoraggio e logging centralizzato fuori banda; continuità operativa
Disabilitazione dell'alimentazione di soccorso del centro di controllo	M, R	Caratterizzazione dei DAAS critici; prioritizzazione orientata all'impatto
Denial of service telefonico verso i call center	T	Mappatura estesa della superficie d'attacco oltre il perimetro tecnico

scenario illustrativo, e la sua catena di attacco è nota nel dettaglio.

È inoltre accertato che l'interruzione non fu causata dal solo malware impiegato, bensì dall'operatività manuale degli attaccanti sui sistemi di controllo, circostanza che rende il caso particolarmente adatto a saggiare un framework incentrato sull'autorizzazione e sulla verifica dell'accesso.

La Tabella 4 scompone la catena di attacco nei suoi passaggi documentati e associa a ciascuno la fase di MATRIX e la capability che ne avrebbero ridotto la probabilità o l'impatto.

L'analisi mostra che ogni passo della catena trova corrispondenza in almeno una fase del framework e in una capability che ne avrebbe osta-

colato la riuscita o ridotto le conseguenze. Sono particolarmente significativi due punti. Primo, i passaggi decisivi dell'attacco, l'accesso remoto con credenziali legittime e l'apertura manuale degli interruttori, ricadono esattamente nello spazio che la fase I presidia con l'autorizzazione continua e la verifica dell'identità sui comandi critici.

Secondo, il danno più duraturo, la sovrascrittura del firmware dei convertitori, colpì asset non aggiornabili: proprio la categoria per cui MATRIX prescrive controlli compensativi e la contabilizzazione esplicita del rischio residuo, anziché l'illusione di una protezione nativa. La validazione retrospettiva non dimostra che il framework avrebbe impedito l'incidente, affermazione che nessun metodo qualitativo può sostenere, ma conferma che la sua applicazione avrebbe portato all'attenzione, in modo strutturato, i controlli la cui assenza fu determinante.

4.5 Sintesi della validazione

Nel loro insieme, le tre componenti delineano una validazione onesta nei suoi limiti e robusta nelle parti dimostrabili. La copertura rispetto agli standard e il confronto con gli schemi esistenti collocano il framework nel suo spazio metodologico, mentre la prova retrospettiva su un incidente reale ne saggia la pertinenza operati-

va contro un avversario documentato. Permangono, dichiaratamente, la natura qualitativa del metodo e l'assenza di una validazione empirica sul campo in impianti in esercizio, che resta la prova ultima e l'obiettivo prioritario degli sviluppi futuri.

PRINCIPIO GUIDA

Ogni passo della catena trova corrispondenza in una fase del framework e in una capability che ne avrebbe ostacolato la riuscita o ridotto le conseguenze.

05

CAPITOLO 5

Implicazioni

- 5.1 Pregi del framework MATRIX
- 5.2 Limiti e assunzioni
- 5.3 Generalizzabilità e adattabilità del modello



Implicazioni

Pregi, limiti, generalizzabilità del metodo e gestione esplicita del rischio residuo

5.1 Pregi del framework MATRIX

Il valore di MATRIX risiede nel collegamento esplicito che istituisce tra la comprensione dell'ambiente e la selezione dei controlli. Rispetto al processo istituzionale in cinque fasi,⁴¹ che indica cosa fare ma non come decidere tra alternative su asset eterogenei, il framework aggiunge tre elementi distintivi: la profilazione sistematica dell'idoneità, che ancora le scelte alla reale capacità tecnica dei dispositivi; l'analisi esplicita dei compromessi, che impedisce di trattare la sicurezza come variabile indipendente dalla continuità operativa; e la matrice di allocazione, che rende tracciabile e comunicabile l'intera catena decisionale. Quest'ultimo aspetto ha un valore non solo tecnico ma organizzativo: la matrice costituisce uno strumento di dialogo tra i team responsabili delle politiche di sicurezza e i proprietari dei sistemi, le cui priorità - disponibilità e safety - divergono spesso da quelle informatiche.

MATRIX non sostituisce gli schemi esistenti ma li assume e li raffina. Le sue

fasi M e T sono complementari ai primi due passi del processo in cinque fasi; la fase I corrisponde alla costruzione dell'architettura e delle politiche, arricchita però dalla logica di allocazione differenziata; la fase X riprende il monitoraggio continuo. La novità non è dunque nei singoli ingredienti, molti dei quali derivano dalla normativa e dalla letteratura citate, ma nella loro composizione in un metodo coerente, ripetibile e orientato alla missione.

5.2 Limiti e assunzioni

La proposta presenta limiti che è doveroso esplicitare. In primo luogo, MATRIX è una metodologia qualitativa: l'attribuzione dei punteggi di idoneità e la ponderazione dei compromessi comportano margini di soggettività e richiedono competenze multidisciplinari - ingegneristiche, di processo e di sicurezza.

In secondo luogo, il framework non è stato ancora sottoposto a validazione empirica su impianti reali; lo scenario della Sezione 4 ha valore illustrativo, non sperimentale. In terzo luogo, l'effi-

⁴¹ Cloud Security Alliance, *Zero Trust Guidance for Critical Infrastructure*. Seattle, WA, USA: CSA Zero Trust Working Group, ott. 2024.

cacia dell'allocazione dipende dalla disponibilità di tecnologie abilitanti - in particolare di layer intermediari capaci di mediare protocolli legacy - la cui maturità varia tra domini e fornitori. Infine, permane il problema dei componenti non adeguabili: per essi MATRIX offre un quadro per riconoscere e gestire il rischio residuo, non per eliminarlo.

5.3 Generalizzabilità e adattabilità del modello

Quanto alla generalizzabilità, il framework è stato illustrato nel dominio energetico ma la sua struttura è indipendente dal settore: i mission thread, i profili di idoneità e i compromessi cambiano contenuto, non forma, passando alla manifattura, al ciclo idrico, all'oil & gas o ai trasporti.

Resta una minaccia alla validità nel rischio che la flessibilità del metodo si traduca in incoerenza applicativa: senza criteri di scoring condivisi e documentati, due analisti potrebbero giungere a matrici divergenti per lo stesso impianto. La definizione di linee guida di scoring e di metriche di riferimento, indicata tra gli sviluppi futuri, è perciò condizione per un'adozione affidabile.

06

CAPITOLO 6

Conformità normativa

- 6.1 Il quadro regolatorio europeo e nazionale
- 6.2 Mappatura del framework agli obblighi



Conformità normativa

Il framework a supporto degli obblighi regolatori

Le considerazioni sin qui svolte hanno natura tecnica, ma la sicurezza degli ambienti OT critici non è più soltanto una questione ingegneristica: è divenuta un obbligo giuridico. L'evoluzione del quadro regolatorio europeo, e il suo recepimento nazionale, impongono agli operatori dei settori essenziali misure di gestione del rischio adeguate e proporzionate, accompagnate da obblighi di governance, di notifica degli incidenti e di dimostrazione documentale della conformità. Un framework metodologico per lo zero trust in ambito OT, per risultare utile nella pratica, deve perciò collocarsi entro questo quadro e mostrarsi capace di sostenerne gli adempimenti.

6.1 Il quadro regolatorio europeo e nazionale

Il riferimento sovraordinato è la direttiva (UE) 2022/2555, nota come NIS2, recepita in Italia con il decreto legislativo 4 settembre 2024, n. 138.^{42/ 43} La

normativa amplia in misura considerevole la platea dei soggetti obbligati e individua nell'energia - elettricità, gas, petrolio, idrogeno - uno dei settori ad alta criticità, i cui operatori ricadono di norma tra i soggetti essenziali. L'autorità nazionale competente è l'Agenzia per la Cybersicurezza Nazionale (ACN), cui spettano la supervisione, la regolazione e la raccolta delle notifiche tramite il CSIRT Italia.

Il decreto impone, agli articoli 23, 24 e 25, un nucleo di obblighi concatenati: la responsabilizzazione degli organi di amministrazione, chiamati ad approvare le misure di gestione del rischio e a sovrintendere alla loro attuazione; l'adozione di misure tecniche, operative e organizzative adeguate e proporzionate; e la notifica degli incidenti significativi, con una pre-notifica entro ventiquattro ore e una notifica entro settantadue ore dall'evidenza dell'evento. Le misure di sicurezza di base e le relative specifiche sono state dettagliate dall'ACN con la determinazione n.

⁴² Parlamento europeo e Consiglio, *Direttiva (UE) 2022/2555 (NIS2), relativa a misure per un livello comune elevato di cibersecurity nell'Unione*, 14 dicembre 2022. GU UE L 333.

⁴³ *Decreto Legislativo 4 settembre 2024, n. 138, recepimento della direttiva (UE) 2022/2555 (NIS2)*. Gazzetta Ufficiale della Repubblica Italiana, n. 230, 1° ottobre 2024.

379907/2025 e con le linee guida che l'accompagnano,⁴⁴ mentre la legge 28 giugno 2024, n. 90 ha ulteriormente rafforzato l'architettura nazionale della cybersicurezza.⁴⁵ Il quadro non si esaurisce nell'adozione di un catalogo di controlli: esige un sistema governato, documentato e continuamente verificabile, soggetto a poteri ispettivi e a un regime sanzionatorio severo.

Sul piano dell'attuazione tecnica, il regolamento di esecuzione (UE) 2024/2690 ha specificato, per alcune categorie di soggetti a rilevanza transfrontaliera, i requisiti tecnici e metodologici delle misure di cui all'articolo 21 della direttiva, organizzandoli in tredici ambiti tematici; l'ENISA ne ha corredato l'applicazione con una guida tecnica che, per ciascun ambito, fornisce indicazioni operative ed esempi di evidenza documentale.^{46/ 47}

A questo strato orizzontale se ne sovrappone uno settoriale, particolarmente rilevante per il dominio energetico assunto a riferimento in questo lavoro. Il regolamento dele-

gato (UE) 2024/1366, primo network code dell'Unione dedicato alla cybersicurezza del settore elettrico, stabilisce regole specifiche per gli aspetti di sicurezza informatica dei flussi transfrontalieri di energia elettrica.⁴⁸

Il codice introduce una classificazione delle entità ad alto impatto e a impatto critico fondata su un indice dedicato (Electricity Cybersecurity Impact Index), un insieme di controlli minimi e avanzati - comprensivi di misure sulla supply chain - e un processo ricorrente di valutazione del rischio coordinato a livello europeo.

Significativa è la sua complementarietà con la NIS2: la conformità a uno dei due regimi può costituire elemento di prova della conformità all'altro, evitando duplicazioni. Completano il quadro la direttiva (UE) 2022/2557 sulla resilienza dei soggetti critici, che presidia la dimensione fisica e organizzativa, e il regolamento (UE) 2024/2847 - il cosiddetto Cyber Resilience Act - che introduce requisiti di sicurezza per i prodotti con elementi digitali, e dunque per i fornitori

⁴⁴ Agenzia per la Cybersicurezza Nazionale, *Determinazione n. 379907/2025 - Misure di sicurezza di base e specifiche per gli incidenti significativi*. Roma, Italia: ACN, 2025

⁴⁵ *Legge 28 giugno 2024, n. 90*, disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici. Gazzetta Ufficiale della Repubblica Italiana, 2024.

⁴⁶ Commissione europea, *Regolamento di esecuzione (UE) 2024/2690 del 17 ottobre 2024, che stabilisce i requisiti tecnici e metodologici delle misure di cui all'articolo 21, paragrafo 2, della direttiva (UE) 2022/2555*. GU UE L, 2024/2690.

⁴⁷ Agenzia dell'Unione europea per la cibersicurezza (ENISA), *Technical Implementation Guidance on Cybersecurity Risk Management Measures*, v1.0. Atene, Grecia: ENISA, giugno 2025.

⁴⁸ Commissione europea, *Regolamento delegato (UE) 2024/1366 che istituisce un codice di rete sugli aspetti settoriali di cibersicurezza dei flussi transfrontalieri di energia elettrica*, 11 marzo 2024. GU UE L, 2024/1366

Tabella 5. Mappatura sintetica tra le fasi del framework MATRIX e gli obblighi di gestione del rischio della normativa europea e nazionale

Fase MATRIX	Contributo alla conformità	Riferimento
M - Mission context & DAAS	Identificazione e classificazione di asset e servizi critici; analisi del rischio orientata all'impatto sulla missione	Art. 24; NCCS (ECII)
A - Asset suitability	Gestione degli asset e base per misure proporzionate alla loro effettiva natura tecnica	Art. 24; proporzionalità
T - Threat & attack surface	Analisi di minacce e vulnerabilità; sicurezza della catena di approvvigionamento	Art. 24; NCCS
R - Risk & tradeoff	Trattamento del rischio e selezione di misure adeguate e proporzionate	Art. 24; Linee Guida ACN
I - Implementation	Controllo accessi, MFA, crittografia, segmentazione; documentazione delle misure	Art. 24; Det. ACN 379907/2025
X - eXecution & evoluzione	Monitoraggio continuo, continuità operativa, gestione e notifica degli incidenti	Artt. 24-25; NCCS

Nota: i riferimenti agli articoli rinviano al D.Lgs. 138/2024 (recepimento della direttiva NIS2); "NCCS" indica il regolamento delegato (UE) 2024/1366 sul settore elettrico.

degli stessi apparati OT.^{49/ 50} In tutti questi strumenti, le misure attese sono ancorate allo stato dell'arte e ai pertinenti standard europei e internazionali, tra cui la serie ISA/IEC 62443 e le pubblicazioni del NIST già richiamate.

6.2 Mappatura del framework agli obblighi

MATRIX non è una checklist di conformità, ma le sue fasi producono in modo naturale gli elementi che la normativa richiede. Le misure di gestione del rischio previste dall'arti-

⁴⁹ Parlamento europeo e Consiglio, *Direttiva (UE) 2022/2557 relativa alla resilienza dei soggetti critici*, 14 dicembre 2022. GU UE L 333.

⁵⁰ Parlamento europeo e Consiglio, *Regolamento (UE) 2024/2847 (Cyber Resilience Act)*, relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali, 2024. GU UE L, 2024/2847.

colo 24 del decreto - analisi del rischio, sicurezza dei sistemi, gestione delle vulnerabilità e della catena di approvvigionamento, controllo degli accessi e autenticazione a più fattori, continuità operativa e gestione degli incidenti - trovano corrispondenza nelle attività che il framework articola e documenta. La Tabella 5 propone una mappatura sintetica tra le sei fasi e i corrispondenti obblighi.

Il valore della metodologia, sul piano della conformità, è duplice. Da un lato, il principio di applicabilità differenziata e l'analisi esplicita dei compromessi danno contenuto operativo al requisito di misure adeguate e proporzionate, evitando tanto la sottoprotezione quanto l'adozione di controlli insostenibili.

Dall'altro, la matrice di allocazione costituisce di per sé un artefatto documentale: registra, per ciascun asset, quali capability sono state applicate, con quali modalità e con quale rischio residuo, fornendo agli organi di amministrazione e agli auditor l'evidenza tracciabile che il quadro regolatorio esige - in linea con l'approccio basato sugli esempi di evidenza adottato dalla guida tecnica europea.⁵¹

In questa prospettiva MATRIX non si configura come un adempimento ag-

giuntivo, ma come uno strumento che rende la conformità un sottoprodotto di un processo di sicurezza ben condotto.

PRINCIPIO GUIDA

Matrix non è un adempimento aggiuntivo: rende la conformità un sottoprodotto di un processo di sicurezza ben condotto.

⁵¹ Agenzia dell'Unione europea per la cibersicurezza (ENISA), *Technical Implementation Guidance on Cybersecurity Risk Management Measures*, v1.0. Atene, Grecia: ENISA, giugno 2025.

07

CAPITOLO 7

Conclusioni e sviluppi futuri



Conclusioni e sviluppi futuri

Sintesi del contributo e direzioni di ricerca per portare MATRIX dalla teoria alla pratica

La convergenza tra IT e OT ha reso le infrastrutture critiche bersagli raggiungibili e appetibili, e ha imposto di ripensarne la sicurezza oltre il paradigma perimetrale. Lo zero trust offre i principi adatti, ma la sua applicazione all'OT non può essere una trasposizione meccanica di soluzioni nate per l'EIT: deve fare i conti con l'eterogeneità, i vincoli di tempo reale e di safety, la disponibilità continua e il peso del legacy. Questo lavoro ha proposto MATRIX, un framework metodologico che affronta tale sfida attraverso sei fasi - dalla caratterizzazione del contesto di missione all'esecuzione con evoluzione incrementale - e attorno a un artefatto centrale, la matrice di allocazione delle capability, che lega le scelte di protezione all'idoneità tecnica degli asset e alla loro criticità per la missione. Il contributo non risiede in un nuovo meccanismo di sicurezza, ma in un metodo che rende le decisioni selettive, tracciabili e proporzionate, complementare agli standard e alle linee guida esistenti.

Diverse direzioni si aprono alla ricerca futura. La prima è la definizione di metriche quantitative e di criteri di scoring condivisi per la profilazione dell'idoneità e per l'analisi dei compromessi,

così da ridurre la soggettività e accrescere la riproducibilità. La seconda è lo sviluppo di strumenti di supporto che assistano gli analisti nella compilazione della matrice e nella generazione automatica della roadmap. La terza è l'integrazione con flussi di threat intelligence e con tecniche di intelligenza artificiale per la rivalutazione continua del rischio, tenendo conto che gli stessi progressi dell'IA possono ampliare e accelerare le capacità offensive. La quarta, e più rilevante, è la validazione empirica del framework su impianti reali in settori diversi, condizione necessaria per misurarne l'efficacia e per affinarne i criteri alla prova dei fatti. Affrontare queste sfide consentirà di trasformare MATRIX da proposta metodologica a strumento operativo maturo per la protezione, consapevole e sostenibile, delle infrastrutture critiche.

Riferimenti bibliografici

J. Kindervag, *Build Security Into Your Network's DNA: The Zero Trust Network Architecture*. Cambridge, MA, USA: Forrester Research, 2010.

S. Rose, O. Borchert, S. Mitchell e S. Connelly, *Zero Trust Architecture*, NIST Special Publication 800-207. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2020, doi: 10.6028/NIST.SP.800-207.

K. Stouffer, M. Pease, C. Tang, T. Zimmerman, V. Pillitteri, S. Lightman, A. Hahn, S. Saravia, A. Sherule e M. Thompson, *Guide to Operational Technology (OT) Security*, NIST Special Publication 800-82r3. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2023, doi: 10.6028/NIST.SP.800-82r3.

International Electrotechnical Commission, *IEC 62443: Security for Industrial Automation and Control Systems* (serie). Ginevra, Svizzera: IEC.

T. J. Williams, "The Purdue enterprise reference architecture," *Computers in Industry*, vol. 24, n. 2-3, pp. 141-158, 1994.

Agenzia dell'Unione europea per la cibersicurezza (ENISA), *Technical Implementation Guidance on Cybersecurity Risk Management Measures*, v1.0. Atene, Grecia: ENISA, giugno 2025.

Cloud Security Alliance, *Zero Trust Guidance for Critical Infrastructure*. Seattle, WA, USA: CSA Zero Trust Working Group, ott. 2024.

Commissione europea, *Regolamento di esecuzione (UE) 2024/2690 del 17 ottobre 2024, che stabilisce i requisiti tecnici e metodologici delle misure di cui all'articolo 21, paragrafo 2, della direttiva (UE) 2022/2555*. GU UE L, 2024/2690.

C. J. Alberts, T. Morrow, R. Brown e C. M. Wallen, *Tailoring Security and Zero Trust Principles to Weapon System Environments*, Special Report. Pittsburgh, PA, USA: Software Engineering Institute, Carnegie Mellon University, 2025.

R. Brown, "Implementing Zero Trust in Operational Technology: A Practical Case Study," *SEI Insights* (blog), Software Engineering Institute, Carnegie Mellon University, 16 giugno 2026.

N. F. Syed, S. W. Shah, A. Shaghaghi, A. Anwar, Z. Baig e R. Doss, "Zero trust architecture (ZTA): A comprehensive survey," *IEEE Access*, vol. 10, pp. 57143-57179, 2022.

E. B. Fernandez e A. Brazhuk, "A critical analysis of zero trust architecture (ZTA)," *Computer Standards & Interfaces*, vol. 89, art. 103832, 2024.

E. Bertino, "Zero trust architecture: Does it help?," *IEEE Security & Privacy*, vol. 19, n. 5, pp. 95–96, 2021.

X. Feng e S. Hu, "Cyber-physical zero trust architecture for industrial cyber-physical systems," *IEEE Transactions on Industrial Cyber-Physical Systems*, vol. 1, pp. 394–405, 2023.

C. Zanasi, S. Russo e M. Colajanni, "Flexible zero trust architecture for the cybersecurity of industrial IoT infrastructures," *Ad Hoc Networks*, vol. 156, art. 103414, 2024, doi: 10.1016/j.adhoc.2024.103414.

F. Federici, D. Martintoni e V. Senni, "A zero-trust architecture for remote access in industrial IoT infrastructures," *Electronics*, vol. 12, n. 3, art. 566, 2023, doi: 10.3390/electronics12030566.

P. Phiayura e S. Teerakanok, "A comprehensive framework for migrating to zero trust architecture," *IEEE Access*, vol. 11, pp. 19487–19511, 2023.

R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Security & Privacy*, vol. 9, n. 3, pp. 49–51, 2011.

R. M. Lee, M. J. Assante e T. Conway, *Analysis of the Cyber Attack on the Ukrainian Power Grid*. Washington, DC, USA: E-ISAC e SANS Industrial Control Systems, 2016.

Parlamento europeo e Consiglio, *Direttiva (UE) 2022/2555 (NIS2), relativa a misure per un livello comune elevato di cibersicurezza nell'Unione*, 14 dicembre 2022. GU UE L 333.

Decreto Legislativo 4 settembre 2024, n. 138, recepimento della direttiva (UE) 2022/2555 (NIS2). Gazzetta Ufficiale della Repubblica Italiana, n. 230, 1° ottobre 2024.

Agenzia per la Cybersicurezza Nazionale, *Determinazione n. 379907/2025 - Misure di sicurezza di base e specifiche per gli incidenti significativi*. Roma, Italia: ACN, 2025.

Legge 28 giugno 2024, n. 90, disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici. Gazzetta Ufficiale della Repubblica Italiana, 2024.

Commissione europea, *Regolamento delegato (UE) 2024/1366 che istituisce un codice di rete sugli aspetti settoriali di cibersicurezza dei flussi transfrontalieri di energia elettrica*, 11 marzo 2024. GU UE L, 2024/1366.

Parlamento europeo e Consiglio, *Direttiva (UE) 2022/2557 relativa alla resilienza dei soggetti critici*, 14 dicembre 2022. GU UE L 333.

Parlamento europeo e Consiglio, *Regolamento (UE) 2024/2847 (Cyber Resilience Act), relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali*, 2024. GU UE L, 2024/2847.

Agenzia dell'Unione europea per la cibersicurezza (ENISA), *ENISA Threat Landscape 2024*. Atene, Grecia: ENISA, settembre 2024, doi: 10.2824/0710888.

Forum ICT Security

24^a Edizione

Auditorium della Tecnica, Roma

Novembre

18 e 19 NOVEMBRE 2026

**08 am -
04 pm**

Iscriviti sul sito web:

ictsecuritymagazine.com