EUROPEAN CYBER SECURITY ORGANISATION

Organizzazione europea per la sicurezza informatica

Documento tecnico ECSO sugli scenari di cybersecurity e Digital Twins

Maggio 2023 – v1.0

INFORMAZIONI SULL'ECSO

L'Organizzazione europea per la sicurezza informatica (ECSO) ASBL è un'organizzazione senza scopo di lucro completamente autofinanziata ai sensi della legge belga, fondata nel giugno 2016.

ECSO rappresenta la controparte contrattuale della Commissione Europea per l'attuazione del Partenariato Pubblico-Privato contrattuale sulla Cyber Security (cPPP). I membri dell'ECSO includono un'ampia varietà di portatori di interessi negli Stati membri dell'UE, nei paesi SEE/EFTA e nei paesi associati a Orizzonte 2020, come grandi aziende, PMI e start-up, centri di ricerca, università, utenti finali, operatori, cluster e associazioni, nonché Amministrazioni locali, regionali e nazionali degli Stati membri europei. Maggiori informazioni su ECSO e il suo lavoro possono essere trovate su www.ecs-org.eu.

Contatto

Per domande relative a questo documento, contattare wg6_secretariat@ecs-org.eu.
Per domande da parte dei media su questo documento, utilizzare media@ecs-org.eu.

Disclaimer

ECSO non è responsabile per l'uso da parte di terzi del contenuto di questo documento. Utilizzando/facendo riferimento alle informazioni contenute in questo documento, non si crea alcun rapporto tra ECSO e qualsiasi persona che acceda o utilizzi in altro modo il documento o qualsiasi parte di esso. ECSO non è responsabile per azioni di qualsiasi natura derivanti da qualsiasi utilizzo del documento o parte di esso. Né l'ECSO né alcuna persona che agisce per suo conto è responsabile dell'uso che potrebbe essere fatto delle informazioni contenute in questa pubblicazione.

Le fonti di terze parti sono citate ove appropriato. ECSO non è responsabile del contenuto del fonti esterne, inclusi i siti Web esterni a cui si fa riferimento in questa pubblicazione.

Sintesi

I Digital Twin (DT) possono essere concettualizzati come una tecnologia che migliora i processi e prevede guasti e individua situazioni anomale. Per questi motivi, i DT stanno diventando attori cruciali nella tendenza globale alla digitalizzazione che sta influenzando la nostra economia, industria e società. In grado di virtualizzare e simulare le risorse del mondo fisico per potenziare azioni di ottimizzazione innovative in molti dei domini applicativi odierni, l'adozione dei dispositivi DT apporta vantaggi in termini di resilienza e sicurezza informatica in vari scenari applicativi. Grazie alle funzionalità di simulazione offline e online, i dispositivi DT forniscono servizi interessanti, in particolare: manutenzione predittiva, monitoraggio in tempo reale, controllo remoto, ottimizzazione dei processi, gestione della sicurezza, analisi e monitoraggio dei guasti, valutazione della strategia, monitoraggio dello stato, gestione del rischio, formazione e sicurezza informatica.

In linea con quanto sopra, questo documento tecnico ECSO esplora la definizione di Digital Twin, i suoi limiti e dipendenze tecniche, presentando le sfide che la tecnologia sta attualmente incontrando, *in primis* nel settore della sicurezza informatica.

Innanzitutto, l'analisi del documento ECSO WG6 discute quattro diversi casi d'uso che coprono le applicazioni del DTS, inteso come sinergia cyber-fisica, in un'ampia varietà di settori, tra cui: affari, istruzione e competenze, industrie collaborative, sicurezza informatica *industriale* . Successivamente, l'accento sarà posto sulle architetture e sui framework DT progettati in gran parte da organizzazioni ed enti accademici.

Inoltre, per comprendere appieno la rilevanza dei DT, vengono esaminati due aspetti cruciali della suddetta tecnologia: da un lato, le capacità di simulazione dei DT come risorsa per soluzioni di cybersecurity, e dall'altro, la virtualizzazione dei DT come strumento laboratorio unico per sviluppare, convalidare e testare approcci alla sicurezza per condurre azioni di mitigazione e prevenzione.

Data l'ampiezza della superficie di attacco che caratterizza i DT, la seconda parte della ricerca mira a portare alla luce una serie di raccomandazioni e linee guida di best practice da considerare nel prossimo futuro per configurare e implementare DT affidabili e sicuri. Nello specifico, il documento delinea i requisiti di sicurezza, in linea con il quadro di sicurezza informatica fornito dal National Institute of Standards and Technology (NIST), che sia i professionisti che gli esperti di sicurezza IT/OT dovrebbero considerare per evitare potenziali scenari di attacco.

Infine, il WG6 ECSO fornisce una serie di raccomandazioni per assistere le varie parti interessate nel governare la natura complessa e dinamica dei DT. Nel complesso si può affermare con certezza che questo documento tecnico dell'ECSO delinea lo stato attuale della tecnologia e la sua domanda dal punto di vista della ricerca, dell'industria e della società.

Sommario

Acronimi

AAA Autenticazione, autorizzazione e contabilità

ADSS Airbus Difesa e Spazio

AI Intelligenza artificiale

ANGEL Guardiano automatico di rete per impianti elettrici

API Interfaccia di programmazione applicazioni

APP Minaccia persistente avanzata

BIM Building Information Modeling

C2PS Sistemi cyber-fisici basati sul cloud

CAMERA Produzione assistita da computer

CAS Progettazione assistita da computer

CPPS Sistema di produzione ciberfisico

CPS Sistemi ciberfisici

CVE Esposizioni a vulnerabilità comuni

DLT Tecnologia di contabilità distribuita

DTaaS Il gemello digitale come servizio

DTN Rete del gemello digitale

GE Generale Elettrico

HMI Interfaccia uomo macchina

ICS Sistemi di controllo industriale

ID Sistema di rilevamento delle intrusioni

IIC Consorzio industriale IoT

IIoT Internet delle cose industriale

IoT Internet delle cose

IP Proprietà intellettuale

IPC Comunicazione tra processi

DPI Diritti di proprietà intellettuale

IRTF Task Force per la ricerca su Internet

ISO Organizzazione internazionale per la standardizzazione

ESSO Tecnologie dell'informazione

KPI Indicatore chiave di prestazione

MDT Gemello digitale per la mobilità

Trasporto di telemetria dell'accodamento messaggi **MQTT**

NIST Istituto Nazionale di Standard e Tecnologia

OT Tecnologia operativa

P2P	Peer to peer
ANIMALE DOMESTICO	Tecnologie per il miglioramento della privacy
PLC	Controllore logico programmabile
SBL	Apprendimento basato su scenari
SDK	Kit di sviluppo software
SDN	Rete definita dal software
Analisi del comportamento degli utenti e delle entità **UEBA**	
V/AR	Realtà virtuale o aumentata
W3C	World Wide Web Consortium

1. Introduzione

Il Digital Twin (DT) è un paradigma emergente che sta ricevendo crescente attenzione da parte dell'industria, degli istituti di ricerca e del mondo accademico. L'evoluzione è catalizzata dalla digitalizzazione, dall'emergere di ambienti di simulazione convenienti e accessibili e dalla crescente domanda di una soluzione economicamente vantaggiosa ma realistica per sperimentare infrastrutture basate sulla tecnologia dell'informazione (IT) e sulle tecnologie operative (OT), senza le relative infrastrutture. rischi operativi e costi finanziari.

Secondo il Consorzio DT in [DTC22], un DT può essere definito come *"una rappresentazione virtuale di entità e processi del mondo reale, sincronizzati con frequenza e fedeltà specifiche",* mentre alcuni altri autori, come [WU21], lo classificano come (1) un modello virtuale/rappresentazione digitale (ovvero, *un DT è un insieme di informazioni virtuali che descrivono completamente una produzione fisica potenziale o effettiva dal livello micro atomico al livello macro geometrico* [ZHE18]); (2) un software/simulazione (ovvero *basato su algoritmi di ottimizzazione più rapidi, maggiore potenza del computer e maggiore quantità di dati disponibili* [SDE17]); e (3) un sistema integrato (ovvero, *un DT è in realtà un modello vivente dell'asset o del sistema fisico, che si adatta continuamente ai cambiamenti operativi sulla base dei dati e delle informazioni raccolti online e può prevedere il futuro della corrispondente controparte fisica* [LIU18]).

Inoltre, la Commissione Europea compila anche in [NAT20] una serie di definizioni tratte da diverse comunità e organizzazioni di standardizzazione, come quella fornita dal W3C (World Wide Web Consortium). Il W3C afferma che un DT è *"una rappresentazione virtuale di un dispositivo o di un gruppo di dispositivi che risiede in un cloud o in un nodo edge. Può essere utilizzato per rappresentare dispositivi del mondo reale che potrebbero non essere continuamente online o per eseguire simulazioni di nuove applicazioni e servizi, prima che vengano distribuiti su dispositivi reali" [W3C20, NAT20] .*

Inoltre, l'ideatore del concetto tecnologico, M. Grieves, ha affermato in [GRI14] che il DT è composto principalmente da due spazi essenziali (uno virtuale e uno fisico) collegati tramite collegamenti di comunicazione bidirezionali tra entrambi gli spazi. Questo modo di connettere gli spazi è proprio ciò che differenzia un DT da altri sistemi di simulazione correlati. In [KRI18], Kritzinger *et al.* affermare che esistono tre diverse concettualizzazioni con diverse modalità di integrazione a seconda del flusso di dati: (i) *Digital Twin* (basato su collegamenti di comunicazione bidirezionali con flussi di dati automatici in entrambe le direzioni), (ii) *Digital Shadow* (comunicazione bidirezionale con flussi di dati manuali da dallo spazio virtuale allo spazio fisico) e (iii) *Modello digitale* (con flussi di dati manuali in entrambe le direzioni). La bidirezionalità automatica del DT è ciò che rende questa tecnologia attraente, consentendo ai DT di prendere decisioni da soli e agire di conseguenza.

A causa di questa autonomia, è evidente che la costruzione di un DT implica la considerazione di altre tecnologie che, insieme, possono spiegare gli stati rilevanti a beneficio del modello di business, della produzione e della catena del valore. Attraverso la simulazione, i dati storici, i modelli e le specifiche del modello digitale, è possibile creare una comprensione più olistica e standard di un elemento, contesto e situazione osservati, migliorando la consapevolezza situazionale di un'organizzazione e in termini di componenti, processi o strutture . Come affermato in [DTC22], i DT sono sistemi di per sé che possono essere adattati a molteplici casi d'uso, sincronizzati con il mondo reale attraverso le attuali tecnologie IT/OT e i loro protocolli di comunicazione.

Inoltre, questo impatto ha attirato l'attenzione di molte organizzazioni internazionali. Ad esempio, le organizzazioni di standardizzazione sono coinvolte nella standardizzazione delle architetture di riferimento e nelle relative tecnologie abilitanti, come l'Internet Research Task Force (IRTF) in [ZHO21] (descritta in dettaglio di seguito) o l'International Standard Organization (ISO) in [ISO22]; E

stanno nascendo consorzi e associazioni per dare risposta ai bisogni attuali. Nel caso particolare dell'ISO, è stato recentemente pubblicato un primo documento riguardante un quadro standard per le tecnologie DT. Lo standard è composto da quattro parti: ISO 23247-[1-4]:2021. La prima parte [ISO21a] fornisce una panoramica e i principi generali di un quadro DT per la produzione, inclusi termini, definizioni e requisiti del quadro DT per la produzione, mentre la seconda parte dello standard [ISO21b] mostra un'architettura di riferimento.

Allo stesso modo, il National Institute of Standards and Technology (NIST) si è unito al dibattito sugli standard emergenti per i DT. Nel 2021, hanno pubblicato la loro prima bozza sull'argomento chiamata *"Considerazioni sulla tecnologia dei gemelli digitali e sugli standard emergenti"* - NISTIR 8356 [NIST21]. La bozza fornisce una definizione dettagliata di DT, la motivazione e la visione per il loro utilizzo, operazioni comuni di basso livello, scenari di utilizzo e casi d'uso di esempio. Concentrandosi su considerazioni tecniche relative alla sicurezza informatica e alla fiducia di DT, il rapporto analizza le nuove sfide di sicurezza informatica derivanti dall'uso delle architetture DT ed esamina le tradizionali sfide di sicurezza informatica che si applicano. Infine, la bozza di rapporto valuta le sfide tecnologiche legate alla sicurezza informatica e discute l'impatto che la mancanza di fiducia e di standard può avere sulla funzionalità e sulla qualità di DT.

Per quanto riguarda consorzi e associazioni, uno dei più rilevanti è il Digital Twin Consortium [DTC22], che mira a essere la nuova *"Autorità sui gemelli digitali",* riunendo industria, governo e mondo accademico per promuovere la coerenza nel vocabolario, nell'architettura, nella sicurezza e interoperabilità della tecnologia DT. Promuove la consapevolezza, l'adozione, l'interoperabilità e lo sviluppo della tecnologia DT. Attraverso una partnership di collaborazione con l'industria, il mondo accademico e le competenze del governo, il Consorzio si dedica allo sviluppo complessivo delle tecnologie DT. I principali contributi sono stati finora stato il tentativo di standardizzare termini e processi ricorrenti all'interno di un'architettura DT, importanti contributi sono stati dati anche nella strutturazione di qualsiasi business e mercato, nonché nell'approccio open source.

Un altro consorzio interessante è l'Industry IoT Consortium (IIC) [IIC22], fondato nel 2014. Il consorzio è focalizzato sulla promozione dell'innovazione tecnologica che favorisce lo sviluppo del business. Ha lo scopo di aiutare le organizzazioni a identificare le migliori pratiche tecnologiche, costruire marchi credibili e far crescere le proprie attività facilitando il networking, la collaborazione e i collegamenti tra i membri. Il suo principale contributo alla comunità DT è stato il documento tecnico [IIC20] per DT per applicazioni industriali. A differenza del precedente consorzio, l'IIC è più verticalizzato sui temi dell'Internet of Things. Nonostante ciò, il Libro Bianco offre un importante contributo trattando aspetti legati a: definizione e caratteristiche di un DT; le relazioni tra i DT per formare sistemi compositi; il ruolo del DT nel ciclo di vita delle entità, considerando scenari con e senza DT e il valore aggiunto di business del DT; la progettazione interna del DT; ed esempi dell'uso dei DT in vari settori.

Sfortunatamente, tutte queste azioni sono attualmente in corso, quindi non esiste una definizione unificata [BAR19, ALC22] che garantisca una metodologia di implementazione comune a livello tecnico, operativo e amministrativo. Quindi, ad oggi, è ancora una sfida parlare di cosa comporterebbe il lancio di ecosistemi basati su DT. Probabilmente uno dei motivi principali di ciò è l'enorme boom tecnologico che l'implementazione dei DT potrebbe comportare. In linea con l'Industria 4.0/5.0 e i relativi scenari, sono molteplici le tecnologie che possono essere integrate nell'ambito di un DT quali: Intelligenza Artificiale (AI), Sistemi Cyber-Fisici (CPS), Internet of Things (Industriale) ((I)IoT), edge computing, 5G/6G e così via [XU21, MIH22, ALC22]. Pertanto, rimane difficile trovare un modo per stabilire un approccio unificato *e valido per tutti* ai progetti basati su DT.

Per quanto riguarda l'applicazione della tecnologia DT per casi d'uso specifici, vale la pena sottolineare la sua grande rilevanza oggi per la resilienza e la sicurezza informatica. Attraverso le sue capacità di simulazione (sia offline che online), è possibile prevedere i rischi e anticipare le situazioni di minaccia [ALC22] che possono essere prevenute e/o mitigate in tempo, soprattutto in quegli scenari applicativi critici (ad esempio, sanità, produzione, energia [NAT20]). Questo dettaglio è sottolineato anche in [AHE21], dove gli autori sottolineano la fattibilità della tecnologia per i vari scenari applicativi dell'Industria 4.0. Le sue capacità di simulazione consentono, ad esempio, di fornire servizi interessanti che altre tecnologie da sole non sarebbero in grado di offrire, come la manutenzione predittiva, il monitoraggio in tempo reale, il controllo remoto, l'ottimizzazione dei processi, la gestione della sicurezza, l'analisi e il monitoraggio dei guasti, la valutazione della strategia, monitoraggio sanitario, gestione dei rischi, formazione e cybersecurity.

In linea con quanto sopra, questo documento tecnico ECSO esplora la definizione di base di Digital Twin, i suoi limiti e dipendenze tecniche e presenta alcuni dei casi d'uso e delle sfide che attualmente la tecnologia deve affrontare, in particolare nel settore della sicurezza informatica. Va notato che il rapporto in sé non intende fornire una ricerca esaustiva sull'argomento in questione, ma piuttosto illustrare lo stato attuale della tecnologia e la sua domanda dal punto di vista della ricerca e dell'industria.

2. Casi d'uso generali

Come affermato in precedenza, un DT è una rappresentazione digitale di un oggetto o sistema reale, che viene aggiornata da dati in tempo reale, modelli di apprendimento automatico, modelli di specifica e ragionamento per aiutare il processo decisionale. In altre parole, un DT crea un modello digitale altamente complesso che è la replica di un oggetto fisico. Questa sinergia cyber-fisica implica che le copie virtuali (composte principalmente da pezzi di proprietà intellettuale come protocolli di proprietà, configurazioni, informazioni sulla topologia, componenti software, ecc.) rappresentano risorse fisiche del mondo reale, dove comportamenti, proprietà e stati sono rigorosamente simulati da l'aereo virtuale. Esistono già diverse applicazioni che fanno uso di DT e per diverse tipologie di scenari applicativi, quali: business, istruzione, industria e cybersecurity.

2.1.Caso d'uso n. 1: affari

L'uso di architetture o framework basati su DT nella modellazione aziendale consente ai decisori di prendere decisioni basate su dati reali e consapevolezza della situazione. In particolare, l'utilizzo della tecnologia per simulare flussi e processi aziendali consente di introdurre soluzioni nuove o modificate per garantire maggiore efficienza. La visione è quella di implementare il DT come processo complementare piuttosto che aggiungere barriere e punti di controllo, dove la tecnologia aggiungerà preziose informazioni e set di strumenti. In tal modo, i problemi di sicurezza o di prestazioni aziendali verrebbero rilevati e risolti nelle prime fasi del ciclo di vita.

Per funzionare correttamente, la modellazione aziendale deve implementare e analizzare costantemente processi e tecnologie (fili). A tal fine, i sistemi aziendali critici devono essere replicati nell'ambiente di simulazione attraverso l'orchestrazione e la fornitura di infrastrutture e servizi. Le attuali operazioni aziendali in cui è possibile applicare i DT sono solitamente basate su infrastrutture IT e OT, con il potenziale coinvolgimento di più cloud. L'ambiente DT deve mantenere la mappa degli elementi utilizzati nell'infrastruttura di produzione e consentire il provisioning, la riconfigurazione e lo smantellamento automatizzati di tali elementi e la loro assegnazione ai ruoli all'interno del sistema nel suo complesso.

L'energia è un esempio di ambito applicativo in cui la sicurezza delle infrastrutture e quella del business sono strettamente interconnesse. Mappando l'intera infrastruttura elettrica e collegando gli asset critici agli operatori del business (sia gestori dei sistemi di trasmissione che operatori delle reti di distribuzione) attraverso i DT, è possibile identificare e analizzare potenziali compromissioni e malfunzionamenti del sistema che potrebbero avere un impatto significativo sul business. Questo approccio consente inoltre di valutare il ritorno sull'investimento di potenziali misure di mitigazione, consentendo una valutazione accurata di quanto bene proteggano l'infrastruttura e, di conseguenza, il business. Il progetto di ricerca CyberSEAS [CYB24] approfondisce questo aspetto.

Il sistema DT supporterà la gestione automatizzata dei sistemi replicati, distribuirà, aggiornerà, riconfigurerà e rimuoverà applicazioni e sistemi nell'infrastruttura simulata. Affinché ciò sia sostenibile non è necessario solo un sistema di riferimento, ma una biblioteca digitale che racconti i componenti del sistema insieme agli indicatori chiave di prestazione (KPI) operativi dell'azienda.

2.2.Caso d'uso n.2: istruzione e competenze

"Dimmi e dimentico, insegnami e potrò ricordare, coinvolgimi e imparo". Benjamin Franklin.

La convenienza e l'accessibilità delle gamme cibernetiche e degli ambienti di simulazione aumentano l'integrazione delle tecnologie DT nei programmi di formazione e istruzione. Secondo diversi studi, l'apprendimento basato sulla simulazione migliora la motivazione, l'auto-responsabilità per l'apprendimento, facilita l'apprendimento tra pari e migliora l'attività di apprendimento complessiva, oltre a fornire conoscenza pratica.
Durante l'ascesa dell'apprendimento online, è diventato ulteriormente chiaro che l'apprendimento basato sulla simulazione contribuisce a ricreare l'esperienza sociale della classe, con impegni in classe più improvvisati.

L'implementazione dei DT riduce i tempi e i costi associati alla costruzione e alla messa in servizio di nuovi sistemi. In aggiunta a quanto sopra, va sottolineato che l'attrezzatura fisica è costosa e necessita di spazio per essere immagazzinata e il processo di apprendimento è solitamente lento. I DT forniscono un mezzo/strumento altamente flessibile, poiché il numero di macchine e servizi connessi è facile da regolare sia nella natura che nei numeri rispetto alla loro controparte fisica. Inoltre, la tecnologia DT rende possibile la migliore esperienza di apprendimento immersivo. Utilizzando un DT, i partecipanti possono apprendere compiti altamente coinvolgenti, sperimentare attività pratiche realistiche che possono essere troppo pericolose, complesse o costose per essere eseguite nel mondo reale. Invece della sperimentazione pratica, ad esempio, di un vero impianto manifatturiero o nucleare, i partecipanti possono utilizzare un DT del sistema reale e dei suoi componenti per esercitare le proprie capacità.

Lo sviluppo di competenze virtualizzate basato su DT consente un'esperienza di formazione personalizzata, poiché ciascun partecipante può concentrarsi sul segmento o sulla parte del quadro generale a cui vorrebbe partecipare o che deve comprendere in base al proprio profilo lavorativo. Lo sviluppo delle competenze basato sul Digital Twin può comportare un'esperienza di apprendimento basata sulla realtà virtuale o aumentata (V/AR), ottenendo il massimo coinvolgimento attraverso la lettura rapida di concetti astratti. Inoltre, l'ambiente di simulazione offre l'opportunità di eseguire simulazioni in modo sicuro e di sperimentarne l'impatto. I comportamenti del sistema possono essere esplorati in diverse condizioni, comprendendo guasti o parametri del sistema senza mettere in pericolo apparecchiature costose, operazioni aziendali o vite umane.

Pertanto, mentre le gamme informatiche e le attività connesse di sviluppo delle competenze informatiche offrono già capacità di sperimentazione pratica con sistemi simulati, DT ha un enorme potenziale nello sviluppo di abilità e competenze che operano sistemi reali e comprendono il loro comportamento utilizzando dati e simulazioni in tempo reale.

2.3.Caso d'uso n.3: industria collaborativa (4.0/5.0)

Una delle sfide dell'Industria 4.0 è il modo in cui la tecnologia modifica il ruolo dei lavoratori umani, che diventa una collaborazione con i robot in officina, piuttosto che attività manuali o attività automatizzate supervisionate da operatori umani [WAN17]. Al contrario, il concetto di Industria 5.0 fornisce un focus diverso ed evidenzia l'importanza della ricerca e dell'innovazione per sostenere l'industria nel suo servizio a lungo termine all'umanità entro i confini planetari. Una delle transizioni paradigmatiche più importanti che caratterizzano l'Industria 5.0 è lo spostamento dell'attenzione dal progresso guidato dalla tecnologia a un approccio completamente incentrato sull'uomo.

Il comportamento umano nella sfera digitale è stato affrontato mediante sofisticate tecniche di rilevamento note come User and Entity Behavior Analysis (UEBA) [RAG20]. Tuttavia, comprendere una catena di eventi che rivelano modelli comportamentali umani nelle sfere informatiche e fisiche rimane una sfida irrisolta. L'integrazione della modellizzazione del comportamento umano nel DT consentirà il perfezionamento della progettazione di fabbrica sia dal punto di vista delle prestazioni che della resilienza [ZAD16].

Il concetto di DT umana è stato affrontato in precedenza in letteratura. Ad esempio, Bao *et al.* [BAO19] considerano il DT come un metodo o strumento da utilizzare nella simulazione e nella modellazione del comportamento e dello stato delle entità. Graessler e Poehle [GRA17] hanno sviluppato un DT che assume compiti di comunicazione e coordinamento dei dipendenti con il sistema produttivo. Il concetto abituale di un DT che emula le proprietà e il comportamento di un sistema è stato adattato dagli autori per fungere da rappresentante di un dipendente umano in un sistema di produzione ciberfisica (CPPS), poiché la proprietà e il comportamento del DT umano necessitano basarsi sul feedback degli utenti e sui modelli registrati invece che sui dati misurati effettivi. Buldakova e Suyatinov [BUL19] hanno anche sviluppato modelli per valutare lo status dell'operatore umano nei sistemi cyber-fisici. Questi modelli vengono utilizzati per valutare lo stato funzionale degli operatori umani. In [EC20a] l'idea è di considerare un DT multi dominio, in cui il comportamento umano è monitorato per mezzo di sensori non intrusivi, che raccolgono dati sul comportamento umano per supportare modelli digitali. Va notato a questo punto che anche il comportamento emotivo umano viene preso in considerazione e contribuisce al raggiungimento degli obiettivi di sicurezza.

2.4.Caso d'uso n.4: sicurezza informatica industriale

CyberFactory#1 (ITEA4 17032) Obiettivo del progetto è l'ottimizzazione e la resilienza delle Fabbriche del Futuro1 . Coordinato da AIRBUS Cyber Security France, uno degli obiettivi di CyberFactory#1 è stato quello di dimostrare le ipotesi formulate da [BEC18] e [BEC20] secondo cui DT può supportare efficacemente l'applicazione della sicurezza, in particolare nelle fasi di progettazione, messa in servizio ed esecuzione di un progetto programma di digitalizzazione industriale.

Airbus Defence and Space (ADSS) possiede diversi stabilimenti in Spagna, Tablada, San Pablo Sur e Cadice, dedicati alla produzione e all'assemblaggio finale di aerei commerciali e militari [AIR21]. ADSS ha lanciato un importante programma di trasformazione digitale che si basa sull'implementazione di una piattaforma IIoT multi-sito e multi-asset per supportare una maggiore automazione, ottimizzazione e controllo di qualità sui processi industriali sensibili coinvolti nella produzione di parti aeronautiche critiche per la sicurezza del volo.

Un DT, supportato dalla piattaforma Airbus CyberRange, è stato sviluppato per tre casi d'uso. Uno di questi è legato al sistema Roboshave, implementato nello stabilimento di Tablada per automatizzare le operazioni di rasatura dei rivetti sui timoni del Boeing 737 [BOE21]. Il sistema RoboShave potrebbe essere descritto come un braccio robotico il cui ruolo è quello di radere i rivetti del timone e di verificare automaticamente che l'operazione di rasatura sia stata eseguita con successo. Il DT include tutte le risorse fisiche, come il robot FANUC M-20iA/35M, il profilometro Gocator 2120 e i controllori logici programmabili (PLC), nonché la connettività del sistema e i diversi protocolli necessari, come il collegamento S7Comm, ModbusTCP e il simulatore Airbus CyberSecurity (Profilometro) e Profinet. Diversi protocolli in uso all'interno

[1] https://itea4.org/project/cyberfactory-1.html

questo elenco non era supportato dalle soluzioni del fornitore, come il livello Profinet che è stato sviluppato da Airbus CyberSecurity e supporta alcune funzionalità risultanti dalle specifiche indicate in IEC 61158-5-10 e IEC 61158-6-10 [5]. Ad esempio, **Errore! Fonte di riferimento non trovata.** UN
secondo **errore! Fonte di riferimento non trovata.** illustrare il sistema fisico Robotshave e il suo DT.

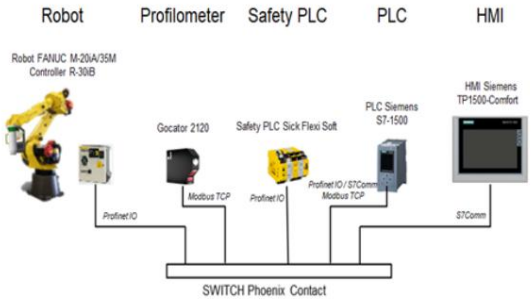

Figura 1. Panoramica della connettività del sistema Roboshave [PRA22]

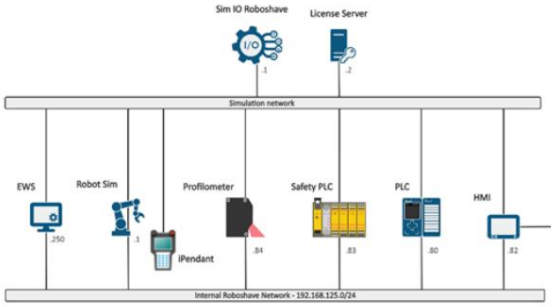

Figura 2. Visualizzazione della topologia di Roboshave DT [PRA22]

Sulla base dell'analisi del rischio, sono stati definiti e implementati nell'ambiente di simulazione [PRA22] i seguenti scenari di attacco: (1) compromettere il funzionamento di Roboshave rimuovendo la connettività tra asset (perdita di controllo dal punto di vista dell'operatore, sull'HMI); (2) scrivere nelle variabili interne dell'HMI per visualizzare informazioni errate (queste verranno segnalate nella Rete Corporativa); generare dispositivi IIoT non autorizzati accessibili tramite software legacy; e manipolare gli ordini di lavoro da un GapGun aggiungendo, modificando ed eliminando configurazioni.

3. Architetture e Tecnologie per i DT

In letteratura esistono già diversi approcci basati su DT, sia attraverso architetture che framework, con l'obiettivo di favorire lo sviluppo di soluzioni DT specifiche. A tal fine, esaminiamo la letteratura per mostrare il grande boom tecnologico e l'interesse dell'industria e del mondo accademico nel lanciare soluzioni tecnologiche basate su DT nei prossimi anni.

Pertanto, in questa sezione, presentiamo innanzitutto alcune architetture e framework, progettati principalmente da organizzazioni ed enti accademici. Successivamente, menzioniamo alcune soluzioni commerciali e open source per sviluppare approcci o applicazioni DT.

3.1.Architetture e framework basati su DT

Nonostante i recenti sforzi da parte delle organizzazioni internazionali, non esiste un riferimento chiaro o un'architettura standard di Digital Twin Network (DTN) generalizzata per ogni scenario di sistema informativo. Sulla base della definizione degli elementi chiave del DTN discussi, l'architettura di riferimento formalizzata più interessante è quella descritta in [ZHO21] dall'IRTF (Internet Research Task Force). Questa architettura mira a generalizzare il concetto di Digital Twin Architecture (come illustrato anche in Figura 1) per i DTN, la cui costruzione è molto simile a quella proposta dallo standard ISO 23247-2 in [ISO21b] per i sistemi di produzione. A loro volta, e sulla base di questo tipo di architetture di riferimento, esistono già lavori correlati che propongono il concetto di DT in scenari specifici.

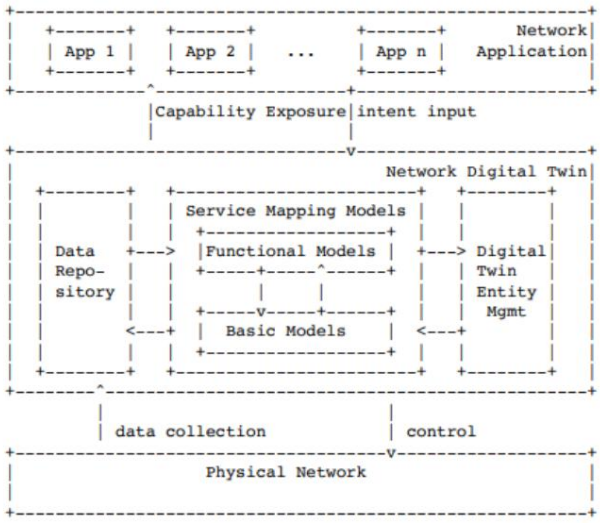

Figura 1. Architettura di riferimento DT definita dall'IRTF in [ZHO21]

I lavori correlati, presentati in [RED19, TAO17, ZHE19, YUQ20, JIE20], propongono architetture di riferimento per l'applicazione dei DT a domini specifici, quasi esclusivamente connessi al settore manifatturiero. In queste proposte, il Digital Twin è principalmente un raccoglitore di informazioni provenienti dall'impianto fisico, sfruttate per la simulazione, la previsione, la connessione ad applicazioni aziendali disparate e l'archiviazione di dati. Viene considerato un feedback molto limitato dal DT al sistema fisico, soprattutto in termini di applicazione delle impostazioni calcolate con algoritmi di ottimizzazione sul DT.

Dei lavori sopra elencati, solo [RED19] riconosce esplicitamente la sicurezza come una questione chiave per i sistemi cyber-fisici, attraverso un'architettura a sei livelli (L1: dispositivi fisici, L2: fonti di dati per il sistema fisico, L3: repository di dati locali, L4 : Gateway IoT, L5: archivi di informazioni basati su cloud, L6: emulazione e simulazione). Tuttavia, la discussione di questo argomento è limitata agli aspetti convenzionali della protezione delle informazioni e delle comunicazioni, della codifica sicura e della corretta implementazione dell'AAA (Autenticazione, Autorizzazione e Contabilità). Non viene fatta menzione dei rischi specifici derivanti dall'integrazione di DT nel sistema.

Tuttavia, prendendo come riferimento l'architettura e i lavori appena discussi, si può osservare che esistono numerose somiglianze con quelle architetture basate su Software Defined Network (SDN).
In effetti l'approccio è sostanzialmente lo stesso: separare il livello fisico dal livello di controllo, dal livello applicativo. È quindi possibile a questo punto virtualizzare le tecnologie e gestirle a livello di controllo, secondo le esigenze del livello applicativo. Il vantaggio principale di questo approccio è che tutta la logica principale dell'architettura si riduce al processo di orchestrazione delle tecnologie coinvolte (virtualizzazione). Questa orchestrazione presenta quindi diversi vantaggi: (i) flessibilità nell'uso di tecnologie eterogenee, (ii) riconfigurazione dinamica di uno scenario e (iii) portabilità.

Considerando le caratteristiche dell'SDN, l'IRTF presenta anche in [HAL15] il rapporto tecnico *"Software-Defined Networking (SDN): Layers and Architecture Terminology",* inclusa un'architettura SDN di riferimento. Da tale specificazione si può notare che i livelli/piani possono essere collocati con altri piani oppure possono essere fisicamente separati. L'SDN si basa sul concetto di separazione tra un'entità controllata e un'entità titolare. Il controller manipola l'entità controllata tramite un'interfaccia. Le interfacce, quando locali, sono per lo più invocazioni API (Application Programming Interface) tramite alcune librerie o chiamate di sistema. Tuttavia, tali interfacce possono essere estese tramite alcune definizioni di protocollo, che possono utilizzare la comunicazione interprocesso locale (IPC) o un protocollo che potrebbe anche agire in remoto; il protocollo può essere definito come uno standard aperto o proprietario

maniera.

Sulla base dell'analisi di questa architettura di riferimento basata su SDN, siamo quindi in grado di isolare e spiegare i componenti principali di un'architettura DT. I loro componenti principali sono classificati in livelli, che corrispondono agli strati che l'architettura DT espone agli utenti in [ZHO21].
Ciascuno di questi livelli ha un risultato e uno scopo specifici e può essere riassunto in tre livelli principali: *fisico, rete* e *applicazione.* Di seguito e per ciascuno di questi livelli, discuteremo i blocchi fondamentali.

- Il **livello fisico** distribuisce tutti quegli elementi di rete che scambiano dati di rete in massa e controllano con l'entità DT di rete, attraverso interfacce in direzione sud. In questo livello i componenti più importanti sono i wrapper dei protocolli di comunicazione. Il livello fisico virtualizza i componenti di rete della controparte fisica. Per questo motivo, deve essere in grado di emulare anche i protocolli di rete utilizzati in tale ambiente di virtualizzazione. A questo livello, il DT deve fornire un protocollo gateway di rete in grado di consentire la comunicazione all'interno del livello fisico.

- Il **livello di rete** è ovviamente la parte principale dell'architettura e comprende tre sottosistemi: Data Repository, Service Mapping Models e DT Entity Management.

    o Data Repository: fornisce informazioni accurate e complete sulla rete e sui suoi componenti per la costruzione di vari modelli di servizio mediante raccolta e aggiornamento

i dati operativi in tempo reale di vari elementi della rete attraverso l'interfaccia in direzione sud.

o Modelli di mappatura dei servizi: completa la modellazione dei dati, fornisce istanze del modello di dati per varie funzionalità di rete e massimizza l'agilità e la programmabilità dei servizi di rete.

o DT Entity Management: completa la funzione di gestione DTN, registra il ciclo di vita dell'entità, visualizza e controlla vari elementi della rete DT, inclusa la gestione della topologia, la gestione dei modelli e la gestione della sicurezza.
A questo livello, tra le componenti principali che possiamo identificare vi è un servizio di monitoraggio delle attività in grado di tracciare tutti i compiti e le funzioni all'interno del DT; un servizio di estrazione dati, in grado di analizzare e visualizzare i dati sia delle attività di monitoraggio che del repository dati; un servizio di gestione, che traccia i diversi agenti all'interno del DT in base al loro livello di privilegio.

- Il **livello applicativo,** che solleva requisiti che devono essere affrontati dal DTN.
Tali requisiti vengono scambiati attraverso un'interfaccia in direzione nord; quindi il servizio viene emulato da varie istanze del modello di servizio. Una volta verificate, le modifiche possono essere implementate in modo sicuro nella rete fisica. Si noti che in questo livello, la comunicazione in direzione nord rappresenta il principale collo di bottiglia/sfida. Le applicazioni a livello di rete devono essere distribuite senza la necessità di aggiungere wrapper o gateway aggiuntivi. Per questo motivo, il componente principale deve essere il servizio di distribuzione dell'applicazione, che ha il compito di associare correttamente l'applicazione all'API corrispondente del livello di rete.

Come accennato in precedenza, la rappresentazione di tutti questi strati descritti può essere vista nella Figura 1 [ZHO21], che illustra il principale riferimento IRTF per i DT.

Altri modelli di riferimento

Nonostante la mancanza di standardizzazione dell'architettura dei DT, basata sulla descrizione a strati e sui componenti principali da noi forniti, è anche possibile raccogliere alcuni contributi scientifici riguardanti le applicazioni verticali dei DT. Entrambi questi contributi hanno in comune l'approccio stratificato dell'architettura, quindi l'implementazione dei componenti principali, personalizzati per le loro specifiche esigenze. Questi contributi sono riepilogati nella Tabella 1 seguente.

Ai fini della presente Relazione Tecnica, è illuminante notare che tutte le opere citate, ad eccezione di due, non menzionano mai la sicurezza.

Tabella 1. Altri modelli DT di riferimento dell'Accademia

Modelli DT di riferimento accademico	Le loro descrizioni
Architetture basate su DT per integrare CPS con componenti cloud [ALA17]	Gli autori propongono una descrizione analitica di un modello di riferimento dell'architettura Digital Twin per i sistemi cyber-fisici (C2PS) basati sul cloud, in cui ogni cosa fisica accompagna una cosa cyber ospitata nel cloud. Due cose possono stabilire il peer-to-peer (P2P)

	connessioni tramite comunicazioni fisiche dirette o tramite connessioni DT indirette basate su cloud. Nel modello proposto, ogni cosa fisica è rappresentata da un DT basato su cloud, virtualizzandone i sensori, le interfacce, gli elementi computazionali e di archiviazione, ecc. La combinazione dei due può dare vita a un oggetto ibrido che, presupponendo una comunicazione di rete trascurabile costo, può eseguire qualsiasi operazione sul componente (reale o virtuale) più adatto a svolgerlo. Inoltre, il modello considera le diverse modalità di reazione agli eventi, che coinvolgono l'interazione diretta fisico-fisico, gemello-gemello o fisico-gemello, e propone un meccanismo sensibile al contesto per consentire alle cose di scegliere autonomamente quale adottare. Il modello può essere esteso gerarchicamente per costruire sistemi di sistemi.
Un'architettura di sicurezza del sistema di controllo e automazione industriale basata su DT [GEH20]	In questo lavoro, gli autori discutono come utilizzare un modello di replica DT e la corrispondente architettura di sicurezza per consentire la condivisione dei dati e il controllo dei processi critici per la sicurezza. Vengono identificati i requisiti di sicurezza che guidano la progettazione per la condivisione e il controllo dei dati basati su DT. Gli autori hanno dimostrato che il progetto di sincronizzazione degli stati proposto soddisfa i requisiti di sincronizzazione dei gemelli digitali previsti e fornisce una progettazione e una valutazione di alto livello di altri componenti di sicurezza dell'architettura. Uno sviluppo importante in questo documento è rappresentato dal componente gateway di rete sviluppato per emulare la comunicazione del traffico PLC a livello fisico.
Un'architettura DT basata sulla tecnologia IIoT [SOU19]	In questo lavoro, gli autori propongono un'architettura DT, applicando le tecnologie IIoT per rilevare e attuare sulla controparte fisica e utilizzando il protocollo di comunicazione OPC-UA per strutturare e scambiare dati unificati e fornire servizi per gestire ed elaborare i dati della controparte digitale della sistema.
Il concetto di DT come servizio [AHE21]	La proposta DT è stata introdotta per conciliare l'applicazione (solitamente rigida) delle tecniche di virtualizzazione alla produzione con la necessità di una massiccia personalizzazione individuale, come promesso dal movimento Industria 4.0. Il modello concettuale di riferimento proposto per raggiungere questo risultato è composto da tre strati (fisico, digitale,

	e cyber) e un modello di comunicazione per scambiare dati tra loro. Lo strato fisico definisce i mezzi degli attributi reali, comprese risorse come oggetti, beni, prodotti, personale, attrezzature, strutture, sistemi, processi, ambiente o "cose" che hanno un'esistenza materiale nel mondo fisico. Lo strato digitale è la registrazione di dati in formati di file grezzi o diversi come Computer Aided Design (CAD) o Computer-Aided Manufacturing (CAM) per supportare la creazione, modifica, analisi, ottimizzazione o previsione di un modello statico, dinamico e dati in tempo reale. Esiste un collegamento bidirezionale con lo strato fisico per rendere possibile la modellazione e la simulazione. Il livello informatico include l'elaborazione e l'archiviazione nel cloud per la creazione di un modello di dati dinamico, che può abilitare funzionalità digitali su larga scala. Inoltre, il modello dati crea informazioni, conoscenza e saggezza (DIKW) utilizzando IoT, Big Data e tecnologie cloud.
Mobility DT: concetto, architettura, caso di studio e sfide future [WAN22]	In questo studio viene sviluppato un framework Mobility DT (MDT), definito come un framework per dispositivi cloud-edge basato sull'intelligenza artificiale per i servizi di mobilità. Questo MDT è costituito da tre elementi costitutivi nello spazio fisico (vale a dire umano, veicolo e traffico) e dai relativi DT associati nello spazio digitale. Viene creata un'architettura cloud edge di esempio per accogliere il framework MDT proposto e per soddisfare le sue funzionalità digitali di archiviazione, modellazione, apprendimento, simulazione e previsione A conferma di quanto appena presentato, un recente articolo su [QIA22] mostra una revisione delle architetture del DT, della rappresentazione dei dati, dei protocolli di comunicazione. Gli autori affermano che non esiste uno standard chiaro per tali architetture, ma hanno descritto un pool di diversi componenti del protocollo di rete che è stato sviluppato per emulare lo scenario reale all'interno di una replica DT. Questo lavoro indica una reale tendenza su quali sono le sfide nel mondo DT.

3.2.Soluzioni tecnologiche per l'implementazione dei DT

Finora esistono poche soluzioni software commerciali che implementano la tecnologia DT, sviluppate principalmente da grandi aziende del settore manifatturiero. La tabella 2 mostra un elenco non esaustivo della tecnologia DT dei fornitori più diffusi.

Tabella 2. Soluzioni commerciali disponibili per implementare i DT

Commerciale disponibile soluzioni da implementare DT, venditori	**Le loro descrizioni**
soluzione DT, General Electric (GE)	Un DT avanzato e funzionale che integra modelli analitici per i componenti della centrale elettrica che misurano lo stato di salute, l'usura e le prestazioni degli asset. Il DT è integrabile nella piattaforma distribuita Predix sviluppata da GE per "elaborazione, gestione e analisi dei dati macchina su larga scala" e applicazioni IIoT [ELE22].
PTC Windchill, PTC	Un DT che consente ai produttori di tutti i settori di comprendere come i loro clienti utilizzano i loro prodotti. In questo modo, possono aiutarli a migliorare la progettazione e le prestazioni di tali prodotti [PTC22].
3DS, Dassault Systèmes	Un DT che consente ai produttori di rendere disponibili al mercato prodotti virtuali per la sperimentazione e il test in condizioni realistiche prima di impegnarsi in qualsiasi produzione reale [KAR22].
soluzione DT, Seebo	Si tratta di un'interfaccia grafica che consente la generazione di informazioni utili che massimizzano l'efficacia complessiva delle apparecchiature, riducono i tempi di inattività non pianificati e scoprono la causa principale dei problemi. I dashboard consentono la visualizzazione in tempo reale dello stato operativo delle macchine distribuite e visualizzano avvisi arricchiti con metriche predittive basate sui parametri chiave della macchina, come temperatura, pressione, vibrazione, umidità, fatica e usura della macchina, al fine di identificare e risolvere rapidamente i problemi da remoto [VEDI22].
Strumenti e soluzioni SW di modellazione di simulazione, Qualsiasilogico	Il software Anylogic fornisce funzionalità di simulazione in un unico pacchetto commerciale con licenze di ricerca speciali disponibili. È specializzato in fabbriche e linee di produzione, con capacità di simulazione di eventi discreti e dispone di librerie in grado di supportare diversi tipi di campi [ANY22].
soluzione DT, Ansys	Un DT che può essere utilizzato per monitorare l'analisi prescrittiva in tempo reale e testare la manutenzione predittiva per ottimizzare le prestazioni degli asset. Il DT può anche fornire dati da utilizzare per migliorare la progettazione fisica del prodotto durante l'intero ciclo di vita del prodotto [ANY22a].
quadro DT, IBM	Il framework consente alle aziende di creare, testare, costruire e monitorare virtualmente un prodotto, riducendo la latenza nel ciclo di feedback

	tra progettazione e funzionamento. Consente di identificare e risolvere i problemi e di portare i prodotti sul mercato più velocemente [IBM22].
servizio IoT, Microsoft Azure digitale Software gemello	Servizio IoT che replica virtualmente il mondo fisico modellando le relazioni tra persone, luoghi e dispositivi in un grafico di intelligenza spaziale [AZU22].
I/O di fabbrica, Giochi veri	Si tratta di un software [FAC20] che consente di impostare simulazioni 3D configurabili inserendo componenti di un determinato catalogo di apparecchiature industriali. A tal fine il software prevede aspetti di simulazione dei DT, la sincronizzazione esplicita tra sistema reale e replica virtuale è limitata all'integrazione di più PLC per testare simulativamente la fabbrica virtuale.
Servizi di sviluppo SW per realizzare soluzioni DT, Siemens	Questi servizi includono un'interfaccia uomo-macchina [WAN19] che può essere utilizzata per la costruzione di una DT per l'uomo e un portafoglio denominato Digital Enterprise Suite [SIE20], che comprende, ad esempio, DT per attrezzature di trasporto materiale.

A differenza dei prodotti proprietari, le soluzioni open source consentono alla tecnologia di essere liberamente ridistribuibile e modificabile, aiutando i produttori a combinare apparecchiature legacy con moderne macchine e strumenti basati su sensori di diversi fornitori. In questo caso, identifichiamo una serie di framework disponibili, elencati nella Tabella 3.

Tabella 3. Soluzioni open source disponibili per implementare i DT

Soluzioni open source disponibili per implementare i DT	**Le loro descrizioni**
Gemellaggio CPS	È un framework per generare ed eseguire DT che rispecchiano i CPS [CPS22]. In particolare, CPS Tnning è una prova di concetto che può essere utilizzata come primo approccio per modellare alcuni ambienti, ma presenta anche alcune limitazioni come l'impossibilità di generare DT per dispositivi wireless [ECK18].
Wrld3d	Si tratta di una piattaforma open source che consente la creazione di DT in modo semplice e veloce, utilizzando un set completo di strumenti self-service, kit di sviluppo software (SDK), API e servizi di localizzazione intelligente. Essendo una piattaforma di mappatura 3D dinamica, consente di creare ambienti virtuali interni ed esterni su cui i dati provenienti da sensori, sistemi, dispositivi mobili e servizi di localizzazione possono essere visualizzati con precisione millimetrica [WRL22].

Mago3D	È una piattaforma per la visualizzazione di oggetti 3D massicci e complessi, incluso il Building Information Modeling (BIM) su un browser web. Pertanto, è possibile modellare DT che creano mondi paralleli in una realtà virtuale con diversi sensori [SHI19].
i-Manutenzione	Si tratta di un toolkit che consente di creare un DT di un asset industriale al fine di ottenere informazioni sullo stato di tutti i componenti legati alla produzione e alla manutenzione del processo industriale, raccogliere, monitorare e analizzare i dati del ciclo di vita. È composto da un sistema di messaggistica, una serie di adattatori per integrare sistemi di sensori/attuatori e altri componenti software utilizzati come base tecnica per lo sviluppo di DT [STR18].
Eclissi Idem	È un DT sviluppato da Bosch. Consente la progettazione di DT sotto forma di modelli di sviluppo IoT. Può essere visto come uno strato fondamentale open source della piattaforma IoT di Bosch [ECL22].
imodel.js	È una piattaforma per creare, accedere, sfruttare e integrare DT. Come accade con Eclipse Ditto, si tratta di un'iniziativa commerciale legata alla società di infrastrutture statunitense Bentley. Secondo gli sviluppatori è stato progettato per essere flessibile e aperto, in modo che possa essere facilmente utilizzato e integrato con altri sistemi [CRE22].

All'intersezione tra la pura tecnologia DT proprietaria e la vera tecnologia DT open source, le soluzioni open source sono sviluppate da grandi aziende, che le rendono limitate nella portata, a causa degli interessi commerciali degli sviluppatori [ROE19].

Per riassumere le tecnologie citate, la Tabella 4 mostra le diverse tecnologie DT in base ai termini e alle condizioni del loro utilizzo, ad esempio se si tratta di soluzioni open source, aperte/commerciali limitate, prodotti commerciali o prototipi. Con questo mostriamo anche l'influenza e l'interesse di questa nuova tecnologia nel mercato odierno e come faccia parte degli interessi di molte organizzazioni e aziende.

Tabella 4. Raggruppamento delle tecnologie sopra menzionate in base ai termini e alle condizioni di utilizzo

Tipo	Soluzioni
Open Source	*Mondo3d; Mago3D; i-Manutenzione*
Eclipse ***aperto/ commerciale limitato***	Idem; *imodel.js*

Prodotti commerciali	*PTC Windchill; I/O di fabbrica; Struttura del gemello digitale IBM; SIEMENS Digital Enterprise Suite; Gemello digitale di Microsoft Azure; Qualsiasilogico; Ansis; Gemello digitale GE*
Prototipi	*Gemellaggio CPS*

4. Dichiarazione del problema della sicurezza informatica

DT è una tecnologia emergente in grado di virtualizzare e simulare le risorse del mondo fisico per potenziare azioni di ottimizzazione innovative in molti dei domini applicativi odierni. Attraverso la verifica e la validazione, è possibile migliorare diverse azioni e processi operativi, quali attività di automazione, logistica e persino aspetti relativi alla manutenzione, resilienza e sicurezza informatica di prodotti, processi o sistemi. Ma il DT può essere anche uno strumento efficace per il processo decisionale, e soprattutto nel campo della sicurezza informatica, dove è necessario anticipare potenziali minacce e rispondere di conseguenza. Il presente documento pone quindi una forte enfasi sugli aspetti di protezione e cybersecurity, sia in termini di operatività delle infrastrutture critiche che del sistema DT stesso.

I DT possono infatti essere visti come una tecnologia in grado di ottimizzare i processi, prevedere guasti e rilevare situazioni anomale. Se queste capacità vengono estese alla sicurezza informatica [GE22], allora è possibile prevenire e mitigare potenziali attacchi informatici come le minacce persistenti avanzate (APT) [HOL21]. In [HOL21], gli autori affrontano le potenziali capacità del paradigma di coprire molte delle sfide odierne della sicurezza informatica, esplorando le opportunità per modellare le minacce, testare, rilevare e mitigare le situazioni. Queste capacità possono anche aumentare la consapevolezza situazionale di un'organizzazione fornendo un quadro migliore della situazione e spiegando, continuamente e in tempo reale, lo stato attuale delle controparti fisiche coinvolte, e in termini di vulnerabilità, potenziali exploit e/o rischi.

Nonostante quanto sopra, e sebbene la tecnologia DT offra all'Industria 4.0/5.0 nuove opportunità per creare ecosistemi digitali sicuri e più resilienti (riducendo potenziali rischi che possono compromettere seriamente la qualità e il benessere di molti settori e infrastrutture strategici in Europa), non c'è ancora abbastanza ricerca e lavoro in questo settore. Ad esempio, manca un supporto dedicato per la protezione del cyberspazio di un dispositivo DT, in cui più componenti IT, che dettagliano la natura dei beni fisici (ad esempio, configurazioni di proprietà, proprietà intellettuale (IP), protocolli di proprietà industriale, connessioni , ecc.) – sono ampiamente diffusi. Se a questo punto le misure di protezione non vengono adeguatamente considerate, possono sorgere molteplici problemi di sicurezza: (a) a livello IT (con rischi per la riservatezza, l'integrità e la disponibilità dei dati) – *mondo cibernetico* -; (b) a livello OT (con rischi per la disponibilità operativa e l'integrità dei dati) – *mondo fisico* -; e (c) a livello di comunicazione.

Ne consegue che la superficie di attacco DT può essere ampia e significativa per molti degli ecosistemi e delle infrastrutture supportati o basati su DT, probabilmente a causa delle interrelazioni IT-OT tra gli spazi [ALC22].

Pertanto, il documento tecnico dell'ECSO si concentra principalmente sull'affrontare e discutere due questioni rilevanti di sicurezza informatica:

- ***Come utilizzare il Digital Twin per la protezione*** di altre infrastrutture e sistemi.
- ***Come proteggere il Digital Twin e l'accesso ai suoi modelli*** per assicurarne le principali funzioni senza mettere a rischio la sicurezza di un'infrastruttura e del suo IP.

5. Gemelli digitali per la sicurezza informatica

Attraverso le specifiche digitali, i DT sono in grado di creare opportunità uniche per eseguire simulazioni e test contro attacchi e/o guasti HW/SW, analizzando le possibili conseguenze e impatti, oltre a fungere da laboratorio unico per sviluppare, convalidare e testare approcci di sicurezza e configurazioni per promuovere azioni preventive e di mitigazione efficaci. Queste azioni possono anche essere eseguite parallelamente al sistema stesso in modo da non interromperne i servizi o le funzioni principali

sistema principale. Rispecchiando il comportamento legittimo di dispositivi e servizi all'interno di un'infrastruttura, le funzioni di sicurezza informatica basate su DT implementate dal lato della simulazione non dovrebbero scontrarsi e influenzare i compiti operativi della loro controparte fisica, principalmente perché potrebbero essere eseguite in un ambiente isolato parallelo a quello reale. uno.

Pertanto, le loro capacità di simulazione rendono i DT risorse potenzialmente preziose per le soluzioni di sicurezza informatica. Possono essere utili per:

- monitoraggio e ispezione degli eventi di sicurezza che si verificano nella controparte fisica, a identificare possibili minacce ai propri processi operativi;
- rilevamento di attacchi informatici che tentano di sfruttare le vulnerabilità di un'infrastruttura, per consentire l'adozione di misure di mitigazione; • rilevamento di comportamenti anomali manifestati da dispositivi e servizi, per evitare che vengano compromessi da attacchi zero-day; • simulazione di interi scenari di intrusione, comprese le possibili caratteristiche delle diverse varianti di attacco informatico e il loro impatto sulla sicurezza della controparte fisica; • risposta e ripristino per far fronte ai rischi per la sicurezza offrendo al sistema meccanismi che aiutano ad anticipare le situazioni e fornire misure di mitigazione; • generazione di potenziali fonti di conoscenza su cui applicare tecniche di apprendimento

  migliorare altri servizi di sicurezza informatica (ad esempio rilevamento o risposta); E
- formazione per migliorare la consapevolezza e la conoscenza delle tematiche di cybersecurity e resilienza.

Queste capacità preventive e reattive possono essere fornite sia in modalità offline che online. In [KRI18], Kritzinger *et al.* già menzionate le diverse modalità di costruzione di diverse tipologie di sistemi di simulazione, a seconda del tipo di comunicazione instaurata con l'ambiente fisico. Nel caso particolare di un DT, esso è costruito secondo linee di comunicazione bidirezionali e completamente automatiche, consentendo l'interazione con il mondo reale in modo autonomo e interattivo. Quest'ultima funzionalità consente, attraverso la simulazione, di potenziare la difesa informatica online attraverso soluzioni ibride più complete, dove è possibile individuare, prevedere e neutralizzare le minacce che possono corrompere il sistema reale [GE22].

Sebbene tutte queste funzioni di simulazione possano essere interessanti per diverse comunità, purtroppo si trovano in uno stato molto preliminare dal punto di vista della ricerca, e in particolare nel campo della sicurezza informatica e della resilienza. Come accennato in precedenza, non esiste ancora un approccio standardizzato per la sua implementazione nelle reti IT-OT, né esistono risultati di ricerca affidabili che determinino il grado di realismo e fedeltà per ottenere risultati altamente efficaci. Ma anche in queste circostanze, c'è un grande interesse da parte delle diverse comunità nell'implementazione di soluzioni basate su DT, e in particolare per la difesa informatica online nei diversi scenari applicativi (industria e produzione, trasporti, sanità, catena di fornitura, ecc.).

Il resto di questa sezione discuterà alcuni aspetti dell'utilità della tecnologia per la governance e la gestione del rischio, il rilevamento e la consapevolezza situazionale, la resilienza, la privacy e la formazione, delineando anche alcuni casi d'uso specifici per ciascuna di queste aree applicative. In questo modo, forniamo una panoramica delle attuali capacità che il paradigma può offrire allo stato dell'arte al di là del suo utilizzo convenzionale.

5.1.Gestione e governance del rischio

I DT hanno il potenziale per migliorare radicalmente il modo in cui i rischi informatici vengono identificati, misurati e gestiti all'interno e tra le organizzazioni. Al giorno d'oggi, la governance del rischio informatico si basa principalmente su approcci basati sui processi svolti dai livelli C (ovvero CISO e personale addetto alla sicurezza). Al contrario, le capacità di simulazione offerte dai modelli digitali (su cui si basano i DT) supportano la transizione verso approcci continui e guidati dagli eventi.

Gli eventi che innescano l'esecuzione di nuove valutazioni del rischio includono cambiamenti nel panorama delle minacce informatiche, ad esempio con l'avvento di una nuova minaccia informatica (o fisica), nonché modifiche all'infrastruttura reale, che devono riflettersi in corrispondenti cambiamenti nel DT . In questo contesto, le capacità di simulazione offerte dal modello di un DT potrebbero essere utilizzate per supportare:

- l' **identificazione e la conferma delle vulnerabilità digitali** presenti nella controparte fisica, o che potrebbero apparire come conseguenza di modifiche della controparte fisica;

- la **comprensione della misura in cui queste vulnerabilità possono essere** sfruttate compromettere lo stato e il comportamento della controparte fisica;
- la **simulazione degli effetti a cascata** di potenziali sfruttamenti sul sistema stesso, per comprendere gli impatti su funzioni di livello superiore come privacy, protezione dei dati, sicurezza, continuità operativa e aziendale, ecc.; E
- la **valutazione dell'efficacia dei controlli di cybersecurity "in place" e "to be".** nel diminuire il rischio legato a specifiche tecniche di attacco (es. ransomware), aprendo così la strada a strategie di protezione e gestione più accurate, rispetto alla tradizionale valutazione dei potenziali attacchi e alle strategie di mitigazione, che tipicamente hanno maggiore rilevanza operativa e orizzonte di breve termine.

Pertanto, attraverso la simulazione le organizzazioni possono essere in grado di esplorare, stimare e determinare l'esistenza di vulnerabilità e nuove lacune di sicurezza, anticipando non solo potenziali rischi per la sicurezza informatica ma anche rischi per la sicurezza [HOL21]. Un esempio di quest'ultimo si trova anche in [JAR20], che fornisce un DT in tempo reale del serbatoio dell'idrogeno ad alta pressione per ridurre i guasti e i rischi associati.
Allo stesso modo, il lavoro in [DAN21] presenta l'approccio DT Automatic Network Guardian for ELectrical Systems (ANGEL) per rilevare guasti fisici in un sistema di alimentazione e classificare le aree interessate (IEEE 9-bus e IEEE 39-bus). Ciò significa anche che requisiti essenziali per il funzionamento ottimale dei DT per la valutazione e la gestione dei rischi cyber sono un'adeguata conoscenza del CPS da rappresentare e dei relativi processi, nonché caratteristiche adeguate per descrivere e simulare i rischi cyber con la stessa precisione con cui impatterebbero sul sistema reale.

Un chiaro **esempio applicativo di come i DT possono supportare la resilienza di un CPS è l'assistenza sanitaria.** I dispositivi medici e le loro capacità offrono opportunità senza precedenti per assistere i pazienti da remoto e prevedere tempestivamente diversi tipi di emergenze (ad esempio, arresto cardiopolmonare e respiratorio). Il volume crescente di dati dei pazienti raccolti, trasmessi ed elaborati, nonché il

La pervasività dei dispositivi medici richiede la valutazione e la gestione dei rischi informatici come fattore abilitante dell'innovazione. I DT, creando un modello virtuale e dinamico del sistema, rappresentano una soluzione convincente per considerare attentamente tutte le vulnerabilità di dispositivi, servizi e reti e l'impatto delle relative minacce in termini di prestazioni, privacy e sicurezza. Ciò consente diversi tipi di valutazioni, ad esempio simulando i trasferimenti di dati nella replica virtuale del sistema e ottenendo risultati senza compromettere la controparte fisica. La natura virtuale del DT consentirà inoltre l'applicazione di funzionalità ML avanzate che integrano sistemi di rilevamento delle vulnerabilità statici e dinamici, con un potenziale promettente di rilevamento delle vulnerabilità zero-day e delle varianti.

Un altro esempio concreto è **l'impiego dei DT per scopi di sicurezza nel settore energetico, migliorando la resilienza delle Smart Grid.** I DT svolgono un ruolo importante nel supportare la transizione delle reti verso sistemi cyber-fisici complessi, consentendo di monitorare, condividere e gestire gli scambi di informazioni tra tutti i partecipanti e le parti interessate lungo la catena del valore quasi in tempo reale. Possono specificare efficacemente le dinamiche di interazione tra i nodi del sistema, consentendo di simulare e/o prevedere la causa di una determinata vulnerabilità o guasto, consentendo un'eventuale attuazione preventiva o un'adeguata preparazione. Agendo anche come eccellenti strumenti di formazione, i DT possono essere implementati per simulare una violazione della sicurezza e valutare le capacità di operatori e ingegneri nel riconoscere i sintomi di una compromissione del sistema di controllo e selezionare di conseguenza la migliore azione di mitigazione.

5.2.Modellazione e test dell'attacco

Testare protocolli industriali e/o testare applicazioni di sicurezza in un ambiente isolato e sicuro con le stesse caratteristiche della controparte fisica è una delle principali sfide dei futuri sistemi industriali. Pertanto, in questa sottosezione, vengono presentati alcuni esempi di casi test di scenari industriali, concentrando la discussione soprattutto sui protocolli industriali e sulle regole del sistema di rilevamento delle intrusioni (IDS). **In altre parole, viene dettagliata una simulazione di attacchi contro un protocollo industriale noto insieme ai risultati ottenuti da [WU19], in cui viene presentato un DT che simula alcuni scenari di test specifici per l'industria aerospaziale.**

Una delle prime serie di **test basati su DT** è stata condotta **su protocolli industriali** per determinare e verificare come potrebbero essere affrontati i potenziali vettori di attacco e le corrispondenti regole per un IDS. In particolare, sono stati testati una serie di possibili attacchi di enumerazione e interruzione contro master/server Modbus [MOH22]. La prima serie di test mirava a determinare la raggiungibilità dei master Modbus attraverso la rete, dove gli aggressori sono stati in grado di scansionare la rete di produzione per identificare e localizzare master/server Modbus. Con questo test è stato possibile comprendere la raggiungibilità tra la rete dell'aggressore e la rete di produzione. Una volta completata questa fase di identificazione, è stata eseguita una fase di enumerazione per contare tutti i registri. Vengono quindi eseguite due azioni: (a) lettura dei registri e (b) scrittura dei registri.

La lettura dei registri aveva due obiettivi principali: (i) enumerare l'applicazione che espone il server Modbus e (ii) mappare la superficie di attacco. Nelle prime prove è stata effettuata una lettura massiva dei registri. Questo tipo di azioni, se non ben limitate, potrebbero portare alla divulgazione delle informazioni esposte dal server Modbus, che di conseguenza potrebbe comportare anche un rallentamento del servizio stesso, che non riuscirebbe a soddisfare tutte le richieste, provocando un rifiuto del servizio. Una volta mappata la superficie di attacco di tutti i record esposti, il passo successivo è stato verificare dove fosse possibile scrivere tali record.

La scrittura nei log può causare due effetti principali: (i) interrompere l'applicazione o (ii) modificarne il comportamento in uno dannoso. Per questo motivo era importante sperimentare una possibile iniezione di valore nel registro esposto. Nel complesso, questi test erano estremamente semplici.

Come si può vedere, questi test inizialmente non avevano lo scopo di mostrare tecniche di attacco innovative su specifici master, ma piuttosto di dimostrare che tipo di attacchi o configurazioni errate potevano essere facilmente testati utilizzando la tecnologia DT senza influenzare la controparte fisica. Come esempio base è stato scelto Modbus, ma lo stesso tipo di test può essere eseguito con protocolli più recenti come: MQTT, DNP3, CAN-OPEN, ecc.

Il DT proposto può essere utilizzato anche per testare soluzioni di difesa. Un importante meccanismo di difesa da testare, ad esempio, sono le regole del traffico per un IDS. Queste regole vengono utilizzate per identificare un attacco in base alle firme specifiche del traffico tracciato. L'ultimo test eseguibile va esattamente in questa direzione e vuole mostrare la possibilità di testare regole per un IDS conosciuto. Questi strumenti eseguono un rilevamento su un comportamento anomalo come una lettura massiccia dei registri Modbus. Con un'infrastruttura virtualizzata, come quella che implementa DT, è molto semplice eseguire il mirroring del traffico in modo tale da reindirizzare il traffico clonato su una rete ad hoc per questo tipo di analisi. L'efficacia delle norme potrebbe quindi essere testata in un ambiente sicuro.

5.3.Rilevamento di intrusioni e anomalie

Come accennato, i DT possono replicare le complessità dei sistemi fisici e informatici in modo più dettagliato, essendo in grado di eseguire simulazioni più accurate per migliorare la sicurezza e la protezione dei CPS [ECK19a]. Per descrivere queste capacità, consideriamo le modalità di difesa sopra descritte: modalità online e offline.

In modalità offline, i DT sono in grado di **simulare scenari di minaccia per derivare vulnerabilità** (CVE (Common Vulnerabilities Exposures) tipiche e note, oppure nuove e zero-day), **identificare eventi anomali causati da vettori di attacco predefiniti, testare e definire nuovi modelli di attacco e regole** come indicato nella sezione precedente e **adeguare e rafforzare gli algoritmi ML esistenti**
ad esempio, per **la manutenzione predittiva** (l'area preposta a comprendere quando un determinato componente, linea di produzione o dispositivo necessita di assistenza o manutenzione), **e per il rilevamento di intrusioni e anomalie in scenari critici.** Proprio quest'ultimo caso d'uso DT è attualmente uno dei più diffusi negli scenari CPS e negli ecosistemi industriali. In [XU21], gli autori presentano un nuovo approccio chiamato "Anomaly deTection with digiTAl twIN" (chiamato ATTAIN), che costruisce DT per il rilevamento di anomalie, utilizzando dati in tempo reale ottenuti da un CPS ed euristiche. Inoltre, il lavoro in [CAS21] mostra le potenziali caratteristiche dell'utilizzo di approcci semi-supervisionati per il rilevamento di anomalie in ambienti industriali, che fanno uso di un DT per generare un set di dati di addestramento che simula il normale funzionamento dei macchinari, insieme a un piccolo insieme di dati anomali etichettati. misurazioni da macchinari reali.

D'altro canto, i DT in modalità online potrebbero, inoltre, **rilevare eventi che vanno oltre gli IDS tradizionali,** generalmente basandosi su firme di attacco predefinite o sull'utilizzo di algoritmi di machine learning per il rilevamento di anomalie. I DT potrebbero integrare le azioni di rilevamento derivando deviazioni basate sul comportamento "semantico" delle operazioni naturali di un CPS (quello che di seguito chiameremo comportamento legittimo). Il risultato sarebbe quindi un sistema di rilevamento ibrido in grado di stimare nuove situazioni sulla base di eventi casuali, causati da eventuali comportamenti del sistema

e il suo ambiente (es. traffico di rete), rispetto alle funzioni più sistematiche del CPS stesso.

Sfortunatamente, l'uso dei DT per il rilevamento delle intrusioni rimane un argomento relativamente inesplorato, sebbene siano state condotte alcune ricerche recenti e alcuni casi d'uso come scenari di studio. Nel 2018, Eckhart ed Ekelhart [ECK18a] hanno dimostrato l'applicabilità dei DT per il rilevamento degli attacchi nei **sistemi di controllo industriale (ICS),** monitorando il comportamento legittimo dei CPS. Gli autori hanno introdotto un quadro basato su specifiche che richiede regole fisiche esplicitamente definite per creare una simulazione e confrontarla con un sistema reale, considerando le incoerenze come attacchi informatici o malfunzionamenti fisici. Nel 2020, Akbarian *et al.* [AKB20] ha anche creato un DT per rilevare attacchi contro un ICS, ma stimando il comportamento legittimo del sistema utilizzando un algoritmo statistico. Nonostante non disponga di regole spiegabili, l'adattamento dinamico di una replica virtuale a minacce nuove e più complesse ha il potenziale per migliorare significativamente la resilienza degli ICS.

Un'altra applicazione per i DT è il rilevamento di attacchi mirati ad **ambienti Smart Grid.** Nel 2019, Danilczyk *et al.* [DAN19] ha proposto l'uso di un ambiente simulato per monitorare una microrete e la sua infrastruttura di comunicazione, utilizzando modelli basati sulla fisica per eseguire una stima in tempo reale del comportamento atteso. L'uso di DT per replicare eventi di sicurezza delle reti elettriche e rilevare comportamenti dannosi è un approccio promettente per proteggere sia la stabilità fisica che la rete di comunicazione delle Smart Grid.

5.4.Risposta e recupero

Basandosi sulle informazioni sopra offerte, diventa evidente che le decisioni automatiche di DT possono accelerare i processi di mitigazione in modo accurato e ad alta fedeltà. Un esempio di ciò può essere trovato in [SAA20]. Questo lavoro propone un Digital Twin basato sull'IoT con supporto Cloud per controllare l'effetto causato da un attacco di iniezione di dati falsi individuale o coordinato, nonché attacchi informatici di tipo Denial of Service. Inoltre, gli autori del documento in [HOL21] menzionano chiaramente l'importanza di applicare approcci DT per testare e validare l'effettiva efficacia delle patch di sicurezza a basso costo (in termini di implementazione in complesse infrastrutture IT/OT), e senza richiedere la configurazione e implementazione di sistemi secondari per guidare tali processi di test.

Qualsiasi entità, che mira a implementare in modo efficace la metodologia dei DT sulla propria rete, dovrebbe aver precedentemente raggiunto un elevato livello di maturità e resilienza informatica. È quindi importante che tali entità adottino un approccio olistico alla sicurezza informatica. Ciò può essere ottenuto attraverso l'integrazione della Cyber Threat Intelligence (CTI) al fine di allineare qualsiasi rafforzamento della rete prima dell'implementazione della metodologia DTs. In particolare, l'implementazione della CTI avrà conseguenze significative per qualsiasi organizzazione nella risposta e nel ripristino in caso di incidenti, attraverso la comprensione dell'architettura di sicurezza digitale e fisica, la mappatura di potenziali attacchi e quindi incorporando la risposta e la resilienza nella pratica quotidiana e consentendo visibilità su tutte le aree di rischio in termini di Riservatezza, Integrità e Disponibilità (CIA).

La CTI consiste in dati raccolti, elaborati e analizzati al fine di comprendere le motivazioni, gli obiettivi e i comportamenti di attacco di un attore di minacce. Consente alle organizzazioni di prendere decisioni sulla sicurezza più rapide, informate e supportate dai dati e di modificare il proprio atteggiamento da reattivo a proattivo per contrastare le minacce

attori. Esistono tre diversi livelli di CTI: operativo , *tattico* e *strategico.* Ogni livello ha un pubblico, un'applicazione e una natura diversa delle informazioni trasmesse:

- *La CTI operativa* si riferisce all'indagine delle capacità avversarie, delle infrastrutture e delle tattiche, tecniche e procedure (TTP), al fine di utilizzare tale conoscenza per indirizzare e dare priorità agli sforzi di mitigazione. Coloro che sono coinvolti nella gestione delle vulnerabilità, nella risposta agli incidenti e nel monitoraggio delle minacce sono i maggiori consumatori di intelligence operativa poiché li aiuta a essere più competenti ed efficaci nelle loro funzioni quotidiane.

  La CTI operativa è particolarmente importante per la rilevanza dei DT, poiché consente alle organizzazioni di rafforzare preventivamente le proprie reti contro i TTP comuni e di intraprendere azioni preventive e proattive rendendo le reti più robuste e mature. In risposta, ciò consente una rapida mitigazione di qualsiasi impatto e assiste nel ripristino consentendo la definizione delle priorità degli sforzi di ripristino iniziali, in particolare l'allineamento agli sforzi di mitigazione.

  La CTI tattica si concentra sull'analisi e sull'arricchimento del malware. In questo contesto, gli Indicatori di Compromissione (IoC) – come domini, indirizzi IP, email – sono particolarmente rilevanti e utili per aggiornare i sistemi di difesa basati su firme al fine di difendersi da tipologie di attacchi noti, ma possono essere utili anche per azioni più proattive misure quali esercitazioni di caccia alla minaccia.

  Similmente alla CTI operativa, la CTI tattica è fondamentale per qualsiasi metodologia implementata da DT in quanto consente la mappatura di diversi tipi di minacce di rete attraverso un'ampia gamma di modelli.
  La CTI tattica combinata con la CTI operativa consente simulazioni, test e modellizzazione dettagliati e proattivi, che costituiscono il cuore della metodologia DT. In risposta, ciò consente una mitigazione proattiva contro le aree di debolezza identificate. Per quanto riguarda il ripristino, la CTI tattica offre una panoramica della situazione della sicurezza informatica e consente il rapido ripristino dei sistemi di difesa per prevenire ulteriori attacchi.

- *La CTI strategica* fornisce un quadro completo del panorama delle minacce di un'azienda. È molto utile per informare le decisioni esecutive di alto livello e le informazioni sono spesso orientate al business e fornite attraverso rapporti o briefing, materiali che possono essere preparati solo da esseri umani dotati di conoscenza, non da algoritmi. Una buona intelligence strategica dovrebbe fornire informazioni dettagliate sui rischi associati ad azioni specifiche, modelli generali nelle tattiche e negli obiettivi degli attori delle minacce, eventi e tendenze geopolitici e altri temi correlati.

  Le CTI strategiche possono guidare l'implementazione della metodologia DT, identificando e mappando una minaccia complessiva che può interrompere sia i sistemi digitali che quelli fisici. In particolare, la Strategic CTI può mappare le minacce digitali ai sistemi fisici, comprendendo e identificando chiaramente i rischi in termini di CIA.

Nel complesso, le CTI combinate con i DT possono contribuire ad aiutare la sicurezza dell'organizzazione se implementate correttamente e supportate da un processo chiaro e strutturato. Nello specifico, per quanto riguarda le metodologie DT, incorporare tutti i livelli di CTI può guidare, mappare e maturare la sicurezza informatica in una serie di casi d'uso separati:

- *Teaming rosso e viola:* la CTI per il teaming rosso e viola consente ai team di **ricreare scenari realistici che rappresentano il panorama delle minacce che** con maggiore probabilità si applicheranno all'organizzazione in questione. Di conseguenza, i team rosso e viola sono in grado di imitare le tattiche, le tecniche e le procedure degli attori delle minacce che prendono di mira le funzioni critiche di un'entità sulla base delle CTI fornite, questo è fondamentale quando si lavora sia sul piano fisico che su quello informatico [ECB23] . Questa capacità è strettamente correlata a quella dettagliata nelle sottosezioni 5.1 e 5.2 sopra.
- *Implementazione SOC:* CTI basata su DT fornisce informazioni preziose al team del Security Operations Center (SOC) raccogliendo dati, tra gli altri, su incidenti informatici passati, campagne in corso, vulnerabilità sfruttate attivamente e malware utilizzati attivamente e simulando scenari dannosi. Dal punto di vista della risposta e della resilienza, ciò offre al team SOC gli strumenti per **prevenire e rispondere in modo proattivo agli attacchi, riducendo i tempi di ripristino e l'impatto dell'attacco.**

- *Risposta agli incidenti:* l'utilizzo dei meccanismi CTI basati su DT durante e dopo un incidente informatico può aiutare le entità a **valutare efficacemente l'impatto dell'incidente.** Attraverso la CTI abilitata per DT, le entità possono essere in grado di valutare l'impatto degli incidenti informatici sulla base di precedenti eventi simili e/o scenari simulati predefiniti. Inoltre, l'intelligence raccolta attraverso dichiarazioni e post pubblicati dall'autore della minaccia dal deep e dal dark web può ulteriormente aiutare l'entità nei suoi tentativi di riportare tutti i servizi e le funzioni alla normalità. Ciò è particolarmente importante per le entità che utilizzano la metodologia DT, dato il loro patrimonio di sicurezza vario e ampliato.

- *Recupero post incidente:* la tecnologia CTI basata su DT fornisce **informazioni critiche durante il processo di ripristino post incidente.** Comprendendo i percorsi delle minacce e i potenziali scenari di attacco, le organizzazioni colpite possono comprendere il potenziale impatto dell'attacco, sia interno (come directory, sistemi interessati e potenziali futuri attacchi di danni) che esterno (potenziali problemi normativi e potenziali problemi finanziari). . In termini di eventi significativi o potenziali a livello di estinzione, i DT possono essere utilizzati per identificare potenziali percorsi di recupero, inclusa l'identificazione delle aree del patrimonio informatico che sono la massima priorità in termini di tempo e impatto.

Pertanto, adottare un approccio olistico alla sicurezza informatica e incorporare le CTI nelle pratiche di sicurezza informatica può consentire alle entità di **aumentare il proprio livello di maturità informatica e durata di vita.** Le entità che implementano DT si troveranno ad affrontare un ambiente di sicurezza sempre più complesso, con un panorama di attacchi notevolmente ampliato. Pertanto, la CTI abilitata a DT consentirà a qualsiasi organizzazione di identificare in modo proattivo potenziali minacce e rischi e di implementare test di simulazione mirati, red teaming e monitoraggio. Queste implementazioni sono cruciali per la risposta e la resilienza dell'organizzazione, poiché consentono alle organizzazioni di migliorare il proprio livello di sicurezza e allo stesso tempo di essere preparate sia per la fase di attacco che per quella di risposta a un incidente informatico. Inoltre, l'implementazione della metodologia DT in modo più efficace richiede che le entità dispongano di solide pratiche di sicurezza informatica e di sicurezza informatica. È fondamentale per le entità che desiderano implementare DT incorporare le CTI nelle loro pratiche di sicurezza informatica.

5.5.Consapevolezza della situazione

La consapevolezza situazionale corrisponde a un'area specifica della sicurezza informatica che comprende un insieme di servizi che vanno oltre i tradizionali sistemi di rilevamento e i sistemi basati sulla consapevolezza del contesto. COME

come affermato in [ALC13], la consapevolezza situazionale è un servizio di protezione complesso che tenta di spiegare cosa sta accadendo in uno o più domini applicativi e con un elevato livello di precisione e granularità, dettagliando: cosa, dove, quando e da chi l'evento si è innescato .

Il concetto è stato originariamente definito da Endsley nel 1995 per significare che la consapevolezza della situazione è un'area che comprende tre azioni rilevanti, strettamente legate ai processi cognitivi [END95]: (i) la percezione delle dinamiche rilevanti di un ambiente, (ii) la comprensione del loro significato per comprenderne la situazione e (iii) la proiezione dei loro stati nel prossimo futuro. In questo senso, i vantaggi derivanti dall'utilizzo dei DT per coprire queste azioni sono significativamente ampi, poiché le loro capacità di simulazione, in modalità offline e online, con un alto livello di fedeltà aiutano a descrivere e localizzare un problema e, nel migliore dei casi, a neutralizzarlo in tempo. . Quest'ultimo soddisfa addirittura uno dei principali criteri per la protezione delle infrastrutture critiche [ALC13]. I sistemi che si basano sulla consapevolezza situazionale non dovrebbero solo **garantire una rapida anticipazione e rilevamento di eventi anomali, ma anche fornire risposte per migliorare la resilienza,** restituendo tutta la conoscenza per affrontare minacce simili in futuro.

Pertanto, è facile comprendere che la consapevolezza situazionale assistita dalla DT comprende aspetti già discussi nelle ultime due sezioni. Tuttavia, descriviamo qui alcuni lavori correlati per chiarirne l'attualità. Ad esempio, Eckhart *et al.* dettaglio in [ECK19] che il paradigma DT può essere uno strumento utile per intensificare la consapevolezza situazionale in contesti basati su CPS. Gli autori descrivono chiaramente che l'uso di repliche virtuali in parallelo alle controparti fisiche potrebbe aiutare le azioni di ispezione e determinare comportamenti anomali, rischi e minacce senza interrompere i processi operativi del sistema. Per dimostrarlo, il lavoro propone anche un quadro di consapevolezza situazionale informatica basato su DT (che virtualizza la topologia del sistema, i parametri e le variabili del programma software del dispositivo) al fine di fornire un quadro olistico della situazione informatica dei CPS e rilevare le minacce. In [MYL21], gli autori forniscono uno studio sulla rilevanza dei sistemi immunitari industriali di prossima generazione (guidati dall'intelligenza artificiale) incaricati di proteggere gli ecosistemi industriali da attacchi cyber-fisici sofisticati e furtivi, esplorando ulteriormente come la consapevolezza situazionale possa essere migliorata rapidamente rilevare, localizzare e neutralizzare le minacce.

Inoltre, l'integrazione tecnologica potrebbe fornire **una comprensione più profonda dei vettori, degli strumenti e delle tattiche di attacco reali e realistici degli avversari,** consentendo una maggiore consapevolezza situazionale e quindi una maggiore resilienza e protezione per supportare altre aree correlate come la caccia alle minacce, la gestione degli incidenti e le minacce informatiche. intelligenza [DIE22]. A loro volta questi ambiti potrebbero addirittura contribuire alla sensibilizzazione del DT per un'ulteriore prevenzione del sistema. Ciò significa anche che i DT possono essere in grado di connettersi con entità esterne o altri DT per avere una visione più esplicita della situazione o delle possibili situazioni nel prossimo futuro.

5.6.Privacy

Come accennato in precedenza, i DT possono simulare servizi, dispositivi, funzioni e interazioni all'interno dell'infrastruttura, nonché interazioni con stakeholder esterni (ad esempio, per la cyber intelligence come discusso nella sezione precedente). Per un corretto funzionamento è obbligatorio l'utilizzo dei dati "reali/reali o sintetici" (basati sul reale) di ciascun asset presente nel DT. A seconda del dominio applicativo (es. veicoli intelligenti, fabbriche intelligenti, città intelligenti, ecc.), vengono implementati diversi servizi e dispositivi, mentre iniziano ad emergere nuove tecnologie (5G/6G, cloud, AI, Distributed Ledger Technology (DLT), ecc.) con la capacità di gestire più tipologie di dati (dati personali e segreti industriali), massimizzando i rischi per la sicurezza di tali dati.

Per prevenire questi rischi, i DT possono essere utilizzati per **migliorare la privacy in ambienti così complessi integrando e testando tutte le risorse** (attualmente installate nell'infrastruttura reale così come le tecnologie pianificate per essere utilizzate). Questo approccio consentirà, ad esempio, di rilevare anomalie, vulnerabilità ed errori di configurazione che potrebbero mettere a repentaglio la riservatezza dei dati. Per raggiungere questo obiettivo (i) dovrebbero essere progettati ed eseguiti test multipli (ad esempio, test di penetrazione) basati su diversi scenari; e (ii) dovrebbero essere predisposti strumenti e meccanismi adeguati per la raccolta dei dati/il traffico di rete per raccogliere e analizzare adeguatamente i dati per consentire un'ulteriore valutazione della privacy. Sulla base dei risultati, è possibile successivamente progettare adeguate norme sulla privacy utilizzando diversi approcci, metodologie e tecniche basate sulle rispettive metriche sulla privacy. Inoltre, l'uso dei DT consente non solo di effettuare test iniziali sulla privacy e sulla sicurezza, ma anche di definire e applicare in modo permanente regole, tecniche e approcci sulla privacy più complessi. Ciò, a sua volta, aiuta a identificare il miglior approccio complessivo in un ambiente realistico, comprese tutte le particolarità di ciascuna infrastruttura. Infatti, poiché la privacy è obbligatoria praticamente in tutti gli ambiti di applicazione, i DT possono simulare un'infrastruttura, comprensiva di servizi, comunicazione dati, procedure organizzative e altro ancora.

Un esempio del suo utilizzo può essere il monitoraggio e il controllo degli ecosistemi sanitari, che includono dispositivi medico-diagnostici in vitro (ad esempio peacemaker e defibrillatori interconnessi), dispositivi medici interconnessi e apparecchiature di supporto vitale, dispositivi per il benessere e l'infrastruttura IT/OT di un ospedale. Come descritto nella Sezione 5.1, i dati trasferiti nell'intero ecosistema sanitario contengono informazioni personali e sensibili che devono essere protette per salvaguardare la privacy dei pazienti. Lo sviluppo di un DT di un ecosistema così complesso ed eterogeneo consentirebbe di esplorare le vulnerabilità, le errate configurazioni dei dispositivi e delle regole di rete, i flussi di dati, il comportamento dei pazienti e degli ospedali quando connessi alla rete (ad esempio, quali siti vengono visitati), ecc. Più specificamente, attraverso durante la simulazione, è possibile determinare possibili violazioni e vulnerabilità della privacy che potrebbero portare a fughe di dati e furti non solo a livello di rete ma anche a livello di dispositivo (ad esempio, per verificare la qualità dei modelli ML e il loro livello di accesso a grandi volumi di dati dati). Sulla base dei risultati, vari meccanismi, tecniche e strumenti possono essere testati in una serie di casi d'uso per valutare se il rischio per la privacy è stato eliminato e le implicazioni che potrebbero essere introdotte. Questo approccio può anche portare alla privacy attraverso l'architettura di progettazione.

5.7.Formazione, riqualificazione e miglioramento delle competenze

Un DT può essere utilizzato come strumento di formazione, ad esempio, per operatori umani e personale in ambienti ad alto rischio e servizi pericolosi (ad esempio macchinari pesanti, miniere, ecc.). In questo contesto applicativo, la simulazione includerà e guiderà diversi flussi e processi informativi, tutti concorrenti a supportare il processo di apprendimento, tipicamente applicato per comprendere il funzionamento di un sistema, la sua gestione e la sua sicurezza in termini di safety e cybersecurity.

Infatti, nel campo del funzionamento e della sicurezza, i dipendenti/utenti possono essere formati a gestire vari dispositivi, macchine, sistemi (ciberfisici), nonché processi operativi, senza mettere a rischio la propria vita o quella di altri causando un incidente o incidendo sul sistema. In questo modo, **la formazione basata sulla simulazione preparerà i dipendenti/utenti a gestire tutti i tipi di elementi operativi che hanno bisogno di conoscere** in una pletora di scenari, sia per le operazioni quotidiane che per le situazioni di emergenza/avverse. Inoltre, questo tipo di formazione/apprendimento in ambienti altamente minacciosi, pericolosi o critici aiuterà i dipendenti/utenti junior ad acquisire esperienza, conoscenza, abilità e competenze in termini di applicabilità e sicurezza [SIN21], [BEL20]; ma anche per dipendenti/utenti senior che necessitano di riciclare le proprie conoscenze e/o migliorare le proprie competenze.

Nel dominio della sicurezza informatica, un DT può essere utilizzato per numerosi scopi quali (i) test di sicurezza e debugging (ii) convalida della progettazione della sicurezza dei prodotti contro attacchi informatici simulati (ad esempio test di penetrazione), (iii) rilevamento di configurazioni errate, (iv) test di diversi impostazioni dei componenti di sicurezza che vengono implementati nell'ambiente reale e (v) formazione. L'utilizzo del DT per la formazione consentirà **agli esperti di sicurezza** (ad esempio i team SOC) **di interagire con le funzioni del sistema in modalità offline e di familiarizzare con le varie soluzioni di sicurezza in situazioni e casi d'uso realistici** [VIE21]. Permetterà inoltre di modellare gli impatti di attacchi/contromisure sui processi cyber-fisici [ECK19a], e successivamente di evitare gravi interruzioni e conseguenze future, migliorando la sostenibilità e l'integrità dell'intera catena del valore.

Continuando con la capacità dei DT per la formazione sulla sicurezza informatica, e come affermato in [HOL21], i DT possono essere efficaci nel promuovere le competenze in materia di sicurezza informatica attraverso esercizi digitali pratici e seri giochi d'azzardo. In questo caso, gli aspetti relativi ai modelli cyber-range possono essere integrati come parte del DT per consolidare competenze, apprendimenti e conoscenze. Attraverso il cyber range è possibile implementare ambienti di apprendimento realistici basati su esercizi pratici e attraenti legati al *blue team/ red team, al capture the flag* o *agli hackathon.*

5.8.Esplorazione di nuove capacità di simulazione

In questa sezione, associamo le capacità della tecnologia DT per la protezione del sistema, la resilienza e la sicurezza informatica con i requisiti di protezione delle infrastrutture critiche identificati dal NIST in [NIST18].
Per fare ciò, raggruppiamo queste capacità in base alle cinque funzioni di sicurezza informatica fornite dal NIST: **identificare, proteggere, rilevare, rispondere e ripristinare,** e in base a questo raggruppamento colleghiamo le capacità ai requisiti di protezione.

Tabella 5. Associazione dei potenziali contributi dei DT rispetto alle misure di difesa proposte dal NIST in [NIST 18].

Sez. funz.	Potenziale contributo di Gemelli digitali	Supporto alle categorie NIST (rispetto a [NIST18])
	• **Identificazione delle vulnerabilità (conosciute e sconosciute)** del gemello fisico nonché delle possibili conseguenze del loro sfruttamento e correzioni	• Gestione delle risorse (ID.AM), in particolare per l'inventario delle risorse (ID.AM-1) e la definizione delle priorità (ID.AM-5) • Valutazione dei rischi (ID.RA), in particolare per l'identificazione e la documentazione delle vulnerabilità (ID.RA-1)
	• **Valutazione del possibile sfruttamento** delle vulnerabilità rilevate	• Valutazione del rischio (ID.RA), in particolare per la stima della probabilità (ID.RA-4, ID.RA-5)
	• **Analisi degli impatti di possibili situazioni avverse** e simulazione di **effetti a cascata**	• Risk Assessment (ID.RA), in particolare per la stima dell'impatto aziendale (ID.RA-4) • Gestione del rischio della catena di fornitura (ID.SC), in particolare per la valutazione del rischio della catena di fornitura (ID.SC-2)

	• **Valutazione di IL attuale controlli di cybersecurity in atto** e gap analysis per analizzare gli effetti dei possibili miglioramenti prima di applicarli al sistema reale.	• Ambiente aziendale (ID.BE), in particolare per le dipendenze tra asset e requisiti di resilienza (ID.BE-4, ID.BE-5) • Governance (ID.GV), in generale • Valutazione del rischio (ID.RA), in particolare per l'identificazione e la definizione delle priorità delle risposte al rischio (ID.RA-6) • Gestione del rischio della catena di fornitura (ID.SC), in particolare per i test di recupero (ID.SC-5)
	• **Analisi dei dati per identificare in modo proattivo errori/guasti all'interno del sistema,** ad esempio, consentendo di prevedere o pianificare la manutenzione predittiva (utilizzando la tecnologia DT) • **Verifica e applicazione delle norme sulla privacy e sulla sicurezza,** coinvolgendo tecniche e approcci per consentire l'identificazione dell'approccio migliore in un ambiente realistico	• Sicurezza dei dati (PR.DS), in particolare per determinare il livello di qualità e integrità dei dati (ad esempio, PR.DS-5) e delle risorse (PR.DS-3-4, PR.DS-6, PR.DS -8) • Manutenzione (PR.MA) in azioni controllate, accesso (PR.MA-2) e strumenti (PR.MA-1). • Processi e procedure di protezione delle informazioni (PR.IP) attraverso la progettazione di piani di gestione delle vulnerabilità (PR.IP-12)
	• Supportare l'uso sicuro e corretto del sistema **fornendo capacità di sensibilizzazione e formazione** basate sulla simulazione del sistema reale	• Consapevolezza e formazione (PR.AT), in particolare per gli utenti con accesso all'ambiente operativo (PR.AT-1), e comprensione dei propri ruoli e responsabilità rispetto al sistema (PR.AT-2-5)
	• **Convalidare il corretto funzionamento degli strumenti e delle politiche di protezione/ difesa** (ad esempio meccanismi di controllo degli accessi) e la loro adeguatezza negli ambienti operativi	• Tecnologia di protezione (PR.PT) e gestione dell'identità, autenticazione e controllo dell'accesso (PR.AC), seguendo il principio di minima funzionalità (PR.PT-3) e privilegi minimi (PR.AC 2-4)
	• **Verificare lo stato effettivo del sistema e il rispetto delle migliori pratiche e politiche di sicurezza** confrontando ciò che viene fatto nel mondo reale con quello virtuale mondo. Pertanto, i DT potrebbero sostenere il concetto di *"governance e conformità continue"*	• Tecnologia di protezione (PR.PT) attraverso registri e audit in conformità con i quadri normativi (PR.PT-1)
	• **Testare e convalidare nuovi modelli, vettori e regole di attacco** basati sulle caratteristiche del gemello fisico • **Testare l'output di una risorsa specifica** per comportamenti anomali (ad esempio, perdita di dati)	• Le attività di rilevamento rispettano tutti i requisiti applicabili, per ogni bene sensibile (DE.DP-2, DE.DP-3, DE.DP-4) ed evento di anomalia particolare (DE.AE-2, DE.AE-3),

	• **Adeguare e rafforzare gli algoritmi ML esistenti per il rilevamento precoce delle anomalie,** ad esempio generando set di dati di addestramento che simulano operazioni di sistema normali/anomale	• DT può migliorare il rilevamento delle anomalie. La rete è monitorata per rilevare potenziali eventi di sicurezza informatica (DE.CM 1); Viene rilevato codice dannoso (DE.CM 3); È stato rilevato un codice mobile non autorizzato (DE.CM-5)
	• **Supportare azioni di ispezione approfondita** a seguito del rilevamento di comportamenti anomali, rischi e minacce senza interrompere i processi operativi del sistema • **Testare e migliorare la forza di** Modelli e regole **dei sistemi di rilevamento delle intrusioni** basati su p(host/rete) per gli eventi di sicurezza informatica	• Migliorare l'analisi post-rilevamento. Vengono stabilite soglie di allerta per gli incidenti (DE.AE-5); L'attività del personale è monitorata per rilevare potenziali eventi di sicurezza informatica (DE.CM-3)
	• **Supportare la consapevolezza della situazione informatica per il rilevamento delle minacce** (virtualizzando la topologia del sistema, i parametri e le variabili del programma software dei dispositivi o delle risorse mobili) al fine di fornire un quadro olistico della situazione informatica dei CPS	• I ruoli e le responsabilità per il rilevamento sono ben definiti per garantire la responsabilità (DE.DP-1); Le attività di rilevamento rispettano tutti i requisiti applicabili (DE.DP-2); Viene effettuato il monitoraggio del personale non autorizzato, delle connessioni, dei dispositivi e del software (DE.CM-7); Viene determinato l'impatto degli eventi (DE.AE-4); Le scansioni delle vulnerabilità vengono eseguite a scopo preventivo (DE.AE-4)
	• **Supportare la consapevolezza della situazione informatica** per la pianificazione e il monitoraggio della risposta, **tramite identificare tempestivamente i danni e le relative cause,** controllando al tempo stesso gli effetti causati da un attacco di iniezione di dati falsi, individuale o coordinato, nonché da attacchi informatici di tipo Denial of Service, e stima delle funzioni residue • **Supportare la consapevolezza della situazione informatica** per la pianificazione e il monitoraggio della risposta, **riproducendo o prevedendo incidenti complessi,** che possono guidare non solo il normale monitoraggio e la prevenzione dei disastri, ma anche la mitigazione degli incidenti	• Il piano di risposta viene eseguito durante o dopo un incidente (RS.RP-1); Vengono esaminate le notifiche provenienti dai sistemi di rilevamento (RS.AN-1); L'impatto dell'incidente è compreso (RS.AN-2); Per gli esami di laboratorio vengono eseguiti (RS.AN-3); Gli incidenti sono classificati in base ai piani di risposta (RS.AN-4) • La condivisione volontaria delle informazioni con le parti interessate esterne avviene per ottenere una più ampia consapevolezza situazionale della sicurezza informatica (RS.CO-5); Gli incidenti sono mitigati (RS.MI-2); Le vulnerabilità appena identificate vengono mitigate o documentate come rischi accettati (RS.MI-3)

	• **Sostenere la definizione di strategie di emergenza** e vie di evitamento • **Identificare il ruolo dell'agente e classificarlo gli asset e i possibili attacchi** in base all'analisi della valutazione del rischio	• Il personale conosce i propri ruoli e il proprio ordine operazioni quando è necessaria una risposta (RS.CO-1); gli incidenti vengono segnalati in linea con i criteri stabiliti (RS.CO-2); Le informazioni sono condivise in linea con i piani di risposta (RS.CO-3); gli incidenti sono contenuti (RS.MI-1); gli incidenti sono mitigati (RS.MI-2); e sono stabiliti processi per ricevere, analizzare e rispondere alle vulnerabilità comunicate all'organizzazione da fonti interne ed esterne (ad esempio test interni, bollettini sulla sicurezza o ricercatori sulla sicurezza) (RS.AN-5)
	• **Eseguire ottimizzazioni interattive dei processi delle organizzazioni** in varie condizioni di incidenti • **Stabilire controllato processi di miglioramento** basati sulle recenti scoperte	• I piani di risposta incorporano le lezioni apprese (RS.IM-1); Le strategie di risposta vengono aggiornate (RS.IM-2)
	• **Supportare la consapevolezza della situazione informatica per la pianificazione del ripristino,** fornendo una **comprensione realistica ai partecipanti durante l'intero ciclo di vita di un sistema,** che comprende anche incidenti e periodi di disastro • **Facilitare lo sviluppo, il test e il mantenimento di strategie e piani per il ripristino di emergenza.** Ciò vale in particolare per i sistemi critici caratterizzati da componenti legacy e vincoli di disponibilità (ad esempio infrastrutture energetiche), che non possono essere facilmente testati senza mettere a rischio la continuità operativa dell'infrastruttura	• Pianificazione del ripristino (RC.RP), azioni di supporto sia durante che dopo un incidente di sicurezza informatica (RC.RP-1) • Miglioramenti (RC.IM), aggiornamento delle strategie di ripristino (RC.IM-2)
	• **Accelerare/facilitare i processi di ripristino** in modo molto accurato e ad alta fedeltà (1) mediante **decisioni supportate da diversi gradi di automazione** e (2) consentendo il **corretto ripristino dello stato pre-incidente e della configurazione del gemello fisico,** che avrebbe potuto essere memorizzato e salvato nel DT	• Pianificazione del ripristino (RC.RP), azioni di supporto sia durante che dopo un incidente di sicurezza informatica (RC.RP-1) • Miglioramenti (RC.IM), a supporto dell'aggiornamento delle strategie di recupero (RC.IM 2)
	• **Testare e convalidare l'attuale l'efficacia delle patch di sicurezza a basso costo,** senza incidere sul sistema reale	• Miglioramenti (RC.IM), a supporto sia dell'incorporazione delle lezioni apprese (RC.IM-1) che dell'aggiornamento delle strategie di ripristino (RC.IM-2)

Dalla Tabella 5 determiniamo che DT è una tecnologia potenzialmente efficace, in grado di offrire molteplici e attraenti funzionalità non solo per virtualizzare e caratterizzare un oggetto o un sistema per attività di analisi, validazione e test, ma anche per ottenere molteplici vantaggi in termini di sicurezza, sicurezza, sostenibilità e redditività della catena del valore. Attraverso la simulazione (sia in modalità offline che online), è possibile offrire l'integrazione di strumenti difensivi in grado di proteggere continuamente i domini di un sistema, rilevare e rispondere a potenziali minacce e, nel peggiore dei casi, riprendersi da soli da tali minacce. minacce.

6. Migliori pratiche e linee guida per i professionisti

Come notato in [ALC22], la superficie di minaccia della tecnologia DT si estende considerevolmente grazie alla sua capacità di connettersi e interagire con il mondo reale, manualmente o automaticamente. In questo caso, gli aggressori possono pianificare le loro minacce di attacco dallo spazio fisico a quello virtuale, o da quello virtuale a quello fisico, al fine di esfiltrare informazioni sensibili (ad esempio, proprietà intellettuale, segreti industriali) verso entità esterne, interrompere funzioni critiche dello spazio reale sistema o distruggere risorse essenziali per il mondo reale.
In altre parole, gli aggressori potrebbero essere principalmente interessati a (i) raggiungere il DT per apprendere deliberatamente dalla natura del gemello fisico (ad esempio, topologie, protocolli, conf, ecc.) e, una volta conosciuto, attaccare con attacchi più sofisticati e avanzati vettori (ad esempio, minacce più avanzate e persistenti); o (ii) assumere il controllo del DT per accedere e manipolare successivamente le risorse critiche distribuite nello spazio fisico dallo spazio digitale. In entrambi i casi, le conseguenze sarebbero disastrose per l'organizzazione, responsabile del sistema stesso, e in termini di perdita di servizi essenziali per l'utente finale o perdita di informazioni sensibili che possono mettere a repentaglio la catena del valore, la reputazione di un'organizzazione e i suoi prestigio.

Una tassonomia completa degli attacchi ai DT si trova anche in [ALC22], organizzata secondo le tecnologie che potrebbero essere integrate come parte dei DT. La tassonomia contempla attacchi contro (1) CPS e IIoT, tipicamente implementati nel mondo fisico per fornire informazioni al DT o ricevere comandi per l'attuazione, (2) infrastrutture informatiche per ospitare le risorse DT, come cloud ed edge, (3) sistemi di virtualizzazione, (3) tecniche e modelli informatici per gestire modelli digitali e i relativi dati (ad esempio, tramite AI, Big Data) e (4) sistemi di visualizzazione, HMI o tecnologie avanzate di realtà virtuale, aumentata, mista o estesa. Per semplificare la tassonomia dettagliata in [ALC22] e riassumere l'insieme degli attacchi che possono verificarsi in ambienti basati su DT, evidenziamo: attacchi software (exploit di vulnerabilità e malware), nodi canaglia e man-in-the-middle (in termini di dispositivi IIoT/CPS, modelli digitali, sistemi di virtualizzazione, server), estrazione di informazioni sensibili, escalation di privilegi, manipolazione (in termini di dati, nodi virtuali, modelli digitali, conoscenza, rappresentazione e visualizzazione), denial of service e attacchi fisici e privacy perdita. Pertanto, è chiaro che un DT può essere considerato una tecnologia molto potente per migliorare la catena del valore, ma allo stesso tempo può essere considerato uno strumento vettore di attacco efficace e pericoloso per gli aggressori.

Per evitare tutti questi scenari di attacco e il loro corrispondente impatto, proponiamo in questa sezione una serie di raccomandazioni e linee guida sulle migliori pratiche da tenere in considerazione nel prossimo futuro, al fine di configurare e implementare DT affidabili e sicuri. Considerando il quadro di sicurezza informatica fornito dal NIST in [NIST18], la Tabella 6 descrive in dettaglio i requisiti di sicurezza che sia i professionisti che gli esperti di sicurezza IT/OT dovrebbero considerare per implementazioni sicure di DT.

Tabella 6. Possibili soluzioni di protezione basate su DT per implementazioni future

NIST Funz.	Requisiti di sicurezza informatica del NIST per la protezione	Buone pratiche che utilizzano la tecnologia DT	Codice NIST
	Valutazione del rischio (ID.RA)	• A seconda delle diverse tecnologie integrate nel DT, deve essere effettuata **un'analisi delle vulnerabilità** di tali tecnologie • Associata ad ogni minaccia, deve essere effettuata una **valutazione del rischio** di ogni blocco DT	ID.RA-1, ID.RA-4
	Gestione del rischio della catena di fornitura (ID.SC)	• **Una valutazione del rischio della catena di fornitura** • **Risposta, pianificazione del ripristino e test** con i fornitori	ID.SC-2, ID.SC-5
	Gestione dell'identità, autenticazione e controllo dell'accesso (PR.AC)	• **Le identità** assegnate alle risorse fisiche e informatiche dovrebbero essere **uniche e legittime** • Qualsiasi **accesso** al DT deve essere **controllato** e protetto da entità interne ed esterne • Rispettare il **minimo privilegio e la minima funzionalità**	PR.AC-1-2-3-4-5-6-7
	Sensibilizzazione e Formazione (PR.AT)	• Tutti gli **operatori IT e OT siano consapevoli dei rischi legati alla sicurezza informatica** e dell'uso adeguato della tecnologia • Tutti gli **operatori IT e OT sono consapevoli del proprio ruolo e responsabilità,** comprese terze parti (ad esempio, fornitori) e dirigenti senior	PR.AT-1, PR.AT 2-5
	Sicurezza dei dati (PR.DS)	• Garantire **la riservatezza** eseguendo regolarmente stress test sui dati o database archiviati al fine di verificare eventuali punti deboli su dati crittografati • Applicare **principi/tecniche** di integrità delle regole/ configurazioni di sicurezza dei DT e dei loro dati e convalidare periodicamente tutte queste configurazioni, comprese quelle relative alla privacy. • Implementare un **meccanismo di risposta alla segnalazione per** incidenti di fuga di informazioni **e azioni proattive**	PR.DS-3-4-5-6, PR.DS-8
	Tecnologia protettiva (PR.PT)	• Poiché la resilienza è un elemento rilevante per il DT paradigma, **misure di risposta/ripristino** devono essere implementate come parte della tecnologia, al fine di raggiungere la resilienza	PR.PT-5

		esigenze in ogni tipo di situazione e per ogni spazio del DT	
	Anomalie ed Eventi (DE.AE)	• **Eventi generati dai DT** e associati Anche le piattaforme IT dovrebbero essere **valutate SOC** per scoprire vulnerabilità, exploit e potenziali attacchi • **Gli eventi DT devono anche essere correlati per avere una migliore comprensione dei problemi di sicurezza** che si verificano tra gli spazi di un DT e all'interno di un DT, supportando ulteriormente la consapevolezza situazionale	DE.AE-2, D.AE-3
	Monitoraggio Continuo della Sicurezza (DE.CM)	• Gli amministratori IT devono **monitorare e monitorare costantemente consapevole di ciò che accade all'interno del DT**	DE.CM-1, DE.CM-3
	Processi di rilevamento (DE.DP)	• Garantire un'adeguata **rilevazione nei diversi spazi di un DT** • Fornire un rilevamento adeguato attraverso test e validazioni continui (nei processi di rilevamento). Pertanto, è necessario garantire **il miglioramento continuo dei processi di rilevamento**	DE.DP-3-4-5
	Piano di risposta (RS.RP)	• Per gli scenari basati su DT, un **piano di risposta** viene eseguito durante o dopo un incidente	RS.RP-1
	Comunicazioni (RS.CO)	• **Qualsiasi informazione dovrebbe essere condivisa internamente ed esternamente** con le parti interessate, anche attraverso una rete DLT tra DT federati, e dovrebbe essere coerente con il piano di risposta. • Sono necessari criteri stabiliti per la segnalazione degli incidenti	RS.CO-2-3-4-5
	Analisi (RS.AN)	• **Le notifiche di minacce ed eventi anomali** di DT devono essere sempre **sotto controllo e indagati** • Attraverso **tecniche forensi,** esso È possibile recuperare configurazioni, dati e conservare prove per il futuro • Impostare **processi efficienti per ricevere, analizzare e rispondere** alle vulnerabilità divulgate	RS.AN-1, RS.AN 2, RS.AN-5
	Mitigazione (RS.IM)	• **Gli incidenti** che si verificano **nei domini DT devono essere contenuti e mitigati,** così come le nuove vulnerabilità	RS.MI-1-2-3
	Piano di ripristino (RC.RP)	• Il ripristino è un approccio di sicurezza prioritario per l'implementazione dei DT. Per questo motivo, durante o dopo un incidente di sicurezza informatica in un DT (o in alcuni dei suoi spazi), viene eseguito e implementato un **piano di ripristino**	RC-RP-1
	Miglioramenti (RC.IM)	• I piani di recupero **incorporano le lezioni apprese** per le attività future, considerando	RC.IM-1-2

		metriche o indicatori che aiuteranno a migliorare l'accuratezza del processo di recupero e i tempi di recupero	

Dalla Tabella 6 è facile notare che la protezione dei DT diventa necessaria e obbligatoria, soprattutto quando vengono impiegati in ambienti operativi critici. Tuttavia questa tabella ne riporta solo una parte molto semplificata, fornendo una panoramica generale delle possibili soluzioni preventive e correttive. Altri autori, come quelli del documento [ALC22], descrivono in dettaglio anche molte altre possibili soluzioni da prendere in considerazione in futuro, coprendo aspetti di protezione corrispondenti al livello normativo (ad esempio la necessità di implementare sistemi dinamici di gestione del rischio, agenti software che lavorano come ispettori , ecc.) sia sul piano tecnico, contemplando, ad esempio, la necessità di implementare soluzioni di gestione della fiducia, tracciabilità degli attacchi in tempo reale, tracciabilità e auditing dei dati, sistemi distribuiti di gestione degli eventi, cyber-intelligence, apprendimento e consapevolezza continui ma controllati, ecc. .

7. Raccomandazioni e prospettive future

Come descritto in questo documento tecnico ECSO, il paradigma DT non è standardizzato ed è ancora in evoluzione, così come le tecnologie e i modelli sottostanti. Sulla base di questi tecnologici progressi, i DT consentiranno progressivamente di simulare il funzionamento di sistemi e ambienti sempre più complessi, dall'ecosistema naturale agli ambienti urbani e persino al corpo umano. Ciò aprirà opportunità senza precedenti per comprendere, gestire e proteggere meglio le controparti fisiche. Tuttavia, man mano che i DT acquisiscono sofisticazione e connessione con il mondo reale aumentando il valore aggiunto, diventano più sensibili e aumentano i loro requisiti di sicurezza.

Tabella 7. Associazione delle raccomandazioni future e delle parti interessate interessate

Raccomandazione / Portatore di interessi	europeo Commissione / Responsabili politici	Utenti DT	DT ricercatori	DT sviluppatori	Fornitori di sicurezza
R1		X		X	
R2	X	X		X	X
R3	X	X			X
R4		X			X
R5	X				
R6			X	X	
R7		X	X	X	
R8		X	X	X	X
R9		X	X	X	X

Questa sezione fornisce una serie di Raccomandazioni (R), rivolte a diverse tipologie di stakeholder, intese come supporto nel governo della natura complessa e dinamica dei DT. Sono elencati come segue.

- **R1 – Adattare la sicurezza informatica dei DT alle specificità dei DT.** I DT differiscono ampiamente in termini di caratteristiche, complessità, tipologia di dati gestiti, ecc. Queste differenze hanno un impatto sull'insieme di proprietà di sicurezza che la sicurezza dei DT dovrebbe mirare a garantire, e quindi sull'insieme specifico di controlli e soluzioni che ciascun DT dovrebbe implementare . Per fare un esempio: *se il DT trattasse dati sanitari o simulasse il funzionamento di una nuova turbina, le principali proprietà di sicurezza da abilitare sarebbero rispettivamente la riservatezza dei dati e la riservatezza del modello,* che si tradurrebbe nell'adozione

di Privacy Enhancing Technologies (PET) nel primo caso, e controlli avanzati di accesso nel secondo.

- **R2 – Utilizzare una metodologia olistica e ben condivisa per proteggere i DT.** Come da R1 sopra, le soluzioni specifiche e i controlli da implementare dipendono dalle specificità del DT. D'altra parte, la metodologia per definire, implementare e gestire la sicurezza informatica DT dovrebbe essere il terreno comune per garantire che tutte le possibili questioni di sicurezza informatica siano prese in considerazione. Tale metodologia, possibilmente promossa dalle autorità di regolamentazione, dovrebbe basarsi su principi di sicurezza ampiamente accettati (come, ad esempio, la *sicurezza fin dalla progettazione)* e tecnologie (ad esempio, l'utilizzo dell'intelligenza artificiale) e specializzarli per i DT considerando le architetture, i componenti e le tecnologie di riferimento dei DT.
- **R3 – Esplora l'utilizzo delle capacità dei DT per rafforzare le funzioni di sicurezza informatica.** Come brevemente introdotto nella Sezione 5, le capacità di simulazione dei DT potrebbero essere utili per integrare l'analisi relativa alle funzioni di sicurezza informatica (ovvero identificare, proteggere, rilevare, rispondere e ripristinare). A questo proposito, è necessario ulteriore lavoro per comprendere meglio la reale applicabilità e l'efficacia di questo approccio, nonché i vincoli, le implicazioni e gli effetti collaterali che potrebbero avere in contesti specifici (ad esempio DT per scenari critici basati su CPS).
- **R4 – Se pertinente, esplorare il potenziale del continuum informatico.** Il collegamento di DT con dispositivi di elaborazione all'edge e attraverso il continuum apre nuove opportunità per i sistemi autonomi [FLA22]. Un DT eseguito ai margini potrebbe migliorare il monitoraggio e la protezione in tempo reale, le capacità di previsione e controllo e nuove possibilità di trasferimento dei dati. Utilizzando dati in tempo reale e apprendimento automatico, un DT potrebbe autoapprendere ed evolversi continuamente.
  Il valore aggiunto di queste possibilità dovrebbe essere attentamente valutato rispetto ai relativi costi di implementazione e manutenzione.
- **R5 – Collegare la ricerca, la politica e il quadro normativo riguardanti gli spazi dei dati ai DT.** Man mano che i DT aumentano in potenzialità e complessità, sono ancora più capaci di elaborare e correlare diversi tipi di dati provenienti da domini diversi. I DT scalabili possono rappresentare sistemi complessi come catene logistiche, sistemi alimentari, reti energetiche, che richiedono infatti la cooperazione tra diverse organizzazioni. Poiché la condivisione dei dati è cruciale in queste interazioni, gli spazi dati e i DT saranno sempre più correlati. Infatti i DT, essendo una riproduzione quanto più fedele possibile di un sistema reale, rappresentano una delle applicazioni più avanzate del concetto di spazi dati. Pertanto, collegando DT e spazi dati a livello di ricerca, politica e regolamentazione.
- **R6 – Ricercare e progettare approcci di sicurezza leggeri (o *"verdi")* che non entrino in conflitto con i requisiti operativi dell'ambiente.** Poiché i DT vengono applicati per migliorare strategie operative e modelli di business, è fondamentale ottimizzarne la sicurezza, tenendo però conto dell'attuale necessità di progettare soluzioni di sicurezza efficienti e leggere che non causino un sovraccarico significativo nel normale sviluppo di un DT stesso. Qualsiasi mancanza di accesso ai dati DT per rappresentare scenari coerenti può modificare il processo decisionale finale con un impatto sul modello di business.

- **R7 – Ricercare e progettare modelli digitali secondo principi di robustezza e fiducia e criteri di privacy.** Le rappresentazioni DT e le loro connessioni con il mondo reale per catturare il contesto attuale e riprodurre uno scenario reale devono essere basate su dati validi, costantemente protetti e condivisi da entità fidate. Ciò significa anche che i modelli digitali e la costruzione complessiva di un DT devono basarsi su principi di fiducia e privilegio minimo in grado di gestire interazioni logiche e fisiche molteplici ed eterogenee. Questo livello di protezione deve essere supportato non solo da tecniche di riservatezza dei dati, ma anche da tecniche che salvaguardino la privacy degli utenti. Grandi volumi di dati e tecniche di intelligenza artificiale possono corrompere questa condizione di privacy, che deve essere regolata da politiche e regolamenti e controllata da sofisticati meccanismi di protezione e conservazione.

- **R8 – Ricerca su come sfruttare il potenziale della DT per misurare le proprietà di sicurezza.**
  La sicurezza è per lo più considerata un requisito non funzionale. Uno sforzo riuscito per ideare parametri quantitativi di sicurezza avrebbe applicazioni potenzialmente dirompenti, consentendo l'applicazione di metodi di ottimizzazione alla progettazione di architetture, politiche e meccanismi.
  I DT giocherebbero un duplice ruolo in tale scenario: (1) come "generatori" di metriche, sia quando ne testano di nuove per valutarne il realismo e l'utilità, sia in fase di esecuzione, quando fornirebbero l'accesso alla replica sintetica dello stato interno di un sistema complesso; (2) come banco di prova per misurare le proprietà di sicurezza di un sistema in fase di progettazione o aggiornamento, consentendo anche di automatizzare il processo di esplorazione di soluzioni alternative alla ricerca di quella ottimale.
- **R9** – **Essere consapevoli delle tecnologie future e dei rischi connessi.** Sono previste ulteriori ricerche in futuro e prima che le tecnologie nuove ed emergenti si adattino o utilizzino le capacità di un DT. Ci riferiamo, in questo caso, ai rischi che, ad esempio, la quantistica può comportare. Gli attacchi quantistici potrebbero far parte degli obiettivi di aggressori avanzati e futuri che desiderano corrompere simulazioni e dati DT.

La tabella 7 corrisponde alla pertinenza di alcune delle raccomandazioni identificate dalle parti interessate (principalmente dal mondo accademico e industriale) e dagli esperti nel campo del DT.

8. Riferimenti

[AHE21] S. Aheleroff, X. Xu, RY Zhong, Y. Lu, "Digital Twin as a Service (DTaaS) in Industry 4.0: An Architecture Reference Model", in Advanced Engineering Informatics, volume 47, 2021, 101225, ISSN 1474-0346 , https://doi.org/10.1016/j.aei.2020.101225.

[AIE21] Airbus, [in linea]. "Aerobus In Spagna", 08 07 2021. Disponibile: https://www.airbus.com/company/worldwide-presence/spain.html (accesso 02-2022).

[AKB20] F. Akbarian, E. Fitzgerald e M. Kihl, "Rilevamento delle intrusioni nei gemelli digitali per sistemi di controllo industriale", conferenza internazionale del 2020 su software, telecomunicazioni e reti di computer (SoftCOM), doi: 10.23919/SoftCOM50211.2020.9238162. 2020, pag. 1–6,

[ALA17] KM Alam e A. El Saddik, "C2PS: un modello di riferimento dell'architettura Digital Twin per i sistemi cyber-fisici basati sul cloud", in IEEE Access, vol. 5, pp. 2050-2062, 2017, doi: 10.1109/ACCESS.2017.2657006.

[ALC13] C. Alcaraz e J. Lopez, “Consapevolezza situazionale su vasta area per la protezione delle infrastrutture critiche”, IEEE Computer, vol. 46, pp. 30-37, 2013.

[ALC22] C. Alcaraz e J. Lopez, "Digital Twin: A Comprehensive Survey of Security Threats", in IEEE Communications Surveys & Tutorials, vol. 24, n. 3, pp. 1475-1503, terzo trimestre 2022, doi: 10.1109/COMST.2022.3171465.

[ANG18] Angrish, B. Craver, M. Hasan e B. Starly, "Un caso di studio per la Blockchain nel settore manifatturiero: “FabRec”: un prototipo per una rete peer-to-peer di nodi di produzione", Procedia Manufacturing, vol. 26, pp. 1180-1192, 2018.

[QUALSIASI22] "Software di simulazione AnyLogic", disponibile online: https://www.anylogic.com/ (accesso 02-2022)

[QUALSIASI22a] "Digital Twin", disponibile online: https://www.ansys.com/en-gb/products/systems/digital twin (accesso 02-2022).

[AZU22] "Azure Digital Twins", disponibile online: https://azure.microsoft.com/en-gb/services/digital twins/ (accesso 02-2022).

[AZU22] "Azure Digital Twins", disponibile online: https://azure.microsoft.com/en-gb/services/digital twins/ (accesso 02-2022).

[BAO19] Bao, J.; Guo, D.; Li, J.; Zhang, J. La modellazione e le operazioni per il Digital Twin nel contesto della produzione. Ent. Inf. Sistema 2019, 13, 534–556.

[BAR19] BR Barricelli, E. Casiraghi e D. Fogli, "Un'indagine sul gemello digitale: definizioni, caratteristiche, applicazioni e implicazioni di progettazione", in IEEE Access, vol. 7, pp. 167653-167671, 2019, doi: 10.1109/ACCESS.2019.2953499.

[BEC18] A. Becue, Y. Fourastier, I. Praça, A. Savarit, C. Baron, B. Gradussofs e C. Thomas, "CyberFactory# 1—Securing the Industry 4.0 with cyber-ranges and Digital Twins", nel 14° IEEE del 2018 Workshop internazionale sui sistemi di comunicazione di fabbrica (WFCS), 2018.

[BEC20] A. Becue, E. Maia, L. Feeken, P. Borchers e I. Praca, "Un nuovo concetto di gemello digitale a supporto dell'ottimizzazione e della resilienza delle fabbriche del futuro", Scienze applicate, 10(13), pp. 44- 82, 2020.

[BEC20a] A. Becue, E. Maia, L. Feeken, P. Borchers e I. Praca, "Un nuovo concetto di gemello digitale a supporto dell'ottimizzazione e della resilienza delle fabbriche del futuro", Scienze applicate, 10(13), pp. 44- 82, 2020.

[BEL20] Beloglazov, II, PA Petrov e V. Yu Bazhin. "Il concetto di gemelli digitali per la progettazione di simulatori di formazione per operatori tecnologici per l'industria mineraria e di trasformazione." *industrie chimiche* 18 (2020): 19.

[BOE21] Boeing, "Boeing 737", 08 07 2021. Disponibile In linea: https://www.boeing.com/commercial/737max/ (accesso 02-2022).

[BUL19] Buldakova, T.; Suyatinov, S. Gerarchia dei modelli di operatori umani per il gemello digitale. Negli atti della conferenza internazionale sull'automazione russa del 2019 (RusAutoCon), Sochi, Russia, 8–14 settembre 2019.

[CAS21] A. Castellani, S. Schmitt e S. Squartini, "Rilevamento di anomalie nel mondo reale mediante l'utilizzo di sistemi gemelli digitali e apprendimento debolmente supervisionato", in IEEE Transactions on Industrial Informatics, vol. 17, n. 7, pp. 4733-4742, luglio 2021, doi: 10.1109/TII.2020.3019788.

[CPS22] "CPS TWINNING", disponibile online: https://github.com/sbaresearch/cps-twinning (accesso nel 2022).

[CRE22] "Crea connessioni immersive con il tuo gemello digitale dell'infrastruttura", disponibile online: https://www.imodeljs.org/ (accesso nel 2022).

[CYB24] Cyberseas, https://cyberseas.eu/, Progetto europeo, 2021-2024.

[DAM19] V. Damjanovic-Behrendt e W. Behrendt, "Un approccio open source alla progettazione e all'implementazione dei gemelli digitali per la produzione intelligente", International Journal of Computer Integrated Manufacturing, vol. 32, 2019.

[DAN21] W. Danilczyk, YL Sun, H. He, Rilevamento di anomalie della rete intelligente utilizzando un Digital Twin con apprendimento profondo. Nel 2020 si terrà il 52° North American Power Symposium (NAPS), IEEE, pp. 1-6, 2021.

[DIE22] M. Dietz, D. Schlette e G. Pernul, "Harnessing Digital Twin Security Simulations for systemsystem Cyber Threat Intelligence", 46a edizione della IEEE 2022 su computer, software e applicazioni doi: pp. Conferenza (COMPSAC), 2022, 789-797, 10.1109/COMPSAC54236.2022.00129.

[DTC22] Consorzio Digital Twin, Glossario dei gemelli digitali, 2022. Disponibile online: https://www.digitaltwinconsortium.org/glossary/glossary.html#digital-twin (accesso 02-2022).

[DTC22] Digital Twin Consortium, disponibile online: https://www.digitaltwinconsortium.org/about us/, (accesso nel 2022).

[BCE23] Banca centrale europea, https://www.ecb.europa.eu/paym/cyber-resilience/tiber eu/html/index.en.html, 2023

[ECK18] M. Eckhart e A. Ekelhart, "ASpecific-Based State Replication Approach for Digital Twins", Atti del workshop del 2018 sulla sicurezza e privacy dei sistemi ciberfisici, pag. 36-47, 2018.

[ECK18a] M. Eckhart e A. Ekelhart, “Towards Security-Aware Virtual Environments for Digital Twins”, in Atti del 4° workshop ACM sulla sicurezza dei sistemi ciberfisici, 2018, pp. 61–72, doi: 10.1145/3198458.3198464.

[ECK19] M. Eckhart, A. Ekelhart, E. Weippl, “Migliorare la consapevolezza della situazione informatica per i sistemi ciberfisici attraverso i gemelli digitali”. Nel 2019 24a conferenza internazionale IEEE sulle tecnologie emergenti e l'automazione di fabbrica (ETFA), IEEE, pp. 1222-1225, 2019.

[ECK19a] M. Eckhart e A. Ekelhart, “Digital Twins for Cyber-Physical Systems Security: State of the Art and Outlook”, in Sicurezza e qualità nell’ingegneria dei sistemi cyber-fisici: con prefazioni di Robert M. Lee e Tom Gilb, S. Biffl, M. Eckhart, A. Lüder e E. Weippl, Eds. Cham: Springer International Publishing, 2019, pp. 383–412.

[ECL22] "Eclipse Ditto", disponibile online: https://www.eclipse.org/ditto/ (accesso nel 2022).

[ELE22] G. 2016. online: https://www.ge.com/digital/sites/default/files/download_assets/Digital Elettrico, Digitale Gemelli, Disponibile digital-power-plant-.pdf (ultimo accesso nel 2022).

[FINE95] R. Endsley, “Verso una teoria della consapevolezza della situazione nei sistemi dinamici”, Human Factors: The Journal of the Human Factors and Ergonomics Society, vol. 37, numero 33, pp. 32-64, 1995.

[FAC20] "Factoriy I/O Next-Gen PLC Training", Real Games, 2020. Disponibile online: https://realgames.co/ (accesso nel 2022).

[FLA22] F. Flammini, C. Alcaraz, E. Bellini, S. Marrone, J. Lopez e A. Bondavalli, "Towards Trustworthy Autonomous Systems: Taxonomies and Future Perspectives", in IEEE Transactions on Emerging Topics in Computing, doi: 10.1109/TETC .2022.3227113, 2022.

[GE22] General Electric, "GE presenta la soluzione di difesa informatica attiva in tempo reale per i sistemi di controllo industriale denominata Digital 2022, online: https://www.ge.com/research/newsroom/ge-unveils-real-time-active-cyber -soluzione di difesa-sistemi-di-controllo-industriale-denominata (accesso 02-2022). Disponibile

[GEH20] C. Gehrmann e M. Gunnarsson, "Un'architettura di sicurezza del sistema di controllo e automazione industriale basata su digital twin", in IEEE Transactions on Industrial Informatics, vol. 16, n. 1, pp. 669-680, gennaio 2020, doi: 10.1109/TII.2019.2938885.

[GRA17] Graessler, I.; Poehler, A. Integrazione di un gemello digitale come rappresentazione umana in una procedura di pianificazione di un sistema di produzione cyber-fisico. Negli atti della conferenza internazionale IEEE 2017 sull'ingegneria industriale e sulla gestione dell'ingegneria (IEEM), Singapore, 10-13 dicembre 2017.

[GRI14] M. Grieves, “Digital Twin: eccellenza produttiva attraverso la replicazione della fabbrica virtuale”, Libro bianco, 2014. Disponibile online: https://www.3ds.com/fileadmin/PRODUCTS SERVICES/DELMIA/ PDF/Whitepaper/DELMIA-APRISO-Digital-Twin-Whitepaper.pdf

[HAL15] E. Haleplidis, K. Pentikousis, S. Denazis, J. Hadi Salim, D. Meyer, O. Koufopavlou, "Software-Defined Networking (SDN): livelli e terminologia dell'architettura", IRTF, 2015. Disponibile online: https://www.rfc-editor.org/rfc/pdfrfc/rfc7426.txt.pdf (accesso 04-2022).

[HOL21] D. Holmes, M. Papathanasaki, L. Maglaras, M. Ferrag, S. Nepal, H. Janicke, “Digital Twins e Cyber Security: soluzione o sfida?”. Nel 2021 6a conferenza South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media (SEEDA-CECNSM), pp. 1-8, IEEE, 2021.

[IBM22] "Digital Twin: Helping machines tell story", disponibile online: https://www.ibm.com/internet-of-things/ trending/digital-twin (accesso 02-2022). loro

[IIC20] Industrial IoT Consortium (IIC), Digital Twins for Industrial Applications, un consorzio Internet industriale Disponibile online: https://www.iiconsortium.org/pdf/IIC_Digital_Twins_Industrial_Apps_White_Paper_2020-02-18.pdf (accesso nel 2022). Biancoa Carta,

[IIC22] Industrial IoT Consortium (IIC), disponibile online: https://www.iiconsortium.org (accesso nel 2022).

[ISO21a] Organizzazione internazionale per la standardizzazione (ISO), ISO 23247-1:2021, Sistemi di automazione e integrazione — Quadro dei gemelli digitali per il settore manifatturiero — Parte 1: Panoramica e principi generali, 2021, Disponibile online: https://www.iso.org/standard/ 75066.html (accesso nel 2022).

[ISO21b] International Standard Organization (ISO), ISO 23247-2:2021, Sistemi di automazione e integrazione — Digital twin framework for manufacturing — Parte 2: Architettura di riferimento, 2021, disponibile online: https://www.iso.org/standard/78743. html (accesso nel 2022).

[ISO22] International Standard Organization (ISO), disponibile online: https://www.iso.org/about us.html, (accesso nel 2022).

[JAR20] A. Jaribion, SH Khajavi, M. Öhman, A. Knapen, J. Holmström, "Un gemello digitale per la sicurezza e la gestione del rischio: un prototipo per un recipiente ad alta pressione a idrogeno". In Conferenza internazionale sulla ricerca scientifica del design nei sistemi e nelle tecnologie dell'informazione, Springer, pp. 369-375, 2020.

[JIE20] L. Jiewu, L. Qiang, Y. Shide, J. Jianbo, W. Yan, Z. Chaoyang, Z. Ding, C. Xin, “Riconfigurazione rapida guidata da Digital Twin del sistema di produzione automatizzato tramite un modello di architettura aperta, "Robotica e produzione integrata con computer, volume 63, 2020, 101895, ISSN 0736-5845, https://doi.org/10.1016/j.rcim.2019.101895

[KAR22] Karin, "Che cos'è un 3DEXPERIENCE Twin?", 07/01/2019. Disponibile online: https://blogs.3ds.com/exalead/2019/07/01/what-is-3dexperience-digital-twin-part-1-12-2/ (accesso 02-2022).

[KRI18] W. Kritzinger, M. Karner, G. Traar, J. Henjes e W. Sihn, Digital Twin nel settore manifatturiero: una revisione e classificazione categorica della letteratura, IFAC-PapersOnLine, 51(11), 1016-1022, 2018.

[LIU18] Z. Liu, N. Meyendorf e N. Mrad, "Il ruolo della fusione dei dati nella manutenzione predittiva utilizzando Digital Twin", vol. 1949, pag. 020023, 04 2018.

[LOC20] A. Löcklin, M. Müller, T. Jung, N. Jazdi, D. White e M. Weyrich, "Digital Twin for Verification and Validation of Industrial Automation Systems – a Survey", 2020 IEEE International Conference on Emerging Technologies and Factory Automazione (ETFA), 2020, pp. 851-858, doi: 10.1109/ETFA46521.2020.9212051.

[MIH22] S. Mihai, M. Yaqoob, DV Hung, W. Davis, P. Towakel, M. Raza, M. Karamanoglu, B. Barn, D. Shetve, RV Prasad, H. Venkataraman, R. Trestian, HX Nguyen, "Digital Twins: A Survey on Enabling Technologies, Challenges, Trends and Future Prospects", in IEEE Communications Surveys & Tutorials, doi: 10.1109/*COMST*.2022.3208773. 2022,

[MIN20] R. Minerva, GM Lee e N. Crespi, "Digital Twin in the IoT Context: A Survey on Technical Features, Scenarios, and Architectural Models", in Proceedings of the IEEE, vol. 108, n. 10, pp. 1785-1824, ottobre 2020, doi: 10.1109/JPROC.2020.2998530.

[MOH22] Abubakar Sadiq Mohammed, Neetesh Saxena e Omer Rana. 2022. Ruote sul Modbus: attacco alle comunicazioni ModbusTCP. Negli atti della 15a conferenza ACM sulla sicurezza e la privacy nelle reti wireless e mobili (WiSec '22). Associazione per le macchine informatiche, New York, NY, USA, 288–289. https://doi.org/10.1145/3507657.3529654

[MYL21] M. Mylrea, M. Nielsen, J. John, M. Abbaszadeh, Sistema immunitario industriale digital twin: sicurezza informatica basata sull'intelligenza artificiale per infrastrutture critiche. In Ingegneria dei sistemi e intelligenza artificiale, Springer, pp. 197-212, 2021.

[NAT20] S. Nativi, B. Delipetrev, M. Craglia, Destination Earth: Survey on “Digital Twins” technologies and actions, in the Green Deal area, EUR 30438 EN, Ufficio delle pubblicazioni dell'Unione europea, Lussemburgo, ISBN 978-92-76 -25160-6, doi:10.2760/430025, JRC122457, 2020.

[NIST18] National Institute of Standards and Technology (NIST), Cybersecurity Framework, versione 1.1, 2018, disponibile online: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (accesso 07-2022).

[NIST21] National Institute of Standards and Technology (NIST), Considerazioni sulla tecnologia dei gemelli digitali e sugli standard emergenti: bozza NISTIR 8356, 2021, disponibile online: https://www.nist.gov/news-events/news/2021/04/considerations- digital-twin-technology e-emerging-standards-draft-nistir (accesso 07-2022).

[PRA22] NH Praddaude, N. Hogrel, M. Gay, U. Baumann e A. Bécue, “Modelling & Simulation of a Rivet Shaving Process for the Protection of the Aerospace Industry Against Cyber Threats”, Atti della 35a conferenza annuale europea di simulazione e modellazione , EUROSIS, in corso di stampa.

[PTC22] "Core PLM Meets IoT and Augmented Reality", disponibile online: https://www.ptc.com/pt/products/plm/plm-products/windchill (accesso 02-2022).

[QIA22] Qian, C.; Liu, X.; Ripley, C.; Qian, M.; Liang, F.; Yu, W. Digital Twin: replica cibernetica di cose fisiche: architettura, applicazioni e direzioni di ricerca future. Il futuro di Internet 2022, 14, 64. https://doi.org/10.3390/fi14020064

[RAG20] Raguvir, S.; Babu, S. Rilevamento di anomalie negli utenti: un approccio UEBA. Negli atti della conferenza internazionale sull'ingegneria industriale e sulla gestione delle operazioni, Dubai, Emirati Arabi Uniti (EAU), 10–12 marzo 2020.

[ROSSO19] AJH Redelinghuys, AH Basson e K. Kruger. "Un'architettura a sei livelli per il Digital Twin: un'implementazione di un caso di studio nel settore manifatturiero." Giornale della produzione intelligente (2019): 1-20.

[ROE19] M. Roest, "Una piattaforma open source per i gemelli digitali?", 6 05 2019. Disponibile online: https://www.linkedin.com/pulse/open-source-platform-digital-twins-mark-roest/ (accesso nel 2022).

[SAA20] A. Saad, S. Faddel, T. Youssef, OA Mohammed, Sull'implementazione del gemello digitale basato sull'IoT per la resilienza delle microreti in rete contro gli attacchi informatici. Transazioni IEEE sulla rete intelligente, 11(6), 5138-5150, 2020.

[SDE17] R. Sderberg, K. Wrmejord, JS Carlson e L. Lindkvist, "Verso un gemello digitale per la garanzia della geometria in tempo reale nella produzione individualizzata", Cirp Annals Manufacturing Technology, 2017.

[VEDI22] "Piattaforma IoT industriale Seebo", disponibile online: https://www.seebo.com/iot-platform/ (accesso nel 2022).

[VEDI22] "Piattaforma IoT industriale Seebo", disponibile online: https://www.seebo.com/iot-platform/ (accesso nel 2022).

[SHI19] S. Shin, "Introduzione a mago3D, una piattaforma di gemello digitale basata su open source", 18 luglio 2019. Disponibile online: https://pt.slideshare.net/endofcap/introduction-to-mago3d-an open-source-based-piattaforma gemella digitale (accesso nel 2022).

[SIE20] "Il gemello digitale completo per l'intralogistica", SIEMENS, 11 marzo 2020. Disponibile online: https://press.siemens.com/global/en/feature/intralogistics (ultimo accesso nel 2022).

[SIN21] Singh, M.; Fuenmayor, E.; Hinchy, EP; Qiao, Y.; Murray, N.; Devine, D. Gemello digitale: dall'origine al futuro. *Appl. Sist. Innov.* **2021,** 4, 36. https://doi.org/10.3390/asi4020036 V. Souza, R. Cruz, W.

[SOU19] Silva, S. Lins e V. Lucena, "Un'architettura gemella digitale basata sulle tecnologie dell'Internet delle cose industriale" ," Conferenza internazionale IEEE 2019 sull'elettronica di consumo (ICCE), 2019, pp. 1-2, doi: 10.1109/ICCE.2019.8662081.

[STR18] F. Strohmeier, C. Schranz e G. Güntner, "i-Maintenance: A Digital Twin for Smart Maintenance", 23 online: https://ercim news.ercim.eu/en115/special/2093-i-maintenance-a-gemello digitale per la manutenzione intelligente (accesso nel 2022).

[TAO17] F. Tao, Y. Cheng, J. Cheng, M. Zhang, W. Xu e Q. Qi, "Teorie e tecnologie per la fusione cyber-fisica nell'officina del Digital Twin". CIMS (Sistemi di produzione integrati al computer), agosto 2017, v. 23, n. 8, pag. 1603-1611.

[VIE21] Vielberth, M., Glas, M., Dietz, M., Karagiannis, S., Magkos, E., Pernul, G. (2021). Una gamma informatica basata su digital twin per gli analisti SOC. In: Barker, K., Ghazinour, K. (a cura di) Sicurezza e privacy dei dati e delle applicazioni XXXV. DBSec 2021. Lecture Notes in Computer Science(), vol 12840. Springer, Cham. https://doi.org/10.1007/978-3-030-81242-3_17

[W3C20] W3C, Digital Twin, Web of Things (WoT) Architecture, 2020. Disponibile online: https://www.w3.org/TR/wot-architecture/ (accesso nel 2022).

[WAN17] Wang, D.; Chen, J.; Zhao, D.; Dai, F.; Zheng, C.; Wu, X. Monitoraggio dell'attenzione e della vigilanza dei lavoratori nelle attività di costruzione attraverso un sistema di elettroencefalografia wireless e indossabile. Autom. costr. 2017, 82, 122–137.

[WAN19] L. Wang e AM Canedo, "Interfacce di programmazione umana per interfacce uomo-macchina", 2019.

[WAN22] Z. Wang et al., "Mobility Digital Twin: concetto, architettura, caso di studio e sfide future", in IEEE Internet of Things Journal, doi: 10.1109/JIOT.2022.3156028.

[WRL22] WRLD3D, disponibile online: https://www.wrld3d.com/ (accesso nel 2022).

[WU19] Wu, Mingtao. "Rilevamento delle intrusioni per attacchi cyber-fisici nei sistemi di produzione informatica." Diss. di dottorato, Syracuse University, 2019. http://dx.doi.org/10.1115/IMECE2019-10135

[WU21] Y. Wu, K. Zhang e Y. Zhang, "Digital Twin Networks: a Survey", in IEEE Internet of Things Journal, doi: 10.1109/JIOT.2021.3079510.

[XU21] Q. Xu, S. Ali, T. Yue, rilevamento di anomalie basato su Digital Twin nei sistemi cyber-fisici. Nel 2021 14a IEEE Conference on Software Testing, Verification and Validation (ICST), IEEE, pp. 205-216), 2021.

[Xu21] X. Xu,, Y. Lu, B. Vogel-Heuser, L. Wang, Industria 4.0 e Industria 5.0—Inizio, concezione e percezione. Giornale dei sistemi di produzione, 61, 530-535, 2021.

[YUQ20] L. Yuqian, L. Chao, IW Kevin, H. Huiyue, X. Xun, "Produzione intelligente guidata da gemelli digitali: connotazione, modello di riferimento, applicazioni e problemi di ricerca", Robotica e produzione integrata con computer, volume 61, 2020, 101837, ISSN 0736-5845, https://doi.org/10.1016/j.rcim.2019.101837.

[ZAD16] Van Zadelhoff, M. Le maggiori minacce alla sicurezza informatica si trovano all'interno della tua azienda. 2016. Disponibile online: https: //hbr.org/2016/09/the-biggest-cybersecurity-threats-are-inside your-company (accesso 02-2022).

[ZHE18] Y. Zheng, S. Yang e H. Cheng, "Un quadro applicativo di Digital Twin e il suo caso di studio", Journal of Ambient Intelligence & Humanized Computing, vol. 10, 2018.

[ZHE19] Y. Zheng, S. Yang e H. Cheng, "Un quadro applicativo di Digital Twin e il suo caso di studio". J Ambient Intell Human Comput 10, 1141–1153 (2019). https://doi.org/10.1007/s12652-018-0911-3

[ZHO21] C. Zhou, H. Yang, X. Duan, D. Lopez, A. Pastor, Q. Wu, M. Boucadair, C. Jacquenet, "Concepts of Digital Twin Network", IRTF, draft-zhou-nmrg-digitaltwin- network-concepts 03, 2021. Disponibile online: https://datatracker.ietf.org/doc/pdf/draft-zhou-nmrg-digitaltwin network-concepts-03.pdf (accesso nel 2022).

Ringraziamenti

Il WG6 dell'Organizzazione europea per la cibersicurezza (ECSO) mira a contribuire a definire la tabella di marcia e la visione della ricerca e innovazione dell'UE sulla sicurezza informatica per rafforzare e costruire un ecosistema UE resiliente. Dall'analisi delle sfide della digitalizzazione della società e dei settori industriali, questo gruppo di lavoro identifica quali sono le capacità e le capacità per sostenere l'autonomia digitale dell'UE sviluppando e promuovendo tecnologie affidabili.

Quello che segue è uno speciale riconoscimento dei contributi attivi a vario titolo da parte dei membri del WG6 ECSO.

CONTRIBUTI DEGLI ESPERTI: Cristina Alcaraz (Università di Malaga), Alessandro Savini (Deloitte), Andrea Melis (Università di Bologna), Adrien Becue (Airbus), Ángel J. Gavín Alarcón (GMV), Andris Soroka (DSS), Costanza Pestarino (ECSO), Csaba Virag (Talgen), David Allison (AIT austriaco
Institute of Technology),Dimitris Kavallieros (Information Technologies Institute), Dimitris Lyras (Ulysses Systems), Eduard Hoeberichts (Sandgrain), Francesco Tozzi (Deloitte), Franco Callegati
(Università di Bologna), Herve Debar (IMT - Telecom-Sud Parigi), Isabel Praça (ISEP), Jacques.Kruse-Brandao (SGS), Jeroen Doumen (Sandgrain), Lorenzo Russo (Deloitte), Marco Prandini (Università di Bologna), Mario Barile (ENG), Mario Reyes De Los Mozos (Eurecat Center Tecnològic), Martin Stierle (AIT Austrian Institute of Technology), Matthias Hiller (Fraunhofer Institut), Paivi Mattila (Laurea University of Applied Sciences), Paolo Roccetti (ENG), Paul Smith (AIT Austrian Institute of Technology), Roberto Cascella (ECSO), Vito Morreale (ENG).