UNIVERSITA' POLITECNICA DELLE MARCHE

FACOLTA' DI INGEGNERIA

Corso di Laurea triennale in Ingegneria Gestionale

I Cyber Physical System per la gestione della sicurezza

Cyber Physical Systems for security management

Relatore:

Prof. Maurizio Bevilacqua

Tesi di Laurea di:

Michela Scrosta

1079479

Anno Accademico 2018 / 2019

Indice

ABSTRACT

I continui avanzamenti della tecnologia nel contesto dell'Industria 4.0 stanno evolvendo sempre più nell'ambito industriale con l'obiettivo di rendere unico e integrato l'intero sistema di strumentazione. La completa integrazione di strumentazione, comunicazione e controllo nei sistemi fisici ha portato allo studio dei sistemi informatici-fisici (CPS), un campo che ha recentemente attirato maggiore attenzione. I sistemi CPS sono dotati di una parte fisica e di una parte informatica mettendo in comunicazione tutte le parti di un intero sistema attraverso processi fisici, reti e calcoli strettamente integrati come IoT (Internet of Things) e Cloud Computing. Se lo sviluppo continuo delle funzioni e la capacità di integrazione sono punti di forza di questi sistemi, non si può dire lo stesso della loro sicurezza, soprattutto nel campo informatico. Una preoccupazione fondamentale che è onnipresente nei CPS è la necessità di garantire la sicurezza di fronte agli attacchi informatici. Lo dimostrano alcuni esempi di attacchi informatici che hanno causato notevoli danni negli ultimi anni come Stuxnet in Iran e l'attacco aereo RQ-170. I principali attacchi informatici sono classificabili e analizzabili a livello di percezione, a livello di trasmissione e a livello di applicazione.

Data l'importanza della sicurezza in questi sistemi si stanno sviluppando alcune soluzioni per proteggere i CPS da possibili attacchi a strato singolo e a multistrato comprendendo tutti e tre i livelli. In particolare, presentiamo STPA-SafeSec, una nuova metodologia di analisi per la sicurezza. I suoi risultati mostrano le dipendenze tra le vulnerabilità della sicurezza informatica e la sicurezza del sistema. Utilizzando queste informazioni, la più efficace delle strategie di mitigazione per garantire la sicurezza del sistema possono essere facilmente identificate. Analizzeremo un approfondimento dei sistemi cyber-fisici robotici collaborativi industriali (CRCPS) nel campo della sicurezza introducendo un quadro di sicurezza per l'applicazione della collaborazione uomo-robot in un contesto futuristico di sistema cibernetico dell'industria 4.0.

Infine, saremo in grado fare un'osservazione conclusiva e generale della sicurezza nel campo cyber fisico e degli sviluppi raggiunti finora in questo ambiente industriale proseguendo in questa direzione, evidenziando le caratteristiche da migliorare e discutendo possibili lavori futuri.

1. INDUSTRY 4.0 e CYBER PHYSICAL SYSTEM

1.1 Industria 4.0

Attualmente diverse tecnologie dirompenti stanno avendo un impatto significativo sulle industrie manifatturiere e di processo, quando si considerano gli aspetti informatici. Questi approcci stanno avendo un impatto significativo e rapido su come sono organizzate e gestite le industrie manifatturiere e di processo. Per inserire questi cambiamenti nel contesto e comprendere il termine Industria 4.0, è necessaria una breve panoramica dello sviluppo industriale per evidenziare i driver significativi:

- Industria 1.0: durante il diciottesimo secolo la produzione passò da un'attività manuale a una macchina basata, in gran parte attraverso lo sviluppo del motore a vapore durante la rivoluzione industriale. Inoltre, i singoli processi produttivi sono stati più compresi con una solida base scientifica.
- Industria 2.0: all'inizio del XX secolo, la produzione è stata razionalizzata utilizzando ingegneria di precisione, divisione del lavoro, standardizzazione e catena di montaggio. Ciò ha consentito la produzione in serie di prodotti che vanno dalla macchina da scrivere all'auto.
- Industria 3.0: lo sviluppo della tecnologia informatica, l'elaborazione delle informazioni e l'automazione portano all'introduzione di sistemi di produzione flessibili, produzione integrata al computer e gestione delle risorse aziendali durante l'ultima parte del ventesimo secolo.
- Industria 4.0: l'uso delle tecnologie dell'informazione e della comunicazione sta avendo un profondo impatto sulla produzione. Attualmente ciò sta portando allo sviluppo di concetti tra cui produzione e fabbriche intelligenti e produzione di cloud. L'industria 4.0 incorpora diverse tecnologie tra cui sistemi cyber fisici, modelli di servizi di cloud computing, intelligenza artificiale e gestione dei dati per raggiungere la massima produttività.

1.2 Cyber Physical System

Cosa sono i Cyber Physical System e in che modo facilitano l'evoluzione delle aziende?

Quando si parla di innovazioni tecnologiche chiave dell'industria 4.0, non si può non fare riferimento ai Cyber Physical Systems (CPS) o Sistemi Cyber Fisici, considerati

efficienti, soprattutto quando si parla di potenzialità, smart manufacturing ed evoluzioni dei business model delle aziende.

L'Industry 4.0 (I4.0) viene indicata da tutti, come l'opportunità di stravolgere i paradigmi industriali previsti dalle tecnologie abilitanti, individuate dal governo nel piano industriale: Industria 4.0.

Quando si parla di tecnologie abilitanti dell'industria 4.0, si fa riferimento a:

- Internet of Things;
- Realtà Aumentata;
- BigData Analitycs;
- Cloud;
- Simulazione di Processo.

Tali tecnologie, insieme al Cyber Physical System, generano un sistema autonomo, intercomunicante e intelligente e, pertanto, capace di facilitare l'integrazione tra soggetti diversi e fisicamente distanti. L'applicazione di ciascuna di queste tecnologie abilitanti dell'I4.0, deve necessariamente comprendere l'armonizzazione di software e hardware, per permettere la comunicazione tra le diverse componenti fisiche di un sistema anche se, molto distanti fisicamente. Ai sistemi che presentano questa particolare caratteristica è possibile associare l'appellativo di Cyber Physical Systems (CPS).

Una delle figure più influenti in questo ambito, Edward A. Lee, definisce i CPS come "integrazioni di processi fisici e computazionali. Reti di sistemi integrati monitorano e controllano il processo fisico, abitualmente con feedback retroattivi, con il processo fisico che influenza la computazione e viceversa". Per ciascuna parte hardware (physical), dovrà quindi essere creata una corrispondente parte software (cyber), che permetterà alle diverse componenti fisiche di sistemi anche molto complessi, di scambiare informazioni sia tra di loro, sia con gli utenti umani, con l'obiettivo di monitorare, gestire e controllare i sistemi stessi. Ad ogni componente ed eventualmente ad un intero sistema, sarà possibile quindi associare quello che comunemente viene indicato come Digital Twin, letteralmente un "gemello digitale" da intendere come un'esatta rappresentazione "cyber" della corrispondente parte "physical". L'utilizzo dei Cyber Physical System (e del Digital Twin) permetterà quindi di riprodurre qualsiasi tipo di sistema che potrà riguardare gli

ambiti più disparati (medicale, industriale, domotica, costruzioni, energia, sicurezza, gestione delle informazioni, trasporti, servizi di vendita ecc.).

La possibilità di comunicazione in tempo reale tra le diverse parti fisiche di uno stesso sistema potrà rendere il sistema stesso autonomo e capace di assumere la migliore decisione strategica possibile. Sarà possibile seguire un prodotto in tutto il suo ciclo di vita, in modo da migliorare l'esperienza di utilizzo e facilitare i rapporti con i clienti. Nonostante siano numerosissime la possibilità applicazioni e i vantaggi che ne deriverebbero, la creazione di un Cyber Physical System non è comunque esente da problematiche tecniche che riguardano ad esempio, la necessità di mettere in rete e quindi in interazione, sistemi di controllo estremamente eterogenee.

I sistemi informatici fisici (CPS) sono una combinazione di processi fisici, reti e calcoli strettamente integrati. Il processo fisico è monitorato e controllato da sottosistemi incorporati (cyber) tramite sistemi in rete con circuiti di feedback per modificare il loro comportamento quando necessario. Questi sottosistemi funzionano indipendentemente l'uno dall'altro con la capacità di interagire con l'ambiente esterno. I processi fisici sono raggiunti da numerosi piccoli dispositivi con capacità di rilevamento, elaborazione e comunicazione (spesso wireless). Questi dispositivi fisici possono essere identificati con attributi fisici o apparecchiature di rilevamento delle informazioni, come sensori a infrarossi o identificazione a radiofrequenza (RFID), e possono quindi essere collegati a un sistema di rete, nella maggior parte dei casi Internet, per inviare i dati acquisiti al sottosistema computazionale.

Con l'accresciuta attenzione alla capacità di gestione dei dati, alla capacità di comunicazione dei dati e all'integrazione dei sistemi di informazione, nonché dei dispositivi fisici, aumenta anche la domanda di integrazione di CPS in diversi settori, con la conseguente attenzione ampiamente acquisita non solo dalle università e dai laboratori di ricerca e sviluppo ma anche dall'industria e dalle agenzie governative.

Prima dell'attuale modulo, CPS si è evoluto attraverso diverse fasi: sistemi integrati, sistemi integrati intelligenti e sistemi di sistemi. L'attuale forma di CPS viene utilizzata in molte aree diverse come l'energia, il petrolio, l'industria dell'acqua, l'ingegneria chimica, l'assistenza sanitaria, la produzione, i trasporti, i sistemi automobilistici, l'intrattenimento, gli elettrodomestici di consumo, oltre a molte altre aree che sono

direttamente correlate alle persone vite quotidiane. È stato stimato che i componenti cyber fisici rappresenterebbero il 40% del valore totale di un'automobile entro la fine del 2015 e che nel 2020 verranno utilizzati circa 25 miliardi di oggetti identificati in modo univoco.

CPS ha molte caratteristiche, come consentire ai singoli componenti di lavorare insieme, producendo sistemi complessi. In CPS, i dati possono essere acquisiti da oggetti fisici o dispositivi sensori e trasferiti attraverso le reti al sistema di controllo con l'assenza, in alcuni casi, di qualsiasi interazione uomo-macchina. Gli oggetti fisici sono sempre più dotati di, ad esempio, sensori a infrarossi, codici a barre o tag RFID che possono essere scansionati da dispositivi intelligenti. Questi dispositivi possono essere collegati a Internet per inviare i dati identificativi e il posizionamento della posizione da utilizzare per il monitoraggio e la gestione dell'ambiente fisico.

Le unità di elaborazione che possono anche essere posizionate nel cloud, con le decisioni risultanti emesse come azioni per gli oggetti fisici. Come esempio di CPS, i sistemi di controllo industriale (ICS) sono isolati dai protocolli di comunicazione e dai sistemi operativi dai sistemi esterni.

Per il momento, questo tipo di sistemi sono sempre più correlati su Internet per migliorare funzionalità e automazione. La maggiore connettività del mondo cibernetico e fisico comporta notevoli sfide per la sicurezza del CPS. L'importanza di questi sistemi sta nel migliorare la funzionalità, l'interconnettività tra i sottosistemi CPS in aumento.

L’approccio è rivoluzionario: disponendo di un’intelligenza decentrata, i sistemi cyber-fisici sono in grado di valutare situazioni e prendere decisioni autonomamente nonché di provvedere che gli altri sistemi cyber-fisici svolgano delle azioni, quando necessario. Questi comportamenti sono stati programmati e sono addirittura in grado di cambiare e di adattarsi. Il processo decisionale gerarchico/verticale come adottato per decenni nella prassi quotidiana degli impianti di produzione, viene così eliminato o comunque ampiamente integrato.

Si ricorda brevemente come funzionava questo processo decisionale in una struttura gerarchica. I componenti (in particolare i sensori) rilevavano lo stato effettivo del processo e comunicavano tutte le informazioni importanti all’unità di controllo centrale. A livello dell’unità di controllo o anche del sistema di gestione sopraordinato veniva poi analizzato lo stato effettivo del processo, venivano prese decisioni e si interveniva nel

processo con l'aiuto di attuatori o con azioni manuali. Con i CPS non si vuole eliminare questa comunicazione dalla struttura gerarchico-verticale, bensì integrarla in maniera ottimale. Tre sottosistemi consentono al sistema cyber-fisico di svolgere con successo il suo nuovo ruolo: sensori, attuatori e sistemi embedded, un'intelligenza decentralizzata basata su microprocessore. Con l'aiuto dei sensori integrati, il CPS è in grado di rilevare autonomamente la sua attuale situazione all'interno dell'ambiente in cui si trova. I sensori ottici di una macchina, ad esempio, possono fornire informazioni approfondite sulla tipologia e sullo stato dei pezzi da lavorare. Gli attuatori servono a svolgere azioni, per esempio ad azionare un braccio di presa per prelevare determinati pezzi da lavorare. L'intelligenza decentrata valuta sia le informazioni dei sensori che le informazioni fornite da altri CPS. Basandosi su di esse, prende le sue decisioni e le comunica a sua volta ai suoi attuatori. Parallelamente contatta altri CPS chiedendogli di svolgere determinate azioni. L'immagine virtuale dei sistemi cyber-fisici non va intesa come "istantanea" dello stato e delle interconnessioni attuali. L'immagine virtuale include piuttosto anche informazioni relative all'intero ciclo di vita del CPS. Già in fase di design nascono dati che comprendono informazioni sulla geometria, sulle caratteristiche meccaniche, su collegamenti logici e sui parametri. Tutte le ulteriori fasi del ciclo di vita come engineering, messa in servizio e funzionamento, manutenzione e assistenza tecnica incluse, aggiungono ulteriori informazioni. Basandosi su tutte queste informazioni, il sistema cyber-fisico è in grado di reagire autonomamente alle svariate situazioni. Idealmente, può impiegare le informazioni del passato a sua disposizione anche per stabilire nuove regole decisionali adattandole alla rispettiva nuova situazione. Su questa base, ogni CPS può ora disporre anche del know-how sulla sua integrazione nell'intero impianto di produzione. Questo può ad esempio essere sfruttato per far sì che i CPS si configurino da soli durante la messa in servizio, che avviino automaticamente la comunicazione con i loro partner di produzione (gli altri CPS), riducendo notevolmente i costosi tempi di messa in servizio. Dopodiché segue la fase di ottimizzazione durante la produzione stessa.

Grazie alla loro intelligenza, i CPS possono ottimizzarsi da soli. Nel più semplice dei casi può significare l'identificazione autonoma del punto di lavoro ottimale. In casi più complessi può tradursi nella scelta tra scenari di svolgimento predefiniti o addirittura nuovi. Qualora si dovessero verificare dei problemi in fase di produzione, ad esempio per un guasto ad un macchinario o per mancanza di materiale necessario, è possibile

sviluppare strategie alternative che "guariscono" il processo e lo mantengono in atto. Tuttavia, simili problemi andrebbero possibilmente evitati del tutto o almeno individuati in tempo debito facendo sì che i CPS generino informazioni di allarme preventivo consentendo di effettuare una manutenzione preventiva. I CPS supportano così in maniera ottimale in cosiddetto "Condition Monitoring", il monitoraggio delle condizioni operative.

La comunicazione decentrata tra i vari CPS non richiede necessariamente che avvenga direttamente da un CPS ad un altro CPS. Si prevede invece che già a breve nasceranno numerose piattaforme di comunicazione fra CPS. Queste piattaforme provvedono ad interconnettere con i loro servizi e le loro applicazioni persone, sistemi esterni e CPS. Entrambe le modalità di comunicazione – sia lo scambio diretto tra CPS che la comunicazione tra piattaforme per CPS – possono essere sfruttate in parallelo e si completano a vicenda in modo ottimale.

In alcune stazioni di produzione, un contenitore di trasporto cyber-fisico può comunicare direttamente con le stazioni poiché dispongono delle caratteristiche tecniche per farlo. Altre stazioni di produzione non dotate di una funzione CPS vengono invece controllate da una piattaforma CPS. In tal modo il contenitore di trasporto CPS può, in tutte le aree di produzione in cui è coinvolto, procedere alla richiesta di forniture o avviare successivi step di lavoro in maniera decentrata, ovvero anche senza passare per il livello di controllo.

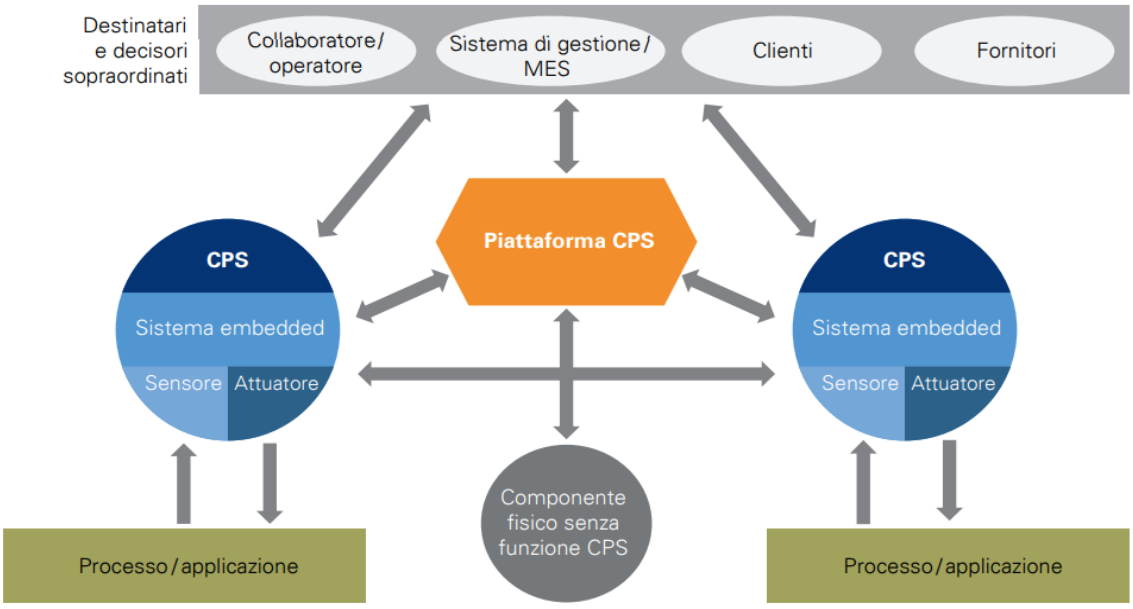


Figura 1

Al momento, ci sono esempi di applicazioni CPS in settori importanti e grandi infrastrutture in tutto il mondo. L'essenza principale di CPS è il sistema di controllo, in cui il software e la rete di comunicazione influenzeranno dinamicamente il sistema fisico. Fig.2 descrive le caratteristiche più chiaramente.

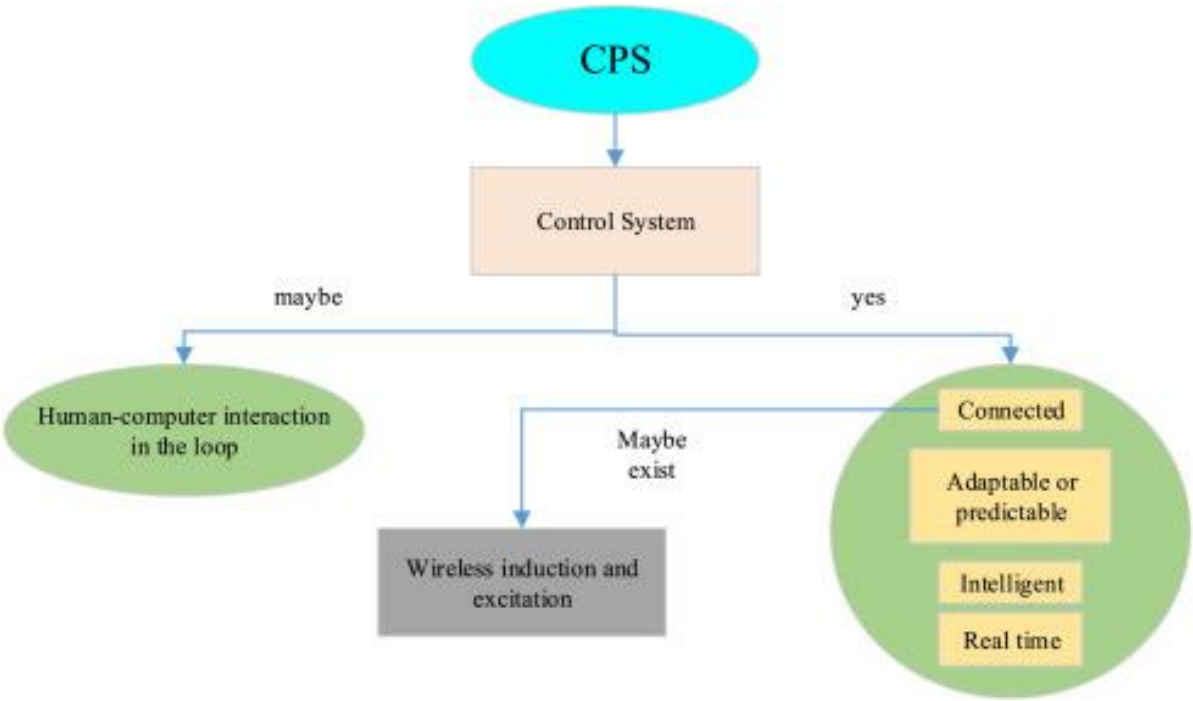


Figura 2

(1) L'interazione uomo-computer esiste in molti circuiti CPS.

(2) Il sistema fisico trasmette segnali continui o discreti al software attraverso la rete connessa. Lo stato del sistema fisico è continuo, ma il software intermedio può solo elaborare informazioni discrete e discretizzarle.

(3) CPS è di solito un circuito di controllo ad anello chiuso. Dopo che il CPS calcola ed elabora i segnali che riceve dal sistema fisico, invia segnali o stimoli ad esso. Il design del CPS deve essere adattabile per riflettere tempestivamente le variazioni delle condizioni. È anche prevedibile e prevede cambiamenti nei processi fisici

(4) L'introduzione dell'intelligence nel CPS è sia un'opportunità che una sfida. CPS sarà in grado di apprendere, comprendere e spiegare. È anche la direzione principale del futuro sviluppo di CPS.

(5) Il software CPS ha requisiti di temporizzazione più elevati. Alcune attività devono essere eseguite periodicamente e le loro scadenze e ritardi sono limitati.

In futuro, la valutazione del rischio di CPS diventerà ancora più importante. Perché non sta solo affrontando i rischi dello spazio fisico tradizionale, ma sta anche affrontando un gran numero di rischi per la sicurezza e attacchi dallo spazio delle informazioni, e può verificarsi la possibilità di guasti a cascata che possono ripetersi la trasmissione in spazi diversi. Lo spazio informazioni e lo spazio fisico in CPS sono strettamente accoppiati per formare una rete eterogenea complessa.

La rete virtuale dello spazio informazioni è senza scale. L'interdipendenza dei due strati di spazio tra queste reti eterogenee rende l'affidabilità del CPS molto più complessa di una singola rete. Pertanto, lo studio della valutazione del rischio di CPS contribuirà a migliorare la sua capacità di operare in modo sicuro e stabile in condizioni ambientali complesse future.

1.3 Un sistema cyber-fisico orientato all'intralogistica nel contesto di Industry 4.0

La logistica interna nell'officina è estremamente sofisticata per la variabilità e la complessità dei prodotti in ambiente Industria 4.0. Il Cyber-Physical System (CPS) che combina informatica, tecnologie dell'informazione e della comunicazione è una soluzione fondamentale per raggiungere l'Industria 4.0. Per far fronte alla produzione personalizzata, in officina sono richieste elevata flessibilità e capacità di riconfigurazione rapida della logistica interna.

Il CPS orientato all'intralogistica è discusso e viene qui di seguito presentata la struttura dei modelli nello spazio informatico per le apparecchiature nell'ambiente. Attraverso l'utilizzo di sensori e controller wireless, viene implementata una piattaforma di gestione remota. L'interconnessione delle apparecchiature, la programmazione logistica e il funzionamento remoto sono realizzati da terminali portatili via Internet.

La concorrenza sempre più agguerrita in tutto il mondo e lo sviluppo di tecnologie come Internet of Things(IoT) hanno promosso la quarta rivoluzione industriale. Le richieste di prodotti e servizi altamente individualizzati hanno causato l'estrema complessità dei materiali nelle fabbriche che non possono più far fronte a metodi per versi.

La logistica interna ed esterna devono adattarsi a questo ambiente per la stabilità e la puntualità della consegna o del trasporto. La programmazione della logistica in officina in questo ambiente è stata uno dei punti di forza della ricerca.

Il Cyber-Physical System (CPS) combina l'informatica, le tecnologie dell'informazione e della comunicazione per l'interazione tra il mondo fisico e quello cibernetico. Sensori e controller sono impiegati per il monitoraggio e il controllo dei processi fisici. Lo spazio informatico, che ha una forte capacità di elaborazione, archiviazione e simili, è responsabile dell'analisi dei dati per prendere decisioni strategiche sul mondo reale. L'intralogistica è il processo di consegna del materiale in officina che ha un impatto enorme sulla produzione.

Secondo il piano di produzione, una certa quantità di materie prime dovrebbe essere consegnata alle stazioni di lavoro in modo tempestivo e stabile. Vari veicoli, le attrezzature chiave che eseguono compiti logistici, ad esempio carrelli elevatori, gru e veicoli a guida automatica (AGV) sono impiegati per la consegna di questi materiali, semilavorati e produzione finita in officina. Gli AGV si sono sviluppati in apparecchiature affidabili ed efficienti dal loro debutto negli anni '50. È fondamentale garantire che gli AGV siano programmati in modo corretto ed efficiente per le elevate prestazioni dell'intralogistica nell'ambiente dell'industria 4.0. Mirato all'interazione di oggetti eterogenei, si tenta di fornire una soluzione basata su CPS per la logistica in officina.

Sono stati stabiliti modelli di processi tipici nel cyber spazio, ad esempio la logistica, mentre sono stati studiati i metodi di implementazione. Il framework del sistema cyber-fisico è stato proposto sulla base di IoT, Information Technology (IT) e altre tecnologie correlate.

Un modello di CPS proposto dal Laboratory for Machine Tools and Production Engineering della RWTH Aachen University è stato diviso in cinque livelli che sono condizioni generali che indicano impostazione di base, generazione di informazioni che significano trasparenza, elaborazione delle informazioni in piedi per aumentare la comprensione, collegamento di informazioni che indica il miglioramento del processo decisionale, e l'ultimo, che interagisce con i sistemi cyber-fisici per l'auto-ottimizzazione. La sensorizzazione del mondo fisico è principalmente nella creazione del livello di trasparenza, noto anche come secondo livello, attraverso la costruzione della condizione

di base per l'implementazione di CPS all'interno del primo livello. Gli altri tre livelli rappresentano il processo di analisi dei dati per una migliore cooperazione e collaborazione tra mondo fisico e cyber. Il modello di maturità sottolinea maggiormente l'analisi dei dati e lo scambio di informazioni. Tuttavia, ci sono alcune descrizioni sulla costruzione di sensori e ambiente di rete per l'implementazione di CPS. I metodi di acquisizione dei dati, la loro trasmissione e feedback sono fondamentali per la cyber fusion fisica. Per gestire l'intralogistica in modo più specifico e diretto, il quadro a quattro livelli per CPS orientato all'intralogistica è stato presentato nella figura 3.

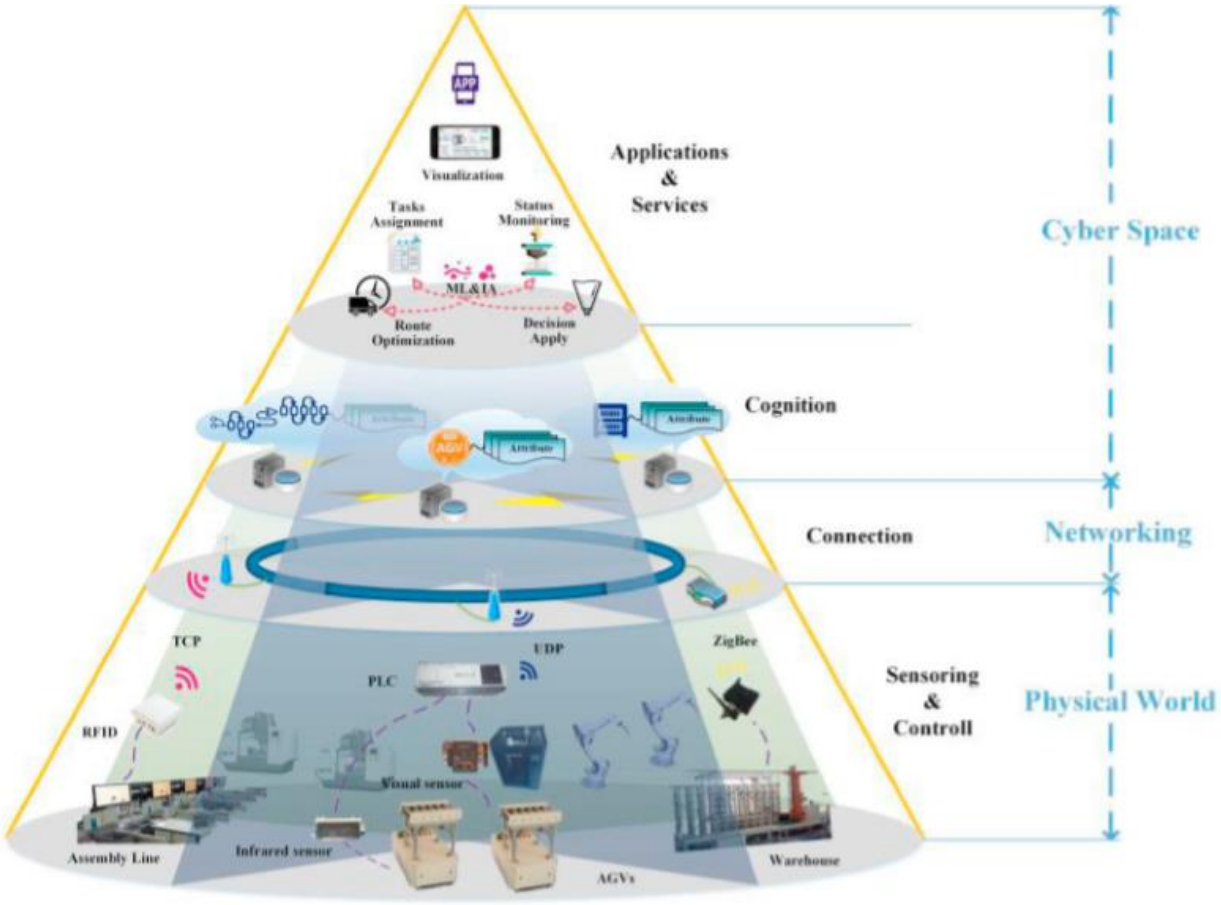


Figura 3

Il primo livello è l'acquisizione dei dati da materie prime correlate, semilavorati, prodotti finiti e attrezzature. Tramite sensori, controller o persino sistemi di gestione, i dati delle entità fisiche vengono misurati o ottenuti.

Ad esempio, le informazioni sulle parti vengono acquisite dal sistema RFID e la posizione degli AGV viene misurata dai sensori di immagine lungo le barre dei codici. Il secondo

livello, mostrato in Fig.3, è il networking. Ogni entità nell'officina è collegata insieme tramite questa rete, il che significa che il mondo fisico e lo spazio cibernetico sono interattivi. Protocollo di trasferimento come TCP (Transmission Control Protocol), UDP (User Datagram Protocol) sono supportati da questa rete per consapevolezza e controllo collaborativi. Nel frattempo, i dati e le conoscenze correlate vengono archiviati al terzo livello, ovvero come livello di cognizione in cui è possibile condurre il cloud computing e l'analisi. In base alla conoscenza, applicazioni e servizi sono distribuiti nell'ultimo livello, per soddisfare il controllo a circuito chiuso con o senza intervento umano.

Le applicazioni supportate da algoritmi intelligenti e machine learning sono suddivise in assegnazione di attività, pianificazione del percorso, processo decisionale e così via. La generazione, l'elaborazione, il collegamento e persino l'interazione delle informazioni del sistema cyber-fisico potrebbero essere realizzate in questo quadro.

1.4 Collocazione dei CPS nel contesto dell'Industria 4.0

Nella vasta nomenclatura dell'Industria 4.0, il concetto dei "Sistemi cyber-fisici", in breve CPS, è quello che probabilmente suscita il maggior stupore ed è tra i meno conosciuti. Prima di approfondire il termine ed il suo significato, desideriamo inquadrarlo nel contesto dell'Industria 4.0.

L'Industria 4.0 (la cosiddetta quarta rivoluzione industriale) punta sostanzialmente ad incrementare al massimo l'adattabilità dell'Europa come sito di produzione in generale e dei singoli impianti di produzione nello specifico.

In ultima analisi si mira a mantenere la competitività a livello internazionale, messa in pericolo dai paesi con un basso costo del lavoro e dai paesi con mercati emergenti. Il concetto di base è semplice: un'unità di produzione deve essere in grado di adattarsi in tempi brevissimi alle nuove richieste ed esigenze dei clienti. Questo adattamento efficiente comporta al contempo un'efficienza a livello di risorse, poiché vengono integrate tutte le fasi di produzione a monte e a valle e si producono unicamente i prodotti di partenza realmente necessari. E poiché solo un'integrazione ottimale dell'uomo e delle sue (rispettive) capacità permette di ottenere un sistema di produzione flessibile e adattabile, si punta ad un'ulteriore umanizzazione del lavoro.

Come si intende quindi realizzare questa individualizzazione e flessibilizzazione? Un aspetto centrale consiste nel collegare fra loro macchine, mezzi di esercizio, utensili, sistemi di magazzinaggio e anche i prodotti da fabbricare. Questa interconnessione viene descritta spesso anche come "Internet delle Cose" e una fabbrica così collegata è definita "Smart Factory". Ma come è possibile interconnettere degli oggetti? Per una migliore comprensione occorre spiegare il concetto dell'immagine virtuale. Nel mondo reale, tutti i componenti fisici non umani coinvolti nel processo di produzione come ad esempio i macchinari, non esistono solo come li percepiamo con i nostri cinque sensi.

Nell'Industria 4.0 esistono anche all'interno di "un'immagine virtuale" che rispecchia il mondo reale e fornisce ulteriori informazioni. Questa immagine virtuale si trova nel mondo dell'information technology (IT) e rappresenta tutte le possibilità e le capacità dei componenti fisici nonché i loro stati attuali.

Sulla base delle informazioni fornite dall'immagine virtuale, il singolo componente fisico decentrato è in grado di prendere decisioni in maniera autonoma e di comunicarle direttamente ai componenti fisici vicini. Un contenitore di trasporto intelligente, ad esempio, invia alla rispettiva macchina la richiesta di fornitura di ulteriori pezzi quando trova lo scaffale in magazzino vuoto. Ogni componente fisico che dispone di una simile immagine virtuale e che può essere interconnesso con altri componenti del processo di produzione ai fini dell'interazione viene chiamato "sistema cyber-fisico". Il prefisso "cyber" fa riferimento all'immagine virtuale, mentre il termine "fisico" si riferisce all'oggetto nel mondo della produzione reale, così come lo percepiamo con i nostri cinque sensi.

Come illustrato nella Figura 4, non è prevista solo l'interazione dei sistemi cyber-fisici tra loro, ma anche la messa a disposizione di informazioni e l'integrazione di destinatari e decisori sopraordinati – dall'operatore locale al sistema di gestione o al Manufacturing Execution System (MES) fino ai clienti o ai fornitori esterni.

Un utensile, ad esempio, riconosce così da solo i primi segni di usura e ordina un suo ricambio presso il fornitore esterno di utensili.

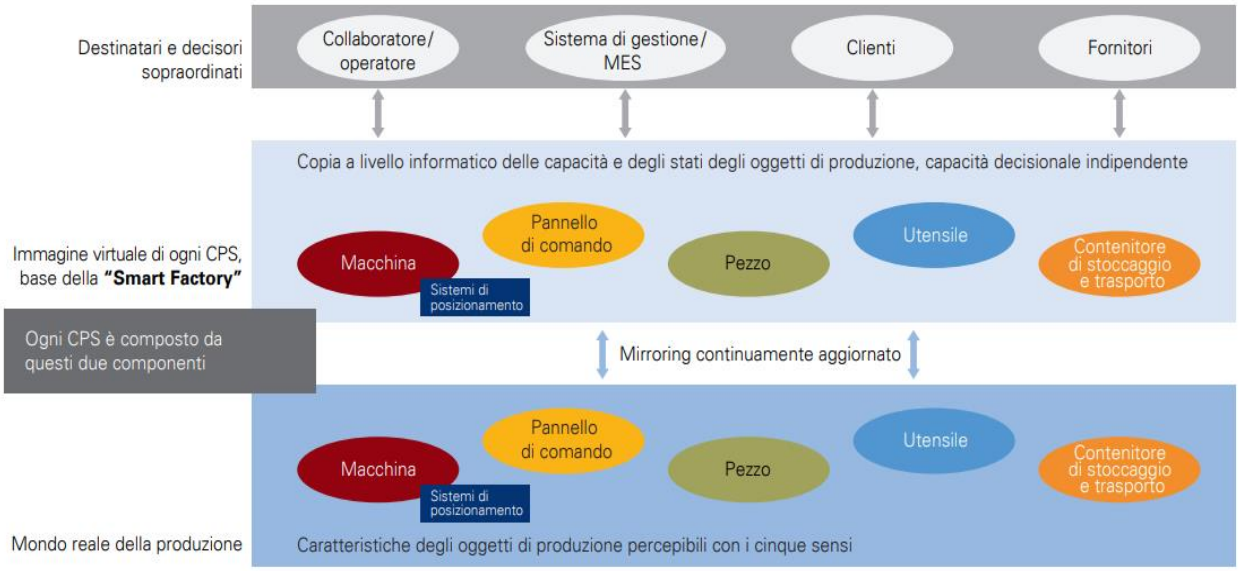


Figura 4

1.4.1 Internet delle cose

L'Internet of Things (IoT) è un concetto di elaborazione che descrive un approccio in cui un'ampia gamma di oggetti è connessa direttamente a Internet. Ciò consente l'implementazione di sensori intelligenti in grado di rilevare l'ambiente circostante, trasmettere ed elaborare i dati acquisiti e quindi utilizzare attuatori intelligenti per interagire con l'ambiente. Ciò ha portato a una vasta gamma di applicazioni basate sul consumatore tra cui l'automazione domestica, la gestione dell'energia e il monitoraggio sanitario.

L'IoT industriale (IIoT) è un sottoinsieme di IoT che descrive le tecnologie di comunicazione machine-to-machine (m2m) e industriali applicate alle applicazioni di produzione e di processo. Sebbene entrambi gli approcci siano simili, l'IoT industriale presenta una serie di differenze chiave, in particolare ogni applicazione presenta un basso rischio, un grado di resilienza è incorporato e la rete complessiva dell'applicazione tende ad essere più ampia di un sistema IoT.

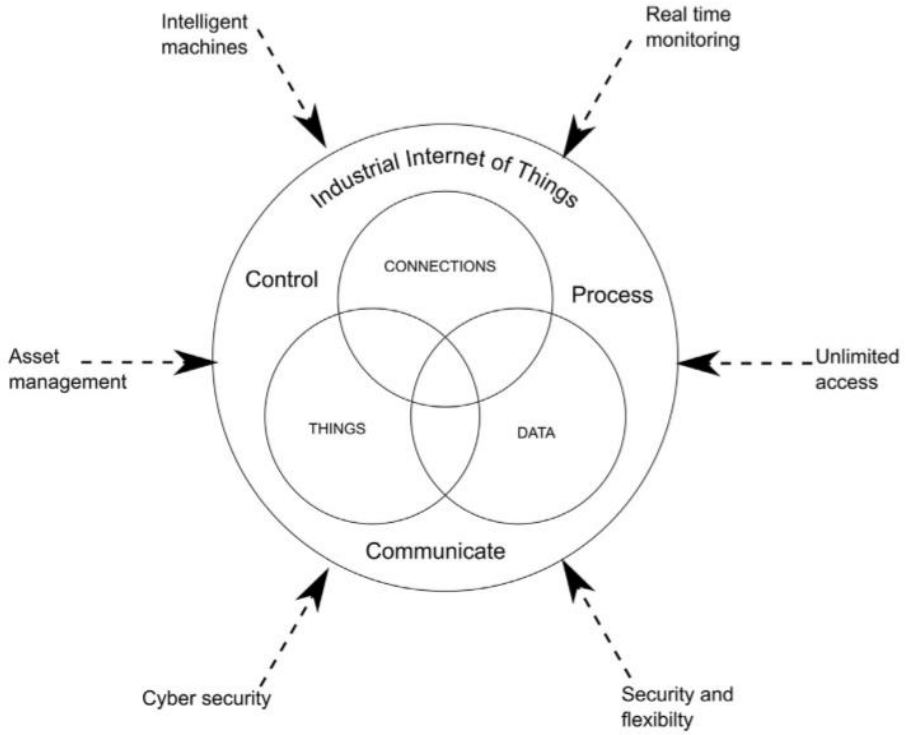


Figura 5

Il concetto di IoT industriale è illustrato in Fig.5. Si ritiene che l'introduzione su vasta scala dell'IIoT spiani la strada a una migliore comprensione del processo di fabbricazione, consentendo una produzione più efficiente e sostenibile, attraverso la capacità di raccogliere notevoli quantità di dati.

Con l'introduzione dell'IIoT, la notevole quantità di dati raccolti, può alimentare soluzioni analitiche e in ogni caso condurre a operazioni industriali ottimali, queste applicazioni potrebbero includere controllo di qualità, manutenzione preventiva e risorse gestione.

La comunicazione nell'IIoT è orientata alle macchine e può essere applicata in molti settori e attività di mercato diversi. Tipici scenari IIoT includono applicazioni di monitoraggio legacy (ad es. Monitoraggio dei processi negli impianti di produzione) e approcci innovativi per sistemi auto-organizzanti (ad es. Impianti industriali autonomi, parchi eolici e condotte). Mentre i requisiti di comunicazione più generali di IoT e IIoT sono simili, ad esempio il supporto per l'ecosistema Internet utilizzando dispositivi a basso costo, limitati dalle risorse e la scalabilità della rete, molti requisiti di comunicazione sono specifici per ciascun dominio e possono essere molto diversi, ad es. Qualità of service (QoS), ad esempio latenza, velocità effettiva, ecc., disponibilità e affidabilità del sistema, sicurezza e privacy.

A differenza di molti elementi del concetto di Industria 4.0, i sistemi di sensori integrati con un collegamento intelligente avanzato sono attualmente ampiamente utilizzati, poiché sono facilmente disponibili soluzioni di sensori integrati che incorporano un bus di campo o un'interfaccia equivalente, fornendo tutte le funzionalità necessarie per soddisfare le esigenze di un sistema completamente integrato sistema di produzione.

1.4.2 Cloud computing e produzione

L'obiettivo del cloud computing è fornire servizi di elaborazione su richiesta con elevata affidabilità, scalabilità e disponibilità in un ambiente distribuito. La definizione del cloud computing dell'Istituto nazionale di standard e tecnologia è un modello per consentire l'accesso alla rete onnipresente, conveniente e su richiesta a un pool condiviso di risorse di elaborazione configurabili (ad es. Reti, server, archiviazione, applicazioni e servizi) che possono essere rapidamente fornito e rilasciato con il minimo sforzo di gestione o interazione dei fornitori di servizi.

Nel concetto di cloud computing, tutto è trattato come un servizio, i principali servizi sono:

- SaaS (Software as a Service): fornisce le applicazioni richieste dal client.
- PaaS (Platform as a Service): fornisce astrazioni e servizi per lo sviluppo, il test, la distribuzione, l'hosting e il mantenimento delle applicazioni all'interno di un ambiente di sviluppo integrato.
- IaaS (Infrastruttura come servizio): fornisce, elaborazione, archiviazione, reti e altre risorse informatiche fondamentali come servizi standardizzati sulla rete.

I modelli di implementazione del cloud computing possono essere classificati come ampiamente appartenenti al cloud pubblico, in cui le risorse sono rese disponibili ai consumatori su Internet o il cloud privato fornito da una singola organizzazione per soddisfare le esigenze dei propri utenti. Il cloud privato offre un ambiente sicuro e un livello di controllo più elevato.

Il cloud computing è ampiamente diffuso in molte aziende in quanto consente a un'organizzazione di acquistare esattamente ciò che è richiesto, in termini di archiviazione e applicazioni. La produzione di cloud è un dominio multidisciplinare relativamente

nuovo che comprende tecnologie come produzione in rete, produzione virtuale, produzione agile, Internet industriale delle cose e cloud computing. Le reti che sono incorporate nelle operazioni di produzione e di processo sono normalmente fortemente vincolate a cosa è possibile accedere alle risorse, quindi l'architettura complessiva è specifica per l'applicazione, non per i singoli servizi che potrebbero essere richiesti. Passare dalla produzione orientata alla produzione a una produzione orientata ai servizi ispirata al cloud computing, la produzione cloud, sembra offrire un'ulteriore soluzione alle sfide affrontate dall'attuale produzione elaborata. Poiché la sicurezza prevista è la principale sfida in qualsiasi sistema informatico in rete, poiché Cloud Manufacturing è fortemente dipendente dalle reti, ci sono notevoli potenziali problemi di sicurezza e fiducia che devono essere gestiti e mitigati.

La produzione di cloud riflette sia il concetto di "integrazione delle risorse distribuite" sia il concetto di "distribuzione delle risorse integrate" che rispecchia la definizione di cloud computing della NIST (National Institute of Standards and Technology). La produzione di cloud può essere definita come un modello per consentire l'accesso alla rete onnipresente, conveniente e on demand a un pool condiviso di risorse di produzione configurabili (ad esempio strumenti software di produzione, apparecchiature di produzione e capacità di produzione) che possono essere rapidamente fornite e rilasciate con il minimo sforzo di gestione o interazione con i fornitori di servizi.

Nella produzione cloud, le risorse distribuite sono incapsulate in servizi cloud e gestite in modo centralizzato. Poiché i clienti possono utilizzare i servizi cloud in base alle loro esigenze, possono richiedere servizi che vanno dalla progettazione del prodotto, produzione, test, gestione attraverso un ciclo di vita dei prodotti.

Va notato che l'Internet of Things industriale basato su cloud è una piattaforma che consente l'utilizzo intelligente di applicazioni, informazioni e infrastrutture in modo conveniente. Mentre IIoT e il cloud computing sono diversi l'uno dall'altro, le loro caratteristiche sono quasi complementari. Questa complementarietà è la ragione principale per cui molti ricercatori hanno proposto la loro integrazione.

2. L’importanza della sicurezza nei CPS

La nozione di sicurezza contro intrusioni e attacchi indesiderati può essere fatta risalire ai tempi di Cesare e alle prime strategie di guerra. Un incrocio tecnologico con questo argomento, tuttavia, ha le sue origini nella proliferazione dei computer nel settore commerciale. Raggruppate sotto la rubrica di InfoSec, le violazioni della sicurezza delle informazioni sono state riconosciute come centrali per le prestazioni soddisfacenti di un sistema.

In particolare, tre violazioni della sicurezza sono state spesso considerate importanti per la protezione delle informazioni: riservatezza, integrità e disponibilità, che indicano rispettivamente un rilascio di informazioni non autorizzato, una modifica non autorizzata delle informazioni e una negazione non autorizzata dell'uso delle informazioni.

Dato il ruolo centrale che le informazioni svolgono in un sistema di controllo del feedback, gli approcci per raggiungere la sicurezza CPS possono essere raggruppati usando la stessa tassonomia.

Una violazione della riservatezza può essere vista come il monitoraggio delle informazioni utilizzate per controllare il sistema, violazione dell'integrità come corruzione dei dati del sensore inviati alla rete per l'elaborazione e violazione della disponibilità come blocco o ritardo delle informazioni tra il blocco computazionale e il nodo di attuazione in un sistema. Se la protezione contro le violazioni della sicurezza di cui sopra può essere vista dal punto di vista di un difensore, si può considerare anche la prospettiva di un attaccante per affrontare la sicurezza CPS.

In linea di massima, gli attacchi informatici sono stati raggruppati in tre categorie; attacchi di divulgazione, attacchi di inganno e attacchi di disturbo indicati come attacchi DDD.

Gli attacchi alla divulgazione si riferiscono a eventuali intrusioni che includono intercettazioni; l'attacco di inganno corrisponde alla corruzione di segnali o un attacco di iniezione di dati falsi e un attacco di disturbo corrisponde a un'altra intrusione attiva in cui il segnale può essere bloccato o ritardato. Questi tre attacchi non si escludono a vicenda: quasi tutti gli attacchi di inganno possono anche essere di disturbo; gli attacchi di disturbo non devono necessariamente coincidere con un attacco di inganno per ottenere un'azione più attiva come il blocco o il ritardo. È chiaro che esiste una mappatura diretta tra questi tre modelli di attacco e i tre obiettivi di sicurezza di riservatezza, integrità e disponibilità.

L'attacco di divulgazione è analogo alla violazione della riservatezza, all'attacco dell'inganno alla violazione dell'integrità e all'attacco di disturbo alla violazione della disponibilità.

In un sistema di controllo ben progettato in cui vengono raggiunti gli obiettivi prestazionali di precisione, velocità e robustezza, consentendo agli attacchi informatici di avere un impatto, per non parlare di un significativo, sembra impossibile. Al contrario, il numero di attacchi, nonché il loro impatto sull'infrastruttura sottostante, è stato abbastanza convincente.

Riassumiamo alcuni dei principali attacchi ai sistemi di controllo nelle infrastrutture di alimentazione e di trasporto. Ciascuno dei principali attacchi viene classificato utilizzando le violazioni della sicurezza e modelli di attacco. Incertezza nell'ambiente, attacchi alla sicurezza ed errori nei dispositivi fisici rendono la sicurezza complessiva del sistema una sfida fondamentale per CPS. Inoltre, un accoppiamento cyber-fisico consente a avversari sofisticati di eseguire attacchi minacciando anche altri attributi chiave del sistema, in primo luogo la sicurezza. Questo è il motivo per cui, tra i diversi requisiti cruciali del CPS, oggi molti ricercatori sono interessati a vari aspetti (unici) della sicurezza del CPS; per esempio indagando su modelli combinati di attacco cibernetico e sui monitor di rilevamento e identificazione degli attacchi.

La sicurezza CPS presenta una serie di caratteristiche peculiari che la distinguono dalla sicurezza dei sistemi IT più convenzionali. Ad esempio, con i sistemi cyber-fisici abbiamo requisiti in tempo reale, in cui la risposta è critica in termini di tempo, il throughput modesto è accettabile, l'elevato ritardo non è tollerabile e la risposta all'interazione umana o di altra natura è essenziale. Tali sistemi sono spesso limitati dalle risorse e potrebbero non tollerare le pratiche di sicurezza IT tipiche. Anche la solita definizione di sicurezza come combinazione di tre principali attributi di sicurezza di riservatezza, integrità e disponibilità assume per CPS un significato completamente nuovo. Dato che gli algoritmi di stima e controllo utilizzati in CPS sono progettati per soddisfare determinati obiettivi operativi, come stabilità ad anello chiuso, sicurezza, vitalità o ottimizzazione di una funzione di prestazione, la disponibilità in CPS può essere vista come la capacità di mantenere gli obiettivi operativi prevenire o sopravvivere agli attacchi denial-of-service (DoS) alle informazioni raccolte dalle reti di sensori, ai comandi impartiti dai controllori e alle azioni fisiche intraprese dagli attuatori. Allo stesso

modo, l'integrità di CPS mira a mantenere gli obiettivi operativi prevenendo, rilevando o sopravvivendo ad attacchi di inganno nelle informazioni inviate e ricevute dai sensori, dai controller e dagli attuatori. L'intento della riservatezza nei sistemi cyber-fisici è impedire a un avversario di dedurre lo stato del sistema fisico intercettando i canali di comunicazione tra i sensori e il controller e tra il controller e l'attuatore o mediante attacchi sui canali laterali su sensori, controller e attuatori.

2.1 Sicurezza CPS

In generale, la sicurezza in CPS è classificata in due aree: sicurezza delle informazioni (dati) e sicurezza del controllo. La sicurezza delle informazioni implica la protezione delle informazioni durante l'aggregazione, l'elaborazione e la condivisione su larga scala nell'ambiente di rete, in particolare reti aperte liberamente accoppiate. Comprende sicurezza di controllo la risoluzione di eventuali problemi di controllo in ambiente di rete e di attenuazione del sistema di controllo da eventuali attacchi su algoritmi del sistema di stima e di controllo. La sicurezza delle informazioni si concentra sulla protezione dei dati, ad esempio utilizzando la crittografia, mentre la sicurezza dei controlli si concentra sulla protezione della dinamica dei sistemi di controllo dagli attacchi informatici. Un importante obiettivo riguarda la sicurezza delle informazioni. Oltre a discutere le caratteristiche distintive tra CPS e sistemi IT tradizionali, questa sezione presenta un'analisi dei più importanti fattori di sicurezza, obiettivi, attacchi e valutazioni dei rischi per CPS.

All'aumentare della connettività ICT (tecnologia dell'informazione e della comunicazione) aumenta anche il potenziale di intrusioni informatiche. I principali incidenti di intrusione hanno confermato l'importanza della sicurezza informatica per i sistemi SCADA (dall'inglese "Supervisory Control And Data Acquisition", cioè "controllo di supervisione e acquisizione dati").

Le reti ICT si basano su TCP / IP (Transmission Control Protocol/ Internet Protocol) ed Ethernet per lo scambio di dati ad alta velocità a costi ridotti. Tuttavia, la tecnologia è nota per essere sensibile agli attacchi basati su IP. I firewall e i perimetri di sicurezza elettronici sono utilizzati per migliorare la sicurezza dei sistemi SCADA che rappresenta un sistema informatico distribuito per il monitoraggio e la supervisione di sistemi fisici; e prevenire le intrusioni informatiche. Tuttavia, questo metodo di controllo dell'accesso

ampiamente adottato contro gli intrusi non garantisce la sicurezza informatica. La configurazione errata dei firewall è una vulnerabilità comune. Anche con una corretta configurazione, le vulnerabilità non vengono ancora completamente rimosse. Ad esempio, un metodo di controllo degli accessi basato esclusivamente sui firewall non è in grado di rilevare attacchi interni e connessioni da un lato fidato.

I punti di accesso remoto alla rete locale (LAN, Local Area Network) della sottostazione sono utilizzati dagli ingegneri del sito, dagli operatori e dal personale del fornitore a fini di manutenzione. L'accesso agli IED (Intelligent Electronic Device) da remoto tramite diverse tecnologie, ad esempio dial-up, reti private virtuali (VPN), wireless, da posizioni esterne alla griglia è diventata una pratica comune. Se non adeguatamente protetti, rappresentano vulnerabilità nel sistema SCADA che possono essere sfruttate dagli aggressori come punti di accesso non autorizzati. Vengono identificati due principali tipi di attacchi a sistemi critici, ovvero attacchi basati su intrusioni e DoS. L'attacco di intrusione si riferisce a intrusi che penetrano nelle reti ICT di una o più risorse critiche, causando danni alle infrastrutture intraprendendo azioni di controllo indesiderate, ad esempio interruttori di circuito operativi per creare interruzioni di corrente. I problemi di sicurezza informatica riguardano le intrusioni dirette e gli attacchi di malware. Le macchine possono essere infettate da virus, worm e cavalli di Troia che ne interrompono il normale funzionamento.

Gli attacchi DoS influenzano l'elaborazione dei dati e le prestazioni di comunicazione attraverso l'esaurimento delle risorse. Possono essere condotti creando valanghe di traffico in brevi periodi di tempo per sovraccaricare i buffer e consumare la larghezza di banda di comunicazione, ad esempio un attacco di allagamento di pacchetti. Gli attacchi DoS ai centri di controllo e alle sottostazioni possono avere gravi ripercussioni sui sistemi SCADA e EMS (Express Mailing System), causando un'interruzione catastrofica dei servizi. Gli attacchi informatici possono avere un grande impatto sulla griglia, il che comporta comportamenti dinamici, perdita di carico, danni alle apparecchiature e blackout parziali o totali.

2.1.1 Alcuni esempi di attacchi informatici

In questa sottosezione, nominiamo alcuni degli scenari di attacco più consequenziali che si sono verificati nei sistemi cyber-fisici reali.

Stuxnet è stato un attacco cibernetico a un impianto iraniano di arricchimento dell'uranio alla fine del 2009. Nel prendere di mira un controllore logico programmabile disponibile in commercio, operando in un ristretto insieme di condizioni, gli aggressori sono stati in grado di garantire che l'attacco raggiungesse il destinatario previsto con ricadute limitate. Hanno inserito un malware che rimarrebbe inattivo nel sistema e non verrebbe rilevato. Con una presenza così furtiva, osservando i dati di sistema critici e confidenziali, l'aggressore ha osservato i risultati chiave del sistema in condizioni stabili e ha riprodotto tali misurazioni su altri siti di monitoraggio della rete. Allo stesso tempo, i segnali di attuazione dannosi sono stati iniettati in altri siti di attuazione critici, causando un danno significativo a un numero di centrifughe. In generale, molti attacchi informatici possono rimanere inosservati dopo l'inserimento, per un periodo significativamente lungo fino a un anno.

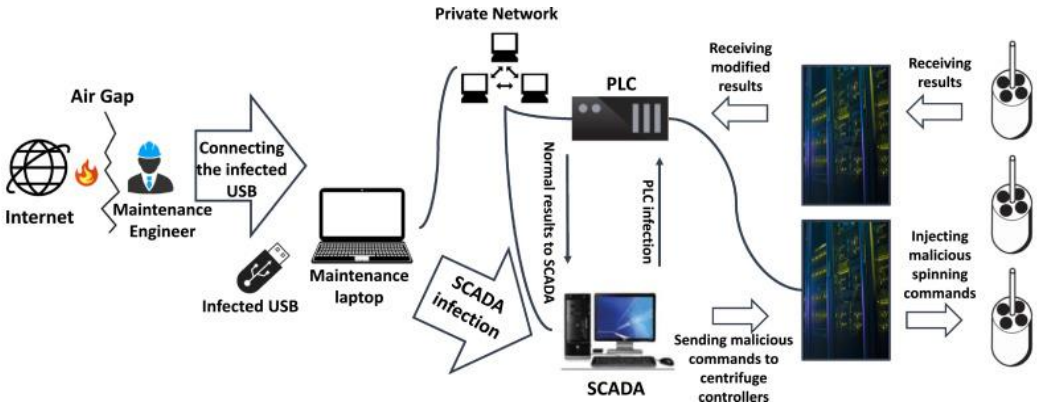


Figura 6

La Fig.6 illustra Stuxnet in una forma schematica. Si può vedere Stuxnet come una combinazione di inganno e attacchi di divulgazione.

Nel 2011, gli operatori statunitensi hanno perso il controllo di un veicolo aereo senza pilota RQ-170 (UAV) che successivamente è atterrato in Iran. Una speculazione su ciò che ha causato ciò è che le forze iraniane hanno bloccato le comunicazioni GPS seguite da una parodia dei segnali GPS, ingannando così il drone nell'atterraggio nella posizione desiderata. Oltre a questo attacco a un UAV, sono stati condotti numerosi studi per mostrare la potenziale minaccia di spoofing GPS sui veicoli. L'attacco RQ-170 può essere visto come un attacco di distruzione seguito da un attacco di inganno.

La pratica tradizionale nelle reti elettriche è quella di istituire protezioni contro i guasti fisici usando dispositivi di protezione. Una singolare partenza da tali eventi è avvenuta

nell'attacco in Ucraina. Ciò consisteva in una serie di attacchi alle reti di distribuzione di energia ucraina che causavano interruzioni e danni permanenti nel 2015. Il primo è stato introdotto tramite e-mail di phishing contenenti il malware Black Energy. Una volta infiltrato nel sistema, ha consentito all'attaccante di rubare dati critici e studiare l'ambiente di sistema. Ciò, a sua volta, ha consentito l'accesso a un livello di controllo più critico e ha permesso lo spoofing dei comandi di controllo. Cioè, prima c'è stata una violazione della riservatezza, seguita da una violazione dell'integrità. Infine, sovrascrivendo il firmware in alcune sottostazioni, l'aggressore è stato in grado di garantire l'operabilità remota degli interruttori, portando a una violazione della disponibilità.

Nel 2016, un altro attacco è stato lanciato su una stazione di trasmissione utilizzando il malware Crash Override. Questo malware potrebbe comunicare direttamente con il software di controllo della griglia e il suo design modulare gli ha consentito di essere modificato per funzionare anche con i protocolli di rete statunitensi o europei.

Nel 2000, i servizi idrici Maroochy nel Queensland, in Australia, furono attaccati da un dipendente scontento. Motivato dalla vendetta, compì l'attacco infiltrandosi nella rete SCADA dei servizi idrici e alterando i segnali di controllo. L'attaccante ha assunto il controllo di 150 stazioni di pompaggio delle acque reflue con conseguente evacuazione di un milione di litri di acque reflue non trattate, per un periodo di tre mesi, negli scarichi delle acque piovane e nelle vie navigabili locali. Questo è chiaramente un attacco di inganno / violazione dell'integrità degli attuatori.

L'hacking automobilistico mostra un elevato livello di vulnerabilità che i moderni sistemi automobilistici sembrano possedere contro le azioni contraddittorie. Uno degli esempi è stato un attacco (sotto controllo) a una Jeep che guidava a 70 miglia orarie su un'autostrada a St. Louis, negli Stati Uniti, dove l'auto veniva dirottata a distanza dagli aggressori per mostrare come varie unità di controllo elettronico, dal tergicristallo al freno e sistemi motore, possono essere manipolati da remoto attraverso la connessione cellulare all'interno del veicolo. Sebbene questo attacco sia stato messo sotto controllo, si afferma che in futuro l'hacking automobilistico remoto può avere conseguenze potenzialmente letali per i veicoli passeggeri.

Gli attacchi sopra elencati non sono affatto esaustivi. Devono essere una panoramica di alcuni dei principali attacchi informatici che hanno avuto un notevole impatto sulle infrastrutture di energia e di trasporto. Il primo attacco informatico alle infrastrutture

critiche si è verificato nel 1982, quando la vendita di software di controllo intenzionalmente danneggiato all'Unione Sovietica ha provocato un'esplosione in Siberia. Negli ultimi cinque anni, ci sono stati molti altri attacchi informatici alle infrastrutture di trasporto terrestre, l'industria dei servizi e l'industria manifatturiera per citarne alcuni. Abbiamo escluso gli attacchi fisici come l'attacco da cecchino Metcalf che si sono verificati su una sottostazione di trasmissione PG&E in California, portando a una grande perdita finanziaria e al crash intenzionale del pilota di Airbus, due terzi degli attacchi sono stati avviati tramite e-mail di phishing. La maggioranza (70-80%) degli attacchi è favorita dagli addetti ai lavori. Il 67% delle minacce informatiche è abilitato da errori delle vittime, il 64% è introdotto direttamente dagli hacker e il 38% da malware.

2.2 Attacchi al CPS

Gli attacchi al CPS possono provocare gravi danni all'ambiente fisico. Ogni strato di CPS è suscettibile ad attacchi passivi o attivi. Inoltre, CPS è vulnerabile a più attacchi rispetto ai sistemi IT tradizionali, che non si limitano a CPS, ma agli attacchi della rete utilizzata, in particolare Internet, che è già impiegato come livello di trasmissione. Gli attacchi del livello di percezione, ad esempio, includono attacchi a nodi come sensori e attuatori; gli attacchi a livello di trasmissione includono perdite o danni ai dati e problemi di sicurezza durante la trasmissione dei dati; gli attacchi a livello di applicazione includono l'accesso non autorizzato che porta alla perdita della privacy degli utenti. Pertanto, sono necessari l'analisi di possibili attacchi e la costruzione di una solida architettura di sicurezza. Sebbene ogni strato sia suscettibile a diversi attacchi, alcuni attacchi potrebbero colpire tutti i livelli ed esempi di questi attacchi includono:

- Denial of Service (DoS): modifica le caratteristiche del comportamento bloccando il traffico per rendere la rete e il servizio non disponibili, ad esempio inondando una risorsa con false richieste, sfruttando la vulnerabilità del protocollo. Inoltre, DDoS è un attacco comune che mira contemporaneamente a più risorse, come i dispositivi finali e la rete, impedendo l'accesso a informazioni e servizi.
- Man-in-the-Middle (MITM): invia un messaggio fabbricato a una risorsa mirata che di conseguenza intraprende azioni indesiderate, ad esempio controllando una funzione primaria, in base al messaggio ricevuto che potrebbe causare un evento indesiderato. Il livello della rete è anche vulnerabile a questo tipo di attacco che, in alcuni casi, è seguito da intercettazioni.

- Eavesdropping: intercetta tutti i dati trasferiti dal sistema. Ad esempio, la trasmissione di informazioni di controllo a fini di monitoraggio nel CPS dalle reti di sensori alle applicazioni potrebbe diventare suscettibile di intercettazione. Inoltre, la privacy degli utenti potrebbe anche essere violata durante il monitoraggio del sistema.
- Spoofing: finge di essere una parte legittima del sistema, quindi tenta di essere coinvolto nelle attività del sistema. Dopo aver ottenuto l'accesso, l'attaccante avrà accesso alle informazioni e potrà eseguire qualsiasi operazione come la modifica, l'eliminazione o l'inserimento di informazioni
- Replay (riproduzione): ritrasmette un pacchetto ricevuto dal nodo di destinazione, per ottenere la fiducia del sistema. Questo tipo di attacco può essere lanciato falsificando e alterando o rispondendo alle informazioni sull'identità di uno dei dispositivi.
- Chiave compromessa: ha come target la chiave segreta utilizzata per proteggere la comunicazione. Ciò può essere ottenuto analizzando il tempo di crittografia richiesto, noto anche come attacco di timing (canale laterale). La chiave compromessa verrà quindi utilizzata per modificare i dati acquisiti ed eseguire analisi computazionali per compromettere altre chiavi segrete nello stesso sistema. In alcuni casi, un avversario potrebbe ottenere l'accesso ai sensori e costringerli a svolgere attività di ingegneria per estrarre altre chiavi interne. In un altro esempio, un utente malintenzionato potrebbe riuscire a sostituire un nodo sensore e considerarsi la versione legittima per scambiare le chiavi con altri nodi, scoprendo così altre chiavi segrete dei nodi coinvolti.

Figura 7

Esistono diversi tipi di rischi per ogni livello del CPS e, in base all'architettura CPS mostrata nella figura 7, gli attacchi comuni per ciascun livello possono essere classificati come segue.

Il livello di percezione è costituito da dispositivi terminali, come tag in RFID e sensori, che sono limitati dalle risorse di elaborazione vincolate e dalle capacità di memoria. Inoltre, questi dispositivi si trovano principalmente in ambienti esterni con conseguenti attacchi fisici, come manomissione dei componenti dei dispositivi o sostituzione dei dispositivi. Quindi, quei dispositivi terminali sono più suscettibili a una varietà di attacchi. Attacchi comuni a livello di percezione includono guasti alle apparecchiature, guasti alle linee, interferenze elettromagnetiche, corruzione dei dati percettivi, analisi della potenza differenziale, divulgazione delle informazioni, tracciamento delle informazioni, manomissione, rilevamento perdita di informazioni, attacchi fisici di distruzione e esaurimento di energia. Le forme comuni di questi attacchi sono:

- Acquisizione nodo: rileva il nodo e ottiene e perde informazioni che potrebbero coinvolgere le chiavi di crittografia, che vengono quindi utilizzate per minacciare la sicurezza dell'intero sistema. Questo tipo di attacco prende di mira riservatezza, disponibilità, integrità e autenticità

- Falso nodo: aggiunge un altro nodo alla rete, attaccando l'integrità dei dati inviando dati dannosi. Questo, a sua volta, potrebbe portare a un attacco DoS, consumando l'energia dei nodi nel sistema;
- Interruzione dei nodi: interrompe i servizi dei nodi, rendendo difficile la lettura e la raccolta di informazioni da questi nodi, nonché lancia una varietà di altri attacchi che incidono sulla disponibilità e l'integrità;
- DOS basato sul percorso: invia un gran numero di pacchetti, pacchetti di flooding, lungo il percorso di instradamento alla stazione base, portando all'esaurimento della batteria del nodo e all'interruzione della rete, riducendo di conseguenza la disponibilità dei nodi;
- Risonanza: impone ai sensori o ai controller compromessi di funzionare a una frequenza di risonanza diversa;
- Integrità: tenta di iniettare input di controllo esterni e misurazioni di falsi sensori, desiderando interrompere il sistema.

Gli attacchi a livello di trasmissione si presentano sotto forma di perdita di dati durante la trasmissione delle informazioni. Ciò si verifica a causa dell'apertura del supporto di trasmissione, in particolare nella comunicazione wireless. Tali attacchi catturano un messaggio trasmesso attraverso l'interfaccia radio, lo modificano e lo ritrasmettono o scambiano informazioni tra reti eterogenee, impersonando quindi l'utente legittimo. Inoltre, altri fattori, come i meccanismi di accesso remoto tra enormi quantità di nodi di rete che potrebbero causare congestione del traffico, aumenterebbero la possibilità di essere attaccati. Attacchi comuni a questo livello includono risposta e Sybil, analisi del traffico, manomissione, esaurimento, collisione, buco nero, inondazioni, botole, nodo del lavandino, direzione di inghiottimento, wormhole, selezione errata del percorso, tunneling. I seguenti esempi sono forme comuni di attacchi a livello di trasmissione:

- Routing: crea loop di routing che possono comportare una trasmissione di rete resistente, un ritardo di trasmissione maggiore o un percorso sorgente esteso;
- Wormhole: crea buchi informativi nella rete annunciando falsi percorsi attraverso i quali vengono instradati tutti i pacchetti;
- Inceppamento: blocca il canale wireless tra i nodi del sensore e la stazione base remota per introdurre rumore o un segnale con la stessa frequenza. Questo attacco potrebbe portare a DoS creando interferenze di rete intenzionali;

- Inoltro selettivo: crea un nodo compromesso per eliminare e scartare i pacchetti e inoltrare i pacchetti selezionati. In alcuni casi, il nodo compromesso interrompe l'inoltro dei pacchetti alla destinazione prevista o inoltra solo i messaggi scelti e scarta tutti gli altri pacchetti mentre questo nodo è considerato legittimo;
- Sinkhole: annuncia il percorso di routing migliore da utilizzare per instradare il traffico verso altri nodi. Questo attacco potrebbe essere usato per lanciare altri attacchi, come inoltro selettivo e spoofing.

Poiché una grande quantità di informazioni degli utenti viene raccolta al livello di applicazione, gli attacchi qui provocano danni ai dati, perdita di privacy come abitudini degli utenti e condizioni di salute e accesso non autorizzato ai dispositivi. Gli attacchi più comuni a livello di applicazione includono la violazione della privacy degli utenti, l'accesso non autorizzato, codice dannoso, attacchi di contraffazione di comandi di database e controllo. Esempi comuni di attacchi livello di applicazione includono:

- Buffer overflow: sfrutta tutte le vulnerabilità del software che portano a vulnerabilità di buffer overflow e lo sfruttano per lanciare attacchi;
- Codice dannoso: attacca l'applicazione utente avviando vari codici dannosi, come virus e worm, e provoca il rallentamento della rete o il danneggiamento;

2.3 Valutazione del rischio

Con un maggiore utilizzo della CPS in molti settori sensibili la sicurezza è diventata una questione urgente e pone la necessità di un adeguato metodo di valutazione del rischio.

Il focus sulla sicurezza della valutazione del rischio è passato dalla valutazione del rischio del computer alla valutazione del rischio della rete, in particolare con una forte dipendenza da Internet. L'obiettivo della valutazione della sicurezza CPS è avere una forma quantificata di rischio che può essere impiegato nella futura protezione del sistema. Tuttavia, la maggior parte degli sforzi e degli studi si concentra su sistemi aziendali che non sono direttamente correlati a CPS. Poiché la sicurezza CPS è in larga misura diversa dai sistemi IT tradizionali, anche le funzionalità di sicurezza sono diverse. Ad esempio, protocolli e tecnologie standardizzati, interconnessioni non sicure e informazioni scambiate sono i principali fattori di rischio per ICS (International Classification for Standards).

Il modello di valutazione del rischio CPS può essere suddiviso in tre fasi: (1) definire cosa accadrà al sistema; (2) valutare la probabilità dell'evento; e (3) stimare le conseguenze. Inoltre, tre elementi devono essere presi in considerazione quando si effettua la valutazione del rischio CPS: identificazioni di attività (valore), identificazione delle minacce e identificazione della vulnerabilità.

Per quanto riguarda l'identificazione delle risorse un'attività, che si riferisce a un valore di risorsa che deve essere protetto, può essere una presenza tangibile (ad esempio dispositivi medici, strutture aziendali, attività di attrezzature, strutture educative, operazioni o informazioni) o una presenza immateriale (ad es. informazioni su un'azienda o reputazione di un'associazione). In effetti, la maggior parte delle attività sono immateriali; pertanto, le attività hanno un valore diretto per molte transazioni e servizi giornalieri e quindi dovrebbero essere protette. Inoltre, la quantificazione delle attività può essere stimata dalle perdite economiche dirette e indirette e dal danno risultante.

Il processo di valutazione del valore comprende l'identificazione dei livelli di difesa, delle risorse critiche e delle funzioni principali (essenziali) del sistema, nonché la determinazione della valutazione del valore delle attività. Le attività CPS possono essere suddivise in tre parti: attività fisiche, attività informatiche e interazioni con altri sistemi. La differenza essenziale tra le risorse CPS e le risorse IT classiche è che le intercomunicazioni di CPS sono complesse, immateriali e interconnesse con altri sistemi.

Il passaggio dell'identificazione della minaccia viene utilizzato per aiutare a identificare i rischi che rappresentano una priorità assoluta nel campo della CPS, che non è una missione facile. I dati storici possono essere utilizzati per quantificare la frequenza della minaccia mentre è possibile utilizzare record e registri di campionamento nel sistema di rilevamento intrusioni (ID, Alternative Distributions System) per determinare la frequenza del rischio, i registri e molti altri metodi. La vulnerabilità è definita come qualsiasi debolezza esistente che potrebbe essere sfruttata a fini di spionaggio da un avversario per intercettare o danneggiare il valore di un bene. È anche definito come una condizione o un ambiente che può essere sfruttato da un avversario per attaccare o danneggiare i sistemi. Una valutazione della vulnerabilità è un processo di analisi di un sistema e delle sue funzioni, che identifica i punti deboli e determina le azioni correttive appropriate o le mitigazioni che potrebbero essere progettate e implementate per ridurre o eliminare eventuali vulnerabilità. Le vulnerabilità di CPS sono generalmente divise in

tre: rete, piattaforma e gestione. La vulnerabilità della rete comporta vulnerabilità di configurazione, hardware e monitoraggio. La vulnerabilità della piattaforma include vulnerabilità di configurazione, hardware e software, nonché carenza di misure di protezione. La vulnerabilità della gestione è principalmente legata alla mancanza di politiche di sicurezza. La quantizzazione della vulnerabilità può essere ottenuta attraverso un meccanismo diverso come i precedenti metodi di valutazione degli esperti, confrontandoli con i record storici o le migliori esperienze nelle industrie. Eliminare o prevenire tutti i rischi è una missione difficile, se non quasi impossibile. Di conseguenza, vengono generalmente adottati metodi a costo minimo per ridurre i rischi a un livello accettabile.

3. Analisi di sicurezza CPS

Poiché il CPS combina i processi cyber e fisici, c'è un aumento del numero di sfide che il CPS dovrebbe essere considerato quando si progetta un meccanismo di sicurezza per tali sistemi. Inoltre, l'ambiente è in continua evoluzione e i dispositivi collegati possono essere uniti dinamicamente in luoghi diversi, il che aumenta la complessità della protezione di sicurezza richiesta.

Le sfide che potrebbero essere affrontate nella progettazione di un meccanismo di sicurezza comprendono la prevenzione, l'individuazione e l'attenuazione. Prevenire l'attacco è una sfida a causa dello spazio di interazione tra cyber e sistemi fisici. Alcuni aggressori non dipendono solo da vulnerabilità dirette, ma provano anche a lanciare attacchi a più livelli. Rilevare gli attacchi è il compito più difficile poiché esiste un'interazione tra cyber e spazio fisico che necessita di tecniche di rilevamento da costruire per tutti i livelli del CPS, inclusi i livelli di applicazione, trasmissione e percezione. La sfida principale è progettare un meccanismo di sicurezza in grado di mitigare gli effetti derivanti dalla violazione del sistema in caso di superamento delle fasi di sicurezza di prevenzione e rilevamento.

Le sfide alla sicurezza in CPS possono essere classificate in due categorie: (1) le sfide risultanti da tecnologie eterogenee connesse per implementare le funzioni richieste; e (2) le sfide derivanti dalle funzioni di sicurezza applicate per ottenere la sicurezza necessaria. A causa della sua vasta connettività a Internet, l'architettura di sicurezza CPS includerà, ad esempio, tutti i problemi di sicurezza in Internet, WSN e reti di comunicazione mobile. CPS non dispone di funzionalità uniformi di esecuzione o elaborazione computazionale per raggiungere requisiti di alta sicurezza, come nell'IT tradizionale. Pertanto, è molto difficile adottare qualsiasi meccanismo di sicurezza consolidato basato su un ambiente che cambia dinamicamente.

La maggior parte delle soluzioni di sicurezza proposte tenta di risolvere diversi problemi di sicurezza a ogni livello. Sebbene tali approcci possano aiutare a proteggere la parte desiderata del sistema, i rischi potrebbero derivare da altre parti di quel sistema. Per ovviare a questo problema, viene utilizzata un'architettura di sicurezza di CPS per proteggere la sicurezza attraverso tutti i livelli, come la raccolta, la trasmissione e l'elaborazione delle informazioni, dal livello inferiore al livello superiore.

Table 1 – Summary of CPS security.

CPS layer	Components	Objective	Security issues	Security parameters	Countermeasures mechanisms
Perception layer	– RFID tag and readers – WSN – Smart Card – GPS	– Information collection	– Terminal Security – Sensor network security – Node reputation – Privacy	– Authentication – Confidentiality – Trust management	– Certification – Access control – Authentication – Data encryption – Lightweight encryption – Sensor data protection – Key agreement – Environment monitoring – Secure routing protocol – Trust management
Transmission layer	– Wireless networks – Wired networks – Computers – Components	– Information transmission	– Large number of nodes – Network routing – Networks security – Internet security – Heterogeneous technology	– Integrity – Availability – Confidentiality – Identity authentication	– Robust routing protocol – Hop by hop data encryption – Across Heterogeneous Network Authentication and key agreement – Network access control – Attack detection mechanism
Application layer	– Intelligent devices	– Information analysis – Control decision making	– Information processing – Access control problem – Information interception – Privacy – Safety	– Privacy – Authentication and key agreement – Cloud security	– End to end encryption – P2P – Intrusion detection – Trust management – User authentication and authorization

Tabella 1

La Tabella 1 con dati adottati da Bhabad, Scholar, 2015, Lu et al, 2015, Suo et al, 2012 e Zhao and Ge (2013) mostra la maggior parte dei requisiti di sicurezza in ogni livello del CPS, nonché le tecniche di sicurezza che dovrebbero essere prese in considerazione nella progettazione di eventuali soluzioni di sicurezza.

Nelle seguenti sottosezioni, presentiamo un'analisi dal basso verso l'alto dei requisiti di sicurezza per ogni livello del CPS poiché ci sono molti problemi di sicurezza in ogni livello che dovrebbero essere considerati al fine di proteggere tali sistemi dagli attacchi.

3.1 Analisi di sicurezza a livello di percezione

L'obiettivo principale di questo livello è la percezione degli oggetti, l'identificazione e la raccolta dei dati. Tuttavia, il numero di dispositivi collegati comporta ulteriori vulnerabilità della sicurezza. Gli attacchi contro tali dispositivi, con capacità limitate e generalmente connessi tramite Internet utilizzando comunemente supporti wireless meno sicuri, potrebbero facilmente ottenere l'accesso a dati sensibili, avviare programmi dannosi e bloccare l'accesso in alcuni casi. Pertanto, è estremamente importante proteggere tali dispositivi e impedire la divulgazione di informazioni. L'installazione di nuovi dispositivi, situati principalmente in ambienti esterni, può anche essere un modo che potrebbe essere sfruttato dagli aggressori per divulgare informazioni o analizzare la

situazione del sistema, causando attacchi fisici, come la manomissione dei componenti del dispositivo o la sostituzione di un dispositivo con un altro. Quindi, l'aggiunta di qualsiasi nuovo dispositivo è un altro problema importante che dovrebbe essere considerato. Molti dispositivi a livello fisico mancano del supporto di autenticazione, che a sua volta consente l'accesso non autorizzato e rivela informazioni private o installa programmi dannosi che potrebbero danneggiare il sistema. Tuttavia, applicare l'autenticazione a tali dispositivi è molto impegnativo per molte ragioni; ad esempio, sono coinvolti molti oggetti ed entità con capacità limitate. Un meccanismo adatto per ottenere l'autenticazione a questo livello è la crittografia. Tuttavia, in alcuni casi non è applicabile implementare sufficienti funzioni crittografiche su dispositivi vincolati (ad es. Sensori, smart card senza contatto e dispositivi sanitari) a causa della limitazione delle loro risorse. Ciò comporta la necessità di una soluzione di autenticazione leggera, data la limitata capacità di calcolo dei dispositivi da campo, che è al centro dell'attuale ricerca.

Riassumendo, i processi di autenticazione e controllo degli accessi bloccherebbero l'accesso da nodi non validi, proteggendo da attacchi fisici; la crittografia dei dati proteggerà la riservatezza dei dati e la divulgazione dei dati privati durante la trasmissione dei dati. L'attenzione nelle due elementi seguenti è sull'analisi della sicurezza delle tecnologie RFID e WSN in quanto sono le tecnologie di comunicazione più ampiamente adottate a livello di percezione.

RFID è una tecnologia wireless che archivia e recupera da remoto i dati sui dispositivi. Il vantaggio principale dell'utilizzo dell'RFID è che il dispositivo target può essere identificato senza interazione manuale. Anche se la tecnologia RFID ha accurate funzionalità in tempo reale, molti tag RFID non includono alcun meccanismo di sicurezza e gli altri che possono fornire tecniche di hashing per uso di sicurezza o approcci simmetrici tradizionali a causa dei vincoli delle limitazioni di potenza, capacità di elaborazione e archiviazione. Sebbene l'RFID sia ampiamente utilizzato e ampiamente adottato, pone molti problemi di sicurezza che includono una codifica uniforme, il risultato di non avere standard uniformi che potrebbero impedire l'accesso da parte del lettore; collisione del conflitto, il risultato della trasmissione di dati da più tag RFID multipli contemporaneamente, che può causare la disabilitazione del lettore; protezione della privacy, a seguito dell'utilizzo di tag RFID a basso costo, che dispongono di risorse limitate (ad esempio capacità di elaborazione deboli e memoria insufficiente); e la privacy della posizione, il risultato della rivelazione della posizione del tag ottenendo

informazioni sull'ID tag e monitorando la posizione del titolare. Con tutte le debolezze di sicurezza menzionate, l'RFID è ancora visto come una parte necessaria del CPS perché può eseguire molte operazioni tra cui il rilevamento di cambiamenti negli oggetti fisici e ambientali, la direzione del movimento e la velocità, la temperatura, l'umidità, il rilevamento di gas e luce.

Per quanto riguarda i problemi di sicurezza, l'autenticazione del dispositivo è un obiettivo importante e l'implementazione di un robusto meccanismo di autenticazione richiede tag con capacità di archiviazione e computazionali appropriate. Tuttavia, i tag RFID a basso costo non hanno le specifiche richieste per implementare solidi meccanismi di sicurezza. Pertanto, è difficile attuare uno qualsiasi dei meccanismi di sicurezza ampiamente utilizzati a causa della limitazione delle risorse dell'RFID.

Codifica uniforme, collisione dei conflitti, protezione della privacy e della posizione sono le quattro sfide della sicurezza RFID. Pertanto, è necessario uno standard di codifica uniforme, il rilevamento e la prevenzione delle collisioni di conflitto e una protezione della privacy dei dati leggera. In RFID, integrità, autenticità e riservatezza possono essere raggiunte utilizzando algoritmi crittografici leggeri e tecnologia di protocollo di trasmissione adatta a risorse limitate.

WSN, chiamato anche Wireless Sensor and Actuator Networks, sono sensori distribuiti per il monitoraggio dell'ambiente fisico o delle condizioni ambientali, quali temperatura, indicatore di gas e pressione. Sono anche definite reti autorganizzanti con topologia di rete dinamica e reti wireless multi-hop ampiamente distribuite. WSN ha risorse limitate, come memoria insufficiente, capacità di calcolo e risorse energetiche limitate (batteria) oltre alle condizioni vulnerabili e minima interazione umana diretta, che si rifletteranno nella capacità di eseguire qualsiasi meccanismo di sicurezza. La ricerca attuale si concentra sull'autenticità e l'integrità dei dati dei sensori, ignorando la riservatezza poiché i dati possono essere rilevati dal dispositivo sostituito di un utente malintenzionato. Una delle preoccupazioni di sicurezza relative ai nodi del sensore è la fiducia reciproca tra i nodi del sensore, in particolare i nodi esterni, per proteggere la trasmissione dei dati; in alcuni casi, i nodi del sensore sono distribuiti in un ambiente aperto e non sono monitorati periodicamente e possono essere suscettibili ad attacchi fisici. I problemi principali che non sono ancora risolti efficacemente quando si applicano algoritmi crittografici stanno supportando un nodo appena aggiunto usando il metodo di pre-distribuzione chiave;

memorizzazione e allocazione delle chiavi; e consumando meno energia dagli algoritmi crittografici.

Per realizzare gli obiettivi di sicurezza di CPS, algoritmi crittografici, gestione delle chiavi, routing sicuro e gestione della fiducia possono in sequenza risolvere o eliminare le sfide di sicurezza di WSN. I due tipi di algoritmi crittografici, asimmetrici e simmetrici, sono stati applicati in WSN. Tuttavia, ciascuno di questi tipi presenta vantaggi e svantaggi. Mentre la crittografia simmetrica è ampiamente adottata poiché richiede meno calcoli computazionali rispetto alla crittografia asimmetrica, il protocollo di scambio di chiavi presenta problemi come la complessità del protocollo di scambio di chiavi e la riservatezza delle chiavi.

Il metodo alternativo, la crittografia asimmetrica (chiave pubblica), è considerato in quanto fornisce una maggiore sicurezza con i seguenti vantaggi: buona scalabilità, corretta autenticazione del nodo e migliore sicurezza per la rete selezionata. La crittografia a chiave pubblica sarà la migliore opzione per il futuro e la ricerca si concentrerà sull'ottimizzazione dei processi computazionali e dei parametri utilizzati (parametri dell'algoritmo). Un algoritmo crittografico leggero adatto ai nodi del sensore non è stato ancora raggiunto. In definitiva, ciascuno degli approcci di crittografia asimmetrica e di crittografia simmetrica ha buone caratteristiche; tuttavia, non è possibile ottenere il superamento di tutte le sfide relative alla sicurezza in WSN applicando solo uno di questi approcci. Possono essere adatti hardware con un consumo energetico ottimizzato e tecniche di crittografia simmetrica e di sviluppo del software sviluppate in modo ottimale. Sebbene la crittografia asimmetrica con chiavi a 1024 bit possa essere applicata a reti ad hoc, non è appropriata per i dispositivi WSN con memoria e capacità computazionali limitate. In alternativa, è possibile applicare tecniche di crittografia simmetrica leggera oltre all'hash e sono al centro della maggior parte degli studi. Inoltre, alcune tecniche crittografiche asimmetriche avanzate (ad esempio la crittografia a curva ellittica (ECC)) possono essere offerte da dispositivi con capacità limitate.

3.2 Analisi di sicurezza a livello di trasmissione

Sebbene le reti siano ampiamente utilizzate in molti campi nel collegamento di dispositivi e nella praticità degli utenti, espongono vari problemi di sicurezza e possono essere facilmente attaccate o intercettate dagli aggressori. Ad esempio, l'accessibilità wireless

offre agli utenti una notevole comodità, mentre gli aggressori possono interagire con la rete e causare alcuni danni o rubare informazioni preziose. La comunicazione CPS, che introduce la comunicazione da macchina a macchina, differisce da quella in Internet, che è limitata da macchina a uomo. L'architettura di sicurezza della rete esistente non è stata progettata principalmente per le comunicazioni macchina (ad es. Comunicazione tra dispositivi nel CPS). La trasmissione dati da macchina a macchina pone problemi di sicurezza a causa della mancanza di compatibilità tra i dispositivi collegati. Questi problemi di sicurezza non possono essere risolti utilizzando i protocolli di rete correnti progettati principalmente per l'uso in Internet. Sebbene tali protocolli forniscano ancora alcuni meccanismi di protezione, non sono la soluzione ottimale. Gli attacchi possono utilizzare qualsiasi debolezza risultante da dispositivi collegati in modo eterogeneo per ottenere l'accesso alle informazioni degli utenti, che possono quindi essere utilizzate per attività dannose. Per proteggere i dispositivi nella rete utilizzata, è molto importante proteggere la rete stessa. I dispositivi dovrebbero avere la possibilità di essere abilitati a rilevare comportamenti o situazioni anomali che potrebbero influire sulla sicurezza del sistema. Ciò richiede l'implementazione di un robusto protocollo di trasmissione e di un software con Intrusion Detection sul lato dei dispositivi.

La sicurezza a livello di trasmissione può essere divisa in due tipi. Il primo proviene dai dispositivi collegati e il secondo tipo proviene dalle tecnologie correlate e dai conseguenti errori dei protocolli progettati attraverso il processo di implementazione. Nelle reti wireless, i nodi sono autorizzati a spostarsi in modo dinamico senza la precedente autenticazione, determinando un numero maggiore di vulnerabilità che possono essere utilizzate in modo dannoso per influire sulla sicurezza della rete utilizzata. L'accesso alle reti può essere realizzato utilizzando una rete ad hoc o reti wireless. Una rete ad hoc (peer-to-peer) è una rete non centrica in cui la comunicazione tra nodi non necessita di una stazione base. In questo tipo di rete, i cambiamenti nei nodi possono essere facilmente adattati in una certa misura. La maggior parte delle minacce alla sicurezza in questo tipo di rete proviene dal canale radio, che può essere intercettato dagli aggressori. Le sfide di sicurezza comuni in questa rete sono l'accesso ai nodi non autorizzato, la sicurezza dei dati e la sicurezza del routing della rete.

Una soluzione appropriata per l'accesso al nodo non autorizzato può essere ottenuta applicando tecniche di autenticazione e autorizzazione. Una soluzione adatta alla sicurezza dei dati può essere ottenuta utilizzando i meccanismi di gestione delle chiavi di

autenticazione e crittografia. La soluzione alla sicurezza del routing può essere realizzata implementando meccanismi di crittografia.

La rete Wi-Fi è la rete wireless più utilizzata. È una rete centrica in cui la comunicazione tra i nodi viene effettuata attraverso ponti fissi (stazione base) come una rete locale senza fili. Qualsiasi dispositivo terminale può connettersi in modalità wireless e comunicare con le applicazioni tramite Internet tramite reti Wi-Fi. Nonostante la comodità fornita dalla tecnologia Wi-Fi, ci sono molti problemi di sicurezza. Per superare tali problemi di sicurezza, vengono utilizzati il controllo degli accessi e la crittografia di rete.

Esistono due meccanismi di crittografia: hop-by-hop e end-to-end. Nel meccanismo di crittografia hop-by-hop, le informazioni vengono crittografate nel processo di trasmissione. Questo metodo deve mantenere il testo in chiaro in ciascun nodo in entrambi i processi, la crittografia e la decrittografia. Nella crittografia end-to-end, le informazioni possono essere visualizzate solo dal mittente e dal destinatario e, attraverso tutti i processi di trasmissione e i nodi di inoltro, i dati vengono crittografati. Se è necessario proteggere solo i collegamenti tra i nodi, è possibile adottare il meccanismo di crittografia hop-by-hop. Sebbene l'utilizzo di questo approccio fornisca alcune funzionalità, come l'elevata efficienza, nonché il basso costo e la latenza, ciascun nodo può decodificare i dati. Pertanto, questi nodi devono essere attendibili. Inoltre, in questo caso, la responsabilità della sicurezza sarà sul processo di applicazione nei nodi. Il meccanismo di crittografia end-to-end offre molti vantaggi, ad esempio solo il mittente e il destinatario possono leggere i messaggi e nessun intercettatore può accedere alle chiavi crittografiche necessarie per decrittografare i dati crittografati. Tuttavia, è molto difficile implementare questo metodo, soprattutto quando si hanno dispositivi terminali limitati come i sensori. Ad esempio, il protocollo SSL (Secure Sockets Layer, Livello di socket sicuri), / TLS (Transport Layer Security) opera end-to-end e consente di impostare alcune funzionalità di sicurezza richieste tra client e server. La sicurezza della rete è un sistema di sicurezza a più livelli e le principali sfide della rete in CPS provengono dalle reti wireless. Per creare un solido meccanismo di sicurezza della rete, è necessaria una solida autenticazione end-to-end e un accordo chiave, autenticazione tra domini, autenticazione tra reti e meccanismi di routing sicuri. Per impedire l'accesso al nodo illegale e fornire un routing di rete sicuro, è necessario considerare l'autenticazione dell'identità per migliorare l'integrità e la riservatezza dei dati.

L'architettura di sicurezza potrebbe essere composta da due sottolivelli: sicurezza punto a punto, protezione della sicurezza del trasporto hop-by-hop come attraverso la certificazione di rete e l'autenticazione reciproca; e sicurezza end-to-end, proteggendo le comunicazioni tra un dispositivo / sistema a un altro. I dati di trasmissione hop potrebbero essere protetti dal primo substrato mentre la riservatezza dei dati e la disponibilità della rete potrebbero essere garantite dal secondo strato. Considerando che la maggior parte delle tecniche classiche di sicurezza della comunicazione non sono progettate principalmente per applicazioni eterogenee, è necessario un nuovo approccio segreto sviluppato per applicazioni eterogenee. È importante prendere in considerazione i problemi di capacità e connettività (ad esempio lo spazio degli indirizzi) che possono causare congestione e ridondanza della rete. La tecnologia IP non è adatta per un gran numero di nodi collegati. Di conseguenza, il protocollo IPSec, che fornisce capacità di autenticazione e crittografia, viene ampiamente adottato. A causa di vincoli nell'uso del protocollo IP, specialmente in CPS, è stato proposto un nuovo protocollo, tuttavia, un sovraccarico aggravante derivante dal sovraccarico residuo è ancora il problema principale di questo protocollo. Alcune soluzioni consolidate di sicurezza della comunicazione includono TLS / SSL, che può fornire integrità, autenticità e riservatezza; e Internet Protocol Security (IPSec), che può fornire integrità, autenticità e riservatezza in ogni livello.

3.3 Analisi di sicurezza a livello di applicazione

Questo livello include molte applicazioni, ognuna delle quali ha una propria vulnerabilità che può influire sulla sicurezza di CPS. Inoltre, ottenere la protezione della privacy degli utenti e l'accesso gerarchico ai dati sensoriali sono le principali sfide per il livello applicativo. Questo livello può contenere diverse applicazioni come servizi e monitoraggio industriale come nelle case intelligenti e nelle città intelligenti. La principale preoccupazione per la sicurezza sono le vulnerabilità che potrebbero derivare dalla progettazione e che possono essere sfruttate dagli avversari per attaccare il sistema. Pertanto, è possibile avviare codice o software dannoso per influire sulla sicurezza del sistema. Un'altra preoccupazione per la sicurezza può essere il risultato dell'integrazione di varie tecniche, che potrebbero impedire l'elaborazione dei dati, causando un collo di bottiglia nel sistema. Questi problemi di sicurezza possono influire sulla disponibilità e sull'affidabilità del sistema. Alcuni riferimenti, come Atzori et al. (2012), menzionano la

fiducia come parte della sicurezza. Tuttavia, la sicurezza non richiede l'esistenza della fiducia e incorporare la fiducia nel sistema è un processo complesso e produce costi generali.

La sicurezza a livello di applicazione include l'accesso alle informazioni, l'autenticazione dell'utente, la privacy delle informazioni e il collasso dei collegamenti dati utilizzati, la stabilità e la gestione della piattaforma. Inoltre, ogni applicazione ha i suoi requisiti di sicurezza e vi è una crescente richiesta di fornire tali requisiti poiché l'applicazione di sistemi importanti e sensibili, che vengono monitorati e controllati in tempo reale, è in crescita.

In effetti, il numero di problemi di sicurezza complessi che devono essere considerati dipende dal tipo di applicazione. Pertanto, è difficile progettare applicazioni che siano completamente attendibili tra loro senza tener conto delle operazioni eseguite sottostanti del sistema, come la connettività e i dati generati da CPS. Un altro problema è che standard industriali diversi hanno applicazioni CPS diverse. Attualmente, nessuno standard globale regola l'interazione e lo sviluppo di applicazioni del livello di applicazione CPS, il che migliora la mancanza di sicurezza. Ciò significa che sono richiesti diversi requisiti di sicurezza per diversi ambienti applicativi. Quando si progettano applicazioni CPS, ci sono molti problemi di sicurezza che dovrebbero essere considerati, tra cui: diversi meccanismi di autenticazione per varie applicazioni, che rendono l'integrazione molto complessa quando si garantisce l'autenticazione dell'identità; un gran numero di dispositivi collegati e dati condivisi che si traducono in un grande sovraccarico di applicazioni, che si rifletterà nella disponibilità dei servizi forniti da tali dispositivi; il gran numero di utenti che interagiscono con le applicazioni; la quantità di dati rivelati e una maggiore responsabilità per la gestione delle applicazioni.

4. Soluzioni di sicurezza CPS

L'importanza e i requisiti di sicurezza sono diversi da un'applicazione all'altra. Ad esempio, in Intelligent Transportation e Intelligent Medical, la privacy dei dati è il requisito più importante, mentre in Intelligent Urban Management e Smart Grid l'autenticità dei dati è più importante. Ci sono stati molti sforzi per produrre un modello CPS sicuro.

4.1 Soluzioni proposte a strato singolo

Per quanto riguarda la gestione delle chiavi per le tecniche di crittografia, viene proposto un migliorato schema di distribuzione delle chiavi basato sull'identità per WSN utilizzando la gestione delle chiavi ECC. Lo studio mostra che, in larga misura, c'è una diminuzione dei processi computazionali usando dimensioni chiave più piccole tra i nodi. Fornisce inoltre una stima dei costi di rottura chiave in una situazione di risorse disponibili limitate (costo in dollari e tempo in un certo numero di giorni) e un compromesso tra il tempo richiesto di protezione della privacy rispetto al carico di elaborazione per un nodo. I risultati mostrano che l'utilizzo di un piccolo modulo di chiave pubblica a 1024 bit richiede che un nodo esegua solo il 3,1% dei calcoli rispetto a un tipico modulo a 3248 bit. Questo studio fornisce anche una stima del numero di giorni necessari richiesti da un avversario per rompere diverse chiavi di piccole dimensioni utilizzate nella comunicazione tra il nodo e gli Smart Meter domestici e i server delle società di servizi.

Un protocollo di autenticazione leggero per proteggere i tag RFID per impedire agli aggressori di accedere alla rete sniffando il codice Product Key elettronico del tag vittima e programmandolo su un altro tag. Inoltre, per prevenire gli attacchi, questo protocollo può garantire l'autenticazione reciproca tra lettori RFID e articoli con tag con sovraccarico sui dispositivi.

Si propone un WSN sicuro potenziato dal cyber-fisico che integra il cloud computing per l'architettura di assistenza agli utenti e le applicazioni sanitarie. Anche il monitoraggio e il processo decisionale sono forniti nello stesso sistema. Questa architettura combina tre parti fondamentali: comunicazione, calcolo e pianificazione e gestione delle risorse. Il nucleo di sicurezza è una combinazione di un nodo del sensore di origine con un numero

casuale crittografato per fornire protezione contro gli attacchi. Il focus del core di sicurezza è sul miglioramento di WSN e sull'integrazione nel cloud computing.

Per migliorare la sicurezza di una Smart Grid, che fondamentalmente dipende da tre requisiti di sicurezza fondamentali (autenticazione, autorizzazione e integrità del messaggio), Fouda et al. propongono un leggero schema di autenticazione reciproca in due fasi per Smart Meter distribuiti su diverse reti gerarchiche. Lo scambio di sessioni di chiavi condivise viene realizzato utilizzando il protocollo di scambio Diffie-Hellman, e i messaggi tra gli Smart Meters vengono autenticati utilizzando la chiave di sessione condivisa e la tecnica del codice di autenticazione basata su hash.

Dal punto di vista della necessità di un'autenticazione a più fattori per i dispositivi CPS, una nuova tecnica di sicurezza basata su hardware per CPS, che è specifico per dispositivi con potenza di elaborazione limitata. Questo metodo utilizza la funzione Physically Unclonable (PUF), anche chiamata Physical Random Function, per la limitazione dell'accesso al dispositivo con tasti assegnati. PUF è una funzione che fornisce un valore univoco a seconda delle proprietà fisiche dell'hardware del dispositivo utilizzato. Questo meccanismo viene utilizzato come identificatore univoco per alcuni dispositivi come prova dell'identità a conoscenza zero. Questo approccio dipende dal fatto che i limiti fisici dei dispositivi di produzione introducono lievi differenze tra le copie dello stesso hardware, il che conferisce a ciascun dispositivo un'identità unica che può essere identificata dal valore PUF. PUF è implementato nell'hardware, come l'utilizzo di SRAM (Static Random Access Memory), per identificare in modo univoco i dispositivi. Inoltre, questa tecnica può essere utilizzata per il controllo dell'accesso e la crittografia della base di localizzazione. Il vantaggio dell'utilizzo di PUF è che produce un valore univoco, che, per ogni istanza hardware, equivale a ripetere l'implementazione PUF sullo stesso dispositivo. Pertanto, il PUF può essere utilizzato per confermare l'identità univoca dei dispositivi CPS, garantendo l'integrità e l'autenticità del dispositivo collegato. PUF può anche essere utilizzato per creare chiavi crittografiche uniche. L'uso comune di questa tecnologia è quello di proteggere l'archiviazione delle chiavi crittografiche. Dal momento che saranno legati all'hardware, sarebbe difficile per un avversario ottenere queste chiavi.

Un altro approccio per migliorare la sicurezza è l'inclusione di tecniche IDS (Intrusion Detection System). Considerata una delle tecnologie per scoprire gli avversari nel livello

di trasmissione, questo può monitorare tempestivamente il comportamento del nodo per identificare eventuali comportamenti sospetti.

4.2 Soluzioni multistrato proposte

Gestire una singola misura, come le soluzioni elencate nella sottosezione precedente, potrebbe non essere sufficiente per risolvere i problemi di sicurezza, che dovrebbero essere considerati da una prospettiva multi-misura. Inoltre, soddisfare la sicurezza in un livello non soddisferà gli obiettivi di sicurezza richiesti, come l'implementazione di una solida soluzione di sicurezza a livello di sensore di un sistema con un livello di applicazione debole. Pertanto, dovrebbe esserci una cooperazione tra i tre livelli del sistema e soluzioni di sicurezza tra domini. Poiché la sicurezza per CPS non sarà interamente realizzata implementando individualmente una singola soluzione in ogni livello, alcuni ricercatori si concentrano sullo sviluppo di soluzioni di sicurezza come framework per tutti i livelli CPS insieme. Tuttavia, ogni strato ha requisiti diversi che, a loro volta, portano alla maggiore complessità di qualsiasi soluzione prodotta.

Un meccanismo di autenticazione off-line che si basa su una chiave pubblica combinata (CPK). L'obiettivo principale di questo meccanismo è risolvere i problemi di sicurezza correlati all'autenticazione tra domini con enormi set di dati di autenticazioni. L'architettura di sicurezza proposta fornisce protezione della sicurezza per i dati dei sensori, la privacy dei tag e la trasmissione dei dati. L'approccio applicato include la validità dell'autenticazione dei nodi integranti e la distinzione di identificazione. Al fine di migliorare la sicurezza informatica, i tre livelli (applicazione, trasmissione e percezione) sono presi in considerazione per la costruzione del sistema affidabile. A livello di applicazione, il controllo di accesso affidabile viene utilizzato per migliorare l'accesso legale, convalidare in modo univoco i dispositivi collegati e garantire il processo di non ripudio. Quindi, vengono eseguiti thread e processi attendibili con autenticazione del codice per salvare il runtime in ambienti di rete aperti e non sicuri. Successivamente, viene utilizzato un database attendibile per fornire l'autenticazione reciproca per l'accesso ai dati. Il meccanismo di autenticazione proposto elimina la necessità di fare affidamento sulla certificazione di terze parti. A livello di trasmissione, uno speciale chip di comunicazione CPK è incorporato con apparecchiature di comunicazione wireless o cablate; quindi, evitando la necessità di certificazione da parte di terzi. A livello di percezione, i tag sono incorporati con algoritmi di crittografia a curva ellittica (ECC) per

fornire accesso autorizzato e utilizzati con il CPK, che è l'autenticazione basata sull'identità, per fornire un'autenticazione rapida. Uno speciale chip di comunicazione CPK è incorporato con apparecchiature di comunicazione wireless o cablate; quindi, evitando la necessità di certificazione da parte di terzi.

Un'analisi di sicurezza del CPS fornisce alcune delle caratteristiche, come gestione e controllo distribuiti, feedback, requisiti in tempo reale e distribuzione geografica, che dovrebbero essere prese in considerazione nella progettazione di soluzioni di sicurezza. Il focus di questo studio è sul controllo fisico del CPS, con suggerimenti per la protezione dei canali di comunicazione, requisiti in tempo reale e applicazioni. Un framework di sicurezza per CPS fornisce un'analisi completa per quanto riguarda tre aspetti degli obiettivi di sicurezza, sicurezza in specifiche applicazioni CPS e approcci di sicurezza. Tuttavia, questo studio non considera l'autenticità negli obiettivi di sicurezza CPS, che è un fattore importante.

Vegh e Miclea propongono un metodo per progettare un modello di sistema cyber-fisico sicuro combinando la crittografia e la steganografia. Gli autori propongono un modello di protezione della sicurezza attraverso l'accesso gerarchico alle informazioni per aumentare il livello di sicurezza. Questo metodo prevede la crittografia e l'occultamento dei dati e l'occultamento della chiave segreta in un diverso file di copertina. Si ritiene che il modello di combinazione di algoritmi di sicurezza nello stesso sistema migliorerà la protezione dei dati richiesta in CPS. Questo sistema è basato su un'idea multi-agente e ogni agente ha dati decentralizzati incompleti per risolvere i compiti. Ciò implica che ciascun agente (utente) ha una visione locale del sistema e non ha alcuna possibilità di visualizzare le informazioni complete di quel sistema. Ad esempio, la radice dell'albero ha pieno accesso alle informazioni all'interno del sistema, mentre il resto ha accesso limitato. L'accesso gerarchico alle informazioni offre alcune restrizioni di accesso alle informazioni.

La fiducia, la probabilità di eseguire le azioni richieste dagli oggetti, non è considerata da molti ricercatori. Ali et al. (2015) propone un approccio basato sulla fiducia con coperte a due livelli, che consistono in livelli di fiducia interni ed esterni, per creare un CPS affidabile e sicuro. Per garantire comunicazioni sicure e affidabili in CPS, gli autori prendono in considerazione i seguenti punti: autenticazione degli utenti prima di entrare nella rete; una relazione di fiducia tra diversi nodi del CPS; unire nodi dannosi che

potrebbero attaccare i nodi chiave del CPS (sensori o attuatori); e riconfigurare il sistema CPS in una situazione di aggressione. L'idea dell'approccio proposto è quella di coinvolgere la sicurezza come parte integrante dell'architettura CPS piuttosto che applicarla come soluzione complementare. Oltre agli obiettivi di sicurezza CPS, gli autori considerano un approccio orientato alla fiducia come un quinto obiettivo che migliorerà l'obiettivo di sicurezza.

Considerando che i dispositivi possono spostarsi fisicamente da un supporto all'altro, Xie e Wang (2014) discutono l'importanza della fiducia tra gli utenti con autorizzazioni e controllo degli accessi adeguati. Questo lavoro presenta un'idea di fiducia reciproca per la sicurezza tra sistemi, che può essere implementata creando un framework di controllo accessi a livello di elemento. Questa fiducia si basa sulla creazione di chiavi e su un token creato dal proprietario o dal produttore dell'RFID e assegnato al dispositivo. Quando si assegna questo dispositivo a un nuovo utente, l'autorizzazione può essere modificata dal proprietario o dal dispositivo stesso. Pertanto, l'autorizzazione del dispositivo può essere sostituita tra l'utente precedente e il nuovo utente, senza costi aggiuntivi. Questo processo mira a ridurre le spese generali di assegnazione delle chiavi, che sono generate dal produttore del dispositivo RFID, da un sistema di diritto.

Un framework di sicurezza CPS è presentato in Lu et al. (2013) basato su un'architettura a tre livelli: interpretazione (percezione), trasmissione (rete) e cyber (applicazione). Più meccanismi di sicurezza sono impostati nel campo delle informazioni (cyber) utilizzando una struttura di rete gerarchica per aumentare i livelli di sicurezza, mentre la sicurezza del dominio di controllo viene trattata, ad esempio, utilizzando la stima distribuita o il controllo tollerante. Questo metodo fornisce principalmente un framework di sicurezza per CPS, a seconda della potenziale analisi delle minacce. Un'operazione di valutazione del rischio è presa in considerazione dal punto di vista delle attività (valori), minacce, vulnerabilità e danni.

Wang et al. (2010) propone un framework di sicurezza sensibile al contesto per CPS generale, che è un insieme di situazioni e impostazioni ambientali per determinare il comportamento di un utente o di un evento di un'applicazione. Il quadro di sicurezza proposto comprende tre parti essenziali di sicurezza: rilevamento, cyber e controllo. Questo framework utilizza parametri per determinare il comportamento del sistema, le informazioni situazionali e le situazioni ambientali per calcolare il livello di sicurezza del

sistema e migliorare le decisioni sulla sicurezza delle informazioni. Rende rilevanti le informazioni di contesto integrate in misure multi-sicurezza, ad esempio crittografia, accordo chiave e controllo degli accessi, per creare una sicurezza CPS adattata per l'ambiente fisico. Gli obiettivi principali del proposto quadro di sicurezza consapevole del contesto sono la riservatezza, la disponibilità, l'integrità e l'autenticità. Questo metodo classifica la funzione di CPS nelle seguenti quattro fasi: monitoraggio dei processi fisici e dell'ambiente; networking, che comprende aggregazione e diffusione dei dati; elaborazione per raccogliere e analizzare dati durante la fase di monitoraggio; e una fase di attuazione per eseguire l'azione determinata nella fase di calcolo. Lo scopo di questo metodo è quello di creare un meccanismo di sicurezza per CPS che si adatta dinamicamente all'ambiente fisico.

5. STPA-SafeSec: analisi di sicurezza per sistemi cyber-fisici

I sistemi cyber-fisici integrano strettamente i processi fisici e le tecnologie dell'informazione e della comunicazione. Poiché le infrastrutture critiche odierne, ad esempio la rete elettrica o le reti di distribuzione idrica, sono sistemi cyber-fisici complessi, assicurando che la loro sicurezza diventi di fondamentale importanza. I metodi tradizionali di analisi della sicurezza, come HAZOP (dall'inglese HAZard and OPerability analysis), non sono adatti per valutare questi sistemi. Inoltre, le vulnerabilità della cybersicurezza spesso non sono considerate critiche, poiché i loro effetti sui processi fisici non sono completamente compresi.

In questo capitolo, presentiamo STPA-SafeSec, una nuova metodologia di analisi per la sicurezza. I suoi risultati mostrano le dipendenze tra le vulnerabilità della sicurezza informatica e la sicurezza del sistema. Utilizzando queste informazioni, la più efficace delle strategie di mitigazione per garantire la sicurezza del sistema possono essere facilmente identificate. Applichiamo STPA-SafeSec a un caso d'uso nel dominio della rete elettrica e ne evidenziamo i vantaggi.

Le infrastrutture critiche, ad esempio la rete elettrica o la rete di distribuzione idrica, sono sistemi cyber-fisici (CPS): i processi fisici e i componenti sono collegati tramite le tecnologie dell'informazione e della comunicazione (ICT), che sono fondamentali per il corretto funzionamento del sistema. Con l'aumentare della velocità di elaborazione e della velocità di trasmissione della rete, nuove applicazioni per i sistemi di controllo industriale (ICS) si basano sui progressi delle ICT per migliorare l'efficienza dei sistemi fisici sottostanti. Queste nuove applicazioni creano una più stretta integrazione tra i processi fisici e il cyber dominio. Inoltre, i sistemi stanno diventando più interconnessi e quindi più complessi. È importante analizzare le implicazioni che questo maggiore uso delle TIC e la conseguente complessità hanno sulla sicurezza di questi sistemi cyber-fisici. Ciò è necessario per garantire che i requisiti di sicurezza siano identificati e affrontati come parte del processo di progettazione del sistema. Accanto agli aspetti di sicurezza, le minacce alla sicurezza informatica ai sistemi cibernetici stanno diventando una preoccupazione. Il virus Stuxnet o un attacco contro un'acciaieria tedesca hanno dimostrato come gli attacchi informatici riusciti possano causare danni fisici. Inoltre, nel settore energetico, si è dimostrato in che modo un attacco informatico a più stadi potrebbe comportare la manipolazione di un inverter fotovoltaico, modificando la sua potenza attiva.

I metodi di analisi tradizionali che mirano a valutare la sicurezza delle infrastrutture critiche non comprendono la complessità dei sistemi cyber-fisici emergenti. Funzionano con modelli di incidenti basati sulla catena errore-guasto. Sebbene questi modelli siano validi per descrivere i guasti dei sistemi lineari e dei singoli componenti, non sono sufficienti per descrivere i guasti del sistema in sistemi interconnessi complessi. Per ovviare a questa carenza, Leveson (2004) ha sviluppato il modello di incidente: modello-processi teorici e processi (STAMP), basato su STAMP, l'approccio System Teoretic Process Analysis (STPA) è stato sviluppato come una nuova tecnica di analisi dei pericoli per valutare la sicurezza di un sistema.

Gli attuali approcci all'esame della cibersicurezza per i sistemi cibernetici si basano spesso su un'analisi dei protocolli TIC o delle configurazioni di rete e sono pertanto fortemente influenzati dalle preoccupazioni in materia di sicurezza delle informazioni. Inoltre, gli effetti degli attacchi informatici devono essere analizzati dal punto di vista della sicurezza. In questo modo, è possibile identificare il potenziale impatto degli attacchi informatici sulla sicurezza dei processi fisici. Per quantificare accuratamente questi impatti, è necessaria una comprensione della relazione tra attacchi informatici e processi fisici, che richiede tecniche dedicate di analisi della sicurezza. Per affrontare questo problema hanno sviluppato STPA-sec, che utilizza i principi fondamentali di STPA nel dominio della sicurezza. Tuttavia, il loro approccio, che indica un metodo di analisi separato per la sicurezza (STPA) e la sicurezza (STPA-sec), deve essere migliorato e chiarito.

Una nuova metodologia di analisi che integra l'analisi della sicurezza (STPA) e l'analisi della sicurezza (STPA-sec) in un quadro conciso: STPA-SafeSec. Superiamo i limiti di STPA introducendo vincoli di sicurezza nell'analisi e mappando il livello di controllo astratto del sistema che viene analizzato da STPA su componenti reali. STPA-SafeSec offre numerosi vantaggi rispetto al lavoro esistente:

1. fornisce un unico approccio per identificare i vincoli di sicurezza che devono quindi essere garantiti dal sistema per operare senza perdite. Questo approccio unico consente di rilevare e utilizzare le interdipendenze tra sicurezza e vincoli di sicurezza nelle strategie di mitigazione;
2. i componenti di sistema più critici possono essere prioritari per un'analisi approfondita della sicurezza (ad es. test di penetrazione);

3. i risultati dell'analisi mostrano le potenziali perdite del sistema che possono essere causate da una specifica sicurezza o vulnerabilità della sicurezza nel sistema;
4. le strategie di mitigazione possono essere progettate più prontamente e la loro efficacia valutata.

I cambiamenti nel processo fisico possono essere utilizzati per mitigare gli attacchi informatici, mentre gli algoritmi di controllo possono mitigare i limiti di sicurezza dei processi o dispositivi fisici.

È possibile identificare due gruppi di tecniche di analisi dei pericoli: tecniche di analisi dei pericoli basate su guasti e tecniche di analisi dei pericoli basate su sistemi. Esempi di tecniche basate sui guasti sono Fault Tree Analysis (FTA) e Failure Mode and Effect Analysis (FMEA). I metodi basati sui guasti si concentrano sull'identificazione degli effetti e delle probabilità di guasti a singolo componente. Le probabilità di guasti ai componenti consentono di quantificare le tecniche basate sui guasti. Tuttavia, l'efficacia delle tecniche basate sui guasti e la crescente complessità dei sistemi moderni hanno portato a un nuovo tipo di incidenti radicati nell'interazione dei componenti. Per comprendere questo nuovo tipo di incidenti, sono necessarie tecniche di analisi basate sul sistema. Una di queste tecniche è la Hazard and Operability Analysis (HAZOP). Sulla base di una solida progettazione del sistema, vengono definiti i parametri di sistema rilevanti e quindi vengono utilizzate le parole guida per identificare come il sistema potrebbe discostarsi dal comportamento progettato.

Nel corso degli anni, i ricercatori hanno cercato di formalizzare HAZOP per ottenere risultati oggettivi e quantificabili. Ma si evidenzia che tutti gli approcci per quantificare i risultati hanno ricondotto all'uso dell'ALS basato sui guasti.

Gli approcci basati sul sistema sono difficili da quantificare perché i sistemi moderni si affidano sempre più ai sistemi software per controllare i processi fisici e sono ulteriormente integrati in ambienti sociotecnici. Sia i bug del software che gli effetti delle influenze non tecniche sul sistema nel tempo sono molto difficili da misurare in fase di progettazione.Lo STPA intende affrontare queste nuove sfide in una nuova tecnica di analisi dei pericoli basata sul sistema. Sebbene non esista un approccio sistematico per quantificare i risultati di STPA, si fornisce un modello matematico alla base di STPA e una procedura per eseguire sistematicamente un'analisi STPA nella sua tesi. Questa

esecuzione sistematica di STPA consente risultati di analisi più oggettivi rispetto all'applicazione ad hoc degli ultimi anni.

La ricerca sui potenziali effetti dei cyber-attacchi sulle infrastrutture fisiche in CPS viene spesso condotta da una ICT o da una prospettiva di ingegneria fisica e di controllo. Nel dominio ICT si analizzano i potenziali attacchi informatici ai sistemi di controllo delle sottostazioni elettriche. Il loro focus di ricerca si trova sulle potenziali minacce di attacchi informatici alle capacità di comunicazione ICT.

I potenziali effetti fisici sono evidenziati ma negli esperimenti non si ottengono effetti fisici critici. Le vulnerabilità specifiche ben note dal dominio cibernetico possono essere sfruttate nel contesto di un CPS. Tuttavia, quando i processi fisici vengono arricchiti dalla comunicazione basata sulle ICT, le misure di sicurezza fisica rimangono in vigore. Questi meccanismi di sicurezza sono spesso usati come argomento per minimizzare il rischio che gli attacchi informatici possono avere sul funzionamento sicuro di questi sistemi. STPA-SafeSec prende in considerazione i meccanismi di sicurezza esistenti durante il processo di analisi e può quindi argomentare in modo più forte sul perché le vulnerabilità della sicurezza informatica debbano essere prese sul serio. Si evidenziano attacchi informatici su disponibilità, integrità e riservatezza, nonché i loro potenziali effetti su diversi casi d'uso e presentano inoltre potenziali strategie di mitigazione. Le firme e la crittografia sono presentate come contromisure crittografiche e vengono spiegate le difficoltà che derivano dalla limitata potenza di calcolo e dai rigorosi vincoli temporali. Le contromisure basate sulla rete sono presentate e raggruppate per i livelli di comunicazione mirati.

L'analisi fornisce una buona panoramica delle considerazioni di sicurezza necessarie per CPS, ma viene applicata ad un'architettura di griglia intelligente molto generica. Ciò rende difficile trarre conclusioni dai risultati a un sistema specifico a portata di mano. STPA-SafeSec incorpora gli aspetti generici di questi risultati in un framework di analisi.

Si presenta un primo passo verso un framework basato su grafici per modellare l'impatto fisico degli attacchi informatici su reti intelligenti. Uno studio di caso mostra che un attacco informatico riuscito può causare una grave situazione di sottofrequenza che alla fine provoca un blackout locale. Per la rete elettrica, Ten et al ha presentato l'applicazione di reti di Petri e alberi di attacco per prevedere la perdita di carico causata da debolezze

identificate. Si utilizzano le macchine a stati per mostrare in che modo le transizioni causate dagli attacchi possono causare errori di escalation, a cascata e cause comuni.

L'uso di modelli di sistemi matematici ha il grande vantaggio di poter essere validati ed eseguiti in modo automatizzato. Ma il loro design richiede molto tempo, le tecniche di modellazione non sono standardizzate e spesso non esiste alcun supporto per gli strumenti. Per un ingegnere di sistema che deve già eseguire un'analisi di sicurezza del sistema, ciò significa spesso uno sforzo temporale incalcolabile che nella maggior parte dei casi non è obbligatorio. STPA-SafeSec può essere utilizzato al posto di un'altra tecnica di analisi della sicurezza e include l'analisi della sicurezza come prodotto secondario.

Si descrive come un utente malintenzionato può modellare la vulnerabilità informatica e fisica di una griglia agli attacchi informatici sulla base di informazioni limitate. Gli autori presentano una classifica di vulnerabilità informatica e come informazioni limitate sulla griglia possono essere utilizzate per identificare i componenti più critici per lanciare un attacco. Gli autori presentano un framework automatico di resilienza della sicurezza informatica per le reti elettriche che incorpora azioni di rilevamento, ragionamento e mitigazione automatiche con un focus sull'uso di alberi di attacco per l'analisi delle vulnerabilità. Al fine di implementare questo framework di resilienza per una specifica architettura di sistema, è necessaria un'analisi dettagliata delle vulnerabilità della sicurezza informatica, dei loro potenziali effetti fisici e delle possibili strategie di mitigazione. STPA-SafeSec è progettato per recuperare esattamente queste informazioni da un sistema.

Si presenta una metodologia di valutazione del rischio indipendente dal dominio per le infrastrutture cyber-fisiche. L'analisi del rischio inizia con una valutazione dettagliata della vulnerabilità dell'infrastruttura seguita da un'analisi dell'impatto dell'applicazione e del sistema fisico. L'esecuzione di un'analisi completa della vulnerabilità di un CPS complesso come una rete elettrica è molto complessa e la completezza è difficile da dimostrare. Un approccio migliore consiste nell'applicare un'analisi dettagliata della vulnerabilità solo ai componenti più critici identificati da una precedente analisi d'impatto. In questo modo, attività che richiedono tempo come i test di penetrazione possono essere programmate nel modo più efficace. Inoltre, il test di penetrazione di un CPS vivo è sconsigliato quando non sono noti i potenziali effetti del comportamento di un componente non valido. STPA-SafeSec fornisce i mezzi per identificare i componenti

di sistema più critici per un'analisi approfondita della sicurezza. Sottolinea inoltre i potenziali pericoli del sistema e le perdite del sistema che possono essere causate dal malfunzionamento di un componente specifico.

Si presentano attacchi di disponibilità sui segnali GPS mediante jamming GPS. Gli autori hanno anche elaborato contromisure contro il disturbo GPS nei moderni ricevitori GPS. Un attacco di integrità ai segnali GPS rispetto alla sincronizzazione dell'ora. Gli autori mostrano come l'iniezione di segnali GPS mirati aumenta l'effetto dell'attacco rispetto all'errore arbitrario introdotto dagli attacchi di disponibilità. La rilevanza di tale ricerca su uno specifico CPS è spesso difficile da identificare. Se ci sono dispositivi distribuiti nell'infrastruttura che si basano sul GPS e quale sarebbe l'impatto di un segnale inceppato o manipolato sono domande a cui è difficile rispondere. STPA-SafeSec fornisce i mezzi per identificare le dipendenze di componenti specifici su specifici collegamenti di comunicazione e l'impatto di diverse categorie di attacco.

Gli alberi di attacco sono uno dei modelli di sicurezza grafica più affermati. Introdotto per la prima volta da Weiss come alberi logici di minaccia, la loro somiglianza con gli alberi di faglia indica che le loro radici sono nel dominio della sicurezza. STPA-SafeSec sfrutta una struttura ad albero per connettersi e presentare i risultati dell'analisi finale. L'albero può quindi essere esteso dai risultati di un'approfondita analisi di sicurezza. Inoltre, gli approcci per associare fattori di costo o probabilità agli alberi di attacco tradizionali hanno il potenziale per rendere quantificabili i risultati di STPA-SafeSec.

5.1 L'approccio STPA-SafeSec

Sistemi di Cyber-fisico (CPS) si basano sempre più sulla interconnessione di dispositivi. Ciò ha causato una crescente attenzione per la sicurezza informatica insieme alle tecniche di analisi tradizionali. STPA-sec mostra che STPA può essere utilizzato anche per analizzare la sicurezza dei sistemi. Cambia il tradizionale approccio alla sicurezza, in cui le minacce sono utilizzate per derivare i requisiti di sicurezza, in un approccio in cui i risultati sono rilevanti. Un approccio dall'alto verso il basso potrebbe anche essere supportato da altre tecniche di analisi della sicurezza (ad esempio FTA, HAZOP) ma ci sono diversi vantaggi di STPA rispetto a questi approcci. Tuttavia, STPA può essere utilizzato non solo per l'analisi della sicurezza del sistema o per prevenire pericoli e perdite. Può essere ulteriormente generalizzato per analizzare un sistema rispetto a tutte

le proprietà di sistema emergenti rilevanti. Una proprietà di sistema emergente è una proprietà che sorge attraverso l'interazione di parti del sistema, mentre le parti stesse non hanno necessariamente la stessa proprietà. Sicurezza e protezione sono esempi di tali proprietà di sistema emergenti. Pubblicazioni precedenti su STPA-sec suggeriscono che l'analisi della sicurezza viene sempre eseguita per garantire la sicurezza del sistema. Inoltre, le pubblicazioni indicano che esiste una differenza tra l'uso di STPA per la sicurezza e STPA-sec per la sicurezza. Si sostiene che la sicurezza deve essere affrontata collettivamente. Questo approccio collettivo è possibile con STPA. Tuttavia, le presentazioni attuali di STPA presentano una serie di fattori limitanti:

1. Non è chiaro che STPA e STPA-sec siano la stessa analisi. Solo un'analisi collettiva di sicurezza e protezione consente all'analista di identificare le dipendenze tra le due proprietà e ottenere i risultati più ottimali.
2. Non esiste alcuna guida per un approccio integrato di sicurezza e protezione che utilizza STPA in cui la sicurezza è considerata proprietà ugualmente importanti che si influenzano a vicenda. Piuttosto, STPA-sec sostiene che la sicurezza è rilevante solo rispetto al suo impatto sulla sicurezza. Questa è una visione limitata del sistema. Nel contesto sociotecnico dei sistemi cyber-fisici moderni la perdita monetaria per l'operatore dovrebbe essere considerata una perdita critica del sistema. Questa perdita può verificarsi a causa di una violazione della riservatezza (ad es. Dati dei consumatori o proprietà intellettuali) senza implicazioni dirette per la sicurezza. Successivamente, il tradizionale STPA-sec deve essere esteso per consentire all'analista di considerare questo tipo di perdite che non sono direttamente legate alla sicurezza.
3. STPA-sec non fornisce indicazioni su come eseguire l'analisi di sicurezza una volta definiti gli aspetti critici del sistema. Innanzitutto, non estende i fattori causali presentati per il dominio di sicurezza nel dominio di sicurezza. Ciò rende più difficile l'analisi e limita la comparabilità tra i diversi risultati dell'analisi. Inoltre, STPA-sec non fornisce alcun mezzo per integrare tecniche di analisi della sicurezza ben consolidate. Questo è un problema non solo per l'accettazione di STPA per l'analisi della sicurezza. È anche importante che la qualità dell'analisi ottenga risultati dettagliati dai test di penetrazione. Non tutti i vincoli di sicurezza possono essere garantiti nel dominio del sistema fisico e guidato dalla sicurezza.

Per ottenere la progettazione del sistema più efficace, STPA deve essere in grado di guidare l'analisi manuale e integrare i risultati.

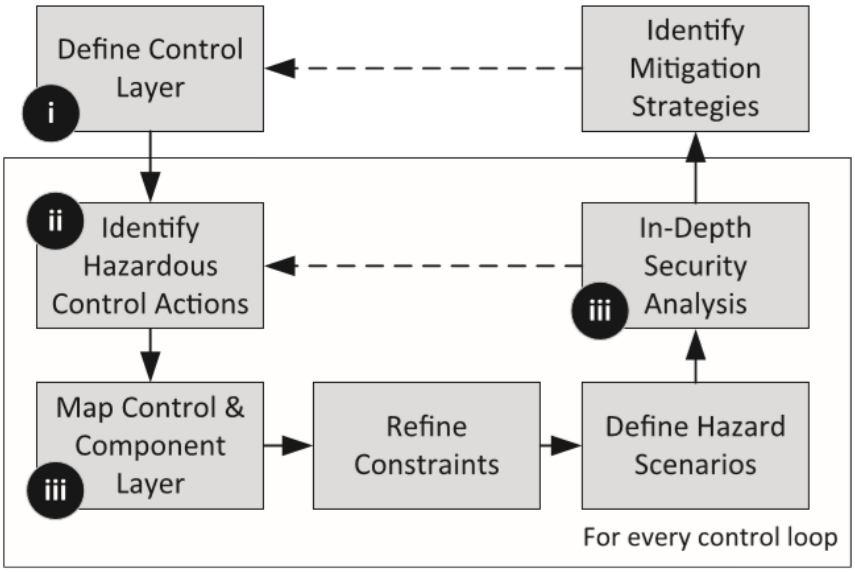


Figura 8

Una panoramica generale di STPA-SafeSec è riportata in Fig. 8 ha lo scopo di affrontare le carenze sopra menzionate e introduce i seguenti miglioramenti rispetto ai metodi STPA tradizionali:

1. La descrizione e la valutazione di un approccio unificato all'analisi della sicurezza basata su STPA e STPA-sec. Questo approccio dà la priorità alla sicurezza e alla protezione allo stesso modo e consente di rilevare una serie più ampia di scenari di pericolo.
2. Un'estensione della guida del fattore causale incentrata sulla sicurezza di STPA nel dominio della sicurezza. Questa estensione fornisce supporto per l'analista e rende i risultati più comparabili.

Un metodo per collegare la struttura di controllo astratta alla progettazione del sistema fisico per integrare i risultati dei tradizionali metodi di analisi della sicurezza. Sulla base della progettazione del sistema fisico, è possibile utilizzare tecniche di analisi della sicurezza tradizionali complementari a STPA-SafeSec. Inoltre, i risultati consentono un'applicazione intelligente di attività di analisi che richiedono tempo nelle parti più critiche del sistema.

L'approccio contiene due loop. I sistemi cyber-fisici moderni non sono statici ma si evolvono nel tempo, influenzati dal loro ambiente sociotecnico. Il ciclo esterno evidenzia che STPA-SafeSec è un approccio iterativo che deve essere riapplicato nel corso della vita del sistema per gestire questa natura in evoluzione. Nel suo nucleo, STPA si basa su vincoli e circuiti di controllo del sistema. Per gestire la complessità dei sistemi moderni, ciascun circuito di controllo viene analizzato separatamente durante l'analisi; questo è mostrato dal circuito interno. I vincoli vengono prima raffinati per il sistema nel suo insieme in base alle perdite che dovrebbero essere prevenute. Quindi, questi vincoli vengono perfezionati e mappati al livello di controllo; la rappresentazione dei circuiti di controllo e la loro interazione. Si verificano pericoli e perdite successive quando vengono intraprese azioni di controllo che violano uno o più dei vincoli precedentemente definite le cosiddette azioni di controllo pericoloso.

L'analisi fornisce i mezzi per derivare i fattori causali che portano a queste pericolose azioni di controllo. Questi fattori causali sono estesi da STPA-SafeSec per includere considerazioni sulla sicurezza. Inoltre, il livello di controllo astratto viene mappato su un livello componente specifico dell'implementazione. Questo strato componente fornisce i mezzi per perfezionare ulteriormente i vincoli e derivare fattori causali più specifici. Può guidare ulteriormente l'analisi approfondita della sicurezza. I risultati finali: una serie di modifiche che devono essere applicate all'architettura di sistema per garantire un funzionamento senza perdite sono infine derivati in base agli scenari che descrivono come le azioni di controllo pericolose sono causate da fattori causali.

STPA-SafeSec risolve le carenze di STPA e STPA-sec presentate precedentemente e fornisce un approccio integrato per analizzare gli aspetti di sicurezza in un unico framework. In questo modo elimina la necessità di eseguire ripetutamente i passaggi dell'analisi e ridurre il rischio di incomprensioni.

5.2 Discussione del metodo

Come tecnica di analisi dei pericoli basata sul sistema, STPA-SafeSec non fornisce direttamente risultati quantificabili. Tuttavia, gli approcci noti per rendere più quantificabili le tecniche di analisi dei pericoli basate sul sistema come HAZOP possono essere applicati a STPA-SafeSec. Inoltre, i metodi per quantificare gli alberi di attacco possono essere applicati anche alla struttura ad albero dei risultati STPA-SafeSec.Questo

mostra come i risultati di STPA-SafeSec possano essere utilizzati per valutare decisioni complesse sui componenti più critici e le strategie di mitigazione più efficaci. Inoltre, STPA-SafeSec evidenzia scenari in cui nessuna strategia di mitigazione fisica è valida. Per limitare il danno si può dare priorità alle perdite del sistema al fine di prevenire le perdite più gravi accettando perdite meno critiche.

L'analisi presentata non presenta modalità automatizzate per eseguire STPA-SafeSec. Tuttavia, i metodi semi-automatici definiti per STPA tradizionale possono essere applicati direttamente ad alcune parti di STPA-SafeSec. Inoltre, è possibile applicare metodi semi-automatizzati simili per i nuovi passaggi di STPA-SafeSec. Per controllare stati operativi, è necessaria una maggiore integrazione dei sistemi di alimentazione con la comunicazione ICT. Questa integrazione motiva nuovi approcci per analizzare i sistemi in termini di sicurezza.

Il nuovo contributo è quello di formalizzare un approccio per analizzare le dipendenze tra le limitazioni fisiche imposte dalle apparecchiature di potenza reali e le capacità di un aggressore nel dominio cibernetico. Questa formalizzazione consente agli analisti di utilizzare i risultati di ricerche precedenti nel settore della sicurezza e di applicarli a un'infrastruttura. Inoltre, STPA-SafeSec può applicare metodi noti per quantificare i risultati delle tecniche di analisi dei pericoli basate sul sistema. La capacità di evidenziare gli effetti fisici delle vulnerabilità della sicurezza o dei difetti di sistema basati su perdite di sistema di alto livello rende i risultati più facili da comunicare a livello di scheda rispetto ai risultati di analisi di sicurezza generici forniti. STPA-SafeSec è inoltre in grado di guidare un'analisi approfondita della sicurezza dei componenti più critici e di integrare i risultati e i risultati di STPA-SafeSec possono essere utilizzati per progettare strutture reattive complesse che garantiscano la sicurezza del sistema.

6. Un approfondimento dei sistemi cyber-fisici robotici collaborativi industriali nel campo della sicurezza

Ora introduciamo un quadro di sicurezza per l'applicazione della collaborazione uomo-robot in un contesto futuristico di sistema cibernetico industriale (CPS) dell'industria 4.0. Vengono spiegati gli elementi di base e i requisiti funzionali di un sistema cyber-fisico robotico collaborativo sicuro e quindi le modalità di attacco informatico vengono discusse nel contesto del CPS collaborativo mentre una strategia di meccanismo di difesa viene proposta per un sistema così complesso.

Gli attacchi informatici sono classificati in base all'estensione della controllabilità e ai possibili effetti sulle prestazioni e sull'efficienza di tale CPS. Si descrive anche la gravità e la categorizzazione di tali attacchi informatici e l'effetto causale sulla sicurezza del lavoratore umano durante la collaborazione uomo-robot.

Attacchi in tre dimensioni di disponibilità, l'autenticazione e la riservatezza sono proposte come base di un piano di mitigazione consolidato. Proponiamo un quadro di sicurezza basato su una strategia su due fronti in cui l'impatto di questa metodologia è dimostrato su un benchmark di teleassistenza. La strategia di mitigazione include una maggiore sicurezza dei dati in importanti nodi adattatori interconnessi e lo sviluppo di un modulo intelligente che impiega un concetto simile al monitoraggio dello stato del sistema e alla riconfigurazione.

I futuri sistemi di produzione industriale sono probabilmente basati sui sistemi di produzione cyber-fisici (CPPS) per produrre prodotti intelligenti con maggiore flessibilità. Questo concetto di produzione intelligente si è evoluto dalla definizione di sistema collaborativo cyber-fisico (CCPS) in cui l'integrazione di componenti fisici e computazionali si traduce in rilevamento e controllo della variazione di stato nei parametri del mondo reale. Tale sistema comprende l'hardware fisico, la rete di sensori, nonché le tecnologie di informazione, computer e comunicazione con interfaccia uomo-macchina (HMI,Human Man Interface). Queste infrastrutture offrono sfide tecnologiche e promuovono nuove opportunità di interazione per l'uomo con attrezzature, macchine e strumenti nell'ambiente. CPS integra i processi di calcolo e fisici per ottimizzare l'utilizzo delle risorse e le prestazioni del sistema. Questi sistemi possono essere collegati a Internet o a una rete sicura esterna. L'hardware fisico può essere un robot, attuatore o un impianto di produzione e può essere definito come il componente fisico (PC) nel CPS.

Il costo del componente fisico può essere molto elevato e varia da un'area di applicazione all'altra. Per un corretto funzionamento di tale sistema robotico collaborativo, è necessario un CPS sicuro al fine di proteggere elementi fisici altamente sofisticati e costosi. La sicurezza di tali sistemi può essere compromessa da attacchi informatici attraverso la rete o la connettività Internet. È certo che tali attacchi entrano nel CPS attraverso il componente informatico (CC) e colpiscono il PC (computer industriale, PLC, robot ecc.) che è controllato principalmente dal CC. La maggiore connettività alle reti esterne costituisce una minaccia per la sicurezza del CPS. Se gli attaccanti sviluppano mezzi per entrare nei sistemi di controllo e modificare il comportamento del sistema, ciò può causare danni irreversibili al PC. Gli attacchi informatici ai sistemi IT hanno portato all'evoluzione degli schermi antivirus per la sicurezza delle reti di computer. Il dominio CPS è diverso in questo contesto poiché la sicurezza di un sistema IT serve solo il CC e non esiste alcun meccanismo per proteggere il PC. Inoltre, l'effetto causale degli attacchi informatici dal cyber layer fino al PC è inerente. In questo contesto, lo sviluppo di piani di mitigazione contro simili attacchi informatici intelligenti è una nuova area di ricerca. Implica l'identificazione di nuovi framework per l'analisi degli attacchi informatici al CPS.

L'aspetto più importante per quanto riguarda la sicurezza di un CPS è la conoscenza del progetto di un attacco informatico. L'aspetto critico di un piano di mitigazione efficace per la sicurezza di CPS è conoscere la struttura di tale attacco informatico. Per studiare questo, sono stati progettati numerosi attacchi informatici contro i componenti CPS e sono stati valutati i suoi effetti sui componenti di controllo cyber, fisico e collaborativo. Stuxnet ed altri attacchi, hanno creato consapevolezza e preoccupazioni diffuse sui danni all'infrastruttura fisica attraverso attacchi informatici. Come affermato, le misure di sicurezza esistenti sono state per lo più sviluppate per sistemi esclusivamente informatici e non possono essere applicate in modo efficace al CPS in una rete collaborativa. Pertanto, sono necessari nuovi approcci per prevenire guasti alla CPS. La differenza nelle proprietà degli strati fisici e cyber all'interno di CPS ha reso l'interfaccia un nodo molto importante in cui i componenti informatici rendono possibile una grande varietà di attacchi. Al contrario, i PC sono poco flessibili e semplici con possibilità di attacchi relativamente basse.

Le funzioni di sicurezza nelle reti sono essenziali per la protezione delle infrastrutture chiave. Per i sistemi di controllo industriale di oggi, le nuove architetture di rete

intelligenti sono un requisito essenziale. Sviluppiamo un quadro di sicurezza industriale per la collaborazione umana-robot sicura (HRC) in un ambiente di produzione industriale connesso, noto come "Collaborative Robotic Cyber-Physical System" (CRCPS).

Vi è un crescente interesse per i clienti industriali dei "produttori di robot collaborativi" che si occupano di processi di assemblaggio automatici e semiautomatici nel portare i loro processi di assemblaggio a uno stadio per consentire una perfetta collaborazione uomo-robot. Ciò è particolarmente valido per i processi semiautomatici nell'industria automobilistica che sono caratterizzati dal fatto che alcuni compiti vengono svolti manualmente dal lavoratore umano. La sicurezza della rete nel CRCPS industriale è cruciale in quanto questo sistema ha lo scopo di evitare qualsiasi situazione critica potenzialmente letale per il lavoratore che lavora con i robot collaborativi industriali con carico utile pesante. Oltre alla sicurezza dei lavoratori, è indispensabile che le informazioni importanti all'interno di CRCPS rimangano sicure e non debbano essere compromesse a causa di un attacco dannoso. Il CPS sicuro deve essere in grado di determinare la responsabilità dei lavoratori umani mantenendo la loro sicurezza e privacy. Il problema diventa complesso a causa delle crescenti interazioni nei moduli di CPS e anche a causa della crescente complessità della progettazione di attacchi informatici classificati in base a 3 dimensioni. Questi attributi sono correlati al tipo di attaccante come insider o outsider del sistema, scopi e obiettivi dell'attaccante e modalità di attacco con cui viene lanciato l'attacco. Un attaccante in modalità attiva tenta disturbare la disponibilità e l'autenticazione del nodo CPS e indirizzare l'attacco verso danni fisici, mentre l'attacco in modalità passiva si mantiene nella rete per estrarre prezioso livello di sistema e controllare informazioni come una missione di ricognizione. Evitando le informazioni da mittenti non attendibili e costruendo una rete sicura, la rete CPS sicura può ridurre la minaccia. Il mittente non attendibile può essere un sensore già sotto attacco informatico che invia informazioni fuorvianti.

Ci concentriamo sui componenti CPS e le interfacce che collegano i diversi componenti specificamente ai nodi interattivi dei componenti fisici e informatici. L'architettura è sviluppata su un framework di strategia di difesa basato su modulo e proteggendo le interfacce. Stiamo proponendo una soluzione sistematica di moduli fisici sicuri intelligenti per prevenire la distruzione fisica tentata dal cyber anche quando lo strato informatico è compromesso. In questo contesto, vengono utilizzati adattatori intelligenti auto-sicuri tra componenti fisici e cyber che preservano l'affidabilità prevalente nel

controllo e nel flusso di dati. Viene adottato un approccio di architettura decentralizzata per la struttura CRCPS in modo che il sistema non possa avere un singolo nodo di errore che un utente malintenzionato può contrassegnare. Tuttavia, contro tale architettura, il nemico attacca i sottosistemi.

Questa area di applicazione nella ricerca sul CPS è un esempio perfetto in cui la sicurezza e la protezione sono integrate e devono essere affrontate nell'architettura CPS. La fusione dei problemi di sicurezza nella progettazione CRCPS è simile al concetto di seguito nella progettazione e rischio valutazione della struttura industriale e controllo che rispecchiano entrambi gli aspetti. La sicurezza è strettamente associata alla sicurezza poiché entrambe queste caratteristiche devono essere affrontate in modo sincrono. L'aspetto della sicurezza protegge tangibilmente i lavoratori dell'industria dalle macchine, mentre i sistemi dalle persone come nemici.

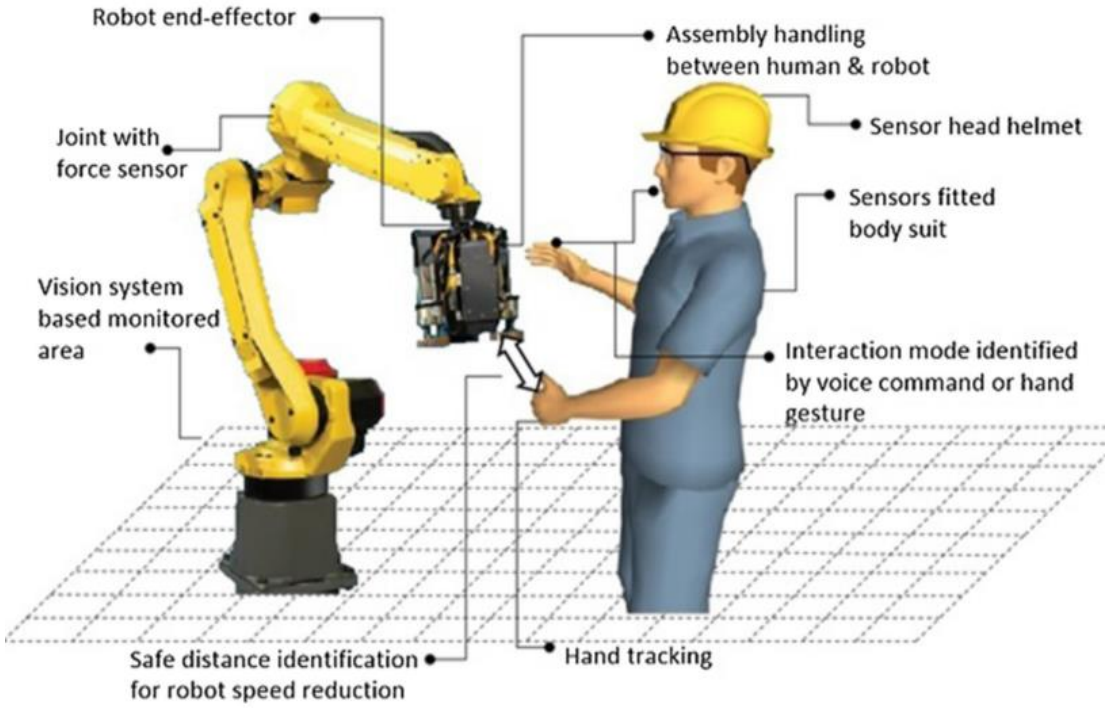


Figura 9

Sulla base di tale approccio integrato, la selezione della tecnologia per tale sistema può presentare molteplici sfide. Come esempio di HRC, in Fig. 9 illustra un sistema collaborativo per il monitoraggio della velocità o della separazione. Il concetto impiega numerosi sensori integrati in rete e l'HRC si sta svolgendo nell'area sotto monitoraggio

per l'esecuzione di un compito industriale. Nel tipo di collaborazione di monitoraggio della velocità e della separazione, il sistema incorpora telecamere o altri sensori per il posizionamento dell'operatore in tempo reale. Inoltre, la velocità del robot viene ridotta o viene applicata una probabile rottura nel caso in cui l'operatore si muova nell'area pericolosa. Le telecamere aeree sono installate per tracciare la posizione umana in tempo reale con l'aiuto di marcatori. Uno scanner laser oppure è possibile installare una barriera fotoelettrica per coprire qualsiasi violazione dell'area monitorata e segnalare al robot la presenza umana. Inoltre, esiste un altro sistema per l'acquisizione della firma della posizione umana attraverso i sensori inerziali. L'operatore deve indossare un giubbotto (o una tuta) durante la collaborazione che comprende diversi IMU integrati in diverse posizioni del corpo, fornendo così i dati di velocità e posizione al CRCPS. I dati del sensore giroscopico vengono comunicati attraverso un protocollo sicuro ai componenti fisici e informatici per ulteriori analisi in tempo reale e le decisioni prese vengono quindi reindirizzate nel sistema. Il casco dotato di IMU per la posizione della testa e i dati di frequenza è un altro dispositivo utilizzato per uno scopo simile.

Poiché l'obiettivo di base per lo sviluppo di CRCPS è mantenere la sicurezza dei lavoratori mentre HRC è in funzione, supponiamo che sia in atto un sistema HRC sicuro. Requisiti CRCPS dettagliati, struttura CPS, classificazioni di sicurezza, scenari industriali e metodologia di sviluppo sono studiati per CRCPS. Qui ci concentriamo sugli aspetti di sicurezza di CRCPS e sulle misure di protezione necessarie per l'implementazione. In CRCPS, i moduli funzionali sono interconnessi tramite sistemi cablati e / o in modalità wireless per conversare con lo stesso tipo di dispositivi. Utilizzando i sistemi HMI (Human Machine Machine Interactive), le macchine si collegano e cooperano con l'uomo attraverso una rete. Quindi, la disposizione di un CPS completo interpreta il collaboratore umano come un componente di sistema vitale.

Nel definire CRCPS, ci sono alcuni componenti principali interconnessi nel modello (Vedi Fig.10). Questi moduli sono il componente umano (HC), il componente fisico (PC) e il componente computazionale (CC). La comunicazione tra le tre entità è soggetta all'avvento delle tecnologie adattatrici abilitanti in CPS. Per definire un CRCPS, i moduli di base di HC, PC e CC interagiscono attraverso gli adattatori mentre il sistema possiede tutte le caratteristiche intrinseche del CPS come integrità, socialità, località, irreversibilità, adattabilità, autonomia e altamente automatizzato. Per CRCPS, il PC deve essere un robot. Il componente umano è accoppiato attraverso diverse tecnologie di

adattamento, ad esempio il tracciamento della posizione del lavoratore è un adattatore cruciale nel CRCPS tramite telecamere aeree o IMU. Il CRCPS è un sistema automatizzato in quanto elimina i limiti tra i vari componenti, favorendo così le loro comunicazioni operative.

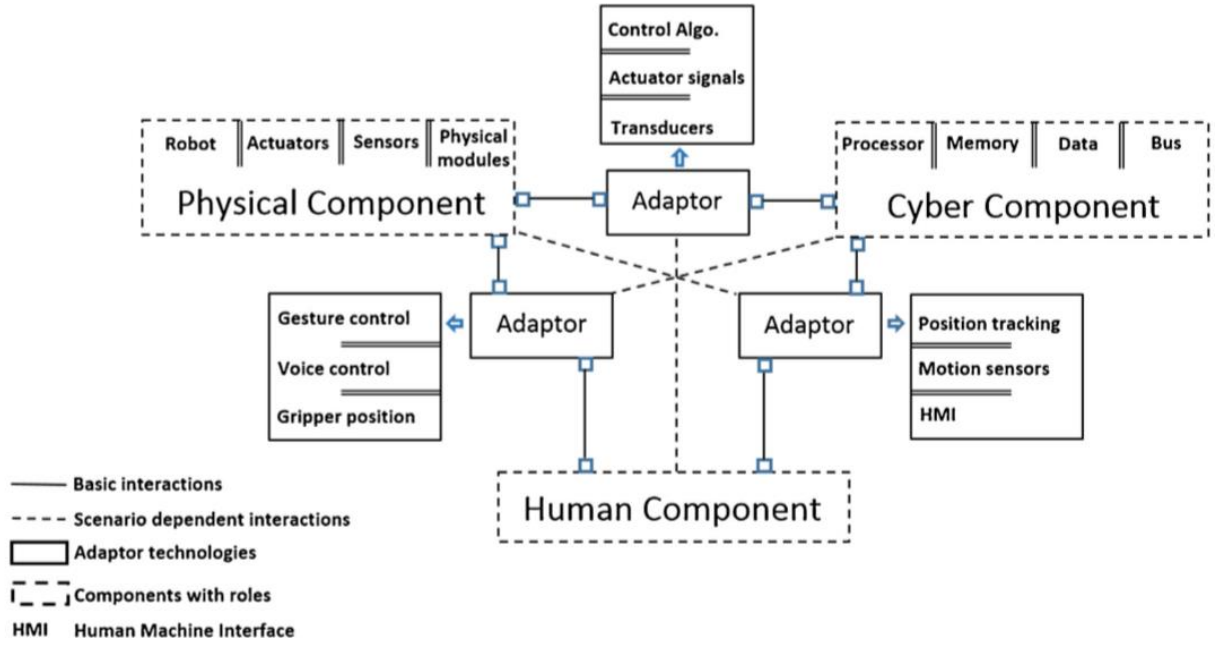


Figura 10

Esistono numerose tecnologie HMI che dipendono dall'acustica, dalla visione e dall'ottica. Il CRCPS pianificato ha utilizzato un sistema di visione per il rilevamento e il monitoraggio della posizione dell'operatore. Il sistema di comando robotizzato collaborativo può anche utilizzare il riconoscimento gestuale dell'operatore e l'acustica come il controllo vocale. Inoltre, una varietà di attuatori e sensori può fornire la comunicazione tra PC, HC e CC. Ci sono connessioni regolari rivelate tra i componenti che contribuiscono a un ruolo. Le tecnologie dell'adattatore sono dispositivi dipendenti dalla situazione (plug and play). Esistono connessioni dipendenti dalla situazione discrezionale tra gli adattatori e i componenti regolari in CRCPS.

In CRCPS, il nodo controller del PC (sistema robotizzato) esegue la parte di controllo intelligente per calcolare comandi precisi di posizionamento e velocità. Viene utilizzato in CRCPS e il sistema di comunicazione è progettato tramite reti e informazioni wireless o cablate. Questa specifica applicazione è analoga a tale strumentazione in cui le misurazioni del sensore a un'applicazione del supervisore sono comunicate attraverso una rete che rende in tempo reale le informazioni importanti come il calcolo della distanza di

sicurezza. Il requisito di comunicazione del sistema mira a presentare la macchina alla macchina (M2M) e integrazione della comunicazione da uomo a macchina (H2M). Principalmente, le informazioni vengono eseguite da una macchina (sensore o modulo fisico) connessa attraverso una rete e quindi arrivano a un sistema utilizzando un gateway in cui possono essere esaminate e proseguite. La comunicazione H2M in CRCPS inizia attraverso l'uscita giroscopica è inviata sulla rete in modo che possa essere analizzata per il calcolo della distanza di sicurezza e altre considerazioni. La selezione di un protocollo appropriato è determinata dalla comunicazione sicura, dall'intervallo e dalla velocità dei dati. Un protocollo di divisione del tempo viene sfruttato per la comunicazione in tempo reale in quanto pratica la lista nera dei canali per evitare le interferenze. A causa della qualità del servizio, alcuni nodi comunicanti sono impiegati come scelta preferita per l'allocazione di tempo / risorse. Tuttavia, il protocollo Bluetooth è adatto in CRCPS a causa della comunicazione di prossimità in prossimità con elevata sicurezza.

6.1 Sfide della sicurezza informatica per CRCPS

Un framework CRCPS sicuro può essere costruito solo se esiste una consapevolezza degli attacchi informatici guidati dalla conoscenza intelligente del target. L'attacco informatico può provenire da fonti sia interne che esterne. Raya et al. hanno descritto un attaccante secondo tre modalità di classificazione, ovvero attivo contro passivo, malizioso contro razionale e esterno contro interno.

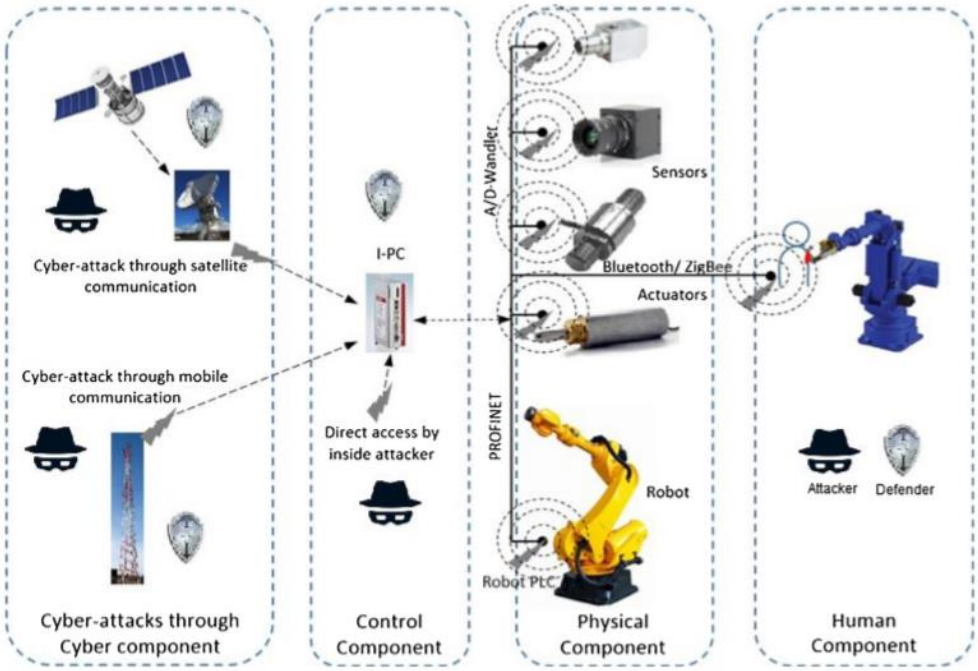


Figura 11

Come mostrato in Fig. 11, un attacco informatico può arrivare da una fonte esterna come canali di comunicazione esterni, trasmissione wireless o da un aggressore interno accedendo fisicamente a una porta dati, ad esempio da un lavoratore coinvolto in HRC in un determinato scenario industriale. L'attaccante attivo inizia l'attacco direttamente mentre l'attaccante passivo ha la tendenza ad osservare / intercettare dal componente di controllo o cyber del CPS bersaglio. La funzione dell'attaccante passivo è di ricognizione sull'attività fisica del bersaglio attraverso il livello di controllo o cyber e riportare le informazioni preziose per aiutare nella progettazione di un attacco informatico attivo intelligente. Un utente malintenzionato attivo utilizza l'autorità di rete, ma limitato dalla sua intelligenza intrinseca, può solo danneggiare in modo significativo le risorse fisiche del bersaglio, se ben equipaggiato con le conoscenze richieste. Un aggressore malintenzionato mira alla distruzione su larga scala mentre un attaccante razionale specifica il bersaglio. Qui, il compito del framework di sicurezza di mitigazione CRCPS è quello di bloccare tutte le classi di aggressori.

Un concetto di sicurezza in un sistema IT è diverso da quello in CPS, principalmente a causa del fatto che un PC è integrato e controllato da un CC in CPS. Nello scenario CPS, è un requisito necessario per proteggere il PC, anche nel caso di un CC con compromissione della sicurezza. Se nel caso del CRCPS, il componente informatico è compromesso da un attacco informatico, il PC composto da robot, umano, attuatori e sensori potrebbe subire un attacco diretto e causare un guasto del sistema come un HRC non sicuro o il verificarsi di un incidente mentre HRC è in funzione in un determinato scenario industriale. Per progettare efficacemente un concetto di sicurezza in CPS, è vantaggioso analizzare come funzionano gli attacchi informatici in un tale sistema. ACPS è un'estensione di un CPS nel dominio sociale, in cui l'essere umano è parte integrante del CPS. In un sistema IT, tutte le fasi di un attacco informatico, ovvero dalla pianificazione al raggiungimento dell'obiettivo finale, vengono condotte in un livello informatico. Tuttavia, in un CPS, queste attività sono divise in base al ruolo svolto da ciascun livello. Ad esempio, la fase di pianificazione degli attacchi è composta da tutti i livelli per raccogliere le informazioni del sistema di destinazione. Qui, la parte di ricognizione dell'attacco informatico viene condotta come attaccante passivo per aiutare a progettare un attacco sofisticato per un attaccante attivo. Nella fase successiva, un'arma da attacco informatico si prepara per ottenere il controllo del sistema bersaglio e raggiungere l'obiettivo finale. La fase di consegna è possibile solo attraverso il cyber layer

e l'esecuzione dell'attacco consiste nel superare la parte di controllo del sistema bersaglio usando le informazioni ottenute dagli attacchi passivi. Tuttavia, l'obiettivo di un attacco informatico in un CPS industriale è quello di distruggere risorse fisiche costose, anche i componenti di cyber e controllo possono far parte dell'obiettivo a seconda dell'applicazione del sistema di destinazione e della struttura di controllo.

In un caso ACPS, il ruolo aggiuntivo dell'essere umano nel meccanismo di attacco informatico è in tre punti, ovvero nella fase di pianificazione per le informazioni di sistema, nella fase di consegna dell'attacco attraverso la porta USB o altri modi interni e anche l'essere umano può essere un obiettivo finale da danneggiare in un CRCPS. Pertanto, è evidente che un meccanismo di attacco informatico per un sistema IT, un CPS e un ACPS ha mezzi e concetti diversi. Allo stesso modo, anche il piano di mitigazione contro attacchi così sofisticati dovrebbe seguire un approccio diverso.

Per soddisfare una varietà di attacchi informatici, è importante vedere le caratteristiche dei nodi nella rete. Una volta che l'attacco entra nel CRCPS attraverso il cyber layer, può condurre una varietà di attacchi come nodi rotti o falsificazione dei dati. L'orizzonte di tali attacchi può estendersi dal cyber allo strato di controllo per perturbare l'obiettivo fisico. Si preferisce un'architettura CPS decentralizzata rispetto a un errore nel nodo univoco che un nemico può mirare. La fase di esecuzione che attacca l'azione di controllo del bersaglio tenta di raggiungere proprietà specifiche guidate da requisiti operativi e le proprietà del livello cyber (riservatezza, integrità e disponibilità) devono essere protette di fronte al cyber-attacco. Nel complesso, è l'obiettivo del cyber-attacco che determina l'estensione acquisita delle particolari proprietà dei diversi componenti CPS. L'obiettivo può variare dalle prestazioni degradate di alcuni aspetti del funzionamento fisico del CPS fino alla completa interruzione o distruzione del PC in un CPS.

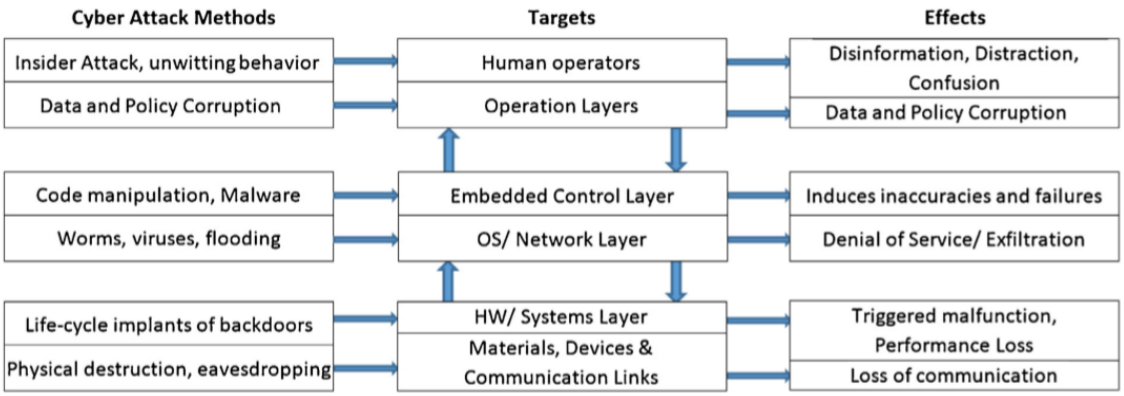


Figura 12

La Fig. 12 mostra l'elenco delle linee guida dei metodi di attacco e le interconnessioni di possibili bersagli ed effetti in diversi livelli CPS. In linea con eccessive interdipendenze tra i componenti funzionali e gli adattatori CPS, gli effetti secondari possono seguire durante le interazioni dei singoli elementi che devono essere confrontati. Questi effetti del secondo ordine possono verificarsi a componenti impegnati in strati diversi o che coinvolgono anche altri domini (cyber o fisici).

La fase di esecuzione del cyber-attacco influenza i componenti di controllo e cyber. I possibili effetti e l'estensione dell'attacco alla controllabilità del CPS dovrebbero essere valutati. È importante classificare e valutare l'impatto del particolare tipo di attacchi nel contesto di CRCPS. Le proprietà del componente di controllo sono la controllabilità e l'osservabilità degli stati interni del sistema. Un algoritmo di controllo per un sistema controllabile è progettato per rendere un sistema stabile. Un sistema osservabile impiega uno stimatore di stato un osservatore che per determinate misurazioni del sensore, può tracciare con precisione lo stato del sistema. In CRCPS, i sensori per le informazioni sulla posizione umana sono un esempio di osservabilità. Le due proprietà sono doppi matematici. Qualsiasi compromesso sulla controllabilità del sistema o sulle variabili di controllo interno può influire sul risultato fisico del CRCPS in termini di stabilità ed efficienza del sistema. La scala (dall'attacco basso al grave) viene sviluppata in base all'esito fisico CRCPS. Sulla base delle tre categorie di attacco informatico, (autenticazione, disponibilità e riservatezza), i possibili effetti possono variare dal più basso al più alto. Gli effetti a bassa e media portata comportano perdite di controllo a breve termine per ridurre l'efficienza del sensore, mentre l'alto rischio è misurato dall'uscita del falso sensore sotto attacco. Ad esempio, se la sicurezza del lavoratore è disturbata a causa dell'uscita del falso sensore, l'estensione ottenuta dall'attaccante attraversa la linea da un attacco parziale a un attacco completo.

Il framework proposto è progettato tenendo presente che l'attaccante ha una forte comprensione della stabilità del sistema, efficienza, sicurezza e vincoli delle risorse. La tabella 1 mostra una valutazione basata su criteri sull'effetto di attacco informatico sull'esito fisico del CRCPS. Gli attacchi informatici da bassi a gravi sono classificati e valutati in base alle degradabili proprietà informatiche del CRCPS, ovvero autenticazione dei nodi, disponibilità dei nodi, riservatezza dei dati e integrità. Il livello di attacchi su CRCPS è considerato basso se il controllo viene perso per un breve periodo.

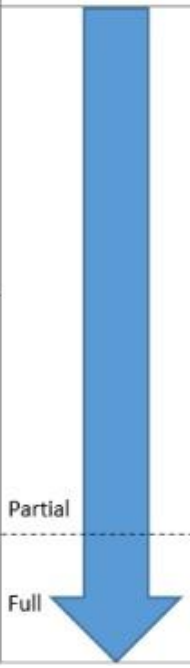
Attack intensity on CRCPS	Authentication	Availability	Confidentiality	Extent of attack on controllability	Possible effects
Low	- GPS spoofing/ Movement tracking/ position faking - Tunnelling - Message tempering - Message suppression - Non-repudiation	- Jamming - Greedy behaviour - Grey hole - Sink hole - Broad cast tempering - Spamming	- Non-repudiation		Short period control loss
Medium	- Sybill - Node impersonation - Key/Certificate replication - Masquerading - Unauthorized pre-emption	- DOS - Jamming - Black hole - Worm hole - DDoS - Malware		Partial	Effect on sensor node efficiency
Serious or high risk	- Replay		- Eavesdropping	Full	Data falsification from sensor output node

Tabella 1

Nella Tabella 1, gli attacchi di autenticazione di categoria bassa includono il tempering, il finto posizionamento e la soppressione dei messaggi in una rete ad area chiusa. Queste sono forme di false tecniche di autenticazione che un utente malintenzionato può seguire per disturbare il sistema. Nodo sensore l'autenticazione è misurata come un prerequisito di sicurezza vitale nelle reti e il componente di sistema più coinvolto è, in effetti, l'utente della rete. Un operatore CRCPS può agire come malintenzionato o intercettatore violando la sicurezza come legittimo utente di rete.

Gli attacchi di disponibilità nella stessa categoria descrivono molti attacchi relativi alla non disponibilità del nodo. La condizione di disponibilità del nodo determina che il traffico di informazioni attraverso tutti i nodi di una rete in qualsiasi momento è possibile. Gli attacchi alla disponibilità disturbano le prestazioni di thread e processi, come ritardi nell'accesso alla memoria, funzioni di trasferimento dati di bus e comunicazioni problematiche. Gli attacchi buco grigio e dolina sono un tipo di attacchi Denial of Service (DoS) in cui i pacchetti cadono e sono possibili aggiornamenti di routing falsi che possono causare il lancio di altri attacchi. Il tempera Broadcast è un altro tipo di attacco che può portare all'incidente nascondendo i messaggi relativi alla sicurezza dai nodi legittimi. Per progettare una rete CPS la protezione, autenticità, integrità dei dati, privacy, riservatezza

e disponibilità sono fattori importanti. Di questi parametri, l'autenticazione, la disponibilità e la riservatezza sono rilevanti per CRCPS, principalmente a causa dell'applicazione della sicurezza del lavoratore umano. Un attacco di riservatezza consente al nemico di raccogliere informazioni di sistema e utilizzare tali informazioni quando l'utente non è a conoscenza della perdita di informazioni. Un attacco di ripudio si verifica quando un sistema non implementa controlli per monitorare correttamente le attività dell'utente, compromettendo quindi la protezione dei dati industriali e l'anonimato dei lavoratori nel caso di CRCPS. Il rischio medio per CRCPS è definito a causa della ridotta efficienza del sensore. Gli attacchi di autenticazione a rischio medio includono l'attacco Sybil, il mascheramento e anche il tipo di attacchi in cui imbrogliare con le informazioni sul posizionamento e la divulgazione dell'ID sono comuni. Il sistema CPS deve essere in grado di identificare il mittente non attendibile e ignorare i segnali di tali sensori all'interno del CPS. Gli attacchi di disponibilità nella categoria media includono gli attacchi buco nero, wormhole, DoS e Jamming. I buchi neri si formano in nodi interconnessi a causa di un nodo rotto. Nella rete CRCPS, un nodo spezzato proveniente da un sensore importante, ad esempio uno scanner laser responsabile del monitoraggio dell'area, può causare sistema collaborativo per essere meno efficiente. Tutti questi attacchi sono classificati come aventi effetti di scala medio-bassa sulla sicurezza informatica del CRCPS. Un attacco al CRCPS è considerato grave quando i dati del sensore sono falsi. Influenzando l'uscita del sensore, le stime di stato possono essere corrotte da un utente malintenzionato che causa segnali di controllo errati agli attuatori. Un attacco di replay è come inviare di nuovo informazioni precedentemente ricevute nella rete, portando a un errore nella propagazione del segnale. Un falso funzionamento di tali sensori nella rete può compromettere la sicurezza del sistema. In CRCPS, le informazioni sulla posizione del lavoratore provengono dal sistema di visione o dai sensori di movimento. Un attacco di riproduzione, ovvero un falso aggiornamento di informazioni sulla posizione del lavoratore, può rendere il sistema non sicuro. Un altro obiettivo è acquisire informazioni sugli algoritmi di controllo, i sensori e gli attuatori e su come vengono utilizzati per monitorare e controllare il CPS. Un attacco alla riservatezza può compromettere le informazioni sullo stato del sistema necessarie affinché un attacco informatico possa perturbare il PC del CPS. Eavesdropping si occupa della raccolta illegittima di messaggi da parte dell'attaccante e migliora la capacità dell'attaccante di influenzare le operazioni fisiche del sistema. CRCPS è costituito da una rete di sensori (vitale) che mantiene l'HC sicuro. La rete non deve essere compromessa a causa dei

risultati fisici associati di stabilità, efficienza e sicurezza. La sicurezza del livello informatico consisteva in attacchi basati su integrità, disponibilità e riservatezza che possono influire negativamente su accesso, prestazioni e altre qualità del CRCPS.

La quantificazione dei metodi di rischio in CPS è studiata su integrità, disponibilità e riservatezza. In risposta a un attacco, vengono identificate le sfide e l'influenza sui principi di sicurezza di riservatezza e integrità. Il rilevamento di nodi ad alto rischio in una rete può essere identificato in modo efficace da un framework di sicurezza per ordinare le risposte appropriate in base ai principi fondamentali di sicurezza. Una categorizzazione efficace degli attacchi informatici nel contesto del CRCPS ha rivelato la possibilità di rischio in base all'estensione dell'attacco alla controllabilità. Poiché il disturbo della stabilità del sistema per un breve periodo è collegato al basso livello di attacchi, una riduzione dell'efficienza del sistema può essere causata dagli attacchi classificati a livello medio in CRCPS. Ciò si basa sul presupposto che l'algoritmo di evitamento umano e i calcoli della distanza di sicurezza in CRCPS non possono essere disturbati in tempo reale.

6.2 Proposta di framework sicuro per CRCPS

La sicurezza del canale di comunicazione è fondamentale per l'implementazione della rete sicura. Fornire autenticità a una rete CPS a breve distanza implica proteggere i nodi legittimi dagli aggressori che penetrano nella rete attraverso un'identità inventata.

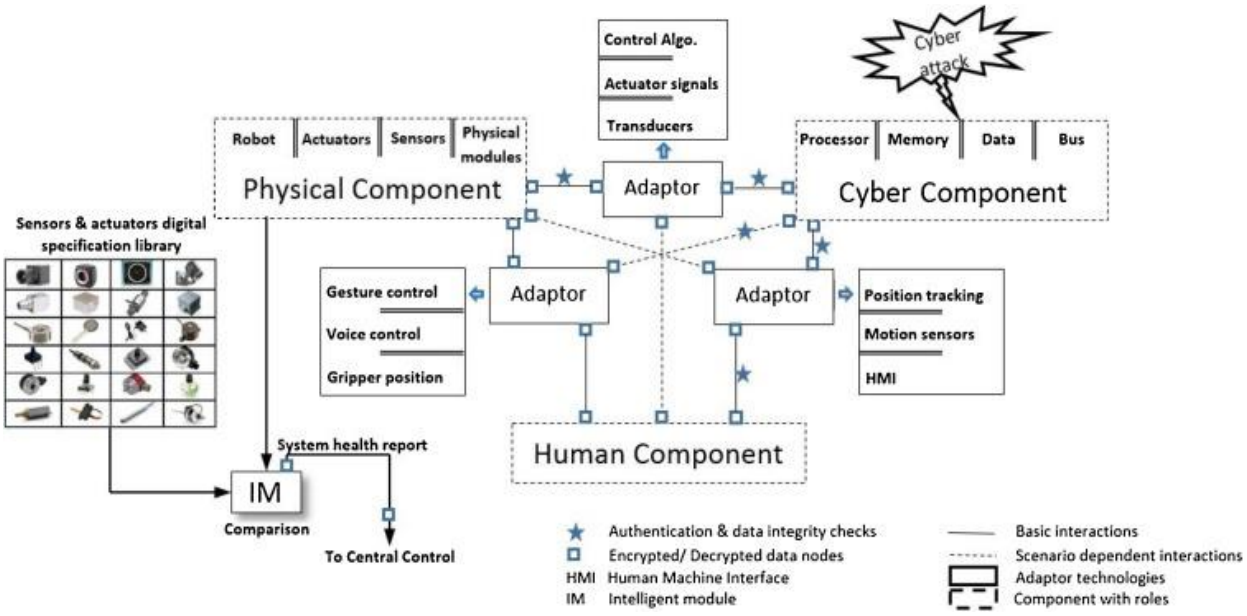


Figura 13

Per l'applicazione CRCPS, è necessario l'aggiornamento affidabile dei dati sicuri, in particolare per i nodi dell'adattatore di interfaccia tra CC e PC in tempo reale e con un sovraccarico limitato. L'idea è quella di sviluppare un quadro di sicurezza (vedi Fig. 13) evolvendo una strategia di difesa su due fronti. La strategia consente di sviluppare adattatori sicuri attraverso una rigorosa sicurezza informatica procedure comprendenti requisiti di autenticazione, disponibilità e riservatezza scegliendo nodi adeguati all'implementazione della soluzione. Il secondo componente della strategia ha un modulo intelligente indipendente che può fornire supporto di calibrazione e confronto in tempo reale dalla libreria di riferimento di sensori e attuatori memorizzati altrove nel sistema. In caso di attacco informatico a un CPS progettato per HRC, gli effetti delle cyber perturbazioni raggiungono infine l'essere umano che lavora con il robot. È necessario elaborare un piano di mitigazione basato su un'architettura protettiva in grado di supportare il CPS sotto attacco. Per costruire un CRCPS sicuro, proponiamo una strategia su due fronti in cui la prima parte si occuperà dei nodi interconnessi e della sicurezza dei dati migliorata in importanti nodi dell'adattatore. L'autenticazione del nodo e il controllo dell'integrità dei dati le procedure sono adottate per tutti i nodi dell'adattatore tra il CC e altri componenti in modo tale che nel caso di un CC compromesso, il CPS rimanente possa essere protetto e prendere una decisione per la sua sopravvivenza. La seconda parte della strategia è quella di sviluppare un modulo intelligente per vedere il controllo dello stato del costoso PC e segnalarlo alla sala di controllo principale nello scenario industriale, per prendere decisioni su ulteriori opzioni se viene rilevato un CC compromesso.

Negli schemi di sicurezza informatica, il concetto di controlli dello stato fisico riflette le informazioni dell'esecuzione fisica, piuttosto che i difetti teorici dell'algoritmo. Questo concetto può essere utilizzato per una strategia di sicurezza preventiva basata su controlli di parametri fisici per identificare se il sistema è sotto attacco. Il concetto originale è quello di far fronte agli "attacchi del canale laterale". Alcuni esempi sono le informazioni di temporizzazione, il consumo di energia o le perdite elettromagnetiche. Inoltre, la misurazione della dissipazione del calore da un chip e i segnali acustici possono essere sfruttati per l'interruzione del sistema target. Sulla base di tali informazioni, gli attacchi del canale laterale sono sviluppati sulla base di strumenti statistici. Nella strategia di sicurezza del CRCPS, la teoria dell'attacco del canale laterale viene utilizzata per

concettualizzare la misurazione dei parametri fisici su nodi chiave, dispositivi e PC in grado di diagnosticare il sistema sotto attacco.

Il framework di sicurezza proposto si basa sul presupposto che un cyber-shield installato su CC agisca come una protezione di sicurezza del sistema IT standard che comprenda l'attacco informatico. Un attacco informatico progettato per CPS può arrivare solo attraverso CC, ma in realtà perturbare il livello di controllo per causare danni al PC. Quindi, questa è una presunzione che CC e qualsiasi altro modulo sicuro nel CRCPS avessero scudi simili possono anche essere compromessi. Un attacco informatico in arrivo ha la possibilità di effettuare importanti funzionalità di base del CPS se gli strati dopo CC vengono controllati dall'attacco. Un sistema di controllo ridondante per eseguire tali funzionalità di sistema di base del PC può essere proposto in caso di CC sotto attacco, ma il suo meccanismo di commutazione è difficile da concepire. Ancora una volta, è necessario un modulo indipendente e intelligente per scoprire lo stato del sistema in tempo reale. Una di queste tecniche sarebbe il confronto dei parametri fisici in tempo reale dei sensori con le informazioni sulle specifiche pre-memorizzate. Nel caso di CRCPS ci deve essere anche un'opzione per giungere a uno scenario industriale manuale se il modulo indipendente (IM) riporta un sistema meno efficiente a causa di un attacco.

Sull'aspetto fisico, il sistema collaborativo è progettato per il funzionamento sicuro e protetto di esseri umani vicino a robot industriali funzionali. L'obiettivo di un possibile attacco informatico a un tale sistema è quello di rompere la sicurezza del sistema, ottenere il controllo di un possibile nodo sensore e attuatore, corrompere i dati e quindi disturbare la funzionalità CRCPS. In uno scenario di attacco informatico su CRCPS vengono discussi i possibili modi e mezzi per infiltrarsi nel sistema. Inoltre, il quadro strategico della difesa è messo in evidenza di fronte a un attacco informatico.

Come mostrato in Fig. 13, le procedure di autenticazione dei nodi e di controllo dell'integrità dei dati sono installate sui nodi dell'adattatore adiacenti a CC per evitare la diffusione di attacchi informatici oltre CC e salvaguardare il costoso PC. I controlli di autenticazione del nodo includono la procedura di handshaking seguita dall'identificazione dei parametri della chiave di sicurezza e quindi dalla generazione, dallo scambio e dalla verifica di un certificato di sicurezza. Una crittografia l'algoritmo può anche essere proposto in particolare per i nodi in cui è richiesta la riservatezza, ad esempio un report sullo stato del sistema generato dall'IM richiede un percorso riservato

verso l'HC o verso qualsiasi luogo centralizzato per l'avviso umano e ulteriori interventi. Il routing per l'IM può essere verificato per il tipo di attacco man-in-the-middle (MiM). Nell'attacco MiM, l'attaccante modifica la comunicazione tra le parti che si affidano al canale per comunicare tra loro. L'ascolto attivo è un esempio di attacco MiM in cui l'attaccante sviluppa connessioni auto-dirette con i bersagli. L'attaccante trasmette segnali tra le parti e l'intero scambio è organizzato dall'attaccante. Un controllo MiM simile può essere introdotto per i nodi tra CC e PC. L'IM viene proposta come strategia per scoprire la salute e l'efficienza del CRCPS sotto un attacco informatico comparatore per confrontare i parametri dei sensori e degli attuatori in tempo reale con la libreria di specifiche pre-memorizzata. Qualsiasi riduzione dell'efficienza del PC può essere monitorata dall'IM e riferire direttamente a un controllo centrale per l'intervento umano per ulteriori decisioni. Tuttavia, esiste un problema fondamentale da risolvere sulla causa di un comportamento così insolito nei parametri fisici o nelle letture dell'IM. I motivi possono essere identificati in due modi. Uno potrebbe essere dovuto all'attacco informatico e l'altro potrebbe essere dovuto al comportamento errato del sensore, del chip o di una macchina a causa di un malfunzionamento. L'importante è distinguere tra il sistema sotto attacco informatico e il comportamento errato del sistema. Esistono metodi di verifica del protocollo in cui sia la verifica hardware che software viene eseguita attraverso la simulazione del sistema prima del funzionamento del sistema. Tuttavia, per garantire l'affidabilità del sistema durante il funzionamento, è necessario abilitare le macchine per eseguire il processo di verifica da soli. Le macchine di autoverifica o autoapprendimento possono anche utilizzare gli algoritmi di regolazione per far fronte all'invecchiamento dei sistemi fisici, possono cercare guasti intenzionali e non intenzionali e prevedere e allarmare meglio in modo accurato contro gli attacchi informatici. Esistono approcci di autocontrollo come la costruzione di moduli multi-compartimenti, o container. Tali metodi possono essere utili per affrontare strane prestazioni del sistema all'interno dei moduli e per cercare la vera fonte del malfunzionamento. Ad esempio, l'approccio container è una strategia di integrazione del sistema che prende i singoli moduli e componenti da diverse fonti non verificate e potenzialmente dannose e costruisce un sistema globale sicuro e corretto. L'approccio container incapsula i blocchi di proprietà intellettuale (IP) in moduli verificabili. Ogni componente IP viene inserito in un contenitore, che implementa effettivamente i meccanismi di protezione richiesti. Ogni container ha più livelli di accordi di verifica e

controlli di protezione che dipendono dal sovraccarico accettabile. L'integrazione di tali contenitori garantisce il funzionamento sicuro del sistema circostante.

6.3 Impostazione benchmark per dimostrazione di CRCPS

Miriamo a discutere uno scenario in cui possiamo simulare lo schema proposto su un sistema in tempo reale. Poiché l'implementazione su vasta scala di una piattaforma robotica multi-DOF altamente precisa è in fase di sviluppo, abbiamo dimostrato che una versione semplificata dell'algoritmo proposto su una rete è guidata dall'impostazione della teleoperazione. Come accennato in precedenza, il framework di sicurezza proposto è una metodologia in due fasi basata sulla sicurezza dei dati migliorata per i nodi interconnessi e un monitoraggio dello stato del sistema intelligente per la mitigazione in tempo reale degli attacchi informatici.

Una configurazione di teleoperazione per azionamento da parte dell'applicazione wireless è considerata un CRCPS generalizzato per la simulazione della strategia proposta. Tali sistemi sono molto popolari nelle applicazioni che coinvolgono operazioni in luoghi sporchi, pericolosi e di difficile accesso. Per il telelavoro a lungo raggio, sono preferibili reti wireless; tuttavia, il controllo su una rete wireless presenta alcune sfide dovute a problemi inerenti ai collegamenti di comunicazione.

La configurazione classica delle parti Master / Slave viene mantenuta nella nostra demo migliorando l'algoritmo di controllo della posizione per l'implementazione in tempo reale. Un controller fuzzy viene utilizzato per soddisfare la degradante qualità del servizio (QoS) del controllo e dei flussi video variando la velocità dei pacchetti del frame video. Inoltre, lo schema adattivo implementato su questo banco di prova consente di migliorare la telepresenza anche in presenza di ritardi e perdite di pacchetti fino a un livello accettabile basato sulla qualità soggettiva del servizio. Lo schema proposto è incorporato con successo in una configurazione di riferimento in cui è implementato il controller basato sulla passività con circuito di monitoraggio neuro-fuzzy adattivo per il controllo QoS.

Un sistema drive-by-wireless è un CPS collaborativo in cui i collegamenti e le trasmissioni meccaniche sono sostituiti da sistemi elettronici e cavi elettrici. I dati multisensoriali vengono passati a una piattaforma di acquisizione e calcolo dei dati, che trasferisce l'energia elettrica in movimento meccanico. Esistono diversi tipi di sistemi

drive-by-wire, quindi più in generale viene definito "x-by-wire". Descriviamo un'applicazione di teleassistenza wireless drive-by in cui il veicolo di prova è progettato per essere teleoperato a distanza da una piattaforma del volante attiva (stazione Mater) che è dotata di un sistema di visione stereo 3D come mostrato in Fig.14.

(a) (b)

Figura 14

Il telelavoro bilaterale viene eseguito utilizzando misurazioni della coppia di contatto della ruota e feedback per la deflessione della forza; al contrario, la connessione wireless consente di testare algoritmi di codifica in presenza di perdita di pacchetti e ritardi di trasmissione. La trasformazione basata sullo scattering è integrata da una strategia di perdita di pacchetti da parte di un osservatore per scegliere tra l'ultimo campione di sospensione (HLS) e l'azzeramento. Il guadagno del circuito di controllo della posizione varia nel tempo rispetto al ritardo, garantendo allo stesso tempo la condizione di stabilità basata sulla passività. Il diagramma del livello di blocco del sistema, in cui il circuito di teleoperazione nominale è integrato da un circuito di retroazione che tiene traccia delle prestazioni della rete per il controllo di QoS.

Se valutiamo un attacco di media intensità su CRCPS operato su un Distributed Denial of Service (DDoS) tale che la controllabilità della teleoperazione circuito chiuso è minacciata a causa della mancata disponibilità delle risorse di rete per alcune specifiche periodo. Si presume che l'attaccante sia in grado di violare la sicurezza ed è in grado di aggiungere più flussi di traffico di rete congestionando così la rete wireless. Ciò comporta una perdita significativa, se non completa, dei dati di comando dalla postazione dell'operatore. Lo schema di attacco influenza gravemente il QoS e di conseguenza il QoC del teleoperatore.

6.4 Osservazioni conclusive dei CRCPS

È necessario un CPS sicuro per proteggere i costosi elementi fisici. La sicurezza del CPS è messa in discussione dal sempre crescente cyber-attacco intelligente sviluppato con l'intuizione strutturale del bersaglio. La chiave per lo sviluppo di un efficace piano di attenuazione per la sicurezza del CPS richiede la conoscenza della struttura di informatici-fisico cyberattacco e interconnessione proprietà del sistema.

Il lavoro precedente in questo settore riguarda gli attacchi informatici intelligenti al CPS, ma finora mancano le strategie globali di mitigazione. Le misure di cyber-security sono per lo più limitate allo strato informatico del CPS, mentre i sistemi di protezione industriale sono rigidi, meno intelligenti e resistenti ai disturbi dinamici causati dagli attacchi informatici. In questo contesto, il CRCPS viene proposto con l'obiettivo di evitare situazioni critiche potenzialmente letali per il lavoratore che collabora con robot industriali con carico utile elevato. Il metodo nella progettazione CRCPS è la fusione delle strategie di sicurezza e protezione in un unico framework. Il quadro di sicurezza si basa anche su una struttura CRCPS in cui l'HC è ben collegato attraverso diverse tecnologie di adattamento con PC e CC.

Una delle funzioni importanti dell'attacco informatico è la ricognizione del bene fisico bersaglio attraverso il controllo o il livello informatico che rivela informazioni preziose. La controllabilità del CRCPS è influenzata dalla capacità dell'attaccante di progettare un attacco informatico che sfida caratteristiche esplicite dirette da necessità funzionali. L'estensione ottenuta dall'attaccante dipende dal danno sulle proprietà del livello cyber da parte degli attacchi di riservatezza, integrità e disponibilità. Abbiamo proposto la scalabilità degli attacchi informatici agli esiti fisici del sistema come disturbo della stabilità per un breve periodo e l'efficienza ridotta del sensore rappresenta minacce di livello medio-basso.

Il problema nel definire le esatte categorie di attacchi è una stima difficile, poiché la capacità di minaccia di questi attacchi è sempre in aumento a causa del continuo avanzamento degli algoritmi di attacco. In tal caso, un attacco considerato di basso livello può danneggiare il bersaglio con gravi conseguenze. Un approccio alla sicurezza o un piano di mitigazione contro gli attacchi informatici devono avere solide caratteristiche. La robustezza è richiesta specificamente per la controllabilità del CRCPS. Come un sistema non lineare, le proprietà di controllabilità e osservabilità possono compromettere il guadagno dell'attaccante e la perdita del difensore del sistema.

Il framework di sicurezza ha evidenziato gli hotspot di rischio e il tipo di attacchi possibili. Può anche portare alla quantificazione delle metriche di rischio derivante dall'estensione scalabile dell'attacco. Abbiamo ridotto il numero di proprietà informatiche e identificato l'autenticazione, la disponibilità e la riservatezza come importanti per CRCPS. Abbiamo discusso le vulnerabilità informatiche in CRCPS e dimostrato l'impatto degli attacchi informatici su diversi elementi di un circuito di controllo. Gli elementi che possono essere influenzati includono misurazioni del sensore, segnali dell'attuatore, controller e segnali di riferimento. Abbiamo menzionato il controllo intelligente dei parametri fisici; ad es. attacchi di canali laterali nella crittografia, per identificare se il sistema è sotto attacco. Tuttavia, la strategia non può differenziare il sistema in stato di attacco dagli effetti dell'invecchiamento su un sistema. Per preservare la riservatezza all'interno di un CRCPS, l'utilizzo di un bus di dati crittografato è considerato utile, in quanto l'attaccante legge i dati senza una chiave di decrittografia. Ciò può fornire in particolare un vantaggio per la sicurezza del sistema in caso di accesso fisico a una porta dati. Inoltre, è stato visto che controllare il QoS da solo per migliorare il QoC non è sufficiente senza proteggere i nodi di comunicazione intelligenti dell'architettura complessiva. Si consiglia di utilizzare i protocolli di sicurezza IP (IPSec) o le sue versioni migliorate per migliorare ulteriormente la sicurezza di CRCPS.

In futuro, si svilupperanno linee guida di progettazione convalidate per il framework di sicurezza del complesso CPS collaborativo multigrado di libertà, con analisi dei rischi quantificabili e seguiremo un approccio solido alla progettazione del framework di sicurezza affrontando gli svantaggi del protocollo IPSec per l'implementazione di CRCPS.

7. Conclusione e lavori futuri

Un'alta integrazione di strumentazione, comunicazione e controllo nei sistemi fisici ha portato allo studio tardivo del CPS con maggiore attenzione. Una caratteristica chiave che è onnipresente in CPS è la necessità di garantire la loro sicurezza di fronte agli attacchi informatici. Abbiamo effettuato un'indagine su sistemi e metodi di controllo che sono stati proposti per la sicurezza di CPS. Abbiamo classificato questi metodi in categorie in base al tipo di difesa proposta contro gli attacchi informatici. La natura varia, incisiva e dannosa degli attuali attacchi informatici sottolinea l'enorme importanza dello studio della sicurezza CPS. Dato l'ambito dei sistemi e la metodologia di controllo per raggiungere la robustezza, l'ottimalità e l'efficienza in presenza di varie perturbazioni, non sorprende che i lavori citati corrispondano a sistemi e metodi di controllo con cui tale sicurezza in CPS può essere raggiunto. I documenti di riferimento e i metodi ivi indicati rappresentano il primo passo verso il raggiungimento della sicurezza in CPS. A differenza dei disturbi esogeni, gli attacchi informatici corrispondono a input personalizzati, specifici del sistema, dannosi e attivi che possono aumentare continuamente di complessità con l'evoluzione del sistema. Di conseguenza, è indispensabile che i meccanismi di difesa proposti continuino a far avanzare lo stato dell'arte, non solo per stare al passo con la complessità dell'attacco, almeno alcuni passi avanti. Quanto sopra indica chiaramente che resta ancora molto da fare per garantire la sicurezza CPS.

Trattandosi di un'area relativamente nuova, sono stati realizzati lavori limitati nel campo della sicurezza di CPS. Prima di sviluppare qualsiasi modello di sicurezza, c'è una reale necessità di un'adeguata analisi e capacità di anticipazione per gli avversari. Inoltre, il processo di verifica di qualsiasi modello di sicurezza proposto non deve influire sulle operazioni in tempo reale nel sistema. Pertanto, l'esecuzione dei processi di valutazione, autenticazione e controllo degli accessi dovrebbe avvenire senza interrompere l'ambiente di runtime. In questo modo è possibile identificare le opzioni di mitigazione dopo aver dedotto la valutazione del rischio.

Il supporto di trasmissione di CPS può includere diversi sensori, tipi di dati, dati generati in tempo reale, analisi di processo e varie interazioni dell'applicazione. Pertanto, è necessario garantire che il sistema sia sicuro mentre interagisce con altri sistemi. Il miglioramento della sicurezza CPS mediante meccanismi di sicurezza quali algoritmi di crittografia, protocolli di autenticazione e steganografia non affronterà tutti i rischi di sicurezza che potrebbero essere affrontati. Tali soluzioni potrebbero aiutare a proteggere

i sistemi target ad un certo punto. Tuttavia, qualsiasi soluzione dovrebbe considerare la situazione e il contesto dell'applicazione come parte della valutazione dei rischi per la sicurezza. Pertanto, il miglioramento della sicurezza dell'applicazione migliorerà la sicurezza dell'intero sistema.

Un meccanismo di sicurezza dovrebbe essere progettato per l'intero sistema piuttosto che in un singolo livello. Ciò implica lo sviluppo di una soluzione di sicurezza integrata a più livelli che si occupa di varie architetture di sicurezza e integra in modo sicuro i dati provenienti da diverse fonti. È difficile produrre un'architettura di sicurezza CPS che gestisca tutti i potenziali attacchi in un singolo modello. Pertanto, è necessario sviluppare un protocollo che gestisca i meccanismi di sicurezza sui tre livelli del CPS. Secondo gli attacchi CPS menzionati, si può concludere che gli obiettivi di sicurezza più comuni sono sensori e attuatori a livello di percezione; perdita di dati, controllo o distruzione a livello di trasmissione; divulgazione della privacy e accesso non autorizzato a livello di applicazione.

La privacy è un'altra questione importante che dovrebbe essere considerata e preservata in qualsiasi soluzione fornita. La protezione della privacy degli utenti da intercettazioni o furti può essere realizzata mediante uno schema di protezione e crittografia della privacy sensibile al contesto, mentre la prevenzione di attacchi e autenticità man-in-the-middle può essere ottenuta utilizzando il protocollo di autenticazione reciproca sensibile al contesto. L'uso del controllo degli accessi in base al contesto può impedire accessi non autorizzati. Prevenire la perdita di chiavi e fornire un meccanismo di gestione delle chiavi può essere ottenuto utilizzando una gestione delle chiavi sensibile al contesto. Infine, è possibile rilevare e bloccare le intrusioni utilizzando il rilevamento delle intrusioni consapevole del contesto. Esiste una reale necessità di sviluppare metodi alternativi oltre a un approccio basato sulla valutazione del rischio basato sui requisiti di sicurezza senza fare affidamento sui metodi di valutazione tradizionali. Un solido modello di valutazione per verificare tutte le minacce e le vulnerabilità è ancora una ricerca aperta. Il sistema si baserà su meccanismi di autenticazione e controllo degli accessi basati sul contesto per attacchi interni, algoritmi crittografici per la riservatezza e un solido modello di valutazione per attacchi di anticipazione e processi di mitigazione.

Sebbene tutti gli obiettivi di sicurezza del CPS siano importanti, l'autenticità, la convalida dell'identità richiesta, dovrebbe essere classificata come il primo obiettivo della sicurezza

su cui sono costruite le altre classi di sicurezza. Senza garantire che la parte autorizzata sia chi afferma di essere, altri obiettivi di sicurezza sarebbero inutili. Inoltre, qualsiasi tecnica crittografica utilizzata per soddisfare gli obiettivi di sicurezza dovrebbe essere leggera al fine di essere conveniente per i dispositivi con capacità limitate. Questo, a sua volta, aiuta a superare i vincoli di tali dispositivi. In definitiva, l'autenticazione è l'approccio più efficace e importante per affrontare molti rischi per la sicurezza. Un solido meccanismo di autenticazione impedirà alle entità non autorizzate di unirsi all'ambiente CPS e causare problemi di sicurezza. Anche se sono state sviluppate molte tecniche di autenticazione, sono ancora necessarie tecniche di autenticazione robuste e utilizzabili che migliorino il processo decisionale coinvolgendo informazioni contestuali.

I sistemi di protezione e controllo nelle sottostazioni diventano sempre meno isolati dal sistema ICT al fine di trarre vantaggio dalle nuove tecnologie di misurazione, ad esempio unità di misura a fasore, e rivoluzionare la capacità di monitoraggio e controllo della rete elettrica. Per facilitare le comunicazioni tra entità diverse, mentre si scambiano più informazioni a costi ridotti, vengono implementati protocolli standardizzati basati su tecnologie TCP / IP ed Ethernet. Lo svantaggio è che introducono vulnerabilità della sicurezza e sono inclini a attacchi informatici. Le intrusioni nella rete ICT della sottostazione sono state testate e la valutazione della vulnerabilità è stata eseguita utilizzando il banco di prova cyber-fisico. Le simulazioni di attacchi informatici al sistema SCADA e alla rete elettrica mostrano un grande impatto. Gli attacchi possono influire sul funzionamento sicuro di entrambi i sistemi di alimentazione e cyber. Inoltre, possono portare a blackout parziale o completo.

Ogni livello del CPS è minacciato da numerosi attacchi. Gestire ogni attacco singolarmente non aiuterà, ma caricherà o esaurirà le risorse del sistema. Molto lavoro è stato realizzato nel campo della sicurezza CPS; tuttavia, l'applicazione di metodi classici comuni, come la crittografia e la stenografia, al CPS non è sufficiente. Inoltre, tali metodi non sono stati progettati principalmente per operazioni di interazione per diverse applicazioni. Qualsiasi modello di sicurezza CPS dovrebbe includere livelli di difesa di sicurezza con le seguenti caratteristiche: penetrazione difficile; robusto meccanismo di autenticazione e controllo degli accessi; tempo di risposta elevato; potenziamento delle capacità e capacità di mitigazione degli attacchi. Tale sistema può essere implementato utilizzando un modello ibrido integrando un robusto modello di accesso gerarchico e un framework di sicurezza sensibile al contesto che coinvolge una tecnica crittografica

leggera e adottando un modello di valutazione della sicurezza immunitaria. Il modello di valutazione dovrebbe considerare che le vulnerabilità e le minacce non sono statiche e che i loro attacchi e comportamenti cambiano periodicamente.

Un altro fattore importante è che gli attacchi potrebbero non provenire solo dall'esterno del sistema ma anche dall'interno, ad esempio da dipendenti che non necessitano di ulteriori conoscenze sul sistema di destinazione. La conoscenza che gli addetti ai lavori possiede spesso dà loro accesso illimitato per rubare o modificare i dati nel sistema o per disattivare quel sistema. Accesso gerarchico alle informazioni migliorerebbe la sicurezza.

L'opzione migliore è adottare un solido modello di controllo degli accessi, che viene arricchito con informazioni contestuali che assicurano autenticità e riservatezza, oltre ad aumentare la sicurezza complessiva di CPS.

Un altro problema dovrebbe essere considerato come una delle sfide per CPS sono i dati eterogenei raccolti da diversi dispositivi, ognuno dei quali utilizza protocolli diversi che portano a problemi di compatibilità relativi al formato dei dati e ai protocolli di comunicazione. La sfida principale in CPS è la progettazione di protocolli che possono funzionare su diversi dispositivi e situazioni. Così, è necessario uno standard di codifica unificato per i protocolli di scambio di informazioni per ciascun dispositivo, come RFID e WSN, che hanno diversi formati di accesso alle informazioni, meccanismi di controllo della sicurezza e formati di archiviazione, ognuno dei quali porta a approcci di elaborazione dei dati diversi. Uno standard unificato di elaborazione dei dati aiuterà a ridurre i costi di trasmissione utilizzando tecniche di compressione e fusione dei dati. Inoltre, il cloud computing può fornire l'archiviazione dei dati richiesta con costi e prestazioni convenienti. Questi vantaggi possono essere sfruttati da CPS collegando un gran numero di dispositivi con capacità limitate. In questo caso, i processi di calcolo possono essere eseguiti in modo efficiente a livello di cloud computing.

Un altro importante problema di sicurezza che non è ancora stato completamente risolto quando si applicano soluzioni di sicurezza è quello del supporto di nodi appena aggiunti. Questo può essere superato migliorando qualsiasi tecnica di sicurezza utilizzata con informazioni contestuali.

Di seguito, prestiamo maggiore attenzione ai limiti di alcuni risultati esistenti e proponiamo diverse problematiche impegnative su questo argomento, che fa luce approfondita su ulteriori ricerche.

1. Modellistica e metodologie del sistema:

- Diversi strumenti esistenti basati su modelli di sistema sono lungi dal soddisfare i requisiti di progettazione CPS. I comportamenti informatici e decisionali combinati con le comunicazioni e le dinamiche fisiche dovrebbero essere ulteriormente astratti e modellati a diversi livelli.
- Nel quadro della teoria del controllo, l'attuale approccio all'analisi con gli obiettivi degli attacchi di mitigazione non può gestire completamente la complessa dinamica del sistema, per non parlare del caso in cui esistono comportamenti di nodo variabili nel tempo, tipologie che variano nel tempo o non linearità.
- Si noti che la sicurezza di solito è un vincolo difficile. Per la natura stocastica dei CPS, le metodologie in senso medio-quadrato espongono un notevole conservatorismo e come creare uno schema efficace in senso quasi sicuro è ancora impegnativo.

2. Rilevamento e compensazione dell'attacco:

- I CPS possono essere soggetti a più attacchi contemporaneamente. Una strategia adattiva che compensa diversi tipi di attacchi non ha ancora ricevuto adeguata attenzione per i CPS industriali e l'impatto sulle prestazioni del sistema dovrebbe essere approfonditamente discusso.
- Una grande perturbazione sugli stati del sistema potrebbe essere causata da dati falsi iniettati, mentre un tasso di rilevamento potrebbe soffrire di un leggero aumento, e quindi la sensibilità e l'affidabilità del rilevamento dell'attacco dovrebbero essere ulteriormente studiate.
- La complessità del sistema è inevitabilmente aumentata quando si prendono contemporaneamente in considerazione protocolli di comunicazione, fenomeni indotti dalla rete e attacchi informatici. Le condizioni di applicazione di schemi e tecnologie di rilevamento tipici potrebbero non essere garantite. Quindi, sviluppare alcuni nuovi approcci di rilevazione e strategie di compensazione per superare le problematiche sopra menzionate è significativo.

3. Le prestazioni del sistema e la qualità del servizio:

- Non è banale fondere il rilevamento degli attacchi e il controllo della resilienza in un quadro uniforme. La corretta attuazione di tale idea può portare a significativi miglioramenti delle prestazioni di sicurezza dei CPS.
- Nell'ingegneria pratica, i requisiti di sicurezza e i vincoli di risorse (larghezza di banda di comunicazione, energia limitata, ecc.) di solito devono essere presi in considerazione contemporaneamente. È importante come co-progettare i parametri di sistema dei CPS considerando sia la sicurezza che la qualità del servizio.
- La fusione di sistemi fisici e sistemi informatici dà luogo a requisiti di prestazioni più elevati, come robustezza, stabilità, sicurezza e affidabilità. Pertanto, può portare a un argomento particolarmente interessante sull'ottimizzazione multi-obiettivo per soddisfare i requisiti dei CPS del mondo reale.

SITOGRAFIA

Alexandru Stefanov, Chen-Ching Liu. (2014). *Cyber-Physical System Security and Impact Analysis.* (IFAC Proceedings Volumes, Volume 47, Issue 3, Pages 11238-11243). https://www.sciencedirect.com/science/article/pii/S1474667016434026

Azfar Khalid, Pierre Kirisci, Zeashan Hameed Khan, Zied Ghrairi, Jürgen Pannek. (7 May 2018). *Security framework for industrial collaborative robotic cyber-physical systems.* (Computers in Industry, Volume 9, Pages 132-145). https://www.sciencedirect.com/science/article/pii/S016636151730088X

Derui Ding, Qing-Long Han, Yang Xiang, Xiaohua Ge, Xian-Ming Zhang, (31 January 2018). *A survey on security control and attack detection for industrial cyber-physical systems*. (Neurocomputing, Volume 275, Pages 1674-1683), https://www.sciencedirect.com/science/article/pii/S0925231217316351

Ivo Friedberg, Kieran McLaughlin, Paul Smith, David Laverty, Sakir Sezer. (June 2017). *STPA-SafeSec: Safety and security analysis for cyber-physical systems.* (Journal of Information Security and Applications, Volume 34, Part 2, Pages 183-196). https://www.sciencedirect.com/science/article/pii/S2214212616300850

Jens Amberg, amministratore delegato di halstrup-walcher GmbH. *Industria 4.0 e sistemi cyber-fisici – Collocazione ed esempio*. https://www.halstrup-walcher.de/halstrup-walcher-wAssets/docs/pressemeldungen/IT/2015_Fachartikel_Industria-4.0-Cambio-di-formato_IT.pdf

Jihong Yan, Mingyang Zhang, Zimin Fu, (2019). "An intralogistics-oriented Cyber-Physical System for workshop in the context of Industry 4.0", *(Procedia Manufacturing,*

Volume 35, Pages 1178-1183), https://www.sciencedirect.com/science/article/pii/S2351978919308005

Juxia Xiong, Jinzhao Wu. (1 April 2020). *Construction of information network vulnerability threat assessment model for CPS risk assessment*. (Computer Communications, Volume 155, Pages 197-204), https://www.sciencedirect.com/science/article/pii/S0140366420301547

Key4 Industry. *Al centro dell'Industry 4.0: i Cyber Physical System*. http://www.key-4.com/al-centro-dellindustry-4-0-i-cyber-physical-system/

Phu H. Nguyen, Shaukat Ali, Tao Yue. (3 March 2017). *Model-based security engineering for cyber-physical systems: A systematic mapping study.* (Information and Software Technology, Volume 8, Pages 116-135). https://www.sciencedirect.com/science/article/pii/S0950584916303214

Rasim Alguliyev, Yadigar Imamverdiyev, Lyudmila Sukhostat. (September 2018). *Cyber-physical systems and their security issues*. (Computers in Industry, Volume 100, Pages 212-223). https://www.sciencedirect.com/science/article/pii/S0166361517304244

Seyed Mehran Dibaji, Mohammad Pirani, David Bezalel Flamholz, Anuradha M. Annaswamy, Aranya Chakrabortty, (2019). *A systems and control perspective of CPS security.* (Annual Reviews in Control, Volume 47, Pages 394-411), https://www.sciencedirect.com/science/article/pii/S1367578819300185

Yosef Ashibani, Qusay H. Mahmoud. (8 July 2017). *Cyber physical systems security: Analysis, challenges and solutions.* (Computers & Security, Volume 6, Pages 81-97). https://www.sciencedirect.com/science/article/pii/S0167404817300809

Yuriy Zacchia Lun, Alessandro D'Innocenzo, Francesco Smarra, Ivano Malavolta, Maria Domenica Di Benedetto. (9 March 2019). *State of the art of cyber-physical systems security: An automatic control perspective.* (Journal of Systems and Software, Volume 14, Pages 174-216). https://www.sciencedirect.com/science/article/pii/S0164121218302681