Politecnico di Torino

Corso di Ingegneria Chimica e dei processi sostenibili
A.a. 2023/2024
Sessione di Laurea Marzo 2024

Sicurezza Informatica e Gestione del Rischio negli Impianti Chimici

Un'integrazione di HAZOP e FTA

Relatore:
prof.ssa Demichela Micaela

Candidato:
Di Carlo Alessandro

INDICE

1. Introduzione

Sono sempre più numerose le notizie riguardanti cyberattacchi diffusi sulla rete italiana ed internazionale. Tali attacchi spesso non si limitano ad una minaccia alla sicurezza quotidiana della/e vittima/e, poiché frequentemente sono motivati da ragioni politiche ed economiche. Numerose sono le violazioni informatiche che vedono come protagonisti gruppi di abili hacker con il solo scopo di carpire informazioni riservate dalle loro vittime. È bene ricordare che la riservatezza dei dati più sensibili, nonché la loro integrità, deve essere sempre garantita con le migliori misure di sicurezza a disposizione: autenticazioni multiple, password, PIN ecc.

La sicurezza informatica nell'industria di processo è stata identificata fin dai primi anni '60, quando i sistemi designati per il controllo dei processi, la supervisione e l'acquisizione dei dati (ad esempio i sistemi SCADA) erano ancora basati sulla tecnologia informatica mainframe.

Dato il continuo sviluppo tecnologico, anche le aziende hanno potuto apportare notevoli miglioramenti alle loro sedi, in termini di produttività, qualità del servizio o del prodotto offerto e di sicurezza. Tuttavia, la sempre più fitta interconnessione tra tecnologie ed apparecchiature ha reso anche più vulnerabili queste ultime, soprattutto dal punto di vista "cyberattacchi". Prendendo spunto dal sito di Microsoft (consultato in data 10/11/2023): "Un cyberattacco è un tentativo di ottenere l'accesso non autorizzato ai sistemi informatici al fine di appropriarsi, modificare o distruggere dati." Si può già intuire quali potrebbero essere le conseguenze di un tale atto all'interno di un sito dove siano presenti sostanze pericolose per la salute, apparecchiature operanti ad alti livelli di pressione o di temperatura o condotti di trasporto di materie prime e prodotti delicati, come ad esempio i siti Seveso. Non a caso, i siti di produzione concernenti l'ingegneria chimica sono stati frequentemente oggetto di cyberattacchi interni e/o esterni. A volte si è trattato di azioni mosse dal rancore di ex dipendenti, altre volte l'intrusione è arrivata da abili "pirati" dell'hacking al di fuori dell'impianto. A tal proposito, si rimanda all'articolo "Analysis of Cybersecurity-related Incidents in the Process Industry" redatto da Matteo Iaiani et al. nel quale è presente un vasto database cronologico dei cyberattacchi suddetti.

Le prime politiche e legislazioni volte a migliorare la preparazione contro gli attacchi alla sicurezza nei confronti degli impianti chimici e di processo sono state sviluppate due decenni fa, soprattutto negli Stati Uniti dopo gli attacchi terroristici dell'11 settembre 2001. In Europa, il settore specifico della cybersicurezza è stato recentemente oggetto della direttiva sulla sicurezza delle reti e dell'informazione (direttiva NIS UE 2016/1148), che ha richiesto lo sviluppo di conoscenze e competenza in tale ambito, oltre ad una maggiore cooperazione a livello dell'UE nella protezione dei servizi essenziali e dei servizi digitali. Tra i servizi essenziali del settore energetico rientrano la produzione, la raffinazione e il trattamento, lo stoccaggio e il trasporto di gas e petrolio nei condotti adibiti.

Secondo quanto riportato in "Analysis of Cybersecurity-related Incidents in the Process Industry" (Iaiani et al., 2021), la sicurezza dei sistemi IT è stata affrontata dalla serie di standard ISO/IEC 27000 sulla gestione della sicurezza delle informazioni. In particolare, lo standard ISO/IEC 27005 è progettato per assistere l'implementazione della sicurezza delle informazioni sulla base di un approccio di gestione del rischio. Questo segue un ciclo tipico che comprende la valutazione del rischio, il trattamento del rischio e il monitoraggio.

D'altro canto, la sicurezza dei sistemi OT è stata affrontata dallo standard ISA/IEC 62443, che fornisce un quadro flessibile per affrontare e mitigare le vulnerabilità di sicurezza attuali e future nei sistemi di automazione e controllo industriale (IACS). In particolare, la parte 3-2 di ISA/IEC 62443 guida le organizzazioni attraverso il processo di valutazione del rischio delle IACS e l'identificazione e l'applicazione di adeguate contromisure di sicurezza, riducendo il rischio a livelli tollerabili.

Per quanto concerne questa tesi, un primo passo è stato, anche in questo caso, l'analisi della cronologia di eventi incidentali industriali correlati ai cyberattacchi. Come database di riferimento è stato utilizzato ARIA, che fra tutti risulta essere quello più arricchito quantomeno dal punto di vista del numero di scenari riportati nel corso degli anni. Tuttavia, non per tutti gli incidenti la relativa documentazione disponibile è altrettanto approfondita. È stato inoltre aggiunto anche un paragrafo dedicato al caso Colonial Pipeline.

La speranza è di mettere in evidenza, a seguito di queste argomentazioni, come il personale addetto ai lavori nei siti di produzione, specialmente quelli in cui vengono trattati materie prime e/o prodotti

pericolosi, debba essere cosciente delle vulnerabilità, dei rischi e delle conseguenze di attacchi informatici, a prescindere dalla tecnica con cui questi avvengano (phishing, blackmailing, virus trojan etc.). L'idea di questo studio è quella di fornire, a seguito di un'identificazione e valutazione dei rischi e delle conseguenze annesse, una sorta di vademecum per gli operatori per "prevenire o curare" un caso di cyberattacco.
L'analisi degli eventi passati, sebbene importante per individuare la credibilità di scenari potenziali, talvolta si potrebbe rilevare non completamente adatta per la valutazione di scenari attesi originati in impianti specifici, in quanto il basso numero di eventi registrati non consente di correlarli con tutti i fattori rilevanti che descrivono situazioni reali (ad esempio, progettazione del sistema, materiali e condizioni operative, interdipendenze nel sistema fisico e cibernetico). Per l'identificazione di vari rischi per la sicurezza dei processi, la sicurezza fisica e la sicurezza informatica in modo integrato, gli approcci strutturati, come l'analisi dei rischi e dell'operabilità (HAZOP), possono essere utilizzati come riferimento. Oltre che ai tradizionali membri del team di base per l'attuazione della HAZOP, sarebbe opportuna l'inclusione di un esperto di sicurezza fisica e informatica che intervenga durante il "brainstorming", per garantire che i contributi relativi alla sicurezza siano integrati nella stessa analisi HAZOP. Tuttavia, la tecnica HAZOP è prevalentemente qualitativa e mira a stimolare l'immaginazione dei partecipanti per identificare potenziali pericoli e problemi di operatività, mentre l'inclusione degli aspetti di sicurezza non è supportata dalle parole guida comunemente utilizzate. La principale critica all'uso diretto dell'HAZOP può derivare dalla prassi della sua applicazione, che tendenzialmente non tiene conto di cause o fonti di rischio esterne e non casuali, a meno che non venga integrata con delle checklist specifiche per questi rischi.
Ad oggi, dalla ricerca scientifica e dalle pubblicazioni disponibili, il lavoro è stato progressivamente sviluppato nell'ambito dell'identificazione del rischio, associando le varie tecniche di analisi già presenti con i cyberattacchi oppure creandone nuove ad hoc, come la metodologia PHAROS (Iaiani, Tugnoli et al.). Quando si valutano nuove tecnologie da adottare o si introducono modifiche al controllo dei processi in generale, bisognerebbe essere consapevoli del fatto che le modifiche proposte debbano essere progettate in modo tale da non introdurre o aumentare il rischio di attacchi informatici, in particolare per applicazioni critiche e ad alto rischio.

Tabella 1.1: Esempio di integrazione del metodo HAZOP con LOPA (Fonte: "Integrating cybersecurity in hazard and risk analysis", Addie Cormier, Christopher Ng, Journal of Loss, Prevention in the Process Industries, 2020 DOI 104044)

Initiating Event	IEF	PFD for PSV	PFD for BPCS	Likelihood (Years between occurrence)	Risk Level (Per severity of 100)
Pump Failure	0.1	1%	10%	10,000	A
Cyber-attack	0.02	1%	100%	5000	B

A proposito dell'interconnessione tra sistemi IT ed OT, essa viene definita come Cyber Physical System. I Cyber Physical Systems (CPS) sono designati come i componenti essenziali dell'Industrial Internet of Things (IIoT) e dovrebbero svolgere un ruolo chiave nell'Industria 4.0. I CPS consentono alle applicazioni e ai servizi intelligenti di funzionare in modo accurato e in tempo reale. Inoltre, essi sono in grado di rilevare l'ambiente circostante, con la capacità di adattarsi e monitorare l'ambiente stesso.
Si basano, per l'appunto, sull'integrazione di sistemi cyber e sistemi fisici, che scambiano vari tipi di dati e informazioni sensibili in tempo reale. In parole semplici, si tratta di una rete di sistemi integrati che interagiscono con gli input e gli output fisici. Lo sviluppo dei CPS è portato avanti sia dai ricercatori che dai produttori. Tali sistemi comprendono tre componenti centrali principali: sensori, aggregatori e attuatori.
Nonostante i loro numerosi vantaggi, i sistemi CPS sono vulnerabili a varie minacce e attacchi per minare la loro sicurezza informatica e/o fisica. Ciò è dovuto, ancora una volta, alla loro natura eterogenea, alla loro dipendenza da dati privati e sensibili e alla loro distribuzione su larga scala. Pertanto, l'esposizione intenzionale o accidentale di questi sistemi può provocare effetti catastrofici. Ecco perché anche qui è fondamentale mettere in atto solide misure di sicurezza.

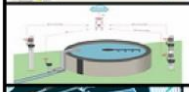
Naming	Classification	Description
 Smart House	Industrial-Consumer IoT	• Control Smart Devices • Homeowner Security & Comfort
 Oil Refinery	Industrial-Transportation IoT	• Naphta, Gasoline, Diesel • Asphalt, Petroleum, Fuel, Oil
 Smart Grid	Industrial IoT	• Smart Efficient Energy • Energy Control & Management
 Water Treatment	Industrial-Consumer IoT	• Improved Water Quality • Overcome Contamination & Undesirable Components
 Medical Devices	Medical-Wearable IoT	• Improved Patients Life • Enhanced Medical Treatment • Remote Patient Monitoring
 SCADA	Industrial IoT	• Control & Monitor Telecoms. • Control & Monitor Industries
 Smart Cars	Industrial-Transportation IoT	• Echo Friendly • Enhanced Driver Experience • Advanced Safety Features
 Supply Chains	Industrial-Transportation IoT	• Real-Time Delivery Source/Destination • Less Delays & Echo Friendly

Figura 1.1a: descrizione e classificazione dei CPS (Fonte: Cyber-physical systems security: Limitations, issues and future trends, Jean-Paul A. Yaacoub et al., 2020)

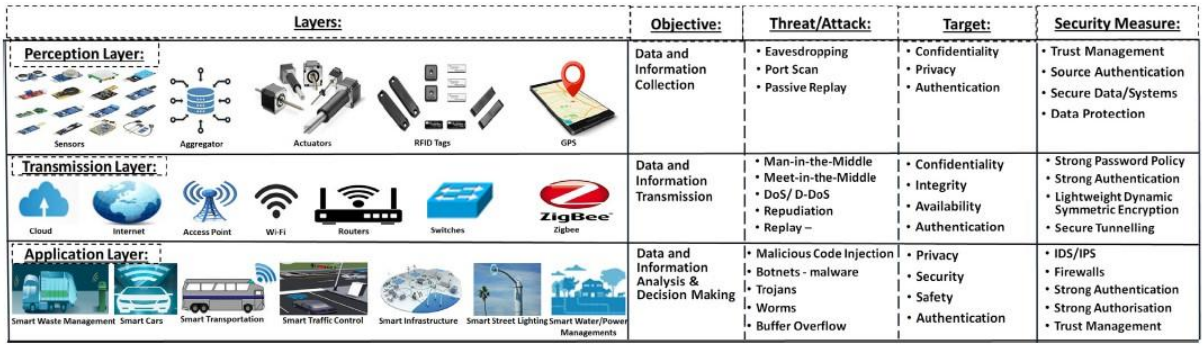


Figura 1.1b : CPS layers (Fonte: Cyber-physical systems security: Limitations, issues and future trends, Jean-Paul A. Yaacoub et al., 2020)

1.1. Cenni su: “I linguaggi memory-safe”

Si riporta qui quanto descritto nell’articolo a cura di Valerio Porcu, Senior Editor di Tom’s Hardware.
“*La Casa Bianca, attraverso l'Ufficio del Direttore Nazionale per la Sicurezza Informatica (ONCD), ha consigliato agli sviluppatori di utilizzare linguaggi di programmazione "memory-safe", escludendo C e C++ dalla lista. Questa mossa fa parte della strategia di cybersecurity del presidente Biden e mira a garantire la sicurezza delle fondamenta del cyberspazio e di ciò che ne concerne.*
Sicuramente risulta una sorpresa vedere il governo statunitense dare consigli ai programmatori, per di più mettendo alla gogna due tra i linguaggi più usati al mondo. Sono infatti al nono e al decimo posto della classifica elaborata da Statista e presumibilmente la posizione reale è anche più alta visto che questa lista include HTML come linguaggio di programmazione, quando invece è un linguaggio di MarkUp.
I linguaggi di programmazione "memory-safe", a cui fa riferimento il governo guidato da Joe Biden, offrono una protezione dai bug e dalle vulnerabilità legata all'accesso alla memoria, contrastando problemi come i buffer overflow e i dangling pointers. Java è considerato un linguaggio "memory-safe" grazie ai suoi controlli di rilevamento degli errori durante l'esecuzione, ma C e C++ permettono entrambi puntatori arbitrari con indirizzi di memoria diretti e nessuna verifica dei limiti.
Il report evidenzia che circa il 70% delle vulnerabilità di sicurezza segnalate dagli ingegneri specializzati in cybersecurity di Microsoft nel 2019 e da Google nel 2020 sono state causate da problemi di sicurezza della memoria. Questo ha portato a identificare C e C++ come linguaggi non sicuri in quanto non hanno meccanismi per prevenire quel tipo di problema.
L'obiettivo del rapporto è trasferire la responsabilità della cybersecurity non solo a individui e piccole imprese, ma anche a organizzazioni più grandi, aziende tecnologiche e infine al governo. In altre parole, anche chi crea i linguaggi di programmazione dovrebbe fare la sua parte. Se questa dottrina dovesse evolversi, potremmo presto assistere a veri e propri divieti su questo o quel linguaggio.”

È importante tenere conto l’utilizzo di linguaggi “memory safe” previene dunque la possibilità che le parti di codice eventualmente non necessarie possano essere eliminate per evitare che, in maniera forzata, possano essere violate ed usate per eseguire codici malevoli. Soprattutto il linguaggio C, avendo oggi molti anni sulle spalle, è da tenere sotto controllo, in particolare l’uso delle stringhe di testo. Il linguaggio C è ancora molto diffuso, date le sue veloci prestazioni e la sua perfetta possibilità di simbiosi con i sistemi operativi Linux, ma ora sono disponibili linguaggi altrettanto performanti e più sicuri come Rust.

2. Cronologia scenari incidentali

Come già accennato all'interno del paragrafo introduttivo, nell'articolo "Analysis of Cybersecurity-related Incidents in the Process Industry" di Matteo Iaiani et al. è presente un ricco database contente i vari scenari incidentali correlati a differenti tipi di cyberattacchi. Citando le loro parole: "Un attacco informatico, oltre a danni economici e reputazionali, può potenzialmente innescare eventi gravi (ad esempio rilasci di materiali pericolosi, incendi, esplosioni) con gravi conseguenze sui lavoratori, sulla popolazione e sull'ambiente.
Dovrebbero essere presi in considerazione gli aggressori con motivazioni diverse: terroristi (motivati da guadagno politico/monetario, vendetta o distruzione), attivisti (motivati da ribellione o guadagno politico), dipendenti o appaltatori scontenti (motivati da ego, vendetta o curiosità) e criminali (motivati da sfida, status o denaro). Nel caso dell'industria di processo e dell'Oil&Gas, gli aggressori possono essere particolarmente attratti dallo specifico profilo aziendale (multinazionali, aziende con una posizione di leadership in uno specifico sottosettore, possibilità di accedere a informazioni proprietarie, ecc.) o dall'ubicazione socio-politica dell'impianto bersaglio".
Lo studio di Iaiani et al. si basa sullo sviluppo e la compilazione di un database di incidenti in rapporto alla sicurezza informatica (CSI) del passato, per comprendere come questi abbiano interessato strutture appartenenti all'industria di processo e a settori industriali simili. Viene poi applicata la metodologia PHAROS per rilevare tutte le combinazioni di ciò che è ritenuto come "manipolabile" per scatenare le conseguenze incidentali riportate (la descrizione della metodologia PHAROS è disponibile in un paragrafo successivo).
Un incidente relativo alla sicurezza informatica (CSI) è inteso come un evento consistente in un accesso non autorizzato al sistema IT-OT di una struttura, che può o meno aver avuto un impatto sulle sue risorse.
La scelta degli incidenti da includere nella banca dati è stata basata su due criteri:

- l'incidente deve avere origine da un'infezione intenzionale o accidentale del sistema IT-OT;
- l'incidente coinvolge un impianto appartenente ad uno dei seguenti settori industriali: chimico, petrolchimico, produzione di energia, trattamento acque/acque reflue.

I dati sono stati raccolti da diverse fonti: letteratura scientifica, web, banche dati open-source su incidenti/inconvenienti industriali ecc. Tuttavia, gli scenari incidentali inseriti nel database definitivo provengono essenzialmente da:

1. Banca dati ARIA (Analisi, Ricerca e Informazione sugli Infortuni)
2. Banca dati RISI (Repository of Industrial Security Incidents)
3. Altre fonti di letteratura aperta come articoli scientifici o ulteriori banche dati, rapporti sulla sicurezza e pagine web

Il database RISI raccoglie gli incidenti relativi alla sicurezza informatica che hanno interessato o hanno avuto il potenziale per influenzare i sistemi di controllo dei processi, i sistemi di automazione industriale o i sistemi SCADA, con l'obiettivo di aumentare la consapevolezza della sicurezza informatica tra i diretti interessati. Sfortunatamente, la caratterizzazione dell'attacco è povera nelle informazioni fornite, concentrandosi principalmente sugli impatti degli eventi e sulle azioni correttive intraprese dalle strutture colpite, con mancanza di dettagli sui modelli di attacco. Il database copre un arco di tempo che va dal 1982 al 2015.
Il database ARIA raccoglie gli eventi (originati principalmente da guasti accidentali ed errori umani) che hanno danneggiato o mostrato un potenziale danno alla salute o alla sicurezza pubblica e all'ambiente. Pertanto, viene registrato solo un numero limitato di incidenti legati alla cybersicurezza, ovvero quelli con gravi impatti. La maggior parte dei record presenti nel database ARIA è caratterizzata da una descrizione a testo libero con informazioni generali sulle cause e sugli esiti finali subiti dalle strutture. Il database copre un arco di tempo che va dal 1866 fino agli ultimi anni recentemente trascorsi.
Dalla figura 2.1, tratta dall'articolo stesso, si evidenzia dai grafici quale sia la distribuzione nel tempo e nello spazio degli scenari incidentali presenti nella banca dati. Si notino in particolare gli alti valori di

incidenti accaduto nel settore petrolchimico e quello relativo agli incidenti accaduti in America durante i primi anni del nuovo millennio.

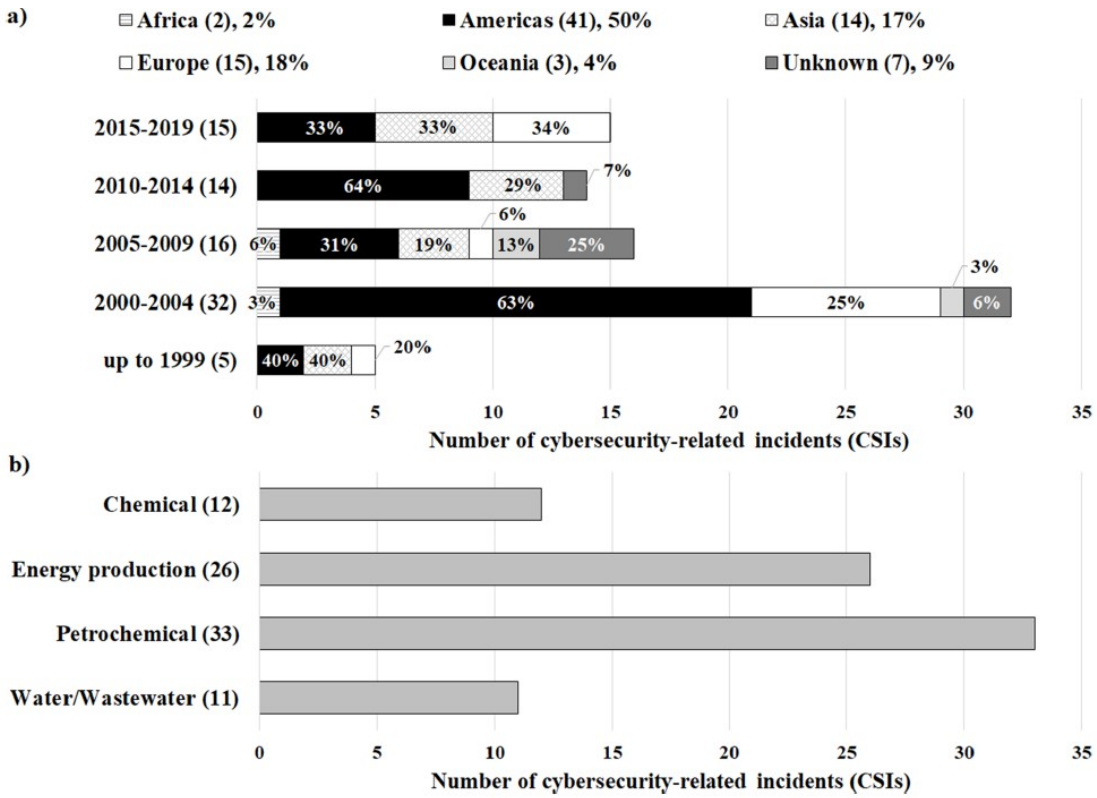


Figura 2.1 a) andamento temporale e distribuzione geografica (%) dei CSI registrati nella banca dati; b) distribuzione (%) tra i settori industriali dei CSI registrati. I numeri tra parentesi si riferiscono al numero di CSI. (Fonte: "Analysis of Cybersecurity-related Incidents in the Process Industry", Matteo Iaiani et al. 2021)

Nel database sono stati inclusi un totale di 82 incidenti legati alla sicurezza informatica con un arco di tempo di 37 anni (dal 1982 al 2019). Uno dei problemi principali nella stesura della banca dati è stata la disponibilità di dettagli rilevanti sulle voci CSI, principalmente a causa della mancanza di informazioni specifiche dedicate alla sicurezza nelle fonti.
La banca dati è stata analizzata al fine di ottenere dati statistici e lezioni apprese in merito agli attacchi informatici che hanno coinvolto una struttura appartenente all'industria di processo e alle attività correlate. I dati sono stati estrapolati per mezzo del conteggio dei CSI sulla base delle informazioni disponibili in ciascun campo del database. I risultati sono stati tracciati separatamente o incrociando diversi aspetti. Sempre stando a quanto riportato nell'articolo, sono stati esaminati i seguenti aspetti:

1. andamento temporale: il conteggio dei CSI è stato basato su un periodo di 5 anni;
2. collocazione geografica: il conteggio dei CSI è stato effettuato in base ai continenti;
3. settori industriali: il conteggio dei CSI è stato effettuato in base al campo dettagliato "Settore industriale";
4. tipo di aggressore: il conteggio dei CSI si basava sul campo dettagliato "Tipo di attaccante";
5. sistema infetto: il conteggio dei CSI si basava sul campo dettagliato "System Infected";
6. impatto: il conteggio dei CSI si basava sui campi dettagliati "Impatto principale" e "Impatto secondario".

Questa analisi è stata applicata a tutti i dati raccolti nel database, nonostante sia indicato che una frazione di dati inferiore all'8% risulta come “dati non classificabili o sconosciuti” per ciascun aspetto indagato. Poiché l'analisi si è basata su un numero non elevato di CSI registrati, occorre prestare attenzione ad attribuire un valore statistico rigoroso ai risultati. Si riporta di seguito come è stato strutturato il database. Per ogni voce, sono stati compilati campi di testo libero e campi dettagliati. I campi dettagliati vengono utilizzati per introdurre una classificazione univoca degli scenari. Il primo campo dettagliato è "Settore industriale" che classifica i CSI in base al settore industriale di appartenenza dell'impianto interessato: settore chimico, settore petrolchimico, settore della produzione di energia, settore del trattamento delle acque e delle acque reflue. Il campo dettagliato "Tipo di aggressore" categorizza i CSI nelle classi "intenzionale-interno", "intenzionale-esterno" e "accidentale", in base al tipo di attacco informatico a cui si riferiscono. In particolare, gli attacchi informatici intenzionali sono quelli effettuati con l'intento di generare impatti su obiettivi specifici, sfruttando specifiche debolezze del sistema bersaglio. Al contrario, gli attacchi informatici accidentali non sono specifici per un sistema bersaglio, ma possono mirare un qualsiasi punto vulnerabile. Nel caso di un attacco informatico intenzionale, il CSI è ulteriormente classificato come "interno" se è stato eseguito da un insider, cioè un individuo che normalmente ha autorizzato l'accesso alle risorse di una struttura e come "esterno" in caso contrario. In caso di attacchi informatici accidentali, non viene introdotta alcuna ulteriore etichettatura, poiché considerati solo quelli originati da cause esterne. Gli addetti ai lavori, come i dipendenti poco formati o negligenti che accidentalmente influenzano il sistema di rete della propria azienda, non sono quasi mai i veri autori dell'attacco, ma solo mezzi inconsci della sua propagazione.
Per quello che concerne il campo dettagliato "System Infected", esso divide i CSI in due classi: quelli caratterizzati solo dall'infezione del sistema IT e quelli caratterizzati dall'infezione del sistema OT. Le infezioni dei sistemi OT possono essere sia in concomitanza che a sé stanti rispetto all'infezione del sistema IT. A causa del basso livello di dettaglio nella descrizione disponibile di alcuni CSI, è stato difficile adottare una classificazione più precisa del sistema interessato (ad esempio in base al livello Computer Integrated Manufacturing interessato) applicabile a tutte le voci della banca dati. Pertanto, i dati sono stati classificati in forma aggregata: sistema OT (i.e. livelli CIM 0, 1 e 2) e sistema IT (i.e. livelli CIM 3 e 4). In caso di disponibilità di informazioni più precise sui sottosistemi interessati, queste sono state registrate nell'ambito del campo di testo libero "Descrizione degli impatti".
L’ultimo campo dettagliato è quello riguardante l’"Impatto" e classifica i CSI in base agli esiti che seguono un attacco informatico alla rete IT-OT di una struttura di processo. Gli impatti sono stati diversificati in 6 classi: il verificarsi di un evento importante (IC-01), la perdita economica (IC-02), il verificarsi di un arresto locale (LSD) o di un arresto del processo (PSD) (IC-03), l'infezione del sistema OT (IC-04), la perdita o il danneggiamento dei dati (IC-05) e l'infezione del sistema IT (IC-06). Ogni classe di impatto è stata definita adattando all’analisi di Iaiani et al. le classificazioni proposte da Casson et al. e quelle riportate nelle norme ISO/IEC 27005 e ISA/IEC 62443. Il campo dettagliato "Impatto principale" riporta la conseguenza più grave registrata per il CSI. Qualsiasi altro impatto disponibile nella descrizione è classificato nel campo dettagliato "Impatto secondario".
Di seguito, vengono riassunte le conclusioni ottenute dalle analisi della banca dati:

1. Mentre le voci del database coprono un periodo di 37 anni, solo 5 incidenti si sono verificati prima del 1999
2. L'andamento temporale mostra un picco di CSI nel quinquennio 2000-2004 (32 CSI registrati), dovuto principalmente alla diffusione di vermi molto infettivi
3. Negli ultimi quindici anni, come si evince dalla figura, l'andamento temporale dei CSI è costante
4. Nell'ultimo periodo, le aziende hanno implementato sempre più processi di gestione dei rischi di sicurezza dei propri sistemi IT-OT
5. La maggior parte degli incidenti segnalati si è verificata in Nord America (41 CSI registrati, 50% del totale), seguito dall'Europa (15 CSI registrati, 18% del totale) e dall'Asia (14 CSI registrati, 17% del totale).

Per quanto concerne invece questa tesi, il database di riferimento per l'analisi degli scenari incidentali è stato solo ARIA il quale è stato consultato un'ultima volta, ai fini di integrazione con le analisi riportate in questo documento, in data 7/10/2023. Sostanzialmente, oltre ai criteri applicati nello studio di Iaiani et al. , per decidere quali scenari incidentali inserire all'interno di questa tesi è stata anche valutata la disponibilità di dati, augurandosi di trovare maggiori informazioni rispetto all'ultima volta in cui gli autori precedentemente citati hanno consultato il sito Internet.
Se si desiderano maggiori informazioni sugli scenari incidentali rispetto a quelle presenti in questo documento, in un'appendice di supporto è stato riportato il codice identificativo, il luogo (se indicato nel database), la data, il settore lavorativo coinvolto e le conseguenze riportate in termini di produttività, di risorse umane, di danno ambientale ed economico. Qui per ogni incidente verranno considerati solamente i dati in quelli che sono i precedentemente citati "campi dettagliati".
Gli incidenti scelti ed inseriti nella banca dati di questa tesi coprono l'arco temporale che comprende gli ultimi 40 anni trascorsi, nel quale ovviamente il numero di attacchi è incrementato per i motivi già discussi. Per la categorizzazione dei CSI inseriti nel database, è stata adottata l'etichettatura dello studio di Iaiani et al., anche al fine di rendere più semplice il confronto fra le due analisi. Le ricerche sono state effettuate definendo una serie di parole chiave specifiche nel motore di ricerca del database ARIA: "cybersecurity", "Industrial plants", "Chemical Plants", "Industrial Safety", correlate tipicamente fra loro con la parola chiave AND.
Il primo fatto che risulta praticamente in comune fra quasi tutti gli incidenti scelti è la distrazione o la disattenzione, volente o nolente che sia. Si tratta infatti di atteggiamenti che hanno portato a fronteggiarsi con situazioni dove qualcuno avrebbe dovuto prevenire ma non ha preso le adeguate precauzioni o contromisure.
Si prenda per esempio quello che si ritiene uno tra i maggiori incidenti inseriti nella banca dati, così etichettato sul sito Internet di ARIA:

N° 5989 - 01/12/1994 - FRANCE - 60 - RIBECOURT-DRESLINCOURT
C20.15 - Manufacture of fertilizers and nitrogen compounds

Durante la manutenzione prestabilita dei condotti dell'impianto, lo svuotamento parziale dei tubi dell'ammoniaca e un errore di programmazione nel robot ausiliario hanno causato l'apertura della valvola automatica al momento del ripristino. Ciò ha provocato l'incidente a seguito di operazioni non coordinate eseguite contemporaneamente da due squadre di manutenzione separate. Tralasciando ulteriori dettagli, basti sapere che l'errore di programmazione del robot di manutenzione era stato generato partendo da un cyberattacco che ha sfruttato una falla nei suoi sistemi di sicurezza/ autenticazione. Una disattenzione banale che ha provocato un morto e due feriti di cui uno grave.
Effettivamente, un buon numero di occorrenze viene segnalato per impatti che richiedono solo l'accesso al sistema IT. Ciò può essere spiegato dalla presenza di un numero maggiore di barriere di sicurezza (ad es. funzioni strumentali di sicurezza, contromisure di sicurezza informatica, dispositivi di sicurezza passiva, ecc.) tra l'attaccante e il sistema di destinazione quando è richiesto l'accesso al sistema OT. Inoltre, mentre il sistema IT degli impianti di processo è generalmente simile a quello di altri settori di business, il sistema OT ricorre a soluzioni progettuali proprietarie e quindi specifiche. In altre parole, sono necessarie fasi di scansione e di escalation più profonde e difficili per un utente malintenzionato che mira a infettare il sistema OT, piuttosto che solo il sistema IT.
Se analizziamo più in generale i risultati ottenuti dalla banca dati, possiamo notare che il settore in cui è maggiore la quantità di scenari incidentali accaduti è quello correlato alla "Chemical Manufacturing", come del resto sarebbe stato lecito aspettarsi. Si ricordi che tale settore è solito operare con differenti sostanze considerate dannose per la salute e/o l'ambiente circostante. Nell'ultimo decennio, le industrie chimiche e manifatturiere hanno optato per l'isolamento del firewall, l'autenticazione a più fattori e sviluppato protocolli di protezione informatica per migliorare la sicurezza informatica, in particolare per quanto concerne i sistemi IT. Tuttavia, durante gli stessi anni è accelerata l'integrazione di sistemi IT e OT nell'ambito dell'Industria 4.0, di pari passo con lo sviluppo di attacchi informatici intelligenti e mirati che hanno accesso ai dettagli tecnici del sistema di controllo e dei processi produttivi dell'impianto che mirano a modificare le azioni dell'operatore e del sistema di controllo applicate a un processo chimico.

Conseguentemente, la necessità di sicurezza informatica delle attività OT è aumentata in modo significativo.
Il secondo classificato è il settore della produzione di energia, anch'esso attraente per un malintenzionato disposto a mettere a soqquadro il mercato energetico per i propri fini o tornaconti personali. Se si considerano i sistemi di trasporto e distribuzione, gli oleodotti per il trasporto di petrolio e gas sono stati l'obiettivo principale di azioni dannose. Effettivamente, come anche citato all'interno dell'articolo "Analysis of physical and cyber security-related events in the chemical and process industry" (Casson Moreno et al., 2018)", la protezione di tali dispositivi comporta difficoltà intrinseche e costi elevati dovuti alla loro estensione che può essere nell'ordine delle centinaia di chilometri (US Department for Homeland Security, 2008b). Anche in questo caso, gli attacchi informatici potrebbero essere guidati da ragioni di mercato/affari, in quanto possono essere finalizzati ad ottenere informazioni su statistiche di produzione, strategie di mercato e listini dei prezzi di materie prime e di prodotti finiti. Inoltre, anche l'ottenimento di mere possibilità di business (inteso come la possibilità di raccogliere dati di valore economico) e il causare potenziali danni alla reputazione delle imprese possono contribuire a rendere attraenti i bersagli di cui sopra.
Riguardo la tipologia di attacco subito dal sistema oggetto d'esame, i due più rilevanti in numero sono gli attacchi accidentali e quelli intenzionali provenienti dall'esterno. Tuttavia, il principale fattore che distingue questi due casi è il tempo: come è possibile osservare dai dati raccolti, gli scenari incidentali prevalgono soprattutto negli anni più remoti del database, fino ad arrivare al primo decennio degli anni 2000. Successivamente, in particolare a partire dal 2018, è notevolmente incrementato il numero di incidenti causati da cyberattacchi intenzionali provenienti dall'esterno delle strutture. Sebbene non presenti all'interno di questo database, si potrebbero annoverare altri incidenti accaduti durante la pandemia di COVID-19, oltre a quelli accaduti negli ultimi due anni a seguito anche dello scoppio della guerra in Ucraina. A tal proposito, riguardo al settore petrolchimico, si prenda come lampante esempio il caso della Colonial Pipeline descritto in seguito in questo documento.
Muovendo la concentrazione sugli stati dove gli incidenti sono avvenuti, è la Francia ad aggiudicarsi il primo posto, seguita dalla Germania e dagli Stati Uniti d'America. Ovviamente, questo non è dovuto a negligenze da parte dei francesi, ma al fatto che essendo ARIA un database francese esso viene arricchito in primo luogo dai nostri "cugini d'Oltralpe". Non a caso, gli incidenti accaduti in Francia sono spesso anche quelli più dettagliati dal punto di vista delle informazioni disponibili.
Riguardo le conseguenze generate dai vari incidenti, la maggior parte dei casi prevede la perdita di contenimento di materiale pericoloso, esplosioni, incendi, dispersioni tossiche, contaminazione del suolo ecc. che hanno anche provocato morti e feriti (IC-01, come nel succitato caso 5989 di ARIA). Al secondo posto troviamo le infezioni del sistema IT (IC-06) e al terzo i casi in cui si è arrivato allo shutdown parziale o totale del sistema (IC-03).
In un numero significativo di casi sono state segnalate ingenti perdite economiche come impatto secondario, mentre solo in un numero più limitato le perdite economiche e/o di produttività sono state la conseguenza principale.
All'interno del materiale di supporto, è anche possibile osservare come vengano implementate le contromisure per ridurre il rischio informatico a seguito dei vari incidenti. La definizione delle contromisure e dei relativi requisiti è realizzata "ad hoc" per ogni sistema e richiede un'analisi dettagliata delle fonti di minaccia (motivazione e capacità), delle vulnerabilità e dei potenziali impatti. Tra le principali contromisure scelte si possono annoverare: il rafforzamento delle password precedentemente utilizzate per le autenticazioni, le protezioni contro i DoS (Denial of Service), l'uso di sistemi di crittografia e la restrizione dell'uso di dispositivi di memorizzazione come chiavette USB, che potrebbe risultare un utile vettore di infezioni informatiche. Inoltre, non si dimentichi il sempre più crescente utilizzo dell'intelligenza artificiale per individuare e stroncare le minacce sul nascere, monitorando i dati dell'intero sistema in tempo reale. L'ottenimento di dati in questa maniera dai processi industriali è stato spesso giustificato dagli ingegneri della sicurezza dei processi per motivi di sicurezza. Infatti, recapitando l'insieme dei dati in tempo reale dalle varie sezioni di processo consente di intervenire tempestivamente qualora dovessero verificarsi alcuni disturbi.

Nella tabella 2.1 e nei successivi grafici sono annoverate le legende per l'interpretazione della tabella sintetica finale sui dati raccolti, nonché i relativi grafici Excel.

Tabella 2.1: Campi dettagliati utilizzati nel database e definizioni dei termini chiave utilizzati. (Fonte: "Analysis of Cybersecurity-related Incidents in the Process Industry", Matteo Iaiani, et al. 2021)

	Descrizione	**Etichetta**
Settore industriale		
Chemical	Impianti di produzione e stoccaggio di prodotti chimici, compresa la produzione di pesticidi, l'industria farmaceutica, la produzione di prodotti chimici di base. Sono esclusi il trasporto e la vendita al dettaglio di prodotti chimici	CM
Petrochemical	Impianti di produzione e stoccaggio petrolchimici, comprese le raffinerie e il trasporto di petrolio e gas tramite oleodotti. Sono esclusi altri mezzi di trasporto e di vendita al dettaglio di carburanti	PC
Energy production	Impianti di produzione di energia elettrica a base di idrocarburi (combustibili a base di petrolio e gas naturale), impianti idroelettrici e nucleari	EP
Water recovery	Recupero dell'acqua per uso industriale	WR
Tipo di attacco		
Attacco informatico accidentale	Un attacco informatico che non è diretto verso un obiettivo specifico, ma che infetta qualsiasi ospite vulnerabile. L'aggressore è generalmente sconosciuto	ACC
Attacco informatico interno intenzionale	Un attacco informatico che viene effettuato contro un obiettivo specifico e progettato per sfruttare specifiche debolezze del sistema bersaglio. L'aggressore è un insider, ovvero un individuo che normalmente ha accesso autorizzato ai beni dell'azienda (ad esempio dipendente, appaltatore, partner commerciale, fornitore, ecc.). L'utente malintenzionato viene generalmente identificato da un'indagine.	INT-INT

Attacco informatico esterno intenzionale	Un attacco informatico che viene effettuato contro un obiettivo specifico e progettato per sfruttare specifiche debolezze del sistema bersaglio. L'aggressore non è un insider, cioè non ha autorizzato l'accesso agli asset dell'azienda. L'aggressore generalmente rivendica l'attacco.	INT-EXT
Sistema infetto		
IT (Information Technology) system	L'hardware e il software dedicati all'archiviazione, al recupero, alla trasmissione e alla manipolazione di dati o informazioni	IT
OT (Operational Technology) system	L'hardware e il software dedicati a rilevare o causare cambiamenti nei processi fisici attraverso il monitoraggio diretto e/o il controllo di dispositivi fisici come valvole, pompe, compressori, ecc.	OT
Impatto		
Principale evento	Perdita di contenimento di materiale pericoloso, esplosione, incendio, dispersione tossica, contaminazione del suolo, ecc.	IC-01
Perdita economica	L'azienda attaccata subisce gravi perdite economiche a causa, ad esempio, della perdita di produttività (interruzione dell'attività), del crollo delle azioni della società in borsa.	IC-02
PSD/LSD	PSD (Process Shutdown) o LSD (Local Shutdown) originato direttamente o inducendo una condizione anomala o un modo di funzionamento anormale.	IC-03
Infezione OT	Infezione del sistema OT (ad es. infezione di postazioni HMI, server OT, ecc.)	IC-04
Perdita o danneggiamento dei dati	Furto e/o corruzione di informazioni sensibili riguardanti il know-how aziendale, i dati dei dipendenti, i dati di processo (es. schede tecniche delle	IC-05

	apparecchiature, PFD, P&ID, dati storici, ecc.), dati economici, ecc.	
Infezione IT	Infezione del sistema IT (ad es. infezione di server IT, PC, ecc.)	IC-06

Tabella 2.2: Sintesi eventi incidentali database ARIA, secondo classificazione di Tabella 2.1

CSI (ID ARIA)	Data	Luogo	Settore industriale	Tipo di attacco	Sistema infetto	Impatto principale
50755	2017	France	PC	ACC	OT	IC-01
51131	2018	EU	WR	INT-EXT	IT	IC-06
42931	2012	France	CM	ACC	OT	IC-01
5989	1994	France	CM	INT-EXT	OT	IC-01
50842	2017	EU	EP	INT-EXT	IT	IC-06
58778	2022	France	EP	INT-EXT	IT	IC-06
56854	2020	France	CM	INT-EXT	IT	IC-06
53738	2019	France	CM	INT-EXT	IT	IC-03
56510	2020	France	CM	INT-EXT	IT	IC-06
57057	2021	France	CM	INT-EXT	IT	IC-06
58868	2022	France	EP	INT-EXT	IT	IC-03
58714	2022	France	EP	INT-EXT	IT	IC-06
58623	2022	Germany	WR	INT-EXT	IT	IC-06
60468	2023	Germany	CM	INT-EXT	IT	IC-06
60545	2023	Germany	CM	INT-EXT	IT	IC-06
40319	2010	Germany	CM	ACC	OT	IC-01
164	1989	France	CM	ACC	OT	IC-01
212	1990	USA	CM	ACC	OT	IC-01
3212	1991	France	CM	ACC	OT	IC-01
3536	1992	France	CM	ACC	OT	IC-01
6327	1986	France	EP	ACC	OT	IC-01
7176	1995	France	CM	ACC	OT	IC-01

11181	1997	France	CM	ACC	OT	IC-01
14619	1998	France	CM	INT-INT	IT	IC-02
17531	1999	France	PC	ACC	OT	IC-01
21466	2000	France	CM	INT-EXT	IT	IC-01
23074	1979	France	PC	ACC	OT	IC-01
24665	2003	France	CM	ACC	OT	IC-01
31630	2006	France	CM	INT-EXT	IT	IC-01
32484	2006	France	CM	ACC	OT	IC-01
38418	2008	USA	CM	ACC	OT	IC-01
36496	2009	France	CM	ACC	OT	IC-01
38431	2010	France	CM	ACC	OT	IC-01

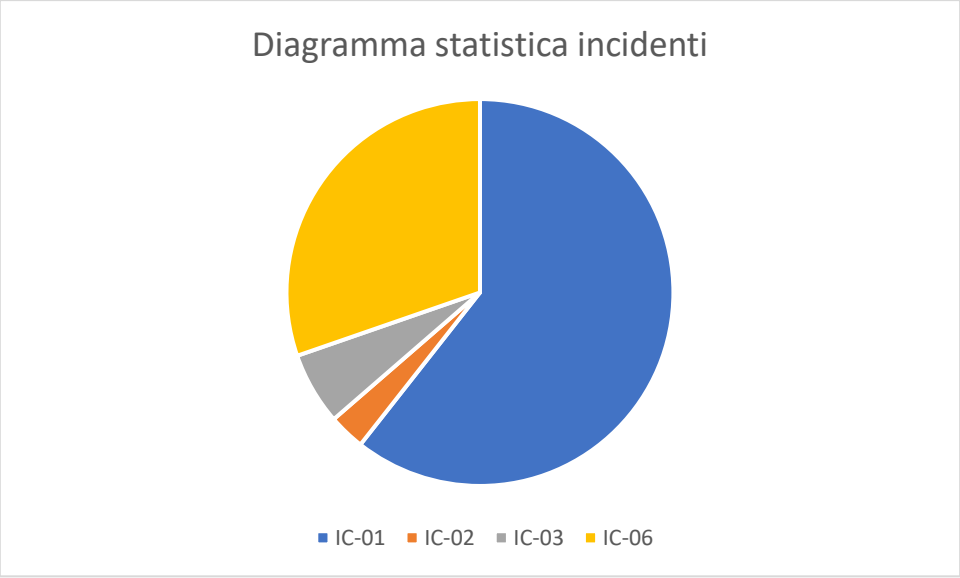


Figura 2.2a: Diagramma statistica incidenti descritti in Tabella 2.2

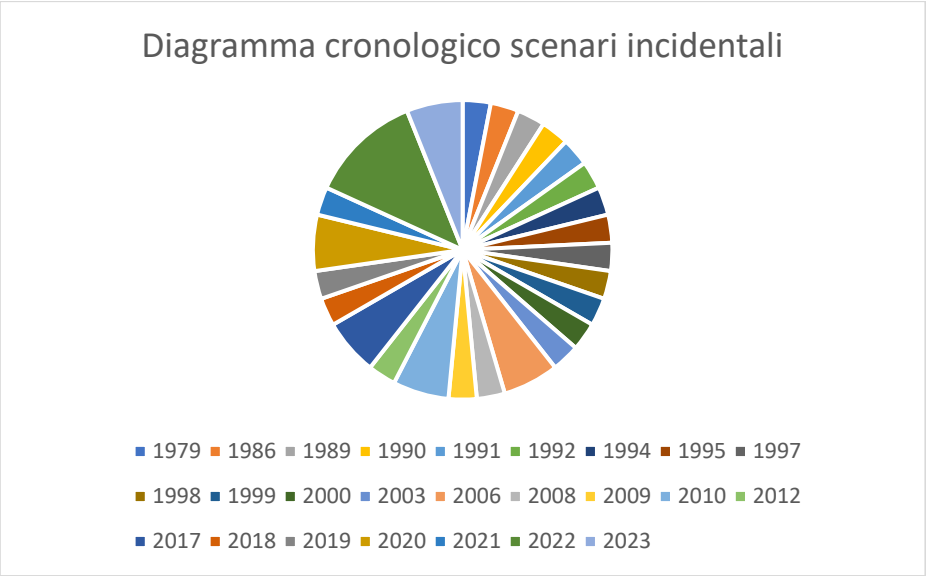


Figura 2.2b: Diagramma cronologico incidenti descritti in Tabella 2.2

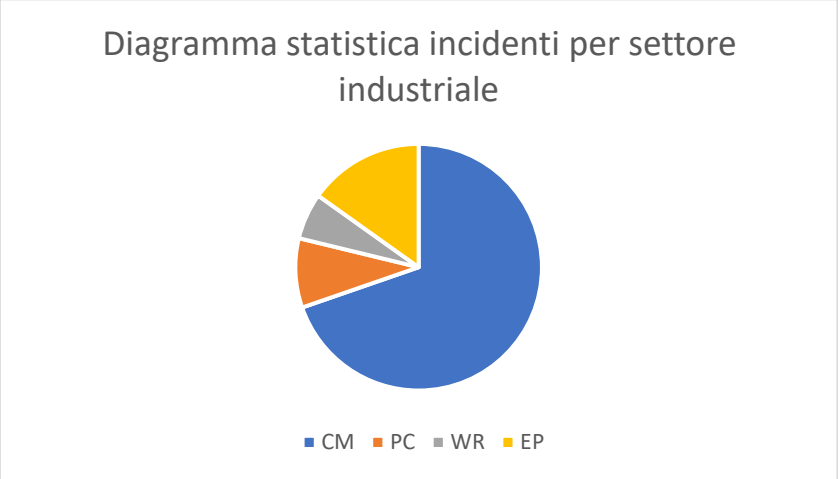


Figura 2.2c: Diagramma statistica incidenti per ognuno dei settori industriali descritti in Tabella 2.2

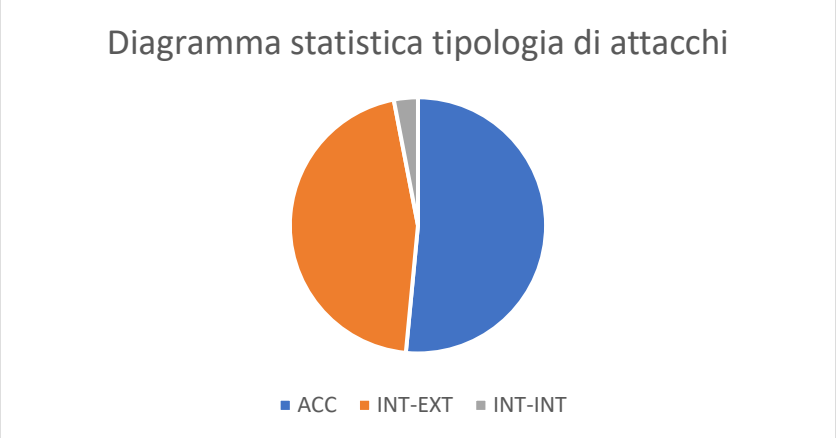


Figura 2.2d: Diagramma statistica tipologia di attacchi descritti in Tabella 2.2

3. Il caso Colonial Pipeline

L'economia americana è fortemente dipendente da reti di oleodotti che trasportano una varietà di prodotti critici ed essenziali per il sostentamento del fabbisogno giornaliero della popolazione. Per quanto riguarda i prodotti petroliferi e il gas, ci sono circa 230.000 miglia di oleodotti che trasportano petrolio greggio e prodotti raffinati e 2,6 milioni di miglia di gasdotti. In gran parte, questi gasdotti sono di proprietà privata, con alcune società che possiedono l'82% delle miglia di condotti di grande diametro e il 62% di tutte le miglia di oleodotti negli Stati Uniti. L'infrastruttura odierna delle condutture è altamente informatizzata e digitalizzata. Le società di oleodotti gestiscono sia sistemi IT sia OT. L'IT comprende i normali dispositivi quotidiani che vengono utilizzati dai dipendenti nel corso delle loro mansioni lavorative, come laptop, software e altro hardware per facilitare le comunicazioni. L'OT, tuttavia, è un insieme molto più complesso e specializzato di sistemi di controllo industriale. (Fonte: "Cybersecuring the pipeline", Ido Kilovaty, 2023).
In data 7/5/2021, la Colonial Pipeline, ovvero la più grande "fuel pipeline" degli Stati Uniti d'America con un fatturato dell'ordine di 8 miliardi di dollari, scopre di essere appena stata vittima di uno tra i più grandi cyberattacchi mai registrati contro una struttura del mercato dell'energia statunitense. L'attacco è stato eseguito per mezzo di un ransomware, sviluppato dal gruppo di hacker anonimi noti solo con lo pseudonimo di DarkSide. Un ransomware è un virus altamente invasivo, capace di avviare automaticamente la criptazione dei file, bloccandone di fatto l'accesso per chiunque non abbia la chiave di decodifica. Il gruppo di pirati informatici lascia un messaggio di testo contenente minacce rivolte all'azienda relativamente al fatto di essere riuscito a criptare 100 GB di dati sensibili e chiedendo, per lo sblocco, un riscatto di 75 bitcoin (che per l'epoca dei fatti, sarebbero circa 5 milioni di dollari). Da quanto emergerà a seguito delle indagini condotte dall'FBI, DarkSide è riuscita a infiltrarsi nei sistemi informatici di Colonial Pipeline grazie a una banale mail di phishing, aperta da un dipendente di cui i pirati sono riusciti a ottenere i dati necessari per superare l'autenticazione del sistema. È anche da tenere conto che l'azienda, sorprendentemente, non era nemmeno dotato di un sistema di doppia autenticazione per l'accesso da dispositivi in locale o da remoto (Fonte della notizia: "Starting Finance"). Una volta eseguito l'accesso, l'obiettivo è ottenere i dati per l'accesso al domain controller, cioè il centro di controllo del sistema informatica dell'intera azienda, da cui poi diffondere il virus.
Per quanto concerne le conseguenze dell'attacco, al fine di evitare ulteriori compromissioni, la Colonial Pipeline si ritrova costretta a chiudere per un'intera settimana. Questo causa enormi disagi alla popolazione degli USA, con la formazione di enormi code di automobili in fila ai distributori sempre più a corto di carburanti. Il tutto ovviamente provoca anche un grande aumento del prezzo dei carburanti stessi. In poche parole, la situazione sembra drammatica, al punto che la Colonial Pipeline si ritrova costretta a cedere al ricatto, pagando i bitcoin richiesti per lo sblocco dei dati criptati.
Si ricordi che, per come è strutturata la blockchain dei pagamenti, è difficile tracciare tutti i movimenti del flusso di denaro fino al portafoglio digitale del destinatario. Difficile, ma non impossibile. L'FBI sarà in grado rintracciare il destinatario mesi dopo la partenza delle indagini.
Per quanto concerne le conseguenze in termini economici, si stima che le perdite per l'azienda si aggirino intorno a 1 miliardo di dollari, quantomeno tenendo conto del prezzo del petrolio al barile all'epoca dei fatti, che si aggirava attorno ai 68 dollari, e della quantità di barili venduti giornalmente, cioè 2,5 milioni.
Molte iniziative in termini di regolamentazioni sono state prese all'indomani dell'attacco alla Colonial Pipeline, che a sua volta ha messo in luce le molte carenze della regolamentazione della sicurezza informatica degli oleodotti negli Stati Uniti. Ad esempio, prima dell'attacco, gli standard di sicurezza informatica per le società di oleodotti erano in gran parte volontari e obsoleti.

4. Sistemi di controllo industriali ed algoritmi

Nel controllo di apparecchiature rivestono una fondamentale importanza gli algoritmi di calcolo, ormai sempre più precisi e sofisticati. Si ricorda che un algoritmo è definito come l'insieme di tutte le operazioni che a partire dai dati in ingresso ottiene dei risultati per mezzo di un'elaborazione attraverso l'uso di funzioni (nei casi ingegneristici, si intende proprio funzioni logico-matematiche). Altrettanto importante è preservare il corretto funzionamento di tali algoritmi, soprattutto in ambito industriale, in quanto l'applicazione corretta di tutti gli step è ciò che può fare la differenza in termini di qualità di un prodotto o di un servizio offerti alla clientela. I membri di amministrazione dovrebbero quindi avere ben chiaro quali siano i controllori ottimali alla regolazione di una data variabile di processo, ma soprattutto come e dove disporre nella planimetria dell'impianto le varie componenti dei sistemi di controllo e sicurezza.

Per quanto concerne i sistemi di controllo industriale (ICS), questi generalmente dovrebbero essere collocati in aree costantemente sorvegliate, in modo da evitare incidenti con conseguenze aventi impatto sia a livello del sito di produzione che nelle aree circostanti, specie nel caso in cui queste ultime siano densamente popolate. Volendo osservare nel complesso, un ICS è tipicamente composto da sistemi di controllo di supervisione e acquisizione dati (SCADA) e sistemi di controllo distribuito (DCS) . Lo SCADA è progettato per l'acquisizione dei dati e il monitoraggio del sistema di produzione. Inoltre, SCADA consente agli amministratori di sistema di controllare i siti remoti tramite un controllo centralizzato. Analogamente allo SCADA, un DCS è formato da controllori autonomi installati in un'unità di produzione. Un sistema DCS utilizza tali controllori per monitorare e supervisionare un'unità da remoto. Tuttavia, lo SCADA è progettato per la gestione dei sistemi in più sedi, mentre DCS viene utilizzato per controllare i sistemi di produzione in un'unica sede. L'interfaccia fra DCS e SCADA è invece il Programmable Logic Controller (PLC). Al fine di stabilire la connessione tra SCADA e PLC, molti fornitori di ICS hanno proposto protocolli di comunicazione specifici (come il Distributed Network Protocol DNP3, ampiamente utilizzato negli impianti di trattamento dell'elettricità e delle acque reflue) che possono essere utilizzati per vari ambienti ICS.

Per ulteriori informazioni si veda "Cybersecurity in industrial control systems: Issues, technologies, and challenges" di Muhammad Rizwan Asghar et al. 2021.

La domanda che potrebbe ora sorgere spontanea è come individuare in maniera sistematica e completa le vulnerabilità caratteristiche di un ICS e come quindi evitare che queste siano attaccate dall'interno o dall'esterno. Le principali vulnerabilità di un ICS possono essere localizzate:

- a livello della rete (network), in particolare si intende la possibilità che la rete venga compromessa a causa di un virus o di un attacco informatico per mezzo di tecniche come il phishing
- a livello di SCADA/DCS, in particolare vulnerabilità a livello del firewall o di software operativo o ancora di server (DoS, cioè Denial of Service)
- a livello di ambiente di produzione, in particolare vulnerabilità nei protocolli di comunicazione (ad esempio DNP3) o nella scarsa protezione di sistemi fisici importanti

Vulnerability Category	Summary Description
Data	• No established sensitivity levels for ICS data • Absence or inappropriate identification and classification of ICS data
Security Administration	• Inadequate security administration in the areas of policy and procedures • Ineffective configuration management due to the application of informal procedures and irregular uncoordinated exercises • Neglect of security training due to cost avoidance
Network	• Legacy ICS network implementations rely on proprietary protocols and relatively primitive, low-bandwidth data channels introduce several security inabilities • Only basic integrity checking is available for data, Accounting and logging are largely non-existent, making laborious configuration management and forensics preposterous • Blind trust in the capability of ICS links to dependably transmit data, and the connections of ICS to external networks
Architecture	• Intermittent physical damage to infrastructure assets as a result of permissible operation of ICS control equipment • Leveraging ICS communication links and networks for the conveyance of signals associated with emergency services like security and fire systems, which geometrically increase the potential for intrusions and disruptions
Platforms	• Password control for ICS proprietary platform or devices can often be defeated locally • The pervasive remote access and configuration available to RTUs and their consequent authentication weaknesses • The gradual systems (applications, databases, and interfaces) shift from proprietary platforms to modern IT-style computers running Windows or UNIX-style operating systems

Figura 4.1: Classificazione delle vulnerabilità per ICS (Fonte: "Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective", Uchenna P. et al. 2016)

Gravi falle di sicurezza dei sistemi di personal computer vengono spesso segnalate e le patch di sicurezza vengono perciò rilasciate molto spesso da chi di competenza, praticamente all'ordine del giorno. In certi casi, le patch di sicurezza creano problemi di natura incerta dovuti a conflitti tra le diverse applicazioni installate. Pertanto, le patch di sicurezza complete vengono raramente applicate a ICS per mantenerne la disponibilità. Per la sicurezza dell'ICS stesso, sono necessari approcci particolari oltre a quelli per i sistemi informativi.
La valutazione del livello di garanzia della sicurezza di ICS è discussa nel protocollo ANSI/ISA99 (Uehara, 2011). La sicurezza del sistema viene valutata in base alle cosiddette "zone" e alle loro interfacce.
Se la rete di controllo è divisa in zone sicure multiple e se i diversi schemi di attacco informatico sono necessari per invadere tali zone, alcune potrebbero essere in grado di resistere agli attacchi informatici. Di conseguenza, le possibili manipolazioni sono limitate solo alle zone invase. Se risulta necessaria la manipolazione multipla in zone diverse per attivare un incidente, la suddivisione riduce ulteriormente la probabilità di incidente. Ad esempio, al fine di causare la sovrappressione di un serbatoio o di un separatore, aumentare la portata in uscita e interrompere l'alimentazione liquida in ingresso sono necessari. Se una di queste azioni non può essere eseguita, è difficile che si verifichi l'incidente. Quando gli attuatori per la corrente in uscita e l'alimentazione si trovano in zone di rete diverse, la possibilità che entrambi vengano manipolati da cybercriminali si riduce.
Dividere la rete di controllo in zone differenti è efficace anche per il rilevamento degli attacchi informatici. Anche se si trattasse di un attacco informatico particolarmente subdolo nella zona invasa, c'è la possibilità che gli effetti fisici dell'attacco appaiano nella zona resiliente. Se la velocità di aumento della pressione viene manipolata e le variazioni di livello di liquido vengono nascoste dagli aggressori informatici, il rilevamento dell'attacco è difficile. Tuttavia, se i sensori di pressione nella zona resiliente sono in grado di rilevare il cambiamento di pressione, l'attacco informatico può essere altrettanto rilevato.
Il concetto fondamentale e basilare nello standard ANSI/ISA 99 è che i firewall che separano una zona da un'altra non devono presentare lo stesso tipo di vulnerabilità, altrimenti diventerebbe ancora più semplice innescare un attacco a catena che comprometta più zone di quanto si possa immaginare.
Si presume ancora che esista un gran numero di vulnerabilità specifiche ICS non identificate a causa del crescente tasso di scoperta delle vulnerabilità e del fatto che anche la ricerca su tali vulnerabilità è in continuo proseguimento. In genere le soluzioni proposte ad oggi per contrastare gli attacchi sono il rafforzamento dei firewall, l'uso dei sistemi di antivirus e dei filtri per le caselle di posta che bloccano mail potenzialmente pericolose, l'utilizzo di autenticazioni multiple per l'accesso a dati considerati di massima importanza o ancora il machine learning, con l'addestramento specifico e intensificato di un'intelligenza artificiale per rilevare ed eliminare le intrusioni.

In genere, la consulenza con gli esperti del settore aiuta non poco a prevedere quali siano le migliori soluzioni da adottare caso per caso. Tuttavia, è sempre necessario informare gli addetti ai lavori dell'esistenza e magari dell'insistenza di coloro che tentano di intrufolarsi anche da un piccolo spiraglio per arrivare a carpire le informazioni protette. La conoscenza delle minacce è il primo modo per prevenirle, potrebbe tuttavia non essere sufficiente nei casi più gravi o in quelli dove l'attacco avviene durante l'assenza fisica del personale. Si ricordi che una buona parte degli attacchi informatici registrati contro i siti di produzione industriale sono avvenuti di notte o alle prime luci del giorno, approfittando magari della distrazione di chi avrebbe dovuto rimanere vigile e pronto per eventuali evenienze.
Lo schema della suddivisione degli odierni sistemi industriali IT/OT e la sintesi delle fasi di un cyberattacco sono descritti nelle Figure 4.2 e 4.3. Le possibili minacce e gli obiettivi futuri di sicurezza dei CPS sono invece mostrati in Tabella 4.1 e in Figura 4.4.

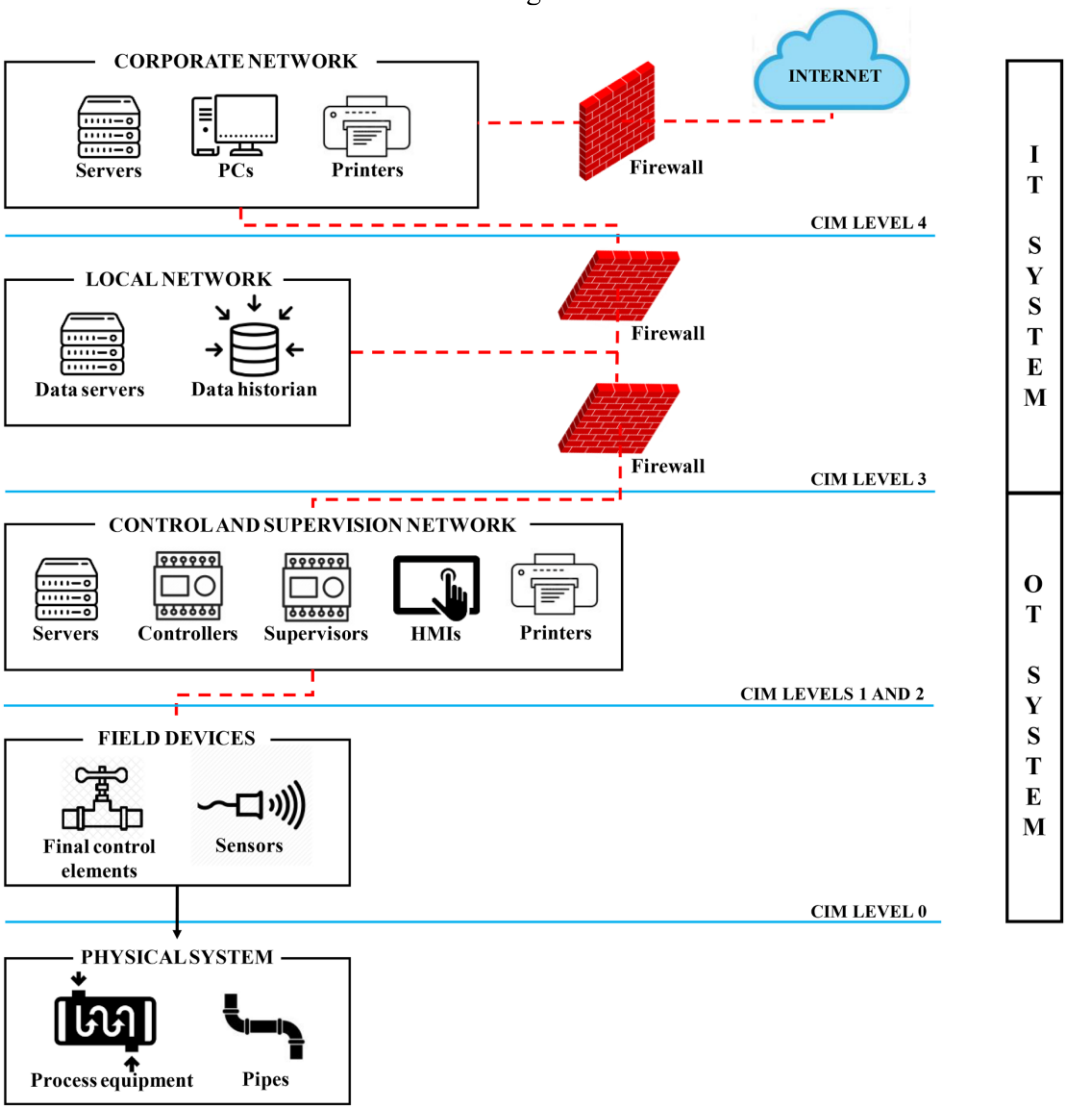


Figura 4.2: La tipica struttura CIM (Computer Integrated Manufacturing) per un impianto di processo. Viene mostrata la corrispondenza con la categorizzazione del sistema informatico e del sistema OT nel database. (Fonte: "Analysis of Cybersecurity-related Incidents in the Process Industry", Matteo Iaiani et al. 2021)

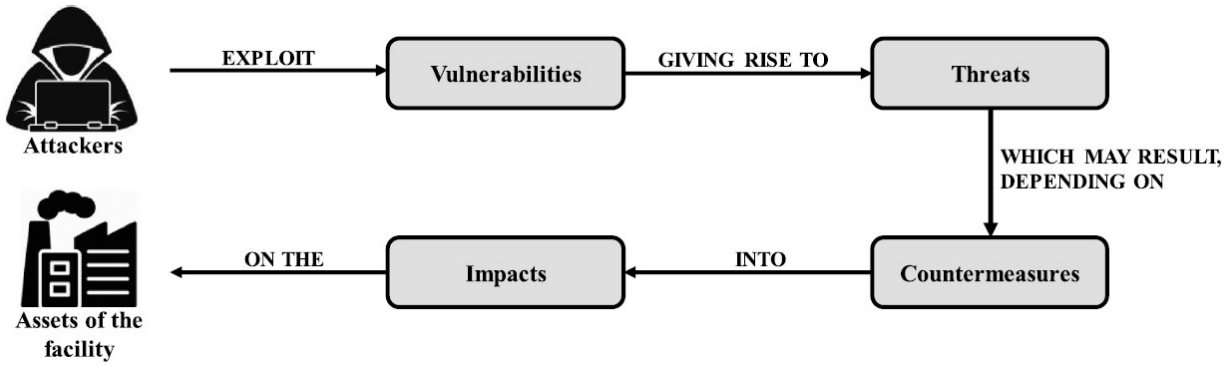


Figura 4.3: Meccanismi di un cyberattacco (Fonte: "Analysis of Cybersecurity-related Incidents in the Process Industry", Matteo Iaiani, et al. 2021)

Tabella 4.1: Agenti di minaccia e potenziali obiettivi di attacco (Fonte: "Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective", Uchenna P. et al. 2016)

	Steal information	System resource utilisation, RAT kit	Botnet and zombie operation	Critical data and information damage	System shut down attack	PLCs, HMIs, MTU/RTUs manipulation	System Hijack
Greedy insider	✓						
Disgruntled insider	✓			✓	✓	✓	
Disgruntled ex-insider	✓	✓		✓	✓		
Greedy ex-insider	✓	✓					
Ordinary hacker		✓	✓				
Malicious hacker	✓	✓	✓	✓	✓		
Greedy outsider	✓						
Extremist group	✓			✓			
Extremist group with former insider	✓			✓	✓		
Extremist group with insider	✓			✓	✓	✓	
Terrorist group	✓			✓	✓	✓	
Terrorist group with former insider	✓			✓	✓	✓	
Terrorist group with insider	✓			✓	✓	✓	✓
Nation-state actors	✓			✓	✓	✓	✓

✓ = Probable actions based on available skills, training, knowledge, resources and proportionate access, and authority levels, Source: [60].

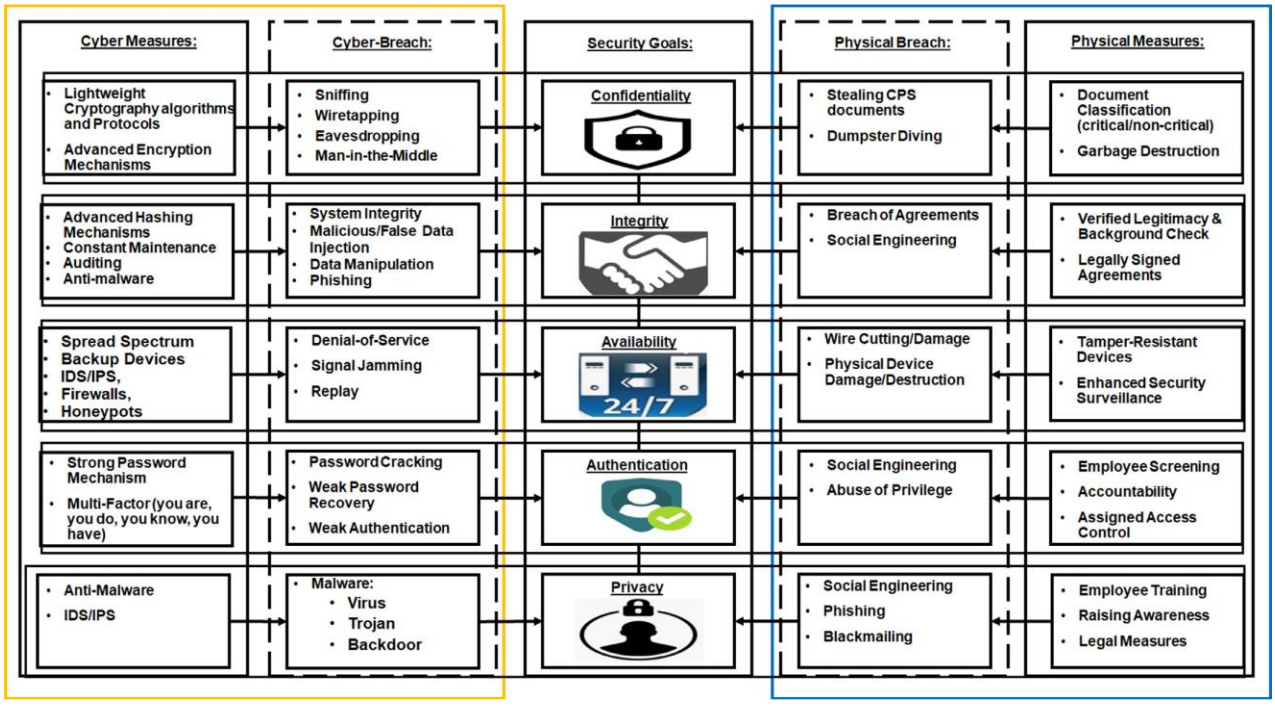


Figura 4.4: Obiettivi di sicurezza dei sistemi CPS (Fonte: "Cyber-physical systems security: Limitations, issues and future trends, Jean-Paul A. Yaacoub et al., 2020)

5. Il fattore umano in ambito cybersicurezza

Il paragrafo in questione si pone di contestualizzare il fattore umano che verrà successivamente considerato all'interno dei calcoli di probabilità di accadimento degli eventi nelle analisi FTA. Quanto descritto in seguito è tratto dall'articolo "Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective", Uchenna P. et al. 2016.
Gli odierni sistemi che coinvolgono l'uomo sono diventati più caotici che mai, soprattutto con l'avvento del cyberspazio, cioè quell'ambiente virtuale dove poniamo di collocare i legami tra le parti hardware e le parti software. Il successo di eventuali abusi commessi nel cyberspazio è spesso attribuito ai comportamenti irregolari e/o deliberati dell'uomo. La cattiva condotta umana è purtroppo uno dei motivi principali per cui anche il settore industriale è diventato vulnerabile agli attacchi alla sicurezza.
Le infrastrutture industriali sono sempre più soggette a un'ampia gamma di minacce e attacchi, tali da mettere a repentaglio il corretto funzionamento dei sistemi.
Le osservazioni mostrano che i successi dei più recenti attacchi informatici all'ICS sono stati ottenuti probabilmente dalle azioni e/o dalle non azioni umane all'interno e all'esterno dei sistemi, volenti o nolenti che fossero. Le strategie, le tecniche e i modelli di attacco informatico più diffusi, come lo spear-phishing, i controller di dominio compromessi, gli attacchi ai server esposti, l'attacco ai client ICS, il dirottamento delle sessioni, gli errori e le omissioni nelle configurazioni dei firewall, gli indirizzi IP falsificati ecc., hanno ovviamente una cosa in comune: porre gli esseri umani come obiettivi primari o di primo punto per consentire la realizzazione di atti dolosi all'interno dei sistemi bersaglio.
L'efficacia delle attività dannose dipende in gran parte dal comportamento delle risposte umane coinvolte nei sistemi di destinazione. Nel 2013, secondo quanto scritto nel rapporto sulle violazioni della sicurezza di PricewaterhouseCoopers (una rete multinazionale di imprese di servizi professionali, che fornisce servizi di consulenza di direzione e strategica, revisione di bilancio e consulenza legale e fiscale) , il 36% delle violazioni della sicurezza più gravi è stato causato da errori umani. Un totale del 31% delle violazioni della sicurezza più terribili nell'autunno del 2014 è stato avviato da errori umani e nel 2015 questa percentuale è salita al 50%. Il rapporto precedente ha anche rilevato un ulteriore 20% di violazioni considerate molto gravi dovute a usi impropri e intenzionali dei sistemi. Si riporta anche che l'80% delle volte in cui le credenziali di utenti sono state rubate, il phishing sia stato il mezzo principale adoperato per le violazioni. Nel report più recente, una non irrilevante parte degli intervistati ritengono che gli errori umani involontari siano fattori che possano contribuire alle peggiori violazioni riscontrate dalle organizzazioni.
Il testo sottolinea anche una crescente tendenza delle persone a diventare i bersagli più vulnerabili degli attacchi informatici alle infrastrutture critiche. Questi bersagli sono indicati come "i vettori di attacco più vulnerabili degli attacchi informatici alle infrastrutture critiche"
Come è stato osservato, numerosi rischi per la sicurezza e l'incolumità abbondano nella gestione delle moderne infrastrutture ICS. Sono necessarie misure di sicurezza per gestire e mantenere il sistema ICS funzionante come desiderato. Sebbene esistano politiche di sicurezza standard (NIST, ISO, ISA, CPNI, ecc.) che prescrivono e sostengono procedure di conformità con misure di sicurezza e protezione per ICS, la criticità delle componenti di un ICS e l'impatto di potenziali violazioni della sicurezza richiedono misure più rigorose da parte dei settori industriali. Un approccio basato sul rischio è considerato più adatto, in quanto mette sul tavolo una misura di analisi della sicurezza approfondita, che raggiunge aree che non avrebbero potuto essere notate utilizzando approcci basati sulla conformità. Le industrie che gestiscono gli ICS devono sviluppare procedure per valutare i rischi relativi alle loro operazioni e alla loro attività e di conseguenza adottare un modo di affrontare i rischi identificati sulla base delle priorità organizzative, tenendo conto dei vincoli interni ed esterni.
A causa della natura evolutiva delle minacce informatiche non solo negli ICS, la gestione dei rischi per la sicurezza dovrebbe essere resa interattiva e iterativa. Dovrebbe essere visto come un processo continuo integrato nelle normali operazioni di routine ed essere sufficientemente olistico da coprire tutti e tre i componenti (persone, processi e tecnologie) dei sistemi informativi e di gestione.
Di conseguenza, le minacce alla sicurezza, le vulnerabilità e i potenziali impatti relativi al personale addetto alla gestione dell'ICS, ai processi operativi e alle tecnologie devono essere chiaramente dettagliati. Questi potrebbero tradursi in varie tipologie di rischi (fisici, operativi, economici, ecc.), che richiedono una risposta adeguata e guidata per essere evitati e per aiutare il medesimo personale ad

acquisire una buona padronanza di ciò che è necessario sapere e saper fare per una corretta gestione dell'ICS.
La consapevolezza della sicurezza è essenziale. Essere informati e continuamente aggiornati sulle attuali tendenze di sicurezza relative ai lavori e all'ambiente di servizio dell' ICS dovrebbe essere una regola piuttosto che un'eccezione. Migliorare le conoscenze e le capacità diagnostiche contro le potenziali minacce informatiche nel dominio ICS può davvero fare la differenza.
L'istruzione e la formazione dovrebbero avere la massima priorità per difendersi dagli incidenti informatici, poiché cresce la domanda di conoscenze e di competenze di sicurezza informatica per i sistemi di controllo specifici del settore. È necessario disporre delle conoscenze opportune per contribuire a identificare le vulnerabilità e i possibili rimedi, nonché valutare gli impatti diretti sugli ambienti digitali e fisici. Uno studio (Ben-Asher N et al.2015) ha dimostrato che una conoscenza supplementare della sicurezza informatica può consentire il rilevamento puntuale di eventi informatici dannosi e ridurre la falsa classificazione di eventi informatici non minacciosi come dannosi.
D'altra parte, le competenze possono guidare gli utenti a prendere decisioni e azioni corrette in grado di ridurre o eliminare il verificarsi di eventi dannosi.
Le tecnologie dell'informazione e della comunicazione sono preziose per la connettività e il controllo delle moderne infrastrutture industriali, in particolare con gli ICS in cui si fa grande affidamento sull'affidabilità e sulla sicurezza delle comunicazioni.
Questo studio mostrerà in seguito anche un pratico esempio economico, seppur approssimativo, che mostrerà quanto quello descritto in questo ed in altri paragrafi sia importante e, in fin dei conti, nemmeno troppo economicamente oneroso grazie alle innovazioni tecnologiche moderne. Infatti è possibile anche disporre di sistemi di sicurezza informatici con un ottimo compromesso fra affidabilità e prezzo.

6. Descrizione dettagliata della metodologia PHAROS (Fonte: “Major accidents triggered by malicious manipulations of the control system in process facilities” di Iaiani, et al. 2021).

Lo scopo di questo paragrafo è la prima descrizione del lavoro di Iaiani et al., il quale risulta, ai fini di questa tesi, il principale termine di paragone con cui confrontare non solo le analisi ma anche i risultati ottenuti. Il primo confronto riguarda proprio la scelta del metodo di analisi del rischio.
All’interno del lavoro sopra citato, per quanto concerne quest’ultimo aspetto, è stata utilizzata la tecnica PHAROS, applicata ad un particolare caso studio di un separatore trifase.
La metodologia PHAROS (Process Hazards Analysis of Remote manipulation through Control Systems) si divide in nove fasi. Nella fase 1 vengono raccolti i dati in input necessari: il PFD (Process Flow Diagram), i bilanci di materia, il P&ID (Piping and Instrumentation Diagram), l'elenco delle sostanze stoccate o manipolate e le loro proprietà pericolose, le condizioni operative di ciascuna unità di processo, le logiche del BPCS e del SIS (ad esempio i diagrammi funzionali a blocchi, gli schemi di controllo, ecc.), e le schede tecniche di ciascuna unità di processo.
Nella fase 2 l'impianto viene suddiviso in nodi di processo. Solo i nodi in cui le sostanze pericolose sono trattate o immagazzinate (ossia i nodi potenzialmente critici) sono studiati nella valutazione, anche a scopo semplificativo. Ogni nodo è tipicamente composto da un'unità di processo principale (ad es. serbatoi di stoccaggio, colonne, reattori, scambiatori di calore, ecc.) ed alcune unità ausiliarie (ad es. pompe, fusti, ecc.) e tubazioni.
La fase 3 consiste nell'identificazione dei nodi critici (ND). Questo passaggio è finalizzato a ridurre ancora il numero di nodi da analizzare, concentrandosi su quelli da cui possono originarsi le conseguenze più gravi. Pertanto, i nodi critici devono essere selezionati sulla base del pericolo intrinseco, quindi sulla base del potenziale di originare scenari incidentali dovuti alle caratteristiche del processo, come l'elevata disposizione di materiali pericolosi o le condizioni operative severe.
La fase 4 consiste nell'identificare i componenti manipolabili a distanza (RMC), i relativi elementi manipolativi (ME) e nell'assegnare gli RMC ai nodi critici. Gli RMC sono gli oggetti fisici dell'impianto il cui funzionamento è regolato dal BPCS e dal SIS (es. valvole automatiche, pompe, compressori, ecc.). Gli ME sono gli elementi del BPCS e del SIS mediante cui viene eseguita la manipolazione (ad esempio i controllori e le loro logiche).
La fase 5 consiste nell'identificare, per ogni ME, tutte le possibili manipolazioni remote (RM) che possono essere effettuate attraverso un attacco informatico.
La fase 6 consiste nell'associare ad ogni nodo critico gli eventi critici (CE) compatibili, cioè una perdita di contenimento (LOC) o una perdita di integrità fisica (LPI) da cui discendono i pericoli materiali o fisici normalmente presenti nel sistema (Delvosalle et al., 2006). Sono disponibili diverse tecniche ben note per identificare i CE: analisi HazOp, analisi what-if, analisi delle modalità di guasto e degli effetti (FMEA), MIMAH, HazId, DyPASI, ecc. (American Petroleum Institute (API), 2004; Center for Chemical Process Safety (CCPS), 2008; Delvosalle et al., 2006; Etowa et al., 2002; International Organization for Standardization (ISO), 2000; Mannan, 2012; Paltrinieri et al., 2011).
La fase 7 consiste nell'identificare tutti i meccanismi d'azione (MA) per mezzo dei quali ogni CE può essere avviato attraverso un attacco al sistema di controllo. Le MA sono i meccanismi fisici che gli aggressori possono utilizzare per avviare il CE.
La fase 8 consiste nell'identificare le combinazioni (CM) di LC dalle RMC assegnate per mezzo delle quali è possibile effettuare ogni MA in un nodo.
La fase 9 consiste nell'individuare, per ogni CM, le protezioni efficaci (cioè i dispositivi di sicurezza) presenti nel nodo analizzato. "Efficace" significa che la salvaguardia è in grado di contrastare, direttamente o indirettamente, l'insorgenza dei corrispondenti CE.

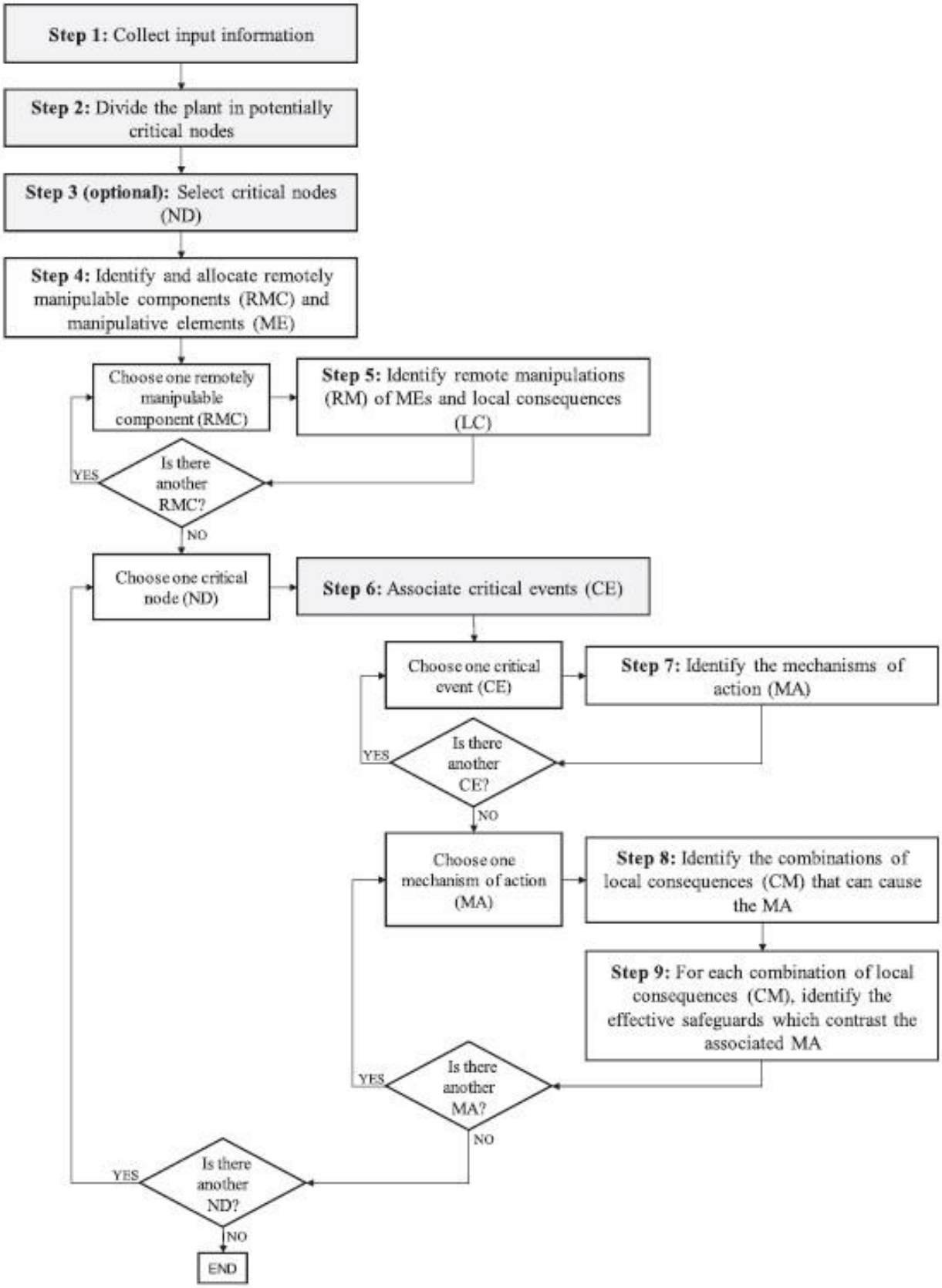


Figura 6.1: flowchart metodo PHAROS *(*Fonte*:* ”Major accidents triggered by malicious manipulations of the control system in process facilities” di Iaiani, et al., 2021).

7. Descrizione del caso studio: Separatore trifase (Fonte: "Major accidents triggered by malicious manipulations of the control system in process facilities" di Iaiani, et al., 2021).

Si tratta di un serbatoio per il trattamento preliminare del crude oil in un impianto di produzione Oil & Gas. Gli obiettivi principali dell'impianto sono la separazione dell'acqua di produzione e la lavorazione di petrolio e gas fino alle specifiche per il trasporto tramite gasdotto. La figura seguente mostra il block diagram ed una breve descrizione del processo

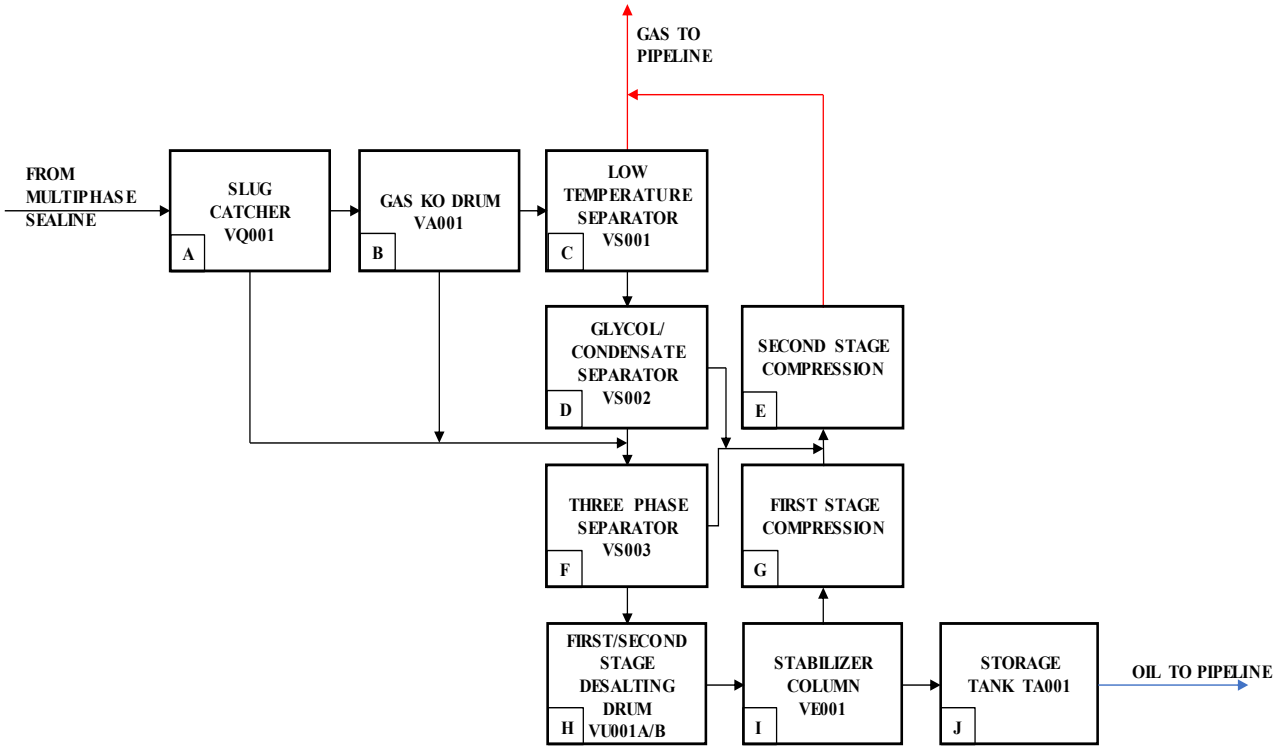


Figura 7.1: Schema a blocchi dell'impianto Oil&Gas considerato nel caso di studio (Fonte: "Major accidents triggered by malicious manipulations of the control system in process facilities" di Iaiani et al. 2021).

Il flusso in ingresso dai pozzi è separato dallo *Slug Catcher VQ001*. Le due fasi liquide vengono ulteriormente separate *nel separatore trifase VS003*; i sali vengono rimossi nel *tamburo di dissalazione del primo/secondo stadio VU001A/B* e la tensione di vapore viene regolata nella *colonna stabilizzatrice VE001*, rendendo il greggio adatto allo stoccaggio nel *serbatoio TA001* e alla consegna in tubazione. Il flusso di gas associato viene inviato a un sistema di separazione *a bassa temperatura (separatore a bassa temperatura VS001,* separatore di glicole/condensa *VS002) e unito al gas compresso del* separatore trifase VS003 *e della* colonna stabilizzatrice VE001.
Il caso studio, tuttavia, si concentra sull'analisi del nodo del separatore trifase VS003 (pressione di servizio = 19 barg; temperatura di esercizio =16 °C; diametro interno=2150 mm; lunghezza=6500 mm). Si è deciso di optare per tale separatore poiché esso si trova in una condizione operativa alquanto pericolosa, anche considerando le sue notevoli dimensioni e la capacità di volume di gas infiammabili che può essere ospitato alla pressione di servizio, pari a 12 m^3. Di seguito si riporta il P&ID relativo a VS003, che mette in evidenza l'insieme delle apparecchiature di controllo e sicurezza che verranno ulteriormente approfondite nelle narrative presenti nei paragrafi successivi.

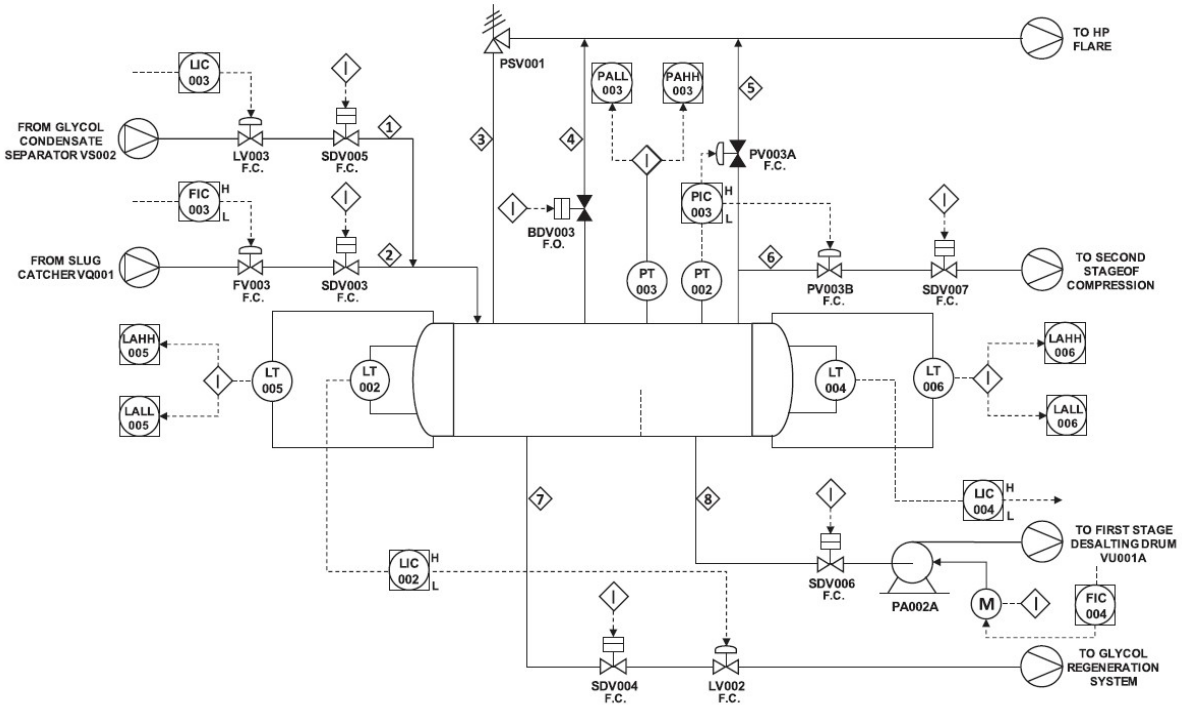


Figura 7.2: P&ID semplificato relativo al nodo ND10 (separatore trifase VS003) (Fonte:“ Major accidents triggered by malicious manipulations of the control system in process facilities” di Iaiani et al., 2021).

EQ codes	Items	Description	Selected CEs
EQ1.2	*Three Phase Separator VS003*	Pressure vessel for the separation of oil, water and hydrocarbon gases (main process unit)	CE5, CE6, CE7, CE10
EQ5.1	*Desalter Feed Pump PA002A*	Centrifugal pump in Stream 7	CE7, CE8
EQ4.1	Line 1	Process inlet stream from *Glycol/ Condensate Separator VS002*	CE5, CE8, CE9, CE10
	Line 2	Process inlet stream from *Slug Catcher VQ001*	
	Line 3	Emergency PSV outlet stream to HP Flare	
	Line 4	Emergency blowdown outlet stream to HP Flare	
	Line 5	Emergency PV outlet stream (gas phase) to HP Flare	
	Line 6	Process outlet stream (gas phase) to second stage of compression	
	Line 7	Process outlet stream (hydrocarbon liquid phase) to *First Stage Desalting Drum VU001A*	
	Line 8	Process outlet stream (aqueous liquid phase) to glycol regeneration system	

Figura 7.3: Correnti, strumentazioni e CE del nodo 10 considerati (Fonte:“ Major accidents triggered by malicious manipulations of the control system in process facilities” di Iaiani et al., 2021).

Si riporta un elenco delle sostanze ritenute pericolose dall'analisi del separatore.

Tabella 7.1: Proprietà pericolose delle sostanze pericolose trattate nel nodo ND10 (Fonte: "Major accidents triggered by malicious manipulations of the control system in process facilities" di Iaiani et al., 2021; it.wikipedia.org | Simboli di rischio chimico – Wikipedia)

Nome	N° CAS	Descrizione
Crude oil	8002-05-9	Liquido e vapore estremamente infiammabili Può essere fatale se ingerito ed entra nelle vie respiratorie Provoca grave irritazione oculare Può causare sonnolenza o vertigini Può provocare il cancro Può causare danni agli organi in caso di esposizione prolungata o ripetuta Tossico per gli organismi acquatici con effetti di lunga durata
Fuel gas	68410-63-9	Gas estremamente infiammabile Contiene gas sotto pressione; può esplodere se riscaldato

Si riportano in Tabella 7.2 la descrizione degli elementi del P&ID relativo al separatore.

Tabella 7.2: Descrizione e posizione di ogni elemento riportato nel P&ID semplificato del nodo ND10 (vedi Figura 4). (Fonte:" Major accidents triggered by malicious manipulations of the control system in process facilities" di Iaiani et al., 2021).

Elemento	Descrizione	Locazione
BDV003	Valvola di spurgo controllata da SIS	Linea 4 da TPS VS003 a HP flare
FIC003	Controllore indicatore di portata	DCS (Distributed Control System)
FIC004	Controllore indicatore di portata	DCS (Distributed Control System)
FV003	Valvola di controllo controllata da FIC003	Linea 2 da Slug Catcher VQ001 a TPS VS003
LAHH005	Allarme alto alto livello di interfaccia	Sala controllo
LAHH006	Allarme alto alto livello dell'olio	Sala controllo
LALL005	Allarme livello interfaccia basso basso	Sala controllo
LALL006	Allarme basso basso livello dell'olio	Sala controllo
LIC002	Controllore indicatore di livello	DCS (Distributed Control System)
LIC003	Controllore indicatore di livello	DCS (Distributed Control System)
LIC004	Controllore indicatore di livello	DCS (Distributed Control System)
LT002	Trasmettitore di livello di interfaccia per DCS	TPS VS003
LT004	Trasmettitore di livello dell'olio per DCS	TPS VS003
LT005	Trasmettitore di livello di interfaccia per SIS	TPS VS003
LT006	Trasmettitore di livello dell'olio per SIS	TPS VS003
LV002	Valvola di controllo controllata da LIC002	Linea 7 da TPS VS003 al sistema di rigenerazione del glicole
LV003	Valvola di controllo controllata da LIC003	Linea 1 dal separatore di condensa di glicole VS002 a TPS VS003
M	Motore elettrico per pompa PA002A	Pianta
PA002A	Pompa centrifuga	Linea 8 da TPS VS003 al tamburo di dissalazione primo stadio VU001A
PAHH003	Allarme alta alta pressione	Sala controllo
PALL003	Allarme di bassa bassa pressione	Sala controllo
PIC003	Controllore indicatore di pressione	DCS (Distributed Control System)
PSV001	Valvola di sicurezza della pressione	Linea 3 da TPS VS003 a HP flare
PT002	Trasmettitore di pressione per DCS	TPS VS003
PT003	Trasmettitore di pressione per SIS	TPS VS003
PV003A	Valvola di controllo controllata da PIC003	Linea 5 da TPS VS003 a HP flare
PV003B	Valvola di controllo controllata da PIC003	Linea 6 da TPS VS003 a compressione secondo stadio
SDV003	Valvola di intercettazione controllata da SIS	Linea 2 da Slug Catcher VQ001 a TPS VS003
SDV004	Valvola di intercettazione controllata da SIS	Linea 7 da TPS VS003 al sistema di rigenerazione del glicole
SDV005	Valvola di intercettazione controllata da SIS	Linea 1 dal separatore di condensa di glicole VS002 a TPS VS003
SDV006	Valvola di intercettazione controllata da SIS	Linea 8 da TPS VS003 al tamburo di dissalazione primo stadio VU001A
SDV007	Valvola di intercettazione controllata da SIS	Linea 6 da TPS VS003 a compressione secondo stadio

7.1. Narrazione di controllo e sicurezza di VS003

Anche ai fini di giustificare alcune ipotesi o scelte adottate all'interno di questa tesi, di seguito viene descritta la control narrative relativa al solo separatore trifase, assieme ai suoi sistemi di sicurezza. Non è possibile applicare tali descrizioni all'intero impianto per mancanza di informazioni da letteratura.

7.1.1. Control Narrative VS003

Nella seguente Control Narrative, si tenga presente che:

- PT002 e PT003 sono trasmettitori di pressione analogici montati sul campo;
- LT002, LT004,LT005 e LT006 sono trasmettitori di livello analogici montati sul campo;
- PIC003 è un indicatore-controllore di pressione digitale montato sul campo
- LIC002, LIC003 e LIC004 sono indicatori-controllori di livello digitale montati sul campo
- FIC003 è un indicatore-controllore di portata digitale montato sul campo

All'interno del separatore trifase VS003 sono inviate la corrente <1> contenente glicole etilenico e la corrente <2> proveniente dallo slug catcher VQ001. La separazione conduce alla formazione di una corrente gassosa idrocarburica (corrente <7>) e di una corrente in fase gassosa (corrente <6>). La prima corrente dovrà quindi essere sottoposta ad un primo stadio di dissalazione, mentre la seconda sarà inviata ad un flare ad alta pressione. Un ulteriore output del processo di separazione sarà la corrente <8>, costituita da una fase liquida acquosa. Questa viene inviata ad un sistema di rigenerazione del glicole in ingresso.
Al fine di mantenere un valore di setpoint delle portate in ingresso è presente:

- un loop di controllo costituito dagli elementi LIC003 e LV003 che regola la portata di corrente <1>
- un loop di controllo costituito dagli elementi FV003 e FIC003 che regola la portata di corrente <2>

Per il controllo del livello di liquido nel serbatoio, sono presenti due loop di controllo. Il loop costituito dagli elementi LT002, LT005, LIC002 e FV002 regola il valore della portata <7> uscente dal serbatoio. Per quanto concerne l'altro loop di controllo, esso è costituito da LT004, LIC004 e FIC004 e contribuisce alla regolazione del livello di liquido nel serbatoio regolando la portata <8> inviata alla pompa PA002A.
Per quanto concerne invece il controllo della pressione, è presente il loop costituito dagli elementi PT002,PT003,PIC003. Come possibile vedere dal P&ID del separatore, in tale loop rientrano anche le valvole PV003A e PV003B, che regolano il valore delle portate in uscita <5> (portata gassosa scaricata in caso di emergenza) e <6>.

7.1.2. Sistemi di sicurezza VS003

Nella seguente descrizione, tutti gli allarmi citati sono da intendersi come digitali e montati sul campo.
Rispetto alle portate di input e output citate nella control narrative, sono presenti 4 valvole di shutdown (SDV003, SDV004, SDV005, SDV006) che intervengono in caso di emergenza, chiudendosi e impedendo il passaggio di ulteriore corrente oppure aprendosi per scaricare in caso di eccessi. Tali valvole sono considerate come operanti in parallelo e si è tenuto conto che quantomeno due su quattro debbano essere sempre operative.
Connessi ai loop di controllo del livello di liquido nel serbatoio, si trovano due coppie di allarmi, una per il controllo di alto livello (LAHH005 E LAHH006) e l'altra per il caso di basso livello (LALL005 e LALL006). Tali allarmi, nelle analisi di operabilità e nei calcoli dei diagrammi FTA, sono stati

considerati come contemporaneamente attivi se l'effettiva emergenza per cui sono progettati dovesse verificarsi.
Il loop di controllo di pressione è connesso a un sistema di sicurezza più complesso. Oltre alle valvole PV003A e PV003B, dal P&ID si osserva la presenza della valvola di sicurezza PSV001, di una ulteriore valvola di blowdown (BDV003) e di un'altra valvola di shutdown (SDV007) che serve a bloccare eventualmente il flusso di portata <6>. Inoltre, sono presenti gli allarmi PALL003 e PAHH003 per i casi di pressione troppo bassa e troppo alta rispettivamente.
Non è stato ritenuto opportuno intervenire con l'aggiunta di altri sistemi di controllo o di sicurezza rispetto a quelli già presenti nel sistema. Tuttavia, ai fini di garantire maggiore sicurezza le logiche dei sistemi di controllo sono state considerate come logiche maggioritarie.

8. Continuazione Metodo PHAROS

Riprendiamo in questo paragrafo la metodologia in oggetto citata precedentemente in questa tesi. A seguito della suddivisione in nodi di cui sopra, sono stati identificati i componenti manipolabili remoti (RMC) presenti nell'impianto Oil&Gas e i relativi elementi manipolativi (ME). Gli RMC identificati sono stati assegnati ai nodi critici del processo. Tali RMC comprendono valvole di emergenza (valvola di spurgo e valvole di intercettazione), valvole di controllo e una pompa a motore. Le valvole di intercettazione e la valvola di spurgo del nodo sono valvole di intercettazione controllate dal SIS per mezzo del PLC, che costituiscono gli ME su cui un malintenzionato può effettuare un attacco in questo caso. Le valvole di controllo sono azionate dai controllori PID del BPCS, mentre la pompa centrifuga è azionata da un motore elettrico controllato sia dal SIS che dal BPCS. In seguito, le manipolazioni remote per le ME sono state identificate. Per quanto riguarda i PLC del SIS che comandano le valvole di intercettazione automatizzate, i RM considerati sono lo spegnimento del segnale (codice RM1) e la riprogrammazione della funzione (RM3). Per i controllori PID del BPCS, che gestiscono le valvole di controllo automatizzate, sono state considerate due manipolazioni: lo spegnimento del segnale (codice RM1) e la modifica del setpoint (RM2). Sono state identificate le conseguenze locali (LC) sulle RMC corrispondenti a ciascuna RM sulle relative ME. Ciò richiede di considerare il tipo fail-safe di tutte le valvole automatizzate (Meier e Meier, 2008), il tipo di azione dei controllori PID (diretta o inversa) e le logiche del SIS.

Tabella 8.1: Manipolazioni remote (RM) e conseguenze locali (LC) per ogni RMC allocato al nodo ND10. (Fonte:“ Major accidents triggered by malicious manipulations of the control system in process facilities” di Iaiani et al., 2021).

RMCs	RMC codes	ME codes	RM codes	LC codes
SDV003, SDV004, SDV005, SDV006, SDV007	RMC1: shut-off valves (F. C.)	ME2: Safety Instrumented System device	RM1: signal shutdown	LC2: valve closing
			RM3: function reprogramming	LC2: valve closing
BDV003	RMC1: shut-off valve (F. O.)	ME2: Safety Instrumented System device	RM1: signal shutdown	LC1: valve opening
			RM3: function reprogramming	LC1: valve opening
PV003A, PV003B, LV002, LV003, FV003	RMC2: control valves(F. C)	ME1: Basic Process Control System devices (PIC003, LIC002, LIC003, FIC003)	RM1: signal shutdown	LC2: valve closing
			RM2: setpoint change	LC7: increase in valve opening degree LC8: decrease in valve opening degree LC9: opening-closing cycles of the valve
PA002A	RMC3: mechanical pump and its driver	ME1: Basic Process Control System device (FIC004)	RM1: signal shutdown	LC5: stop of the pump
			RM2: setpoint change	LC10: increase of the rotational speed of the pump LC11: decrease of the rotational speed of the pump
		ME2: Safety Instrumented System device	RM1: signal shutdown	LC5: stop of the pump
			RM3: function reprogramming	LC5: stop of the pump LC10: increase of the rotational speed of the pump LC11: decrease of the rotational speed of the pump LC12: cycles of increase–decrease of the rotational speed of the pump LC13: start of the pump LC14: start and stop cycles of the pump

ND10						
Critical events (CEs)		CE6, CE7, CE8, CE9, CE10		CE6, CE7, CE8, CE9, CE10, CEa01	CE6, CE7, CE8, CE9, CE10	
Categories of Mechanisms of action		MA13: give rise to internal overpressure		MA16: increase in the liquid level (hold up)	MA13 + MA16: give rise to internal overpressure + increase in the liquid level (hold up)	
Mechanisms of action (MAs)		MA13.1: lock of the gas outlets	MA13.2: maximum opening of the inlet valves + lock of the gas outlets	MA16.1: more liquid flow at the inlet than at the outlet	MA13+16.1: lock of the gas outlets + more liquid flow at the inlet than at the outlet	MA13+16.2: maximum opening of the inlet valves + lock of the gas outlets + more liquid flow at the inlet than at the outlet
Combinations (CMs)		CM1, CM2 (Table D.1)	CM3, CM4 (Table D.1)	CM5 - CM8 (Table D.1)	CM9 - CM16 (Table D.1)	CM17 - CM24 (Table D.1)
Remotely manipulable components (RMCs)	SDV003	NM	NM	NM	NM	NM
	SDV004	NM	NM	LC2 or manipulation on LV002	LC2 or manipulation on LV002	LC2 or manipulation on LV002
	SDV005	NM	NM	NM	NM	NM
	SDV006	NM	NM	LC2 or manipulation on PA002A	LC2 or manipulation on PA002A	LC2 or manipulation on PA002A
	SDV007	LC2 or manipulation on PV003B	LC2 or manipulation on PV003B	NM	LC2 or manipulation on PV003B	LC2 or manipulation on PV003B
	BDV003	NM	NM	NM	NM	NM
	PV003A	LC2 or LC8	LC2 or LC8	NM	LC2 or LC8	LC2 or LC8
	PV003B	LC2/LC8 or manipulation on SDV007	LC2/LC8 or manipulation on SDV007	NM	LC2/LC8 or manipulation on SDV007	LC2/LC8 or manipulation on SDV007
	LV002	NM	NM	LC2/LC8 or manipulation on SDV004	LC2/LC8 or manipulation on SDV004	LC2/LC8 or manipulation on SDV004
	LV003	NM	LC7	NM	NM	LC7
	FV003	NM	LC7	NM	NM	LC7
	PA002A	NM	NM	LC5/LC11 or manipulation on SDV006	LC5/LC11 or manipulation on SDV006	LC5/LC11 or manipulation on SDV006
Active/Procedural safeguards (APSs)		PAH003, PAHH003, ZLL007, LSD logic activated by PSHH	PAH003, PAHH003, ZLL007, LSD logic activated by PSHH	PAH003, PAHH003, LAH002, LAHH005, LAH004, LAHH006, ZLL004, ZLL006, LSD logics activated by PSHH, interface LSHH and oil LSHH, UA unavailable	PAH003, PAHH003, LAH002, LAHH005, LAH004, LAHH006, ZLL004, ZLL006, ZLL007, LSD logics activated by PSHH, interface LSHH and oil LSHH, UA unavailable	PAH003, PAHH003, LAH002, LAHH005, LAH004, LAHH006, ZLL004, ZLL006, ZLL007, LSD logics activated by PSHH, interface LSHH and oil LSHH, UA unavailable
Inherent/Passive safeguards (IPSs)		PSV001, catch basin	PSV001, catch basin	PSV001, catch basin	PSV001, catch basin	PSV001, catch basin

Figura 8.1: Worksheet relativo al nodo ND10 (separatore trifase VS003) (Fonte:“ Major accidents triggered by malicious manipulations of the control system in process facilities” di Iaiani et al., 2021).

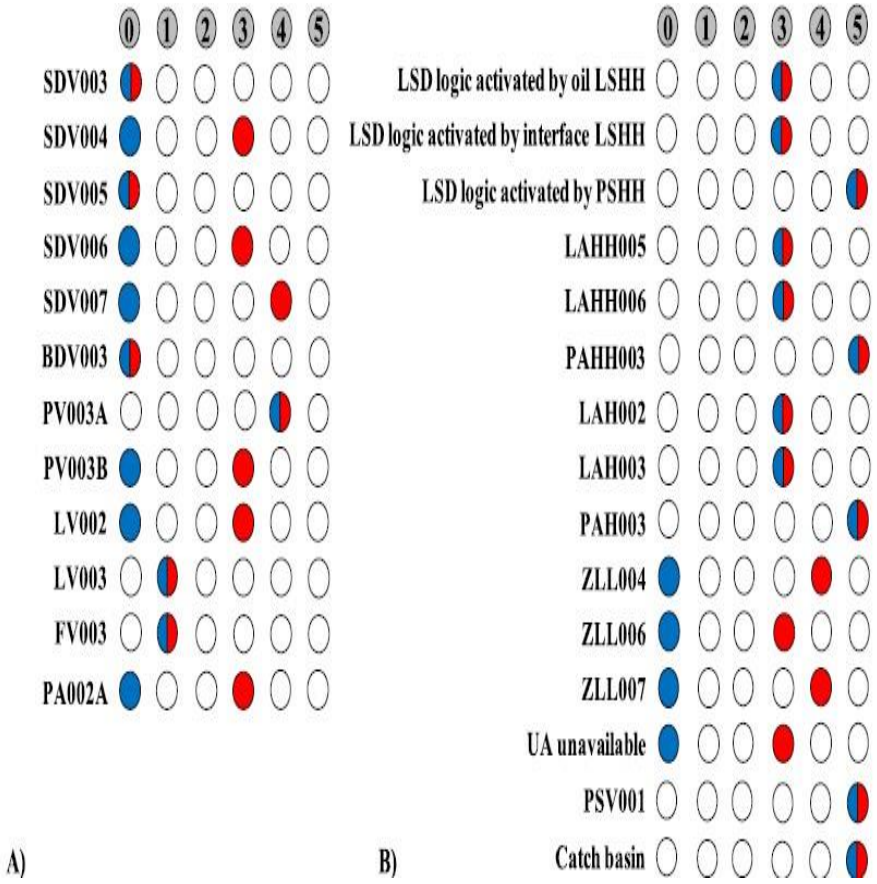


Figura 8.2: Criticità degli RMC e delle componenti di salvaguardia per le MA di ND10. Pannello A: numero minimo (colore blu) e numero massimo (colore rosso) di MA che comportano la manipolazione di ciascun RMC. Pannello B: numero minimo (colore blu) e numero massimo (colore rosso) di MA per le quali ciascuna componente di salvaguardia è efficace (Fonte:“ Major accidents triggered by malicious manipulations of the control system in process facilities” di Iaiani et al., 2021).

Critical event (CE)	MA category	Mechanism of action (MA)
CE5: start of fire	MA11 + MA6: addition of an oxidising substance to the system + give rise to a type of ignition	not feasible + not feasible
	MA11 + MA1: addition of an oxidising substance to the system + temperature increase	note feasible + not feasible
CE6: breach on the shell in vapour phase	MA13: give rise to internal overpressure	MA13.1: lock of the gas outlets
		MA13.2: external source of pressure (maximum opening of the inlet valves) + lock of gas the outlets
	MA16: increase in the liquid level (hold up)	MA16.1: more liquid flow at the inlet than at the outlet
	MA13 + MA16: give rise to internal overpressure + increase in the liquid level (hold up)	MA13+16.1: lock of the gas outlets + more liquid flow at the inlet than at the outlet
		MA13+16.2: external source of pressure (maximum opening of the inlet valves) + lock of the gas outlets + more liquid flow at the inlet than at the outlet
CE7: breach on the shell in liquid phase	same as for CE6	same as for CE6
CE8: leak from liquid pipe	same as for CE6	same as for CE6
CE9: leak from gas pipe	same as for CE6	same as for CE6
CE10: catastrophic rupture	same as for CE6	same as for CE6
CEa01: high liquid fraction in the gas outlet	MA16: increase in the liquid level (hold up)	MA16.1: more liquid flow at the inlet than at the outlet

Figura 8.3: Meccanismi di azione (MAs) identificati per ogni CE associato al nodo ND10. (Fonte:“ Major accidents triggered by malicious manipulations of the control system in process facilities” di Iaiani et al., 2021).

9. Commento dei risultati PHAROS

Se volessimo riassumere le considerazioni degli autori ottenuti sul caso studio, potremmo affermare che i CE causati da manipolazioni di tipo informatico siano: una breccia dell'involucro del sistema gas-liquido; una perdita dai condotti di gas o liquido; la rottura catastrofica del separatore trifase; l'alta frazione di gas in uscita. Più in generale, l'incremento della pressione interna si può ritenere come il MA generico che può condurre alle conseguenze precedentemente citate. Per quanto riguarda l'alta frazione di gas in uscita, la causa scatenante è prettamente il trabocco del separatore trifase.
Secondo quanto riportato nell'articolo dagli autori, "Nel caso studio analizzato, la valvola di regolazione PV003A risulta essere il componente più critico del sistema, in quanto deve essere manipolato in quattro delle cinque MA identificate. La valvola di spurgo BDV003 e le valvole di intercettazione SDV003 e SDV005 risultano essere le RMC meno critiche in quanto non necessitano di manipolazione per alcuna MA. Altri componenti (ad es. SDV004) possono far parte di molte MA che portano a un CE (cioè un punteggio massimo elevato), ma la loro protezione non può essere considerata prioritaria in quanto esistono sempre RMC alternativi che possono essere manipolati ottenendo gli stessi effetti. […] Gli aggressori non hanno sempre bisogno di influenzare entrambi i sistemi (BCPS o SIS) per essere in grado di impartire con successo le manipolazioni necessarie. […] Pertanto, si può concludere che in una configurazione standard, i componenti fisici possono essere in linea di principio manipolati generando eventi critici solo utilizzando il BPCS.
Tuttavia, per condurre con successo un attacco che provochi un evento critico sulle apparecchiature di processo, gli aggressori devono anche aggirare le misure di sicurezza in atto. Se sono presenti garanzie attive e/o procedurali, ciò richiede di manipolare anche il SIS oltre al BPCS. Questo fatto è a favore della sicurezza, essendo il BPCS e il SIS tipicamente separati l'uno dall'altro nell'architettura di rete IT-OT. "
Come può essere notato dall'ultima frase, è importante che nell'architettura di rete i due sistemi vengano separati di modo che la compromissione di uno da parte di un attacco non abbia necessariamente ripercussioni sull'altro.
Lo studio mette in luce l'intera cascata di eventi dall'attacco alle massime possibili conseguenze, come a voler dimostrare "l'effetto domino" di ogni caso individuato nell'identificazione dei rischi. La metodologia appare efficace e sistematica, nonostante non sia stata approfondita la parte di probabilità di accadimento degli eventi (un lavoro che, effettivamente, esulava dagli intenti degli autori). L'intenzione di questo studio, seppure con metodi di analisi del rischio differenti, è continuare sulla scia del lavoro di Iaiani et al. con l'obiettivo di arrivare ad un'analisi il più completa possibile lungo tutte le fasi della valutazione dei rischi.

10. Analisi costi-benefici

Riguardo l'aspetto economico e rimarcando l'enfasi sulla produzione efficiente/soddisfazione del cliente, la sicurezza informatica sta diventando una condizione per l'acquisto, un fondamentale prerequisito dell'impegno aziendale nei vari rami dell'industria.
Per sostenere ulteriormente l'idea di rafforzare la difesa dei sistemi di controllo e di sicurezza industriali attraverso delle adeguate contromisure informatiche, si intende riportare una breve analisi economica per evidenziare il rapporto costi-benefici nella scelta di tali interventi. Ovviamente tale analisi è solo approssimativa, in quanto uno studio approfondito richiederebbe una moltitudine di dati relativi al separatore e/o alle restanti parti dell'impianto di cui non si ha alcuna conoscenza a riguardo. Inoltre, le analisi economiche sono sempre basate sulle scelte di modelli teorici che potrebbero anche essere fin troppo complicati per essere inseriti all'interno di una tesi ingegneristica, pur essendo questa almeno trasversalmente correlata al mercato economico. Conseguentemente, si è scelto di ricorrere a degli esempi di letteratura.
Innanzitutto, è opportuno tenere a mente che l'ottimizzazione di un processo industriale dipende anche dai valori di setpoint delle diverse variabili (temperatura, pressione, portata, composizione chimica etc.), i quali devono essere mantenuti pressoché costanti dall'azione dei loop di controllo connessi alle varie apparecchiature. Secondo quanto riportato in "The economical aspects of control loop performance measures in the remote maintenance center concept" di Vatanski et al., 2004, poiché il numero di personale viene continuamente ridotto (perché sostituito da sistemi automatici), ma le prestazioni devono essere migliorate, le aziende utilizzano, in misura sempre maggiore, una gamma di servizi di esperti remoti per la valutazione delle prestazioni del circuito di controllo. La manutenzione remota può essere un modo semplice ed efficace per aumentare la redditività, pur tuttavia scontrandosi con le eventuali proteste di coloro che vengono rimpiazzati dalle macchine.
La valutazione delle prestazioni del circuito di controllo mediante centri esperti remoti è di solito più conveniente, poiché la valutazione delle prestazioni richiede spesso conoscenze di base e formazione costanti, che il personale dell'impianto non sempre possiede. In questi centri remoti gli esperti utilizzano una serie di strumenti per la valutazione delle prestazioni del circuito di controllo. Questi strumenti di solito utilizzano misure delle prestazioni del circuito di controllo nella valutazione delle prestazioni. Esistono già diverse misure delle performance del circuito di controllo e ne sono in fase di sviluppo di nuove per il monitoraggio a ciascun livello della "piramide" del sistema di automazione.
Generalmente, la valutazione delle prestazioni dei loop di controllo si basa sull'assegnazione di specifici indici, che secondo quanto riportato sono assegnati in tre differenti situazioni: uno attraverso la valutazione di uno stato dopo aver applicato una modifica del setpoint, uno valutato trascurando i disturbi del carico e uno in stato di funzionamento normale prossimo alle condizioni di stato stazionario. È possibile considerare ogni indice come indipendente l'uno dall'altro. Gli indici di prestazione potrebbero essere utili per constatare che le prestazioni dei circuiti di controllo siano state effettivamente migliorate o che ci siano possibilità di miglioramento. Tuttavia, tali indici del circuito di controllo avrebbero un valore aggiunto se potessero essere collegati più chiaramente a considerazioni economiche. Poiché le misure delle performance di controllo sono matematiche, questa connessione aiuterebbe anche il personale dell'impianto nell'interpretazione degli indici. È necessario allora un metodo di analisi dei costi-benefici per collegare i valori degli indici di performance con l'economia del processo.
Si riporta a titolo di esempio un insieme di dati relativo all'analisi economica di un separatore trifase. Si osservi la notevole quantità di dati immessi dagli autori dello studio, relativi alla geometria del separatore ed ai suoi costi capitali e/o operativi.

Fluid Properties	Gas	Oil	Water
Flow rate (m^3/hr)	5400	100	5
Density (kg/m^3)	1.225	850	1000
Viscosity (kg/m-s)	1.7894e-05	0.046	0.001

Variable	Symbol	Value
Norsok Residence Time	Δt_{Nor}	30 Seconds
Norsok Residence Height	Δh_{Nor}	0.10m
Safety Height	Δh_s	0.175m
Density of Steel	ρ_s	7850 kg/m^3
Separator Inlet Length	L_i	0.10m
Cost Factor for Vessel Shell	F_c	5$/kg
Joint Efficiency	E	1
Corrosion Allowance	t_c	0.0032
Tensile Strength	σ	950×10^5
Length of Oil Weir	L_{weir}	0.01

Figura 10.1: Esempio di dati necessari per un'analisi economica di un separatore trifase (Fonte: "Design and capital cost optimisation of three-phase gravity separators", Tariq Ahmed et al.,2020)

Come anche riportato nell'articolo "Design and capital cost optimisation of three-phase gravity separators", (Tariq Ahmed et al.,2020), il modo più semplice per ottenere il costo capitale di un'apparecchiatura industriale sarebbe moltiplicare le dimensioni dell'attrezzatura per il costo per unità di dimensioni indicato dai fornitori. I costi per unità di dimensione, che tengono conto non solo della geometria ma anche dei materiali costituenti e dei valori di pressione o temperatura di servizio, possono anche essere presi da letteratura in forma di grafici o diagrammi. Tuttavia, tale valore sarebbe un'approssimazione alquanto grossolana.
A tutti gli effetti, quello che è necessario risolvere per un valore più accurato è un problema di ottimizzazione, per minimizzare il costo finale del separatore in funzione dei costi capitali e tenendo conto anche dei vincoli da imporre a seconda del progetto.
Nello studio di Tariq Ahmed et al., a causa della non linearità sia nella funzione obiettivo che nei vincoli, è stato scelto l'algoritmo del cosiddetto gradiente ridotto generalizzato (GRG) per ottimizzare il design del separatore. Questo metodo si è dimostrato efficace ed efficiente per tali problemi, con un'accettabile onerosità di costo computazionale. Il concetto di base di GRG prevede la linearizzazione delle funzioni obiettivo e dei vincoli non lineari in una soluzione locale con l'espansione in serie di Taylor.
I risultati mostrati in Figura 10.2, pur essendo solo un esempio, sono comunque basati sui valori medi di produzione di acqua, olio e gas (vedasi diagramma giornaliero sottostante).

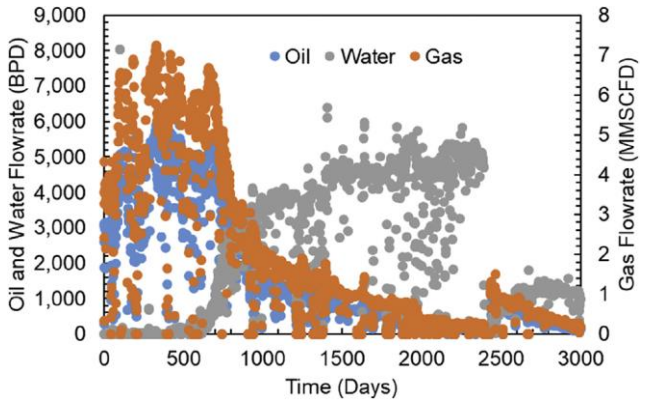


Figura 10.2: dati relativi alla produzione giornaliera di acqua, olio e gas (Fonte: "Design and capital cost optimisation of three-phase gravity separators", Tariq Ahmed et al.,2020)

Variable	Symbol	Value
Separator Cost	C	£33,685
Separator Internal Diameter	Di	1.48m
Separator Length	VL	7.35m
High-High Liquid Level	h_{HHLL}	0.90m
High Liquid Level	h_{HLL}	0.82m
Normal Operating Level	h_{NOL}	0.74m
Low Liquid Level	h_{LLL}	0.66m
Low-Low Liquid Level	h_{LLLL}	0.58m
Weir Height	h_{Wr}	0.57m
High-High Interface Level	h_{HHIL}	0.53m
High Interface Level	h_{HIL}	0.45m
Normal Interface Level	h_{NIL}	0.37m
Low Interface Level	h_{LIL}	0.29m
Low-Low Interface Level	h_{LLIL}	0.21m
Diameter of Gas Outlet	dng	0.744m
Diameter of Oil Outlet	dno	0.14m
Diameter of water outlet	dnw	0.07m
Seam to Seam Length	LT	7.36m
Shell Thickness	tcs	0.01m
Separator Diameter	D	1.17m

Figura 10.3: esempio di risultato numerico dell'analisi economica di un separatore trifase (Fonte: "Design and capital cost optimisation of three-phase gravity separators", Tariq Ahmed et al.,2020)

Dall'analisi è stato stimato come costo finale un valore pari a 33685 sterline (circa 38700 euro). Proviamo a ipotizzare che questo sia indicativamente il prezzo del nostro separatore VS003. Consideriamo ora che sul mercato gli elementi di un loop di controllo costino 35 euro ciascuno (da intendersi come prezzo medio ottenuto ricercando trasmettitori, controllori etc. da vari siti di compravendita online, confrontati per mezzo di Google). Ogni loop presenta quantomeno un indicatore connesso allo strumento di misura, un trasmettitore, un trasduttore ed un controllore che esegue l'azione necessaria a mantenere il setpoint della variabile desiderato. Considerando che nel separatore VS003 sono presenti 5 loop di controllo più gli elementi di sicurezza quali allarmi e valvole di shutdown, immaginiamo di aumentare il prezzo iniziale stimato di un ulteriore 5-10% per gli elementi di controllo e un 5-10% per gli elementi di sicurezza necessari eventualmente per un Emergency Shutdown. Arriviamo così ad ottenere una stima nel range di 42570-46440 euro. Ora, consideriamo i prezzi che in genere sono necessari per l'acquisto di sistemi di antivirus e di autenticazione multipla: in genere l'abbonamento annuale di un antivirus si aggira attorno ad alcune decine di euro all'anno (anche qui si vedano semplicemente i siti delle aziende informatiche che offrono tali servizi come Norton, Avast…), mentre i sistemi di autenticazione multipla possono costare anche alcune centinaia di euro. Si potrebbe allora stimare un'ulteriore spesa del 5-10% del prezzo totale del separatore per i sistemi di sicurezza informatici, ipotizzando di installare un blocco con autenticazione multipla per poter manipolare da remoto o in situ i loop di controllo e/o un sistema di blocco con password digitale o meglio ancora con un sistema di scansione della retina oculare o del palmo della mano.
Pur senza disporre di tutti i dati necessari, risulta evidente che l'aggiunta di sistemi contro le possibili cyberminacce è un sovraprezzo assolutamente piccolo rispetto ai normali costi di un'apparecchiatura industriale e soprattutto molto più basso sia in termini economici sia umanitari del valore di perdita economica che può conseguire da un cyberattacco.
Ovviamente è necessario anche dover considerare le spese di assunzione di tecnici informatici per il monitoraggio e la manutenzione dei sistemi di autenticazione che siano di supporto agli esperti delle squadre di controllo dell'impianto, anche fornendo loro un'adeguata formazione sulle competenze basilari necessarie per l'utilizzo di tali sistemi.

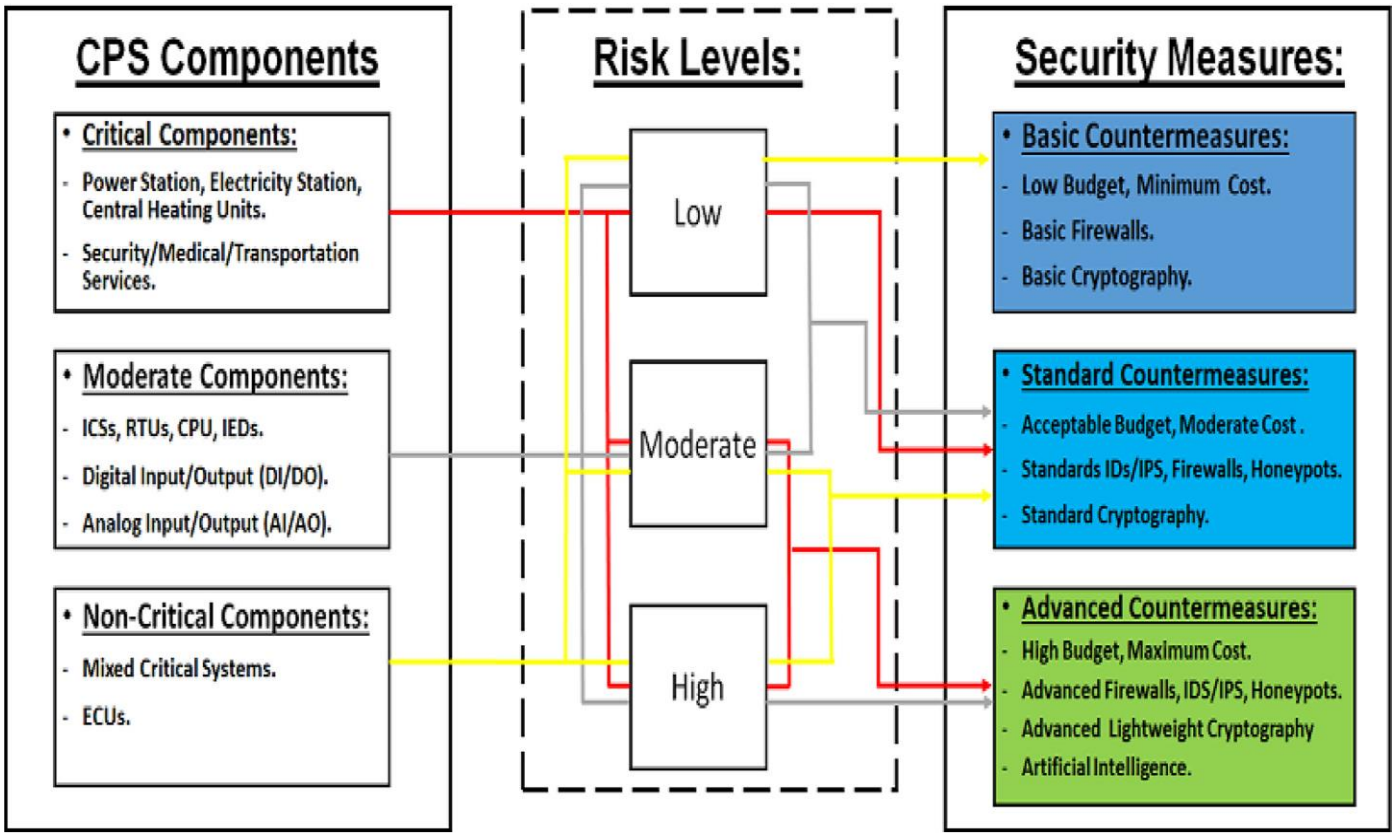


Figura 10.4: Classificazione dei componenti CPS, protezione e budget necessario (Fonte: "Cyber-physical systems security: Limitations, issues and future trends, Jean-Paul A. Yaacoub et al., 2020)

11. Analisi HAZOP e FTA

Prima di procedere ulteriormente, si riportano alcune nozioni fondamentali concernenti le analisi HAZOP ricorsiva ed FTA.
La metodologia di analisi di pericolo e operabilità (o HAZOP, dall'inglese HAZard and OPerability analysis), ha lo scopo di esaminare gli ambienti di lavoro per identificarne i pericoli a cui potrebbe essere esposto il personale operativo in tali ambienti. È una delle tecniche più diffuse e largamente adottate anche dagli Enti di Normazione Nazionali. Questa metodologia è spesso affiancata all'uso di altre tecniche come la "What-if" o l'uso delle cosiddette Check-list, che integrandosi con la HAZOP la approfondiscono ulteriormente. È bene ricordare che tali tecniche prevedano spesso un lavoro di gruppo, dove vari esperti del settore e dell'impianto analizzato discutono a proposito di quanto poi verrà considerato. La HAZOP risulta molto efficace quando si è in grado di unire la conoscenza degli esperti ingegneristici con le esperienze di coloro che operano da tempo all'interno dell'impianto studiato. All'interno di questo studio, viene utilizzata la variante ricorsiva del metodo HAZOP, che prevede l'utilizzo di una tabella come quella mostrata di seguito.

ANALISI DI OPERABILITA' RICORSIVA **Variabile di processo: livello nel serbatoio**

DEVIAZIONE	CAUSE	CONSEGUENZE	SEGNALAZIONI OTTICHE O ACUSTICHE	MEZZI PROTETTIVI AUTOMATICI	TE
Alto livello	Bassa portata in uscita	Altissimo livello	Allarme da A1		
Altissimo livello	Alto livello	Traboccamento	Allarme da A2	hLS (sistema di blocco V-3)	1
Bassa portata in uscita	M.F. regolazione M.F. pompa Tappo in linea *	Alto livello			
M.F. regolazione	V-2 chiusa * M.F. T-1 * M.F. LRC * M.F. V-1 *	Bassa portata in uscita			
M.F. pompa P	P guasta * Manca E.E. *	Bassa portata in uscita			

Figura 11.1: Esempio Hazop ricorsiva (Fonte immagine: "Valutazione dei rischi – parte 3", Micaela Demichela, corso di Tecnica della Sicurezza Ambientale, Politecnico di Torino 2022)

Le iterazioni proseguono fino ad identificare il Top Event (TE), cioè la massima conseguenza possibile. Muovendo ora l'attenzione sull'analisi FTA, la Fault Tree Analysis è un tipo di analisi dei guasti in cui viene esaminato uno stato indesiderato di un sistema. Viene utilizzato principalmente nell'ingegneria della sicurezza e nell'ingegneria dell'affidabilità per capire come i sistemi possano guastarsi, per identificare i modi migliori per ridurre il rischio e per stimare le probabilità di accadimento di eventi di un incidente di sicurezza o di un particolare guasto a livello di sistema. L'analisi FTA può essere realizzata, come avviene in tale studio, partendo dal TE risultato dalla HAZOP ricorsiva, andando quindi a ramificare tutte le cause da cui deriva fino ad arrivare alle cause primarie. Ne verrà fuori un diagramma ad albero, dove i "rami" sono fra di loro collegati attraverso delle porte con logica booleana. Ogni ramo

è un evento o un insieme di eventi con una certa probabilità di accadimento. Le operazioni sui valori probabilistici sono espresse dal tipo di logica booleana con cui i vari eventi sono connessi.
All'interno di questo studio, le analisi sono state prima applicate al separatore trifase VS003 senza considerare gli aspetti di cybersicurezza (né protezioni né minacce), che verranno considerate solo in seguito all'ottenimento di risultati soddisfacenti nelle HAZOP e nelle FTA dei 4 casi analizzati.
Per i valori di tassi di guasto **λ** (espressi in 1/anni), sono state considerate le tabelle fornite dalla prof. Demichela durante il suo corso di studi di Tecnica della Sicurezza Ambientale e quelle nel documento "Idaho Chemical Processing Plant Failure Rate, 1995", anche consultato nella tesi di Mohammad (2018). Inoltre, dall'articolo "COMPARISON OF METHODOLOGIES FOR THE SAFETY AND DEPENDABILITY ASSESSMENT OF AN INDUSTRIAL PROGRAMMABLE LOGIC CONTROLLER" (Andrea Bobbio et al., 2001) è stato considerata una formula per correggere i valori dei tassi di guasto succitati quando le stesse deviazioni sono state analizzate anche tenendo conto delle cyberminacce.
Le analisi sono state basate su 4 diverse deviazioni possibili nel sistema, due relative al livello di liquido e due relative al valore di pressione del serbatoio. In tutto, lo studio riporta 8 HAZOP e 8 diagrammi FTA per il calcolo di probabilità di accadimento degli eventi. Le FTA tuttavia sono presenti solo all'interno degli allegati ausiliari. Di seguito alcune considerazioni effettuate per lo svolgimento dei calcoli.

- Tempo di missione considerato: 1 anno
- Indisponibilità U per valvole shutdown considerato pari a 0.044 anni^{-1} (su tabelle dei tassi di guasto utilizzate, si veda la dicitura "XV: mancato intervento valvola di blocco")
- Le valvole di shutdown sono state considerate come operanti in parallelo
- Indisponibilità **U** per le valvole di blowdown è stato considerato pari a Indisponibilità delle PSV
- Tempo di test considerato: 6 mesi

Per i componenti ove necessario applicare il tempo di test si ricordi che (θ è il tempo di test).:

$$U = \lambda * \frac{\theta}{2} \tag{11.1}$$

Il tempo di test era stato inizialmente impostato ad un anno (valore di default del software utilizzato), ma è stato poi ridotto a 6 mesi che è ritenuto essere un valore piuttosto diffuso.
Nello svolgimento dei calcoli, i valori delle stesse tipologie di strumenti sono da considerarsi uguali per categoria (ad esempio, ogni LIC oppure ogni LT avrà lo stesso valore di lambda nel calcolo dei valori di inaffidabilità R).
In alcuni file relativi alle FTA, sono state aggiunte delle porte OR con eventi con probabilità pari a zero per risolvere alcuni inconvenienti che "sulla carta" non sarebbero comparsi. Ad esempio, il passaggio da una variabile di processo ad un'altra nella HAZOP viene nel parallelo file FTA sviluppato come una porta OR con un ramo nullo e l'altro ramo contenente tutto lo sviluppo successivo dell'analisi.
Da un primo tentativo di stesura dell'albero, secondo anche quanto imparato a lezione, i valori di probabilità di accadimento dei TE in tutti i casi risultano essere troppo elevati per un impianto considerato a norma di legge Seveso. Un primo approccio per ridurre tali valori numerici potrebbe essere il seguente: sul calcolo delle indisponibilità relativi ai loop di controllo, utilizzare dei sistemi a logica maggioritaria (ad esempio 2oo3). Sono stati immediatamente osservati miglioramenti nei risultati.
Nella seconda iterazione di calcolo, per quanto concerne la deviazione "Basso livello di liquido", è stata ignorata la condizione "bassa portata <6>" perché ritenuta sufficientemente improbabile e poco incisiva sull'effettivo valore del risultato finale del TE. Ciononostante, un problema presentatosi più di una volta è l'effettiva probabilità finale di una delle cause scatenanti del TE con valore maggiore di 1. Tale problematica è dovuta al fatto che si sta comunque utilizzando un metodo di calcolo approssimativo e dei dati numerici in input intrinsecamente approssimati. Le iterazioni hanno anche lo scopo di migliorare la precisione dei calcoli affinché questo non accada, sia perché matematicamente impossibile sia perché indice di una sconsiderata leggerezza nella realizzazione dei sistemi studiati.

Tabella 11.1: HAZOP relativa alla deviazione “Alta pressione” trascurando le cyberminacce

Deviazioni	Cause	Conseguenze	Allarmi	Protezioni	Top Event	Note
Alta pressione VS003	Guasto PV003A* Guasto PV0003B* Guasto PT002* Guasto PT003* Guasto PIC003*	Alta alta pressione VS003	PAHH003	BDV003		
Alta alta pressione VS003	Alta pressione VS003	Scoppio separatore		PSV001 SDV007	1	

Tabella 11.2: HAZOP relativa alla deviazione “Bassa pressione” trascurando le cyberminacce

Deviazioni	Cause	Conseguenze	Allarmi	Protezioni	Top Event	Note
Bassa pressione VS003	Guasto* PV003A Guasto PV0003B* Bassa portata <1> Bassa portata <2> Alta portata <6> Alta portata <7> Alta portata <8> Guasto logica maggioritaria su controllo pressione*	Bassa Bassa pressione VS003	PALL003	BDV003		
Bassa Bassa pressione VS003	Bassa pressione VS003	Implosione per “accartocciamento” di VS003		SDV006 SDV004 SDV003 SDV007	2	
Bassa portata <1>	Guasto LV003* Guasto LIC003*	Bassa pressione VS003				

Bassa portata <2>	Guasto FV003* Guasto FIC003* Guasto logica maggioritaria su controllo pressione*	Bassa pressione VS003				
Alta portata <6>	Guasto PV003B*	Bassa pressione VS003				
Alta portata <7>	Blocco in apertura LV002*	Bassa pressione VS003				
Alta portata <8>	MF PA002A	Bassa pressione VS003				
MF PA002A	Mancato apporto corrente* Pompa rotta o bloccata*	Bassa pressione VS003				

Tabella 11.3: HAZOP relativa alla deviazione "Alto livello di liquido" trascurando le cyberminacce

Deviazioni	Cause	Conseguenze	Allarmi	Protezioni	Top Event	Note
Alto livello liquido VS003	Alta portata <1> Alta portata <2> Alta portata <6> Bassa portata <7> Bassa portata <8> Guasto LT002* Guasto LT004* Guasto LT005* Guasto LT006* Guasto LIC002*	Alto alto livello liquido VS003	LAHH005 LAHH006			Ho considerato che gli allarmi si attivino contemporaneamente

	Guasto LIC 004*					
Alto alto livello liquido VS003	Alto livello liquido VS003	Trabocco fase liquida		SDV003 SDV004 SDV006	3	
Alta portata <1>	Guasto LV003* Guasto LIC003*	Alto livello liquido VS003				
Alta portata <2>	Guasto FV003* Guasto FIC003*	Alto livello liquido VS003				
Alta portata <6>	Guasto logica maggioritaria su controllo pressione* Guasto PV003B*	Alto livello liquido VS003				
Bassa portata <7>	Guasto LV002* Guasto LIC002*	Alto livello liquido VS003				
Bassa portata <8>	MF PA002A	Alto livello liquido VS003				
MF PA002A	Mancato apporto corrente* Pompa rotta o bloccata*	Alto livello liquido VS003				

Tabella 11.4: HAZOP relativa alla deviazione "Basso livello di liquido" trascurando le cyberminacce

Deviazioni	Cause	Conseguenze	Allarmi	Protezioni	Top Event	Note
Basso livello liquido VS003	Bassa portata <1> Bassa portata <2>	Basso basso livello liquido VS003		LALL005 LALL006		Ho considerato che gli allarmi si attivino contemporaneamente

	Bassa portata <6> Alta portata <7> Alta portata <8> Guasto LT002* Guasto LT004* Guasto LT005* Guasto LT006* Guasto LIC002 * Guasto LIC 004*					
Basso basso livello liquido VS003	Basso livello liquido VS003	Bassa pressione VS003				
Bassa pressione VS003	Basso basso livello liquido VS003	Bassa bassa pressione VS003	PALL003			
Bassa bassa pressione VS003	Bassa pression e VS003	Implosione per “accartocciamento” VS003		SDV006 SDV004 SDV003	2	
Bassa portata <1>	Guasto LV003* Guasto LIC003 *	Basso livello liquido VS003				
Bassa portata <2>	Guasto FV003* Guasto FIC003 *	Basso livello liquido VS003				
Alta portata <7>	Blocco in	Basso livello liquido VS003				

	apertura LV002*					
Alta portata <8>	MF PA002 A	Basso livello liquido VS003				
MF PA002A	Mancato apporto corrente * Pompa rotta o bloccata *	Basso livello liquido VS003				

In tutto, sono state eseguite 3 iterazioni prima di giungere ai risultati di Tabella 11.5.

Tabella 11.5: Risultati analisi FTA trascurando le cyberminacce

Top Event	Deviazione	Probabilità di accadimento TE (3°tentativo FTA, 1/anni)
Scoppio separatore VS003	Alta pressione	2.22923e-07
Trabocco fase liquida	Alto livello di liquido	7.89955e-05
Implosione "per accartocciamento" VS003	Bassa pressione	2.07686e-05
Implosione "per accartocciamento" VS003	Basso livello di liquido	3.15974e-04

Dopo il 3°tentativo, avendo ottenuto valori relativamente accettabili per i TE, gli stessi casi sono stati analizzati tenendo anche conto delle cyberminacce. Ora è quindi necessario trovare i valori corretti di failure rate da applicare nei nuovi diagrammi cFTA. Come primo approccio, l'idea è stata di sommare manualmente ai normali valori di failure rate per i vari controllori un contributo di 0.1 (su base annua), come se effettivamente si considerasse che il guasto avvenga o per le cause che concernono il generico valore di failure rate da letteratura o per un cyberattacco con tasso pari a quello di cui sopra. Quest'ultimo valore è stato preso dalla tesi "RISK ASSESSMENT IN OIL AND GAS INDUSTRY WITH RESPECT TO CYBERSECURITY di Moin Mohammad, 2018. Nelle analisi comprendenti gli aspetti di cybersecurity, è stato inoltre innalzato il valore del fattore di errore umano a 1e-02. È ritenuto in effetti più probabile il verificarsi di un errore umano in ambito cybersicurezza.
La definizione dei sistemi di sicurezza contro i cyberattacchi si è basata su alcune considerazioni, ragionate anche su quanto trovato in letteratura e riportato nella cronologia dei cyberattacchi. È stato considerato opportuno, anche per semplicità sui calcoli, ritenere che le tre categorie più gettonate di cyberattacchi siano phishing, hacking forzato dei sistemi per mezzo del bypass dell'antivirus o decrittazione delle password. In ognuno dei tre casi, è ragionabile credere che l'hacker sia in grado di violare il firewall/antivirus del sito di produzione oppure che riesca ad ottenere l'autenticazione per manipolare i sistemi di controllo o di sicurezza a cui normalmente non avrebbe modo di accedere. Nello studio in questione, si ritiene che siano gli elementi di controllo quelli più facilmente accessibili e alterabili una volta violate le difese informatiche.

Si ritiene tuttavia necessario ribadire l'importanza di alcuni requisiti fondamentali, come anche citato nell'articolo "Cyber-physical systems security: Limitations, issues and future trends" (Yaacoub et al, 2020):

1. **Autenticazione avanzata del dispositivo/utente:** è necessario un efficiente schema di autenticazione a più fattori reciproca dispositivo/utente, oltre a migliorare le fasi di verifica e identificazione basate sui privilegi di controllo dell'accesso agli attributi (privilegio minimo) per garantire il non ripudio e una maggiore responsabilità.
2. **Protezione delle prove digitali:** questo è molto importante poiché la maggior parte degli attacchi avanzati si concentra sull'eliminazione di qualsiasi fonte di prova che risalga alla fonte dell'attacco.
3. **Miglioramento della politica di sicurezza:** in molti casi, gli attacchi ai sistemi CPS si sono verificati da addetti ai lavori (per caso o di proposito). Di conseguenza, tutti i dipendenti devono sottoporsi a un processo di screening prima dell'assunzione, e i loro privilegi devono essere sospesi al di fuori dell'orario di lavoro e monitorate le loro azioni in caso di compiti avanzati. Ciò significa che la politica di sicurezza del CPS dovrebbe contenere nuove regole per limitare l'accesso e ridurre i potenziali danni

È altrettanto importante constatare che i sistemi di sicurezza come il firewall o gli antivirus citati nell'analisi non sono stati pensati come peculiari per il processo, ma più come sistemi versatili applicabili a casi anche simili a quello analizzato. Conseguentemente, per ottimizzare l'effettiva protezione fornita al nostro sistema, si dovrebbe tenere conto di ulteriori dettagli correlati al serbatoio VS003 e/o alle specifiche di processo che purtroppo non sono disponibili.

Tabella 11.6: HAZOP relativa alla deviazione "Alta pressione" integrando le cyberminacce

Deviazioni	Cause	Conseguenze	Allarmi	Protezioni	Top Event	Note
Alta pressione VS003	Guasto PV003A* Guasto PV0003B* Guasto PT002 Guasto PT003 Guasto PIC003	Alta alta pressione VS003	PAHH003	BDV003		
Alta alta pressione VS003	Alta pressione VS003	Scoppio separatore		PSV001 SDV007 Protezioni informatiche	1	
Guasto PT002	Cyberattacco*	Alta pressione VS003				
Guasto PT003	Cyberattacco*	Alta pressione VS003				
Guasto PIC003	Cyberattacco*	Alta pressione VS003				

Tabella 11.7: HAZOP relativa alla deviazione “Bassa pressione” integrando le cyberminacce

Deviazioni	Cause	Conseguenze	Allarmi	Protezioni	Top Event	Note
Bassa pressione VS003	Guasto PV003A* Guasto PV0003B* Bassa portata <1> Bassa portata <2> Alta portata <6> Alta portata <7> Alta portata <8> Guasto PT002 Guasto PT003 Guasto PIC003	Bassa Bassa pressione VS003	PALL003	BDV003		
Bassa Bassa pressione VS003	Bassa pressione VS003	Implosione per “accartocciamento” di VS003		SDV006 SDV004 SDV007 Protezioni informatiche	2	
Bassa portata <1>	Guasto LV003 Guasto LIC003	Bassa pressione VS003				
Bassa portata <2>	Guasto FV003 Guasto FIC003	Bassa pressione VS003				
Alta portata <6>	Guasto PV003B* Guasto PIC003* Guasto PT002	Bassa pressione VS003				
Alta portata <7>	Blocco in apertura LV002	Bassa pressione VS003				
Alta portata <8>	MF PA002A	Bassa pressione VS003				

MF PA002A	Mancato apporto corrente* Pompa rotta o bloccata*	Bassa pressione VS003				
Guasto PT002	Cyberattacco*	Bassa pressione VS003				
Guasto PT003	Cyberattacco*	Bassa pressione VS003				
Guasto PIC003	Cyberattacco*	Bassa pressione VS003				
Guasto LV003	Cyberattacco*	Bassa pressione VS003				
Guasto LIC003	Cyberattacco*	Bassa pressione VS003				
Guasto FV003	Cyberattacco*	Bassa pressione VS003				
Guasto FIC003	Cyberattacco*	Bassa pressione VS003				

Tabella 11.8: HAZOP relativa alla deviazione "Alto livello di liquido" integrando le cyberminacce

Deviazioni	Cause	Conseguenze	Allarmi	Protezioni	Top Event	Note
Alto livello liquido VS003	Alta portata <1> Alta portata <2> Alta portata <6> Bassa portata <7> Bassa portata <8> Guasto LT002 Guasto LT004 Guasto LT005 Guasto LT006 Guasto LIC002 Guasto LIC 004	Alto alto livello liquido VS003	LAHH005 LAHH006			Ho considerato che gli allarmi si attivino contemporaneamente

Alto alto livello liquido VS003	Alto livello liquido VS003	Trabocco fase liquida		SDV003 SDV004 SDV006 Protezioni informatiche	3	
Alta portata <1>	Guasto LV003 per cyberattacco * Guasto LIC003 per cyberattacco *	Alto livello liquido VS003				
Alta portata <2>	Guasto FV003 per cyberattacco * Guasto FIC003 per cyberattacco *	Alto livello liquido VS003				
Alta portata <6>	Guasto PV003B*	Alto livello liquido VS003				
Bassa portata <7>	Guasto LV002	Alto livello liquido VS003				
Guasto LV002	Guasto LIC002* Blocco LV002 in chiusura*	Alto livello liquido VS003				
Bassa portata <8>	MF PA002	Alto livello liquido VS003				
MF PA002	Mancato apporto corrente* Pompa rotta o bloccata*	Alto livello liquido VS003				
Guasto LT002	Cyberattacco*	Alto livello liquido VS003				

Guasto LT004	Cyberattacco*	Alto livello liquido VS003				
Guasto LT005	Cyberattacco*	Alto livello liquido VS003				
Guasto LT006	Cyberattacco*	Alto livello liquido VS003				
Guasto LIC002	Cyberattacco*	Alto livello liquido VS003				
Guasto LIC004	Cyberattacco*	Alto livello liquido VS003				

Tabella 11.9: HAZOP relativa alla deviazione "Basso livello di liquido" integrando le cyberminacce

Deviazioni	Cause	Conseguenze	Allarmi	Protezioni	Top Event	Note
Basso livello liquido VS003	Bassa portata <1> Bassa portata <2> Bassa portata <6> Alta portata <7> Alta portata <8> Guasto LT002 Guasto LT004 Guasto LT005 Guasto LT006 Guasto LIC002 Guasto LIC 004	Basso basso livello liquido VS003		LALL005 LALL006		Ho considerato che gli allarmi si attivino contemporaneamente
Basso basso livello liquido VS003	Basso livello liquido VS003	Bassa pressione VS003				

Bassa pressione VS003	Basso basso livello liquido VS003	Bassa bassa pressione VS003	PALL003			
Bassa bassa pressione VS003	Bassa pressione VS003	Implosione per "accartocciamento" VS003		SDV006 SDV004 SDV007 Protezioni informatiche	2	
Bassa portata <1>	Guasto LV003* Guasto LIC003 per cyberattacco*	Basso livello liquido VS003				
Bassa portata <2>	Guasto FV003* Guasto FIC003 per cyberattacco*	Basso livello liquido VS003				
Alta portata <7>	Blocco in apertura LV002*	Basso livello liquido VS003				
Alta portata <8>	MF PA002A	Basso livello liquido VS003				
MF PA002A	Mancato apporto corrente* Pompa rotta o bloccata*	Basso livello liquido VS003				
Guasto LT002	Cyberattacco*	Basso livello liquido VS003				
Guasto LT004	Cyberattacco*	Basso livello liquido VS003				
Guasto LT005	Cyberattacco*	Basso livello liquido VS003				
Guasto LT006	Cyberattacco*	Basso livello liquido VS003				
Guasto LIC002	Cyberattacco*	Basso livello liquido VS003				
Guasto LIC004	Cyberattacco*	Basso livello liquido VS003				

Dai calcoli effettuati da primo tentativo si nota che i valori finali sono in alcuni casi accettabili, ma in tutti i casi si presenta in uno dei rami del diagramma un fattore con probabilità di accadimento pari o addirittura superiore al 100%. Pertanto, è necessario ripetere i calcoli per eliminare nuovamente tale problema.

Nella seconda iterazione dei calcoli sono state anche specificate le misure di sicurezza a livello informatico, riassunte in due contributi: protezione firewall/antivirus e autenticazione multipla, considerati da inserirsi in una porta AND, quindi contemporaneamente funzionanti sui sistemi da proteggere. Sempre ispirato dalla tesi di Moin Mohammad, il primo effettivo valore di indisponibilità considerato per entrambi i casi 1e-03. Il valore di 0.1 aggiunto manualmente al software non è stato rimosso durante questa iterazione di calcolo.

Tabella 11.10: risultati della prima iterazione dei calcoli di probabilità di accadimento TE con cyberminacce integrate

Top Event	Deviazione	Probabilità di accadimento TE (3°tentativo FTA + cyberminacce, 1/anni)	Indisponibilità sistemi informatici di sicurezza (1/anni)
Scoppio separatore VS003	Alta pressione	3.78261e-14	0.001
Trabocco fase liquida	Alto livello di liquido	1.09456e-11	0.001
Implosione "per accartocciamento" VS003	Bassa pressione	3.75575e-12	0.001
Implosione "per accartocciamento" VS003	Basso livello di liquido	1.17118e-12	0.001

I risultati sono fin troppo eccezionali e realisticamente improbabili da realizzare in un impianto odierno. Di conseguenza, è stato scelto un valore più opportuno usare dei tassi di guasto relativi alle protezioni informatiche. Il valore definitivo assegnato è pari a 0.1. Questo valore è stato scelto consultando i dati da letteratura, in particolare l'articolo "Detecting Account Takeovers and Defending Users" (www.signalssciences.com, consultato in data 8/2/2024). Tale articolo analizza i vari tassi di guasto nell'autenticazione di sistema, sia per dispositivi interni alla rete di servizio che esterni, cioè collegati in qualche maniera da remoto. Il valore considerato è pur sempre una stima poiché "il failure rate può spaziare largamente da industria ad industria, caso per caso".
Anche tenendo conto dell'aspetto cybersecurity, durante lo svolgimento dele iterazioni di calcolo si è optato per l'uso delle porte a logica maggioritaria ove ritenuto possibile. In effetti, così facendo si tiene anche conto dell'eventuale necessità di agire su multiple variabili di processo al fine di arrivare all'accadimento del TE, tenendo quindi in considerazione gli effetti "a catena" che un cyberattacco può provocare a differenti sistemi di controllo predisposti. Per esempio, affinché un intrusione vada a buon fine potrebbe essere necessario che essa violi sia i sistemi adibiti al controllo di livello che quelli adibiti al controllo della pressione di VS003.
A seguito dei risultati insoddisfacenti delle precedenti iterazioni, il passo successivo è stato correggere i valori dei canonici tassi di guasto tabulati tenendo anche conto dell'aspetto cybersicurezza.
La correzione prevede di aggiungere al valore usato in precedenza nei casi senza "senza cyberminacce" degli elementi ritenuti vulnerabili di cyberattacco (trasmettitore, controllori, indicatori) una somma di contributi descritti nella Tabella 11.11.

Tabella 11.11: tassi di guasto supplementari

λ supplementari	Failure rates ($anni^{-1}$)
λ_{DI}	2,4528e-03
λ_{CPU}	0,422232e-03
λ_{DO}	2,1462e-03
$\lambda_{I/O\ BUS}$	1,752e-05
λ_{Power}	2,95212e-03

Qual è il significato di ciascun tasso supplementare considerato?

- λ_{DI} ➔ Tasso di guasto relativo ad un eventuale errore nella trasmissione del segnale digitale in input nel sistema di controllo
- λ_{CPU} ➔ Tasso di guasto relativo ad un eventuale errore nell'elaborazione del segnale digitale da parte della CPU
- λ_{DO} ➔ Tasso di guasto relativo ad un eventuale errore nella trasmissione del segnale digitale in output dal sistema di controllo
- $\lambda_{I/O\ BUS}$ ➔ Tasso di guasto relativo ad un eventuale errore nella trasmissione del segnale digitale sul bus input/output. Si ricordi che "il bus (da una contrazione del latino *omnibus*), in elettronica e informatica, è un canale di comunicazione che permette a periferiche e componenti di un sistema elettronico - come ad esempio un computer - di interfacciarsi tra loro scambiandosi informazioni o dati di vario tipo attraverso la trasmissione e la ricezione di segnali" (Wikipedia)
- λ_{Power} ➔ Tasso di guasto relativo ad un eventuale errore nella trasmissione del segnale digitale a causa di mancanza di corrente

Un'ulteriore correzione applicata in quest'ultima iterazione è stata l'interpretazione delle protezioni informatiche, cioè come effettivamente esse agiscano sui sistemi da proteggere. L'idea applicata è stata ritenere che la protezione intervenga su tutti gli apparati dei sistemi di controllo e sicurezza (per chiarimenti si vedano i diagrammi FTA).
Nella tabella 11.12 si possono osservare i risultati finali.

Tabella 11.12: risultati finali dei calcoli di probabilità di accadimento TE con cyberminacce integrate

Top Event	Deviazione	Probabilità di accadimento TE (3°tentativo FTA + cyberminacce, 1/anni)	Indisponibilità sistemi informatici di sicurezza (1/anni)
Scoppio separatore VS003	Alta pressione	5.70356e-08	0.1
Trabocco fase liquida	Alto livello di liquido	9.94934 -07	0.1
Implosione "per accartocciamento" VS003	Bassa pressione	2.16496 -07	0.1
Implosione "per accartocciamento" VS003	Basso livello di liquido	3.87722-08	0.1

Tutti i risultati rispettano i termini della legge Seveso, essendo sotto a 10^{-6}. Inoltre, grazie alle cyberprotezioni i valori di accadimento dei TE sono stati ridotti di almeno un ordine di grandezza.

12. Commento dei risultati, conclusioni e confronto con PHAROS

Analogamente a quanto riportato nello studio di Iaiani et al., anche qui si è ritenuto che l'incremento del livello di liquido e soprattutto la manipolazione della pressione interna del serbatoio conduca alla generazione dei TE analizzati. Di conseguenza, la pressione interna è da ritenersi la variabile fondamentale da tenere sotto controllo nel separatore VS003. Anche in questa tesi è stata identificata e constata l'importanza della valvola PA003A, poiché essa è coinvolta nelle analisi HAZOP e FTA di tutti i quattro casi analizzati. Per quanto riguarda invece le valvole di shutdown, poiché sono state considerate come operanti in parallelo e supportate dai meccanismi difensivi di cybersicurezza, si è considerato più opportuno ritenere necessario il guasto di almeno due delle 4 valvole a disposizione affinché si raggiungano le condizioni di sviluppo del TE considerato. Tuttavia, differentemente dallo studio di Iaiani et al, è stato qui anche considerato il fattore umano nel mancato intervento degli allarmi presenti. Eventualmente, tale fattore poteva anche essere associato alle cyberprotezioni presenti nel sistema, quando ad esempio tali protezioni potessero essere accidentalmente disattivate o manomesse. Tuttavia, giacché tali considerazioni avrebbero comportato ulteriori approssimazioni nei calcoli sia a causa dell'uso di un modello matematico sia di valori di inaffidabilità o indisponibilità con incertezza intrinseca, il fattore umano non è stato correlato all'intervento del firewall/antivirus o dei sistemi di autenticazione.

Lo studio di Iaiani et al. ha egregiamente individuato tutte le possibili combinazioni di MA che possano condurre ad una vasta gamma di CE. Tali combinazioni possono anche comprendere casi in cui vengano considerate più variabili di processo. Si prenda a titolo di esempio il caso MA13+MA16, che stando a quanto scritto innalzano sia la pressione interna che il livello di liquido del serbatoio (generando hold up).

Anche in questo studio, sebbene limitato a 4 TE, si è cercato anche di tenere conto dell'eventualità di attacco di più di un sistema di controllo, come evidenziato dalle porte "a logica maggioritaria" presenti nelle analisi FTA o CFTA. Tale circostanza non è da ritenersi improbabile, in quanto i sistemi di controllo sono tutti fra loro interconnessi e comunque collegati ad una sala di controllo remota che altrettanto potrebbe divenire vittima di un cyberattacco. Quest'ultimo caso sarebbe probabilmente il peggiore, in quanto l'intero impianto vedrebbe compromessa la propria integrità.

Ciò che ha ulteriormente aiutato lo sviluppo di questa tesi è stato il database degli scenari incidentali redatto, poiché una maggiore consapevolezza degli avvenimenti del passato è una delle prime basi su cui poter costruire le analisi di sicurezza. L'autore si augura che in futuro le analisi possano essere ancora più accurate ed approfondite, perché in fin dei conti la sicurezza non è mai troppa.

13. Glossario

1. Rischio: eventualità di subire un danno in circostanze più o meno prevedibili (dal sito treccani.it/vocabolario, consultato in data 17/11/2023). Nel rapporto Rasmussen del 1975, la formula proposta per il calcolo del rischio è il prodotto di una frequenza per una magnitudo ("valutazione dei rischi parte 1", prof. Demichela, corso di Tecnica della Sicurezza Ambientale, 2022)
2. Frequenza: in senso relativo, il numero di volte che un fatto si ripete o che un fenomeno avviene in una estensione di tempo più o meno determinata, talora espresso con una precisa entità numerica, altre volte con aggettivi o altre espressioni che indicano genericamente la maggiore o minore distanza che separa tra loro le successive manifestazioni, la loro costanza o regolarità (dal sito treccani.it/vocabolario, consultato in data 17/11/2023)
3. Magnitudo: si può intendere come la gravità delle conseguenze associato all'accadimento del relativo rischio ("valutazione dei rischi parte 1", prof. Demichela corso di Tecnica della Sicurezza Ambientale, 2022)
4. Gestione del rischio: la gestione del rischio è un processo formale che consiste nella definizione del sistema, nell'identificazione dei pericoli, nell'identificazione degli scenari di incidente, nella quantificazione delle probabilità e delle conseguenze, nella valutazione del rischio, nell'identificazione delle opzioni di controllo del rischio, nella decisione sull'implementazione, nell'identificazione e nella gestione del rischio residuo (dalla tesi "Risk in oil and gas industry", Moin Mohammad, 2018)
5. Valutazione del rischio: processo complessivo di identificazione, analisi e valutazione del rischio (dalla tesi "Risk in oil and gas industry", Moin Mohammad, 2018)
6. Pericolo: circostanza o complesso di circostanze da cui si teme che possa derivare grave danno (dal sito treccani.it/vocabolario, consultato in data 17/11/2023)
7. Evento: il verificarsi o il cambiamento di un particolare insieme di circostanze come un guasto del sistema, un terremoto, un'esplosione o lo scoppio di una pandemia". "Un evento può essere una o più occorrenze e può avere diverse cause. (dalla tesi "Risk in oil and gas industry", Moin Mohammad, 2018)
8. Conseguenze: gli effetti dell'attività rispetto ai valori definiti (come la vita e la salute umana, l'ambiente e i beni economici), coprendo la totalità degli stati, degli eventi, delle barriere e dei risultati. (dalla tesi "Risk in oil and gas industry", Moin Mohammad, 2018)
9. Ferimento: lesioni fisiche o psicologici (dalla tesi "Risk in oil and gas industry", Moin Mohammad, 2018)
10. Danno: perdita di qualcosa di desiderabile, conseguenze avverse o sfavorevoli. (dalla tesi "Risk in oil and gas industry", Moin Mohammad, 2018)
11. Impatto: gli effetti delle conseguenze sui valori specifici, come la vita e la salute umana, l'ambiente e i beni economici. (dalla tesi "Risk in oil and gas industry", Moin Mohammad, 2018)
12. Severità: corrisponde alla magnitudo del danno (dalla tesi "Risk in oil and gas industry", Moin Mohammad, 2018)
13. Probabilità: L'interpretazione classica si applica solo in situazioni con un numero finito di risultati che hanno la stessa probabilità di verificarsi: la probabilità di A è uguale al rapporto tra il numero di risultati risultanti in A e il numero totale di risultati, cioè P(A) = Numero di risultati risultanti in A diviso per il numero totale di risultati (dalla tesi "Risk in oil and gas industry", Moin Mohammad, 2018)

Di seguito si riportano altre definizioni correlate all'ambito cybersicurezza e sistemi di controllo.

1. IT/OT: informational/operational technology. Insieme delle tecnologie presenti all'interno di un impianto che comprende sia le apparecchiature e le tecnologie di processo sia quelle adibite per il controllo e il monitoraggio dell'intero sistema

2. ICS: Industrial Control System, ovvero l'insieme di tutte le apparecchiature di controllo e monitoraggio di un sito industriale
3. DCS: distributed control system. La principale caratteristica di un sistema DCS è l'architettura con la quale
4. viene costruito e che viene definita di tipo "distribuito", in contrapposizione alle strutture centralizzate. Il DCS è costituito da un numero variabile di elementi di diversi tipi collegati ad una o più reti locali di comunicazione e ogni elemento è dotato di autonomia propria, sia dal punto di vista della capacità di elaborazione sia da quello di interfacciamento con i dati di processo (dalle slide "Lezione 1" del prof. Fissore, corso di Controllo Avanzato, 2022)
5. PLC: programmable logic controller. Il controllore logico programmabile è un computer industriale specializzato nella gestione dei processi industriali. Il PLC esegue un programma ed elabora i segnali digitali ed analogici provenienti da sensori e diretti agli attuatori presenti in un impianto industriale. (dalle slide "Lezione 1" del prof. Fissore, corso di Controllo Avanzato, 2022)
6. BPCS: basic process and control system. Un sistema che risponde ai segnali di ingresso provenienti dal processo e dalle apparecchiature associate, da altri sistemi programmabili e/o da un operatore e genera segnali di uscita che fanno funzionare il processo e le apparecchiature associate nel modo desiderato ed entro i normali limiti di produzione. (https://www.MAhe.org/ccps/resources/glossary/process-safety-glossary/basic-process-control-system-bpcs, consultato in data 17/11/2023)
7. SIS: safety instrumented system. Un sistema strumentato di sicurezza (SIS) intraprende un'azione automatizzata per mantenere o per metterlo in uno stato sicuro, quando sono presenti condizioni anomale. Il SIS può implementare una o più funzioni per la protezione da vari rischi di processo. Altre nomenclature usate sono sistema di arresto di sicurezza, sistema di arresto di emergenza, interblocco di sicurezza, sistema strumentato di protezione o sistema critico di sicurezza. Nella maggior parte dei casi, ogni funzione di un SIS è costituita da tre componenti:
    a. un sensore che monitora il processo per rilevare una condizione di disturbo o anomala (ad esempio, un sensore di pressione)
    b. un dispositivo logico che riceve il segnale dal sensore, determina se la condizione è pericolosa e, in caso affermativo, invia un segnale per intervenire
    c. un dispositivo di controllo finale, che riceve il segnale dal dispositivo logico e attua l'azione appropriata nell'impianto (ad esempio, apertura o chiusura di una valvola, arresto di una pompa) (https://www.MAhe.org/sites/default/files/2009-07-Beacon-English.pdf, consultato in data 17/11/2023)
8. Minaccia: Qualsiasi indicazione, circostanza o evento che possa causare la perdita o il danneggiamento di un bene. La minaccia può anche essere definita come l'intenzione e la capacità di un avversario di intraprendere azioni che sarebbero dannose per le risorse critiche. (Casson Moreno et al., 2018)
9. Attrattiva ("attrattiva dell'obiettivo"): Una stima del valore di un obiettivo per un avversario basata su fattori quali: potenziale di decessi, danno economico, interruzione dell'attività economica, accesso all'obiettivo, ecc. (Casson Moreno et al., 2018)
10. Vulnerabilità: Qualsiasi debolezza che può essere sfruttata da un avversario per ottenere l'accesso a una risorsa. Le vulnerabilità possono includere, a titolo esemplificativo ma non esaustivo, le caratteristiche degli edifici, le proprietà delle apparecchiature, il comportamento del personale, l'ubicazione di persone, attrezzature ed edifici o le pratiche operative e del personale. (Casson Moreno et al., 2018)
11. Evento: Possibilmente indicato come "evento indesiderabile", definito come un evento (intenzionale) che provoca la perdita di un bene, sia che si tratti di una perdita di capacità, vita, proprietà o attrezzature (Casson Moreno et al., 2018)

14. Bibliografia

Ahmed T., Russell P.A. , Makwashi N. , Hamad F., Gooneratne S., 2020 "Design and capital cost optimisation of three-phase gravity separators", Helyion, DOI e4065

Ben-Asher N, Gonzalez C. Comput Human Behav , 2015, "Effects of cyber security knowledge on attack detection", [Internet].;48:51–61. DOI:10.1016/j.chb.2015.01.039

Bobbio A., Bologna S., Ciancamerl S., Franceschini G., Gaeta R., Minichin M., Portinale L., 2001 "COMPARISON OF METHODOLOGIES FOR THE SAFETY AND DEPENDABILITY ASSESSMENT OF AN INDUSTRIAL PROGRAMMABLE LOGIC CONTROLLER",https://www.researchgate.net/publication/228459927_Comparison_of_methodologies_for_the_safety_and_dependability_assessment_of_an_industrial_programmable_logic_controller, consultato in data 8/2/2024

Casson Moreno V., Reniers G. , Salzanoa E., Cozzani V., 2018 "Analysis of physical and cyber security-related events in the chemical and process industry", Process Safety and Environmental Protection 116, pag. 621–631

Cormier A., Christopher N.g., 2020 "Integrating cybersecurity in hazard and risk analyses", Journal of Loss Prevention in the Process Industries, DOI 104044

Hashimoto Y., Toyoshima T., Yogo S., Koike M., Hamaguchi T., Jing S., Koshijima I., 2013, "Safety securing approach against cyber-attacks for process control System", Computers and Chemical Engineering 57, pag. 181– 186

Iaiani M., Tugnoli A., Bonvicini S., Cozzani V. , 2021, "Analysis of Cybersecurity-related Incidents in the Process Industry", Reliability Engineering and System Safety 209, DOI 107485

Iaiani M., Tugnoli A., Bonvicini S., Cozzani V., 2021 "Major accidents triggered by malicious manipulations of the control system in process facilities", Safety Science, DOI 105043

Iaiani M., Tugnoli A., Cozzani V, 2023 "Identification of cyber-risks for the control and safety instrumented systems: a synergic framework for the process industry", Process Safety and Envirnomental Protection, pag. 69-82

Iaiani M., Tugnoli A., Cozzani V., 2023 "Process hazard and operability analysis of BPCS and SIS malicious manipulations by POROS 2.0",. Process Safety and Envirnomental Protection, pag. 226-237

Kilovaty I., 2023 "CYBERSECURING THE PIPELINE", 60 HOUS. L. REV. 605

Matteini A., Argenti F., Salzano E., Cozzani V., 2019 "A comparative analysis of security risk assessment methodologies for the chemical industry", Reliability Engineering and System Safety 191, DOI 106083

Mohammad M., 2018 "RISK ASSESSMENT IN OIL AND GAS INDUSTRY WITH RESPECT TO CYBERSECURITY", Tesi di Laurea, Politecnico di Torino

Parker S., Wu Z., Panagiotis D. C. , 2023 "Cybersecurity in process control, operations, and supply chain", Computers and Chemical Engineering, DOI 108169

Uchenna P. Ani D, He H., Tiwari A., 2016 “Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective”, Journal of Cyber Security Technology, 1:1, pag. 32-74, DOI: 10.1080/23742917.2016.1252211

Uehara, T., 2011, “SCADA system and cyber security”, Journal of Human Factors in Japan, 15(2), 10–13,

US Department for Homeland Security, 2008b. Pipeline Threat Assessment.

Vatanski N., Harju T., Rantala A., Jamsa-jounela S-L., 2004 “The economical aspects of control loop performance measures in the remote maintenance center concept”, Elsevier

Villa V., Paltrinieri N., Khan F., Cozzani V., 2016 “Towards dynamic risk analysis: A review of the risk assessment approach and its limitations in the chemical process industry”, Safety Science

Yaacoub J.-P. , Salman O., Noura H.N., Kaaniche N., Chehab A., Malli M., 2020, “Cyber-physical systems security: Limitations, issues and future trends”, Microprocessors and Microsystems 77, DOI 103201

Ylonen M. , Tugnoli A., Oliva G., Heikkila J., Nissila M., Iaiani M., Cozzani V., Setola R., Assenza G., van der Beek D., Steijn W., Gotcheva N., Del Prete E., 2022 “Integrated management of safety and security in Seveso sites - sociotechnical perspectives”, Safety Science 151, DOI 105741

Colonial Pipeline: https://www.youtube.com/watch?v=qEyBVat9djk&t=369s (ultimo accesso 12/2/2024)

Database ARIA: https://www.aria.developpement-durable.gouv.fr/the-barpi/the-aria-database/?lang=en

it.abcdef.wiki | Analisi dell'albero dei guasti - Fault tree analysis - abcdef.wiki https://it.abcdef.wiki/wiki/Fault_tree_analysis (ultimo accesso 24/1/2024)

https://it.wikipedia.org/wiki/HAZOP (ultimo accesso 24/1/2024)

www.servitecno.it | La Continuità Operativa per gli Erogatori di Servizi Essenziali, le nuove direttive Europee NIS e l’applicabilità delle soluzioni industriali per la Cybersicurezza https://www.servitecno.it/la-continuita-operativa-per-gli-erogatori-di-servizi-essenziali-le-nuove-direttive-europee-nis-e-lapplicabilita-delle-soluzioni-industriali-per-la-cyber-security-ot/ (ultimo accesso 24/1/2024)

https://www.tomshw.it/altro/attenzione-sviluppatori-c-e-c-non-sono-sicuri-dice-la-casa-bianca (a cura di Valerio Porcu, Senior Editor, pubblicato il 29/02/2024 alle 12:24)

https://www.treccani.it/vocabolario/frequenza/ (ultimo accesso 17/11/2023)

https://www.wikiwand.com/it/Bus_(informatica) (ultimo accesso 24/1/2024)