Analisi dei rischi emergenti connessi con la trasformazione digitale: il progetto DRIVERS

R. Setola[1], B. Fabiano[2], S. Ansaldi[3]

[1] Università Campus Bio-Medico di Roma
[2] Università di Genova
[3] Inail - Dit

Abstract

Nei prossimi anni la progressiva spinta alla digitalizzazione di tutte le attività, unitamente alla transizione energetica ma soprattutto ai mutamenti indotti dai cambiamenti climatici, ci porrà di fronte a scenari di rischio "unknown" con potenziali significativi impatti per la sicurezza degli impianti produttivi. Queste considerazioni impongono lo sviluppo di soluzioni in grado di identificare e monitorare quei fattori che posso accelerare (ovvero frenare) l'insorgenza di tali rischi emergenti. Per rispondere a questa esigenza il progetto DRIVERS sta realizzando una piattaforma di Safety Information per supportare l'operatore nell'evidenziare tempestivamente l'insorgenza di fenomeni di rischio (early-warning) e nell'aiutarlo a valutare la propria esposizione.
A tal fine il progetto ha identificato i fattori maggiormente critici per gli aspetti di safety connessi con i cambiamenti climatici, la transizione energetica e la trasformazione digitale. In particolare, per quest'ultimo aspetto è emersa la rilevanza del tema della cybersecurity e della necessità di avere strumenti in grado di abbinare ad una conoscenza puntuale degli elementi che costituiscono lo strato di Operational Technology (OT) dell'impianto con quelle che sono le vulnerabilità note correlandole al relativo livello di rischio. A tal fine nell'ambito del progetto è in fase di sviluppo una soluzione automatizzata che consente di fare l'inventory della rete OT e di verificare attraverso l'utilizzo di apposite API l'eventuale presenza di vulnerabilità note il cui grado di pericolosità è determinato usando la metrica CVSS (Common Vulnerability Scoring System).

Keywords: Cybersecurity, Operational Technology, OSINT, process and occupational safety.

1. Introduzione

Il Financial Times[1] in un suo recente articolo ha utilizzato la metafora della *tempesta perfetta* per dare un'idea di quelli che sono i "nuovi" rischi che si stanno affacciano nello scenario industriale (e non solo in quello). L'articolo evidenzia come si

[1] https://www.ft.com/content/d4ab879e-6fcd-40a6-9acf-4c60b78c6cbb

concentrano e si sommano gli effetti legati a tre fenomeni, in parte correlati, che cambieranno in modo significativo il nostro modo di vivere con impatti significativi su specifiche filiere industriali. In particolare, l'articolo si riferisce a quelli che sono i rischi indotti dalla **trasformazione digitale**, dalla **transizione energetica** e dai **cambiamenti climatici**. Tre eventi hanno in comune il fatto di essere fenomeni a livello globale, di avvenire su scale temporali estremamente ridotte (quanto meno per ciò che riguarda la manifestazione degli effetti negativi) ma, soprattutto, di essere fenomeni nuovi. Fenomeni per i quali non possiamo, se non in piccola parte, ricorrere all'esperienza passata e all'analisi delle serie storiche. Per tale ultima caratteristica essi sono genericamente etichettati come **rischi emergenti**.
Questi fenomeni avranno un impatto estremamente significativo soprattutto sulla filiera del petrolio, e più in generale sull'industria legata all'utilizzo dei combustibili fossili, che vedrà da un lato una riduzione di interesse economico per il settore (legata a scelte dirompenti quale quella dello stop ai veicoli a motore endotermico) ma al tempo stesso alla necessità di introdurre/subire soluzioni innovative indotte dal mutato scenario (come ad esempio i bio-carburanti e l'utilizzo dell'idrogeno). Il primo fattore indurrà una perdita di interesse nel settore con progressiva riduzione di investimenti per quel che riguarda la manutenzione evolutiva degli attuali siti produttivi, ma al tempo stesso la necessità di introdurre in tali siti elementi esogeni che creeranno gioco forza una maggiore complessità architetturale e la presenza di fattori di interferenza.
A ciò si sommano gli effetti dei cambiamenti climatici in termini di estremizzazione dei fenomeni climatici che rendono non adeguato il dimensionamento di alcune infrastrutture di servizio (come, ad esempio, le vasche di raccolta delle acque reflue sui piazzali) oltre che compromettere la staticità/operatività di alcuni elementi e manufatti (ad esempio a causa di venti di significativa intensità). Per contrastare gli effetti di questi fenomeni sarebbero necessari interventi di adeguamento degli attuali impianti che, però, appaiono, oltre che estremamente onerosi e non in linea con la riduzione di interesse per la filiera del fossile, di difficile identificazione progettazione a causa della natura emergente di tali rischi (e quindi non riferibili a serie storiche).
In questo contesto la transizione digitale rappresenta una leva utilizzabile per gestire questi cambiamenti ma che al tempo stesso introduce una serie di ulteriori rischi connessi sia con la perdita di centralità del fattore umano (in termini sia di numero di addetti che di ridotta capacità di trasferimento delle competenze) ma soprattutto con una crescente esposizione ai rischi di cyber security.

2. Il rischio Cyber

Sebbene l'automazione industriale sia entrata negli stabilimenti a partire dalla metà degli anni settanta, solo verso la fine degli anni '90 si sono iniziate a prendere in considerazione le implicazioni per la sicurezza legati al fattore digitale. O meglio, fino ai primi degli anni '90, il problema della sicurezza della componente di controllo

digitale era relegata agli aspetti connessi con i guasti del sistema informatico, i bug del software e gli errori (più o meno volontari) commessi dagli operatori.
A partire dalla fine degli anni '90 a queste problematiche che potremmo etichettare come di "cyber-safety", iniziano ad affiancarsi problematiche di cyber-security, ovvero di azioni dolose.
Occorre infatti considerare che fino alla metà degli anni '90 la stragrande maggioranza dei sistemi informatici utilizzati in ambito industriale, generalmente indicati come **ICS (Industrial Control System)**, era basata su hardware, software e protocolli proprietari ed operavano sostanzialmente in maniera isolata rispetto alla rete IT aziendale.
Le spinte connesse alla necessità di migliorare la flessibilità e l'efficienza della produzione, ridurre i costi unite alla necessità di aggiornare molti dei sistemi legacy per renderli immuni al *millenium bug* hanno spinto per un rapido cambio di contesto. Questo ha comportato una adozione massiccia all'interno dei siti industriali di prodotti IT off-the-shelf e, anche per soddisfare le esigenze produttive, ad una apertura e integrazione di questi sistemi con le infrastrutture IT aziendali.
Conseguenza non pianificata di ciò è stato che le reti industriali sono divenute soggette ai medesimi rischi propri dei sistemi IT. Purtroppo, i sistemi industriali hanno delle peculiarità in termini di tempi di latenza, capacità di calcolo, vincoli di banda, lifetime che rendono solo in parte replicabili i meccanismi di difesa propri dei sistemi IT [1]. Per sottolineare tale peculiarità nella comunità scientifica si è iniziato ad utilizzare il termine **OT (Operational Technologies)** per indicare i sistemi di controllo impiegati nell'ambito industriale in modo da contrapporlo ai sistemi IT.

3. Il progetto DRIVERS

DRIVERS (Approccio combinato data-driven ed experience-driven all'analisi del rischio sistemico) è un progetto co-finanziato da INAIL che ha quale obiettivo quello di fornire una metodologia ed uno strumento per mappare e riconoscere i rischi emergenti relativi ai cambiamenti climatici, alla transizione energetica e alla trasformazione digitale [9].
A tal fine si è adottato un modello tipo fishbone, per identificare per ciascuno dei tre ambiti i principali fattori acceleranti e frenanti, ovvero quei fattori che agiscono sull'hazard facendolo crescere o diminuire.
Tali fattori sono stati identificati e organizzati, con riferimento alle tre tipologie di rischi emergenti e relativamente alle industrie Seveso, con lo scopo di ottenere una raccolta abbastanza completa degli elementi che hanno importanza ai fini della comprensione e gestione dei problemi delle transizioni concorrenti, organizzati secondo uno schema gerarchico (fattori generali e subfattori specifici).
Con riferimento al rischi cyber, come illustrato nella figura 1, sono stati individuati a livello sistemico 16 fattori "acceleranti", ovvero che amplificano il rischi cyber (obsolescenza; gestione dei dati operativi; gestione dei dati personali; gestione dei sistemi OT compromessi; integrazione; rete wireless; connessioni digitali; patching;

interferenze; ostacoli normativi; terze parti; accesso remoto; invecchiamento; riduzione del personale; turn over; limitata consapevolezza) e 20 fattori "frenanti", cioè che rallentano l'insorgenza di tale rischio (risk assessment; modalità di lavoro; certificazioni di analisi dei rischi; certificazioni di cyber security; automazione dei processi; patching; sicurezza by-design dei dispositivi; audit periodico; backups del cloud; segregazione; riconoscimento dell'utenza; sistemi di protezione; training certificato; simulazioni e test; campagne informative; attività di lesson learned; regolazione specifica degli aspetti socio culturali di contesto; supervisione di competenza; figure di lavoro professionali; ecosistema di supporto).

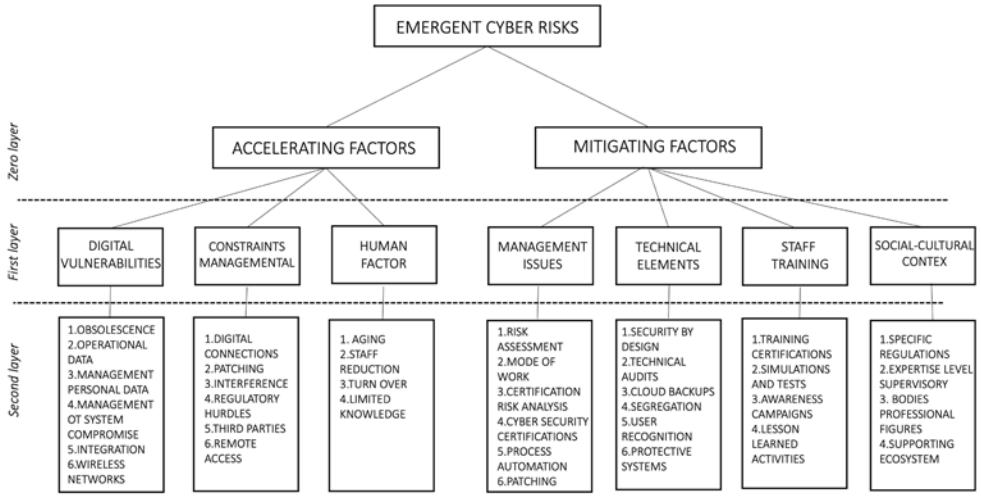

Figura 1. Elencazione fattori e sotto-fattori frenanti ed acceleranti per la trasformazione digitale

Successivamente gli schemi fishbone sono stati ulteriormente arricchiti attraverso l'interazione con i componenti dell'Advisory Board del progetto. Nello specifico a ciascun fattore è stato attribuito un peso attraverso la definizione di una scala di importanza del fattore che quantifica in maniera qualitativa l'incremento dell'hazard rispetto alla situazione tradizionale. A tal fine si è utilizzato l'approccio AHP sparso che si basa sul confronto a coppia dei singoli valori [2].

Tale analisi illustrata in dettaglio in [3] ha consentito di evidenziare come gli elementi maggiormente impattanti in termini di "accelerazione" del rischio cyber siano quelli legati al "fattore umano" a causa dell'invecchiamento della forza lavoro, delle limitate conoscenze degli operatori in campo circa le problematiche cyber e dell'elevato turn over. In Tabella 1 sono riportati i valori normalizzati indentificati per ciascun fattore accelerante. Nello specifico, i fattori acceleranti sono divisi per le macro aree e sono:

- legati alla sfera digitale sono: l'obsolescenza (con peso 0.0099); la gestione dei dati operativi e dei dati personali (entrambi con peso 0.0362); la compromissione di

sistemi OT (0.0693), l'integrazione tra sistemi (0.0362) e la gestione reti wireless (peso 0.0693);
- legati alla gestione dei fornitori: la connessione digitale dei sistemi (0.0238); il patching (0.0149); l'interferenza (0.0238); gli ostacoli normativi (0.0048); la gestione delle terze parti (0.0021) e gli accessi da remoto (0.0009);
- legati al definito "fattore umano": l'invecchiamento del personale (0.2101); la riduzione del personale (0.0420); il turn over (0.2101) e le limitate conoscenze (0.2101).

L'importanza del fattore umano non deve apparire anomalo essendo conclamato che la stragrande maggioranza degli incidenti cyber sono da ricondurre ad un non corretto comportamento di un operatore [4]. Giusto come esempio si riporta che sia il blocco dell'erogazione elettrica in Ucraina nel 2015 e 2016 che la paralisi dell'oleodotto Colonial Pipeline negli stati Uniti nel 2021 sono stati "innescati" da un comportamento non idoneo da parte di un operatore che è stato oggetto di phishing [1].

Accelerating macro-criteria	Accelerating micro-criteria	Weight
Digital Vulnerabilities	Obsolescence	0.0099
Digital Vulnerabilities	Operational data management	0.0362
Digital Vulnerabilities	Personal data management	0.0362
Digital Vulnerabilities	OT system compromise	0.0693
Digital Vulnerabilities	Integration	0.0362
Digital Vulnerabilities	Wireless networks	0.0693
Management constraints	Digital connections	0.0238
Management constraints	Patching	0.0149
Management constraints	Interference	0.0238
Management constraints	Legal barriers	0.0048
Management constraints	Third parties	0.0021
Management constraints	Remote access	0.0009
Human Factor	Aging	0.2101
Human Factor	Staff reduction	0.0420
Human Factor	Turn over	0.2101
Human Factor	Limited knowledge	0.2101

Tabella 1. Pesi attribuiti ai fattori (e sotto-fattori) acceleranti relativi alla trasformazione digitale [3].

Oltre al fattore umano, l'analisi ha evidenziato l'importanza delle problematiche connesse con l'utilizzo della rete wireless e la compromissione dei componenti OT. Quest'ultimo aspetto appare quello più rilevante dal punto di vista dell'analisi del rischio essendo fortemente peculiare ed impattando in modo specifico su come son realizzati, monitorati e gestiti i singoli impianti.

Conseguentemente il progetto DRIVERS ha elaborato una metodologia per mappare i rischi cyber legati ai componenti OT.

4. Valutazione rischio Cyber dei componenti OT

Per la valutazione dei rischi cyber legati ai componenti OT si è optato per la strategia delineata nella Figura 2. Essa consta di tre macro-blocchi:

- **Inventory assesment**: il cui scopo è quello di indentificare i componenti hardware e software che costituiscono la rete OT;
- **Vulnerability Analysis**: il cui scopo è quello di verificare se esistono vulnerabilità note che affliggono una o più componenti della rete OT
- **Risk assesment**: il cui scopo è quello di valutare sulla base di informazioni reperibili sulla vulnerabilità e della rilevanza del singolo componente all'interno dell'infrastruttura qual è la rilevanza del potenziale impatto

Queste attività si concretizzano in un indice di rischio cyber che caratterizza il singolo componente informatico e che a sua volta contribuisce a definire un indice di rischio per ciascun device fisico, per ciascuna area in cui è suddiviso l'impianto e per l'intero impianto.
Si noti che un componente può essere affetto da zero, una o più vulnerabilità e che la medesima vulnerabilità può affliggere più componenti. In ottica conservativa il valore di rischio associato a ciascun componete è assunto pari al rischio maggiore.

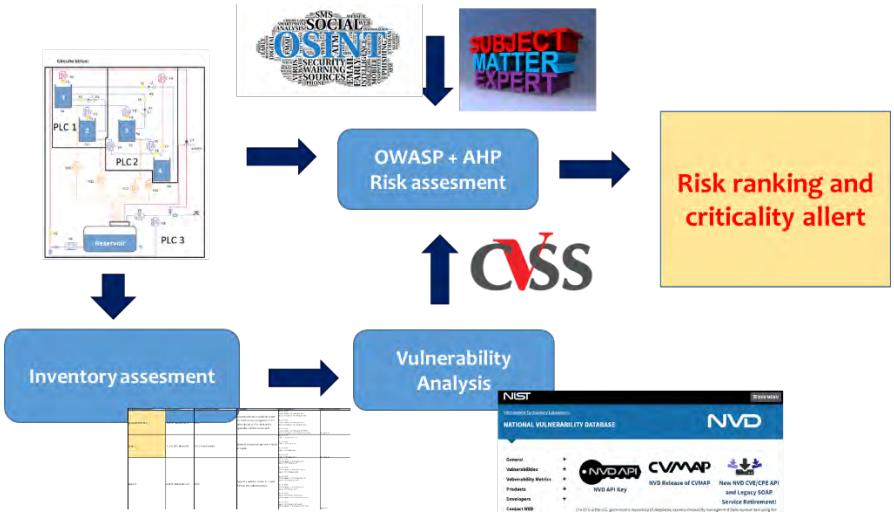

Figura 2. Schema metodologia per determinazione rischio cyber

5. La procedura per effettuare l'Inventory assesment

Sebbene a differenza di una rete IT, la rete OT si caratterizza per una minore dinamicità in termini di evoluzione dei protocolli e delle piattaforme, appare necessario avere un sistema in grado di fornire in modo dinamico un inventory degli apparati presenti nella rete al fine di poter valutare la presenza di eventuali vulnerabilità.
A tal fine si è sviluppato un tool per l'inventory automatico dei componenti hardware presenti in una rete OT. Il tool, realizzato in Python, è in grado di eseguire la scansione al fine di censire i dispositivi connessi alla rete. Il tool identifica,

Figura 3. Schema metodologia per determinazione rischio cyber

in particolare, tutti i dispositivi di livello 3 (network level) che sono connessi alla stessa rete sulla quale esegue lo scan.
Il tool è basato sulle funzionalità del comando “nmap”, il comando rappresenta uno strumento di scansione di rete frequentemente utilizzato per effettuare un check degli elementi connessi ad una rete. Questo consente di eseguire una scansione approfondita di una rete, identificando i dispositivi connessi e le porte aperte su tali dispositivi al fine di valutare i servizi attivi sui dispositivi connessi. L'utilizzo del comando "nmap" può fornire informazioni preziose sulla configurazione di rete al fine di rilevare vulnerabilità e valutare la sicurezza complessiva di un sistema.
L’output prodotto dallo script consiste in un file json che riporta in modo strutturato le informazioni disponibili per ciascun elemento di rete individuato.
Nell’esempio di Figura 3 il dispositivo individuato è un PLC Schneider Electric sul quale risulta attivo un server Modbus/TCP attivo sulla porta 502. Nello specifico il significato dei singoli campi è il seguente

"**service**": Fornisce informazioni sul servizio erogato sulla porta aperta.

"**name**": Indica il nome del servizio, che nel caso specifico Modbus Application Protocol (mbap).

"**hostname**": Questo campo rappresenta eventuali hostname locali associati all'indirizzo IP del dispositivo.

L’oggetto "macaddress” contiene i seguenti campi:

"**addr**": Rappresenta l'indirizzo MAC, che nel caso specifico è "00:80:F4:53:EB:77".

"**addrtype**": Indica il tipo di indirizzo, che nel caso specifico è "mac".

"**vendor**": Indica il produttore del dispositivo associato all'indirizzo MAC, che nel caso specifico è "Telemecanique Electrique" sulla base dei primi 3 byte.

lo script fornisce informazioni riguardanti sia gli aspetti hardware che software del dispositivo identificato mostrando dettagli quali il costruttore dell'hardware relativo alla scheda di rete, prova a stimare il sistema operativo installato sul dispositivo e determina i servizi attivi su ogni porta aperta del dispositivo.

6. La procedura per effettuare la Vulnerability Analysis

Una volta effettuato l'inventory il sistema utilizza le API messe a disposizione dal National Institute for Standards and Technologies (NIST) degli Stati Uniti per individuare vulnerabilità note che posso affliggere uno o più componenti. Nello specifico il NIST gestisce un database, denominato NVD (National Vulnerability Database) [5] che contiene informazioni su tutte le vulnerabilità note di sistemi informativi. Il sistema è aggiornato con frequenza anche più che giornaliera, sia aggiungendo nuove vulnerabilità non appena vengono rese note, sia aggiornando le informazioni su vulnerabilità già censite in relazione ad una migliore comprensione dei rischi associati, ovvero della presenza di remediation. Attualmente il DB raccoglie informazioni su quasi 300.000 vulnerabilità di cui circa 30.000 scoperte nei primi 10 mesi del 2023.
All'interno di questo DB, ogni vulnerabilità è identificata con un codice composto dall'anno in cui è scoperta e da un numero progressivo. Ad esempio, la vulnerabilità CVE-2023-30692 è l'ultima vulnerabilità identificata nel 2023 alla data del 6 ottobre 2023.
All'interno di questo DB per ciascuna vulnerabilità è fornita una breve descrizione e l'elenco dei software, con relativa configurazione e versione, che sono affetti dalla vulnerabilità stessa. Inoltre, sono presenti informazioni sul grado di maturità della vulnerabilità, sull'eventuale esistenza di strumenti di remediation (ad esempio patch).
È pertanto possibile verificare sulla scorta di quanto prodotto dall'inventory se un componente del sistema OT è affetto da tale vulnerabilità
Qualora ciò accada è possibile estrarre dal NVD anche una valutazione della relativa criticità della vulnerabilità.
A tale fine il NIST utilizza la metodologia CVSS (Common Vulnerability Scoring System) [6]. Tale metodologia assegna ad ogni vulnerabilità un punteggio compreso fra 0 e 10, dove il valore 10 indicata la massima criticità. Esso prevede che ad ogni vulnerabilità sia assegnato un valore di criticità intrinseco (definito base) che può essere ulteriormente raffinato mediante la dimensione temporale e quella di contesto.

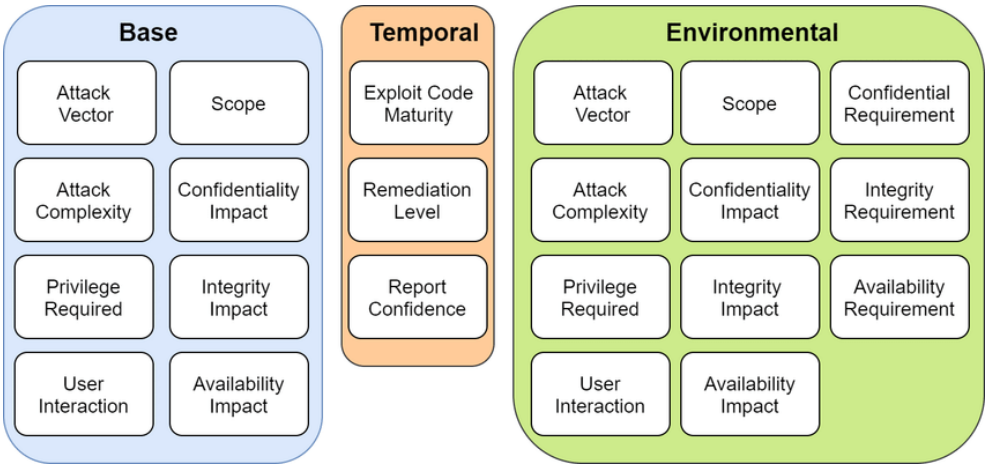

Figura 4. Elementi utilizzati in CVSS per la determinazione del livello di criticità di una vulnerabilità

Nello specifico l'indice base fornisce una valutazione sulla criticità intrinseca della vulnerabilità andando a considerare una serie di parametri che caratterizzano le risorse che l'attaccante deve avere a disposizione per sfruttare la vulnerabilità e quelli che sono gli impatti in termini di compromissione degli attributi di confidenzialità, integrità e disponibilità che si potrebbero generare dall'eventuale sfruttamento della vulnerabilità. Nella figura 4 sono illustrati i diversi parametri con riferimento alla versione 3.1 dello standard.
Il sito del NVD riporta per ciascuna vulnerabilità la valorizzazione di tutti i parametri "Base" definita sulla base delle conoscenze della vulnerabilità stessa. Inoltre, il sito del NVD riporta anche la valutazione del CVSS base di ciascuna vulnerabilità. Si evidenzia che sebbene i valori numerici attribuiti ai singoli parametri siano anch'essi nel range 0-10 con specifiche indicazioni su come graduare la scala, il modello utilizzato per la determinazione dello score finale è fortemente non lineare.
Pertanto, con l'utilizzo delle API è possibile acquisire il valore del Base score per ciascuna vulnerabilità.
Si noti che le schede relative alle diverse vulnerabilità sul sito del NVD sono aggiornate costantemente per allineare lo score (e gli altri parametri) alle nuove informazioni acquisite dai vendor e dai ricercatori.
Per gestire al meglio questo dinamismo il sistema DRIVERS tiene traccia di tutte le vulnerabilità acquisite al fine di verificare se qualcuna di esse presenti degli aggiornamenti.

7. La procedura per effettuare la Risk Assesment

Lo stesso NVD evidenzia che la determinazione della criticità di una vulnerabilità utilizzando esclusivamente il parametro base score rappresenta una prima approssimazione dell'effettivo rischio ad esso connesso.

Per ovviare in parte a tale problematica il CVSS suggerisce di utilizzare la metrica temporale e quella di contesto. Purtroppo, il NVD non valorizza tali valori che sono lasciati alla determinazione dell'utente finale.
Per fare ciò il progetto DRIVERS adotta una strategia basata su tecniche OSINT e sulla valutazione di un digital twin dell'impianto.
Nello specifico per la determinazione del parametro temporale il sistema raccoglie le informazioni presenti sul sito NVD sul livello di maturità della vulnerabilità (ufficialmente confermata, etc.). Tali informazioni potranno, inoltre, essere raccolte ed integrate con informazione acquisite su altri siti, quali ad esempio il CSIRT nazionale [7] o in forum sul dark web. Inoltre, l'utente può inserire un parametro correttivo legato alla eventuale implementazione di contromisure in grado di rimediare in parte o del tutto alla vulnerabilità stessa.
Per la valutazione della dimensione "environment" si è scelto di non utilizzare la metodologia prevista dal CVSS ma definire una diversa valutazione impiegando un modello di dipendenza funzionale schematicamente illustrato nella figura 5.
Nello specifico in fase di localizzazione sulla piattaforma DRIVERS di un impianto è associato ai diversi dispositivi OT il relativo device "fisico". A loro volta i device fisici sono raggruppati in "aree". In fase di inizializzazione è richiesto all'utente di specifica quale è il grado di "inoperabilità" [8] che da uno specifico device si trasmette all'area associata.

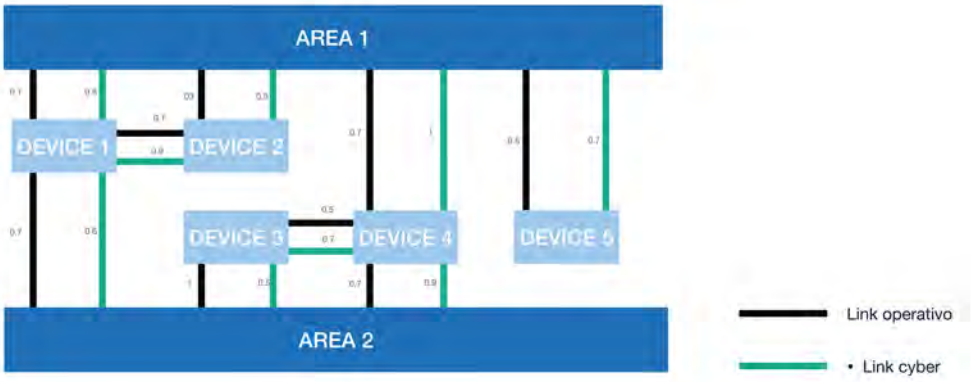

Figura 5. Rappresentazione delle dipendenze funzionali e cyber

Sulla base di tale valore si determina, considerando gli effetti di dipendenza diretta ed indiretta quello che potrebbe essere l'entità dell'impatto associato alla vulnerabilità cyber.

8. Case Study

Nell'ambito del progetto DRIVERS è stata realizzata una piattaforma in grado di acquisire dinamicamente informazioni sui rischi di carattere naturale, operativo e cyber al fine di evidenziare elementi di criticità. La piattaforma, ancora in fase di sviluppo è presentata nella Figura 6.

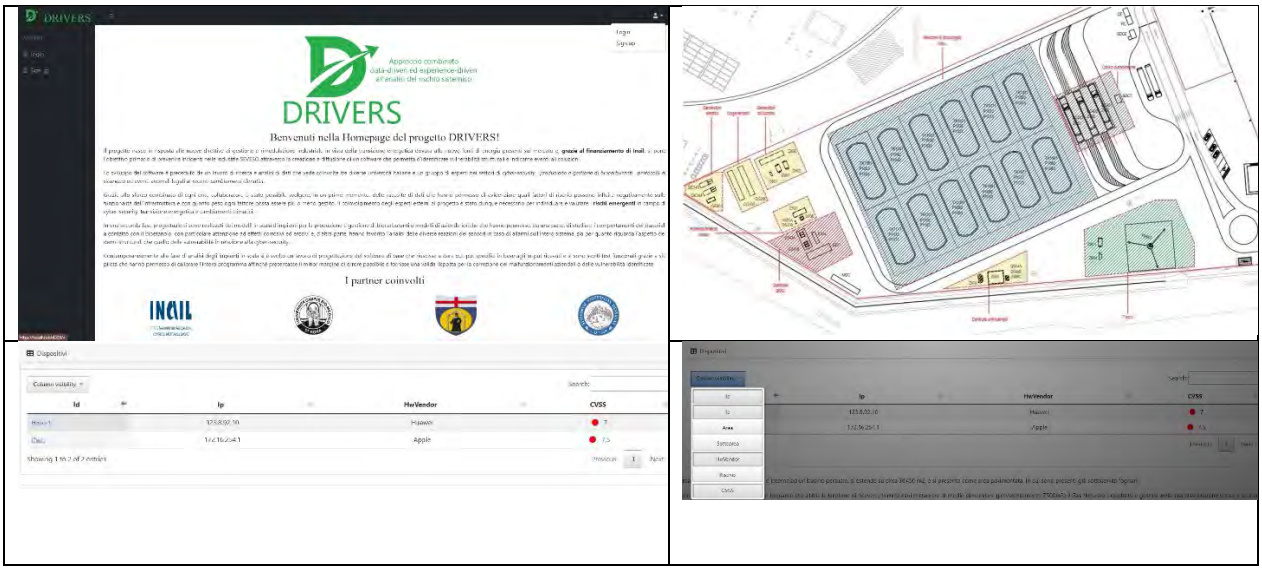

Figura 6. Alcune schermate della piattaforma DRIVERS

L'impianto è suddiviso in tre aree a cui corrispondono tre distinte porzioni del sistema OT come illustrato nella Figura 7. Il sistema con il modulo inventory effettua una disamina su base giornaliera della rete OT per acquisire informazioni su tutti i componenti presenti.

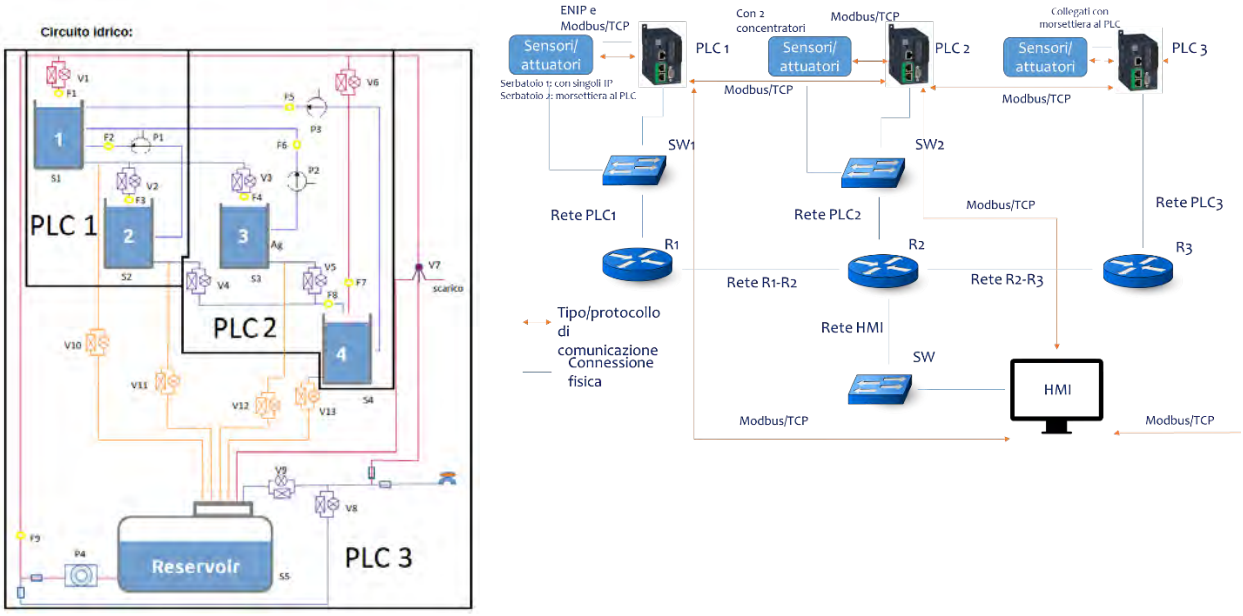

Figura 7. Test-bed impiegato per le attività di inventory.

Tali informazioni sono passate al modulo di Vulnerability Analysis che va a ricercare tramite le API se sul sito del NVD siano presenti vulnerabilità note che affliggono uno dei componenti individuati nella prima fase. L'analisi distingue fra quelle che sono vulnerabilità già analizzate e vulnerabilità nuove. Inoltre, la piattaforma mantiene traccia anche di vulnerabilità "risolte".

9. Conclusioni

Il progetto DRIVERS si è posto quale obiettivo quello di realizzare una piattaforma in grado di fornire all'operatore un'informazione unitaria rispetto a rischi di origine naturale, operativa e cyber. Per ciascuna di queste categorie esso acquisisce elementi sul possibile hazard a partire dal monitoraggio delle vulnerabilità cyber, dalle informazioni sulle attività operative e da previsioni di forecast e nowcast. Tali elementi sono integrati per determinare il livello di rischio associato a ciascun dispositivo e in modo aggregato a ciascuna delle aree in cui è suddiviso l'impianto. A questi elementi vengono fusi con le informazioni relative ai fattori acceleranti / frenanti proprie dell'impianto e dei suoi componenti. In questo modo si fornisce all'operatore un'indicazione di quelle che sono i rischi maggiormente significativi. L'operatore può navigare fra i diversi livelli della piattaforma per meglio comprendere come i singoli elementi si combinano fra di loro e per meglio analizzare la rilevanza sistemica dei singoli elementi.

10. Bibliografia

[1] Assenza, G., Faramondi, L., Oliva, G., & Setola, R. (2020). Cyber threats for operational technologies. *International Journal of System of Systems Engineering*, 10(2), 128-142.

[2] Oliva, G., Setola, R., & Scala, A. (2017). Sparse and distributed analytic hierarchy process. *Automatica*, *85*, 211-220.

[3] Nobili, M., Fioravanti, C., Guarino, S., Ansaldi, S. M., Milazzo, M. F., Bragatto, P., & Setola, R. (2023, June). DRIVERS: A platform for dynamic risk assessment of emergent cyber threats for industrial control systems. In *2023 31st Mediterranean Conference on Control and Automation (MED)* (pp. 395-400). IEEE.

[4] Corradini, I., Nardelli, E., & Ahram, T. (2020). *Advances in Human Factors in Cybersecurity*. Springer International Publishing.

[5] https://nvd.nist.gov/

[6] Scarfone, K., & Mell, P. (2009, October). An analysis of CVSS version 2 vulnerability scoring. In *2009 3rd International Symposium on Empirical Software Engineering and Measurement* (pp. 516-525). IEEE.

[7] https://www.csirt.gov.it/

[8] Setola, R., De Porcellinis, S., & Sforna, M. (2009). Critical infrastructure dependency assessment using the input–output inoperability model. *International Journal of Critical Infrastructure Protection*, *2*(4), 170-178.

[9] https://www.emergentrisk.it/index.php/it/