Atti di Convegno

SAFAP 2023

SICUREZZA E AFFIDABILITÀ DELLE ATTREZZATURE A PRESSIONE E DEGLI IMPIANTI DI PROCESSO

Brescia - 22, 23 e 24 novembre 2023

INAIL

2023

Security di una infrastruttura gas

R. Setola[1], A. Chittaro[2], A. Cestari[2]

[1] Università Campus Bio-Medico di Roma
[2] SNAM

Abstract

Come evidenziato anche dalla Seveso III e reso eclatante da quanto occorso al gasdotto Nord Stream 2, per gli impianti a pressione è fondamentale considerare in aggiunta a quelle che sono le problematiche proprie dell'impianto, anche gli aspetti connessi con eventuali azioni dolose. Tali azioni possono essere condotte da soggetti animati da diverse motivazioni che spaziano da rivendicazioni ambientaliste ad atti estorsivi fino ad azioni riconducibili ad attività geopolitiche. Tali azioni posso essere attuate sia mediante l'utilizzo di vettori fisici che attraverso azioni cyber ma anche con approcci più complessi che prevedono l'impiego di strategie ibride. Per contrastare questa tipologia di minaccia è fondamentale complementare la cultura della safety di processo con le competenze proprie della security aziendale in una visione olistica della sicurezza. Attività che impone agli operatori di svolgere specifiche analisi del rischio al fine di cogliere i potenziali pericoli derivanti da azioni dolose anche in collaborazione con il Ministero dell'Interno, la Presidenza del Consiglio dei Ministri e gli altri organi competenti. Analisi del rischio che deve tener conto in modo esplicito che a differenza di quelli che sono i pericoli di natura accidentale o naturale, le azioni dolose si caratterizzano per la presenza di antagonisti senzienti e ciò impone un orientamento diverso alla valutazione delle probabilità di accadimento (solo in parte riconducibili a serie storiche) ponendo di converso maggiore enfasi sugli aspetti di impatto potenziale e di resilienza. Da questa attività discende la necessità di predisporre un adeguato modello organizzativo che consenta di valutare in modo complessivo le problematiche di "security", che sia in grado di mettere in atto le adeguate contromisure anche sfruttando le moderne tecnologie ma soprattutto in grado di operare nell'ambito di una "security" partecipata che vede una sinergica collaborazione, nel pieno rispetto dei propri ruoli, fra la struttura di security aziendale e le diverse autorità pubbliche.
Questo lavoro illustra questa modalità di approccio prendendo in considerazione due dei progetti di maggiore rilevanza sviluppati negli ultimi anni in Italia ovvero il collegamento Trans Adritiac Pipeline (TAP) che porta in Italia il gas dall'Azerbaigian e il rigassificatore istallato provvisoriamente nel porto di Piombino per sopperire alla crisi energetica innestata dall'invasione Russa dell'Ucraina.

Keywords: sicurezza partecipata, approccio olistico, cyber-physical system, sistemi di sicurezza, LNG.

1. Introduzione

Come evidenziato anche dalla Seveso III [1] e reso eclatante da quanto occorso al gasdotto Nord Stream 2 [2], per gli impianti a pressione è fondamentale considerare in aggiunta a quelle che sono le problematiche proprie dell'impianto, anche gli aspetti connessi con eventuali azioni dolose [3]. Tali azioni possono essere condotte da soggetti animati da diverse motivazioni che spaziano da rivendicazioni ambientalistiche a atti estorsivi fino ad azioni riconducibili ad attività geopolitiche [4]. Esse posso essere attuate sia mediante l'utilizzo di vettori fisici che attraverso azioni cyber ma anche con approcci più complessi che prevedono l'impiego di strategie ibride. Per contrastare questa tipologia di minaccia è fondamentale complementare la cultura della safety di processo con le competenze proprie della security industriale in una visione olistica della sicurezza [5].
Per illustrare come tale integrazione sia possibile, oltre che auspicabile, in questo lavoro verrà presentato quanto fatto in ambito di "security" per la realizzazione del cantiere del TAP e per il rigassificatore di Piombino. Nello specifico il primo ha visto la necessità di realizzare un sistema di security partecipata in grado di contrastare frange anche violente di opposizione cresciute sulla scorta di una visione distorta dei rischi legati all'impianto alimentata da una narrazione basata, essenzialmente, su fake news. Il secondo è stato un unicum a livello nazionale sia per quel che riguarda le tempistiche di realizzazione che per la sua collocazione all'interno di un porto operativo. Questi aspetti, unitamente alle diverse classi di minacce alle quali questi impianti sono potenzialmente esposti, hanno condotto alla definizione di un sistema di security incentrato su competenze professionali, compliance normativa, procedure e tecnologie che prendendo le mosse da una attenta analisi dei rischi, hanno consentito di definire una soluzione sistemica in grado di garantire elevati standard di security pur nel complesso quadro d'insieme.

2. La security nel cantiere del TAP

La realizzazione del Trans-Adriatic Pipeline (TAP) completato nell'ottobre del 2020 ha incontrato una forte opposizione per quel che riguarda l'approdo del gasdotto a Melendugno[1]. Tale opposizione si è caratterizzata anche per episodi di violenza contro le istallazioni della TAP e dei lavoratori[2] imponendo l'adozione di un opportuno modello di security al fine di garantire, in sicurezza, l'esecuzione delle diverse lavorazioni nei tempi previsti. Tale approccio si basa sulla attenta valutazione ed analisi dei fenomeni eversivi da contrastare da cui è scaturita una strategia basata su un modello di cooperazione pubblico privato e sulla installazione di specifiche strutture di sicurezza attive e passive. A tale attività si è

[1]https://bari.repubblica.it/cronaca/2018/11/12/news/tap_manifestazione_all_alba_a_melendugno_per_dire_no_al_cantiere-211439342/
[2] https://www.ilfoglio.it/cronache/2018/01/26/news/cantiere-tap-feriti-tre-poliziotti-175431/

affiancata un'azione di contrasto alle fake-news. Il tutto in una cornice di sinergica cooperazione pubblico-privato con le autorità preposte, a partire dalla collaborazione con la Questura di Lecce.

2.1 Il cantiere di Melendugno

Il cantiere di Melendugno aveva lo scopo di realizzare il micro-tunnel necessario per la creazione della condotta sottomarina che si innestava nella pipeline sottomarina a circa 600 metri dalla costa di San Foca. Il cantiere ha una forma irregolare illustrata nella Fig. 1.

Figura 1. Cantiere TAP di Melendugno

In fase di progettazione, al fine di limitare al minimo i disagi per la popolazione, i progettisti avevano ottimizzato al massimo l'utilizzo dei terreni cercando di limitare al minimo l'espropriazione temporanea delle aree. Ciò ha implicato che su tutte le aree oggetto di espropriazione erano previsti specifici utilizzi funzionali alla realizzazione delle opere senza, però, tener conto delle problematiche di security e quindi non prevedendo né aree di stand-off perimetrali né gli spazi per la installazione delle misure di security. Tale scelta derivava da una visione "semplicistica" del problema della security che si limitava a prevedere un dispositivo basato su una recinsione perimetrale in reticolato utile per evitare l'accesso abusivo al cantiere e prevenire furti di materiale, ma non per contrastare una opposizione violenta ed organizzata [6].
Nel seguito verranno illustrati i principali elementi che hanno costituito il sistema di sicurezza messo in atto.

2.2 Metodologia adottata

La società TAP nel rendersi conto alla luce dell'occupazione del primo cantiere a Melendugno occorso nell'aprile del 2017 con distruzione sia della recinsione che di quanto in esso presente decise di affidare a Snam la gestione della security del cantiere. Snam è stata pertanto chiamata a mettere in campo le proprie

competenze in tema di security per garantire quanto necessario per la realizzazione dell'opera. Per tale attività Snam poteva contare sulle proprie esperienze, procedure e competenze che si sostanziano in un modello organizzativo in grado di approcciare il problema della security di un sito strategico in modo integrato.
Il punto di partenza di questa attività è stata l'analisi dei rischi andando comprendere i *modus operandi* degli oppositori all'opera. Questi erano composti, oltre a strati della popolazione atterriti da una narrazione fake sugli effettivi rischi dell'impianto, da frange violente riconducibili a ideologia ambientalista/antagonista simili ai movimenti no-Tav oppure no-Mose che hanno agito nel Nord d'Italia. Tali gruppi si caratterizzano per supportare la loro ideologia con azioni violente contro beni e materiali riconducibili, nel caso in specie, alla società TAP. All'interno di queste frange c'era, inoltre, l'ulteriore rischio che trovassero spazio anche elementi dell'estremismo anarchico il cui *modus operandi* è più pericoloso agendo questi ultimi anche mediante l'impiego di ordigni incendiari o esplosivi. Infine, si doveva tener conto della possibilità che la criminalità, sia locale che organizzata, potesse sfruttare lo scenario per perseguire propri fine.
Partendo da tali premesse si è andato a definire, unitamente al Ministero degli Interni e alla Questura di Lecce, quelli che dovevano essere i requisiti per il sistema di security del cantiere. Sistema che prevedeva la concorrente presenza delle attività delle forze dell'ordine, per quel che riguarda tutti gli aspetti di ordine pubblico, e dell'organizzazione di Snam per gli aspetti più prettamente di security del cantiere.
Questa attività ha trovato la sua sintesi in una stretta sinergia che ha portato ad una co-definizione dei requisiti anche tecnici del sistema di security. Nello specifico ci si è resi conto della necessità di dover avere da un lato una perimetrazione fisica atta a sopportare la pressione dei manifestanti ed a prevenire che il lancio di oggetti potesse incidere sulla salute di chi operava all'interno del cantiere e dall'altro di avere a disposizione un sistema di monitoraggio fisico e cyber in grado di aiutare le forze dell'ordine nell'individuare e riconoscere iniziative che prevaricavano la legittima protesta caratterizzandosi nella sostanza quali attività estremiste e violente. Lo scopo primario del sistema era quello di salvaguardare dell'incolumità delle maestranze, dei cittadini e delle forze dell'ordine (oltre che la tutela dei beni di TAP). Inoltre, il sistema doveva consentire l'attuazione di una strategia di difesa dinamica e adattativa dei presidi delle forze dell'ordine sul territorio che consentisse una corretta gestione dei momenti di "tensione" oltre che supportare le forze dell'ordine nell'individuare le singole responsabilità degli specifici atti violenti per poterli perseguire secondo quanto previsto dalla normativa vigente.

Si è arrivati ad un modello all'interno del quale l'autorità pubblica attua le sue proprie attività di monitoraggio del territorio sfruttando anche soluzioni tecnologiche innovative messe a punto da Snam.

2.1 La sicurezza perimetrale passiva

Il cantiere ha un perimetro di circa 1,5 km estremante irregolare anche a causa dell'olografia dei luoghi e della presenza di alcuni vincoli imposti e per la tutela di specifiche essenze arboree. Inoltre, per esigenze di ordine pubblico, è stata fatta la richiesta di definire una soluzione che fosse rapidamente installabile e, all'occorrenza, riposizionabile in modo da avere una perimetrazione in grado di essere dinamicamente modificata. Le disposizioni urbanistiche vietavano, per altro, la realizzazione di qualunque tipo di fondazione o di ancoraggio della recisione al terreno.
La soluzione adottata è stata quella di realizzata una recinsione basata su new jersey sormontati da una maglia elettrosaldata e da un concertina sfruttano elementi modulari illustrati nella Figura 2a

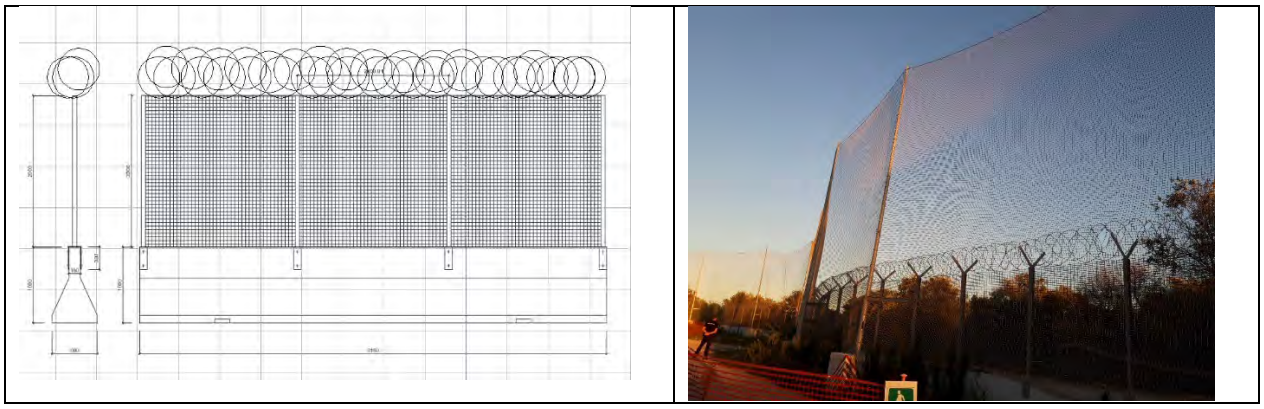

Figura 2. Recinzione di cantiere

Specifici accorgimenti sono stati introdotti per garantire continuità della struttura e l'impossibilità dello smontaggio dall'esterno.
In questo modo si è realizzata una barriera che, anche alla luce della presenza di forze dell'ordine all'interno del cantiere, era in grado di evitare lo scavalcamento da parte dei manifestanti. Inoltre, la struttura presenta sufficiente inerzia da non poter essere abbattuta o divelta oltre che una tempistica di installazione e riconfigurazione estremamente contenuta.
Per una maggiore tutela dei lavoratori che operavano all'interno del cantiere si è istallata, inoltre, una seconda recinsione con una altezza di 9 metri il cui scopo era quello di evitare che eventuali oggetti lanciati dai manifestanti potessero colpire le maestranze.

2.1 La sicurezza perimetrale attiva

La irregolarità del perimetro e la necessità di un sistema velocemente deployabile e riconfigurabile e l'impossibilità di poter realizzare un anello di alimentazione lungo il perimetro ha suggerito di adottare un sistema di video sorveglianza basato su tecnologia multi-spettrale ed una approccio a controllo trasversale.

La soluzione delineata si basa su quattro moduli (torrette) autoportanti con autonomo basamento. Ciascuna torretta prevede la presenza di un palo alto 12 m sulla cui sommità è istallata una telecamera termica rotativa ad alta velocità affiancata da due telecamere ottiche brandeggianti 4k dotate di sistema di visione notturna oltre agli apparati di comunicazione radio. Nel basamento trovano alloggiamento i sistemi di controllo, i pannelli solari per l'alimentazione, un gruppo elettrogeno, un sistema di storage locale.

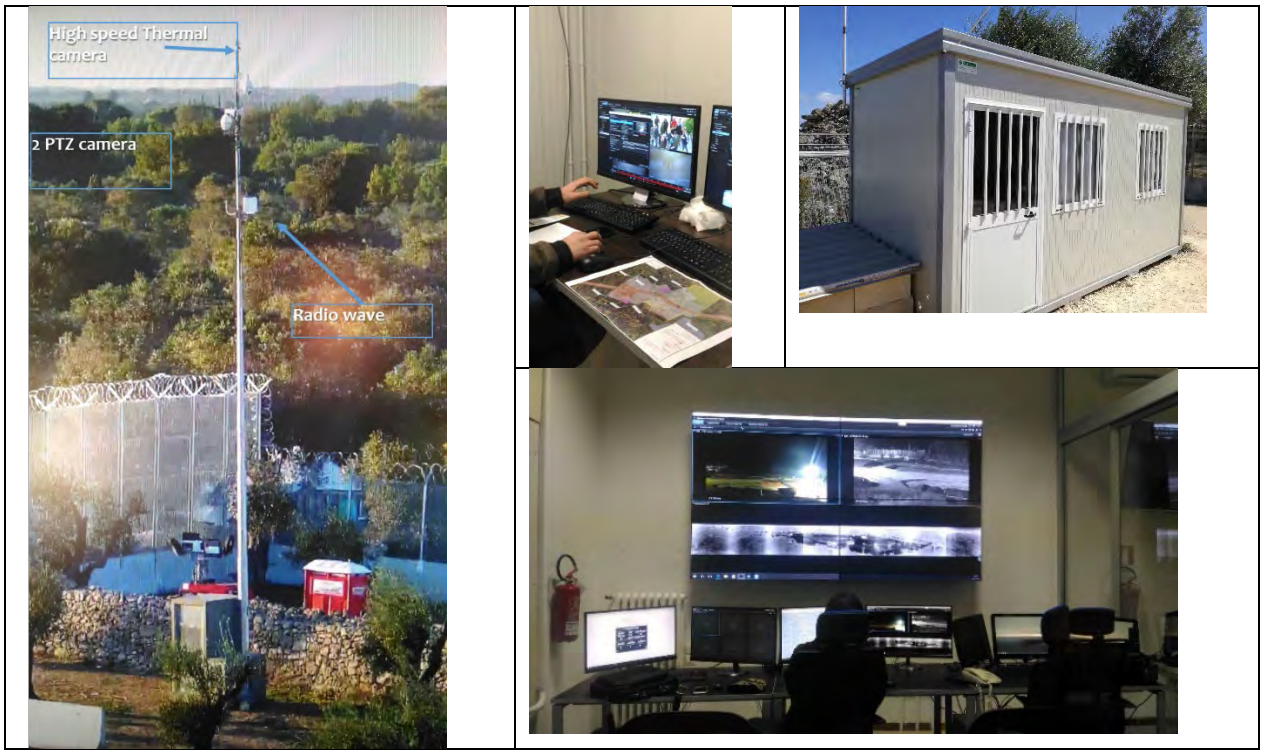

Figura 3. Recinsione di cantiere.

L'elemento maggiormente innovativo è stato l'utilizzo di una telecamera termica rotante in grado effettuare una scansione di 360° ogni 2 secondi. Il sistema è in grado di individuare e classificare, animali, persone e veicoli fino ad una distanza di quasi 200 m fornendone le coordinate geografiche. Queste ultime sono utilizzate per il puntamento automatico delle due telecamere ottiche.

Grazie alla possibilità di inserire delle maschere a livello software è stata possibile creare delle zone di attenzione, a vario livello di criticità (ovvero delle virtual fence) che se oltrepassate fanno scattare specifici allarmi. L'utilizzo di maschere ha inoltre consentito di evitare qualunque violazione dello statuto dei lavoratori in quanto le attività svolte all'interno dell'area del cantiere non attivavano alcun allarme.

Per prevenirne il danneggiamento tutte le telecamere avevano un livello di protezione IP66 e IK10. La posizione delle torrette (sia nella configurazione iniziale che in tutte i successivi riposizionamenti) è stata studiata per ottimizzare la copertura con il vincolo di risultare in copertura ottica reciproca.
Per quel che riguarda la condivisione delle immagini si è preferito (stante l'impossibilità di realizzare connessioni in fibra) l'utilizzo di ponti radio punto-punto fra le quattro torrette operati in banda 5 GHz. Tale soluzione, sebbene maggiormente costosa e più complessa da istallare, è stata preferita alla realizzazione di un LAN wi-fi per evitare rischi di cyber security.
Tutte le immagini arrivavano in tempo reale sulla torretta #1che le rendeva disponibili al centro di controllo locale all'interno del cantiere e tramite un ponte radio in banda 17 GHz alla sala di operativa della Questura di Lecce.
Sia presso il centro di controllo nel cantiere che presso la Questura di Lecce specifici sistemi provvedevano alla conservazione delle immagini.
Per ridondanza ogni torretta è dotata di un su sistema di storage in grado di immagazzinare le immagini provenienti dalle proprie telecamere fino a 7 giorni e di una SIM dati per la trasmissione delle immagini alla Questura di Lecce anche in assenza del ponte radio.

Figura 4. Recinsione di cantiere

Per consentire un flusso constane di immagini in formato full hd 4k si è optato per un protocollo di compressione H265.

Tutte le immagini, sia quelle ottiche che quelle termiche, confluivano all'interno dell'ambiente di video analisi milestone che ne garantiva oltre che la fruizione distribuita anche le funzioni di motorizzazione e sincronizzazione temporale tramite un'interfacci di semplice utilizzo da parte delle forze dell'ordine.
Per consentire una miglior impiego del sistema, le immagini era condivisibili anche su dispositivi mobili.
Si precisa che le immagini era accessibili esclusivamente agli operatori delle forze dell'ordine.

2.4 Le fake news e il monitoraggio cyber

Oltre al monitoraggio del sito fisico, SNAM ha messo in campo una strategia di monitoraggio del web per individuare e contrastare le notizie false che circolavano in rete circa la pericolosità dell'impianto e le potenziali conseguenze negative per l'ambiente e le persone. Tale attività condotta esclusivamente su fonti aperte mediante tecniche OSINT ha consentito di effettuare una corretta narrazione che ha contribuito a ridurre il sentimento negativo nella popolazione.

3. La security nel rigassificatore a Piombino

Per limitare la dipendenza nazionale dalle importazioni di gas dalla Russia, il governo in concomitanza con l'invasione dell'Ucraina ebbe a chiedere a SNAM di attivarsi per incrementare rapidamente la capacità di rigassificazione nazionale, attraverso la l'installazione di Floating Storage e Regasification Unit (FSRU). In particolare, la richiesta del governa era di avere operativa entro la primavera del 2023 almeno una FSRU. Sfida complessa alla luce del poco tempo a disposizione (meno di un anno). Dopo un rapido e accurato studio si è individuato nel porto di Piombino la sede più idonea sulla scorta della vicinanza ad un punto di innesto con la rete nazionale di trasporto del gas, la disponibilità di capacità residua nella condotta (aspetto questo che ha di fatto escluso tutti gli approdi nel sud Italia), la disponibilità di una banchina con adeguato pescaggio e lunghezza. Tutte caratteristiche possedute dal porto di Piombino che aveva anche l'ulteriore aspetto positivo che la banchina da utilizzare si inserisce in un'area industriale dismessa e non urbanizzata.
L'impegno di SNAM e di tutti soggetti coinvolti ha consentito che Il 7 luglio 2023 la nave Golan Tundra ha potuto iniziare ad immettere gas nella condotta nazionale. La Golar Tundra è una nave FSRU lunga 292,5 metri, larga 43,4 metri e alta 55 metri, dotata di 4 serbatoi per lo stoccaggio di 170mila metri cubi di gas naturale liquefatto e una capacità di rigassificazione continua di 5 miliardi di metri cubi l'anno.
L'iniziativa ha trovato però oppostone nella popolazione locale allarmata dai potenziali pericoli legati al funzionamento dell'impianto. Pericoli legati sia alla peculiarità dell'impianto, ma anche a potenziali rischi di security anche alla luce del particolare scenario geopolitico.

L'esperienza maturata nella la gestione della security del TAP, fortemente incentrata su un modello di collaborazione pubblico-privato, ha consentito di mettere a punto in brevissimo tempo un analogo ed efficace sistema di security per l'impianto di rigassificazione di Piombino.
Infatti, per garantire la sicurezza della popolazione, oltre che dell'impianto, SNAM ha realizzato un security risk assessment condiviso anche con l'Autorità Portuale, la Capitaneria di Porto, la Prefettura di Livorno e le altre amministrazioni competenti, le quali hanno definito una specifica analisi dei rischi andando ad individuare le principali minacce. Sulla scorta di questa analisi si è provveduto a definire un Sistema Integrato di Sicurezza (SIS) in grado di ridurre ad un livello accettabile i diversi rischi (come schematicamente illustrato nella figura 5).

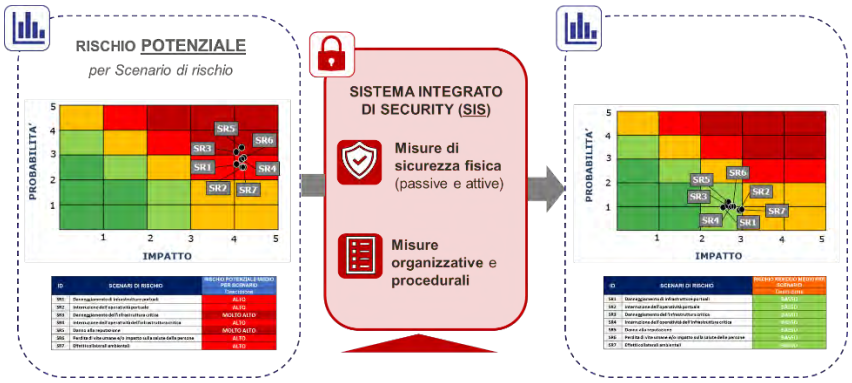

Figura 5. Processo di analisi e gestione dei rischi per la FSRU di Piombino

Tale SIS è stato poi incluso nel Port Facility Security Plan (PFSP) che rappresenta il documento principale sulla quale si basa la gestione dell'intera security, sia in condizioni di normale operatività che di eventuale emergenza.
In particolare, il SIS include tanto misure di sicurezza passive, che sistemi di sorveglianza attivi; oltre che gli aspetti organizzativi e procedurali.
Per ciò che riguarda la sicurezza fisica è stata realizzata sia una recinzione perimetrale alla banchina dove è ormeggiata la Golar Tundra che un ulteriore recinsione a tutela degli accessi alla nave ed alle diverse facility presenti sulla banchina.
Sono stati poi installati un insieme di impianti fra i quali:

- Sistema antintrusione: previsto su recinzioni perimetrali, varchi, locali tecnici/aree sensibili ed integrato con la piattaforma di supervisione e gestione eventi di security (PSIM – Physical Security Information Management).
- Sistema di controllo accessi: per gestire e controllare puntualmente l'accreditamento e gli accessi in ingresso/uscita dai varchi pedonali e carrabili. Previsti in dotazione alla vigilanza strumenti portatili di controllo di persone e bagagli.

- Sistema di comunicazione safety & security: previste postazioni videocitofoniche di chiamata/risposta per gestire gli accessi carrabili e pedonali sia dal posto di guardia locale che dai SOC Snam; sistema di altoparlanti; sistema radio in uso al personale di vigilanza e di emergenza.
- Sistema di videosorveglianza: per monitoraggio accessi, aree di impianto, specchio di mare e locali tecnici/aree sensibili (previste telecamere ottiche HD, termiche, PTZ, radar termici 360°, dotati di algoritmi di analisi video avanzata; è inoltre previsto l'uso delle telecamere a bordo dell'FSRU, utilizzabili anche ai fini security per il monitoraggio delle aree esterne alla nave).
- Sistema di supervisione di security (PSIM): per la gestione integrata dei sistemi di sicurezza, presente localmente presso il posto di guardia ed in remoto negli attuali Security OperationsCenter (SOC) di Snam.
- Infrastruttura di alimentazione elettrica e dati: per consentire l'alimentazione e la connettività SIS degli apparati di Security verso gli apparati di centro ubicati presso la sala apparati SIS locale e gli attuali SOC di Snam; tale infrastruttura è fisicamente segregata rispetto a tutti gli altri impianti elettrici di sito.
- Sistema di illuminazione: a copertura di tutte le aree (banchina, FSRU e specchio di mare).

Per garantire la corretta gestione di tutti gli aspetti di security sono state elaborate specifiche procedure che definiscono le modalità di gestione dei singoli eventi sia in condizioni ordinarie che straordinarie incluso il piano di Business Continuity ed il piano di gestione delle emergenze (HSEQ). Questi documenti sono stati redatti con un approccio KISS (*keep it simple and short*) con l'obiettivo di avere delle procedure snelle, facilmente consultabili e seguibili dai vari operatori. Il tutto, ovviamente, affiancato da un percorso continuo di formazione e familiarizzazione per tutte le figure professionali che operano nel perimetro della security del FSRU.

4. Conclusioni

L'esperienza di quanto fatto per la security del TAP e del FSRU di Piombino hanno evidenziato l'importanza di diversi aspetti.

Il primo è sicuramente quello di dove perseguire un modello di sicurezza partecipato che, nel pieno rispetto dei singoli ruoli, vede una proficua collaborazione fra soggetti pubblici ed operatori privati su un piano di reciproca conoscenza, corretta cooperazione e scambio di informazioni bi-direzionale.

Il secondo, l'importanza di avere modelli di gestione della security che prendano le mosse da una attenta e costante analisi dei rischi faccia seguire l'adozione di specifiche e commisurate misure di sicurezza. Misure che debbono, a causa della variabilità della minaccia, essere dinamiche, riconfigurabili ed adattabili al mutare dello scenario.

Il terzo aspetto riguarda è l'importanza del fattore umano, nessuno dei progetti illustrati si sarebbe potuto realizzare senza la presenza di personale competente, motivato e adeguatamente supportato. Attività questa che passa per la valorizzazione delle competenze e dei meriti dei singoli, a cui si affianca un percorso di crescita e formazione tecnica e aziendale. Il che si traduce, semplificando, nel modo in cui è opportuno che vengano redatti documenti procedurali il cui scopo non è la mera necessità di essere compliant alle norme ma uno strumento agile che può utilizzato proficuamente da chi si trovi a dover operare in situazioni sia ordinarie che di emergenza.

5. Bibliografia

[1] Ylönen, M., Tugnoli, A., Oliva, G., Heikkilä, J., Nissilä, M., Iaiani, M., ... & Del Prete, E. (2022). Integrated management of safety and security in Seveso sites-sociotechnical perspectives. *Safety science*, *151*, 105741.

[2] GÜLCAN, T. A., & ERGİNER, K. E. (2023). NATIONAL AND INTERNATIONAL MARITIME SITUATIONAL AWARENESS MODEL EXAMPLES AND THE EFFECTS OF NORTH STREAM PIPELINES SABOTAGE. *International Journal of Critical Infrastructure Protection*, 100624.

[3] Setola, R., Faramondi, L., Salzano, E., & Cozzani, V. (2019). An overview of cyber-attack to industrial control system. *Chemical Engineering Transactions*, *77*, 907-912

[4] Oliva, G., Faramondi, L., Setola, R., Tesei, M., & Zio, E. (2021). A multi-criteria model for the security assessment of large-infrastructure construction sites. *International Journal of Critical Infrastructure Protection*, *35*, 100460.

[5] Tugnolia, A., Iaiania, M., Olivab, G., Salzanoa, E., Setolab, R., & Cozzania, V. (2019). Physical security barriers and protection distances for seveso sites. *Chem. Eng. Trans*, *77*.

[6] Arata, M. J. (2006). *Construction site security*. McGraw Hill Professional.