io roma

Ordine degli Ingegneri della Provincia di Roma

N 2/2023

Quaderno

5G - NUCLEARE - SANITÀ - CYBERSECURITY

Quaderno

In copertina:
Immagine di repertorio

Il saluto del Presidente

Ing. Massimo Cerri

LA RIVOLUZIONE DIGITALE E IL FUTURO DELLE TELECOMUNICAZIONI IN EUROPA

Sono passati quasi 30 anni dalla pubblicazione del Libro Bianco su «Crescita, competitività e occupazione. Le sfide e le vie da percorrere per entrare nel XXI secolo», nel quale la Commissione Europea aveva identificato con estrema chiarezza la portata socioeconomica pervasiva e decisiva della rivoluzione digitale (Commissione Europea, 1993).
Da allora molte strategie sono state disegnate e attuate nel quadro dell'Agenda Digitale europea ch aveva, e tuttora ha, l'obiettivo di promuovere il Mercato Unico Digitale, nella consapevolezza che i benefici economici, occupazionali e sociali connessi alla trasformazione digitale siano potenzialmente molto rilevanti, ma che l'effettiva possibilità dei Paesi Membri di appropriarsene dipenda dalla loro capacità sistemica di favorire e assorbire il cambiamento.
In tale quadro, la pandemia di Covid-19 ha evidenziato con chiarezza ancora maggiore il ruolo cruciale che la digitalizzazione può avere sulla crescita e sulla resilienza delle società e delle economie. Nuovi concetti di "network" sono emersi insieme a nuovi comportamenti da parte degli utenti, nelle loro abitudini private e professionali, accelerando fenomeni già conosciuti, che sono diventati lo status quo.
Per il settore delle telecomunicazioni la rivoluzione digitale in corso, ulteriormente accelerata dalla crisi, rappresenta una enorme opportunità.

L'utilizzo di tecnologie, quali l'Edge e il 5G, come abilitatori di soluzioni innovative per le imprese, stanno profondamente cambiando le regole del gioco, nonché i ruoli dell'ecosistema che ne fa parte. Alcune delle peculiarità delle Telco, legate alla disponibilità di infrastrutture tecnologiche, contribuiscono a realizzare piattaforme connesse e razionalizzare i processi di innovazione a favore di tutte le imprese, piccole, medie e grandi.

Si tratta di un'opportunità mai vista prima di guidare la prossima ondata di evoluzione dell'industria connessa, poiché richiede risorse e capacità molto specifiche che le Telco hanno in parte già costruito progressivamente nel corso degli anni.

Le Telco hanno già da tempo indirizzato il loro business oltre i tradizionali servizi legati alla connettività, allargando il loro mercato a quello dei servizi digitali e IT e dello IOT.

La Filiera TLC è chiamata, quindi, nei prossimi anni, a raccogliere sfide importanti e complesse. A partire dalla sostenibilità degli investimenti, un prerequisito per la competitività delle imprese. L'implementazione di soluzioni innovative avrà un impatto trasformazionale su tutti i settori, richiedendo una collaborazione tra diverse competenze, per offrire soluzioni integrate.

E ingegneri, siamo pronti e desiderosi di partecipare attivamente a questo processo di cambiamento, guidando l'Europa verso un futuro digitale prospero.

Ing. Massimo Cerri
Presidente
Ordine degli Ingegneri della Provincia di Roma

L’Editoriale

Ing. Maria Elena D’Effremo

Care Colleghe e Colleghi,
eccoci all’uscita 2/2023 della Quaderno IO Roma.
Vorrei aprire questo Quaderno con una domanda: quale ruolo abbiamo noi Ingegneri nello sviluppo dei Megatrends rilevanti per l’UE?
Prima di tutto, cosa sono i Megatrends?
I Megatrends sono settori, processi, forze trainanti che si prevede possano avere un impatto globale a lungo termine nel guidare i cambiamenti, sono utili per definire un probabile futuro.
Rivedendo gli argomenti descritti negli articoli pubblicati nelle precedenti e nell’attuale uscita della Rivista e del Quaderno dell’Ordine, mi sono resa conto di quanto possa essere impattante il ruolo che noi ingegneri abbiamo su quasi tutti i Megatrends rilevanti per l’UE.
Il “Competence Centre on Foresight - Megatrends Hub” della commissione Europea identifica 14 Megatrends più rilevanti per l’UE, Megatrends che sono costantemente aggiornati dal Centro di ricerca della Commissione europea (JRC) “EU Policy Lab”. In qualche modo, tutti i 14 Megatrends sono influenzati dai temi ingegneristici, se non altro perché per la diffusione, il ruolo delle Telecomunicazioni e della Tecnologia sarà prevalente su tutti i processi. Leggendo poi nel dettaglio i Megatrends, non possiamo negare il legame diretto tra ingegneria e i diversi Megatrends, “Cambiamenti climatici e degrado ambientale”, “Diminuzione delle risorse”, “Accelerazione del cambiamento tecnologico e iperconnettività”, “Nuove sfide per la salute”, “Aumento dell’urbanizzazione”, “Cambiamenti nel paradigma della sicurezza”.

Per lo sviluppo di tali Megatrends è importante acquisire nuove competenze, utili per affrontare le nuove complessità. Ad esempio, sappiamo che per essere i protagonisti del cambiamento è importante una Transformational Leadership che possa guidare in modo più creativo il futuro e che abbia come bagaglio anche una forte base tecnica?
Ingegneri, siamo pronti?
Leggendo la pluralità di tematiche affrontate in questo Quaderno e nelle precedenti uscite, credo proprio di sì, ma occorre continuare a studiare e impegnarsi, il cambiamento non aspetta.
Non mi resta che augurarvi buona lettura, ricordandovi che nell'ottica di un approccio più agile e mirato alla condivisione, anche IO Roma si è dotata di una pagina Linkedin "IO Roma Rivista dell'Ordine Ingegneri della provincia di Roma" che vi invito a seguire. Stiamo inoltre implementando delle modifiche che renderanno più fruibile il sito della Rivista IO Roma https://rivista.ording.roma.it/.
Stay tuned!

Ing. Maria Elena D'Effremo
Direttrice Editoriale

Quaderno

Amministrazione e redazione
Piazza della Repubblica, 59 - 00185 Roma
Tel. 06 4879311 - Fax 06 487931223

Direttore creativo e progettazione grafica
Tiziana Primavera

Assistenza Editoriale
Leonardo Lavalle
Antonio Di Sabatino
Flavio Cordari

Referente FOIR
Francesco Marinuzzi

Stampa
Press Up

Ordine degli Ingegneri della Provincia di Roma
Piazza della Repubblica, 59 - 00185 Roma
www.ording.roma.it
segreteria@ording.roma.it
editoriale@ording.roma.it

Finito di stampare: ottobre 2023

Il Quaderno IOROMA è una estensione alla rivista IOROMA

Sommario

N. **2**/2023

GLI EDITORIALI

GLI ARTICOLI

Quaderno

a cura di:
Ing. Giovanni Gasbarrone

Presidente
Commissione Telecomunicazioni e Transizione Digitale

IL RUOLO DELL'INDUSTRIA DELLE TELECOMUNICAZIONI E DEL 5G NELLA TRASFORMAZIONE DIGITALE

La sempre maggiore disponibilità di piattaforme tecnologiche in un'ottica di convergenza tra Reti Mobile di nuova generazione, nuove infrastrutture TLC con architetture per la Gigabit society oltre all'utilizzo di Intelligenza artificiale, Big Data/Analytics, sta drammaticamente cambiando il modo in cui noi viviamo, lavoriamo ed interagiamo. L'industria delle Telecomunicazioni ha fornito tutti i building blocks delle infrastrutture: rete di accesso a larga banda fissa e mobile, l'infrastruttura core, l'interconnessione e le nuove architetture di Software Defined Network e Edge Computing. Tutto il processo di trasformazione digitale dipende dalla Telecom Industry che abilita i cambiamenti anche nell'Industria e nell'organizzazione del lavoro (come nel caso dello smart working). L'industria delle telecomunicazioni sta svolgendo un ruolo fondamentale nel supporto della digitalizzazione di altri settori verticali come logistica, mobilità e autotrasporto, energia, produzione industriale. La trasformazione digitale ha un forte impatto sull'economia e si realizzerà attraverso l'evoluzione delle infrastrutture degli operatori di telecomunicazioni che abilitano le nuove piattaforme di lavoro collaborativo, della produzione industriale nel settore strategico dell'industria 4.0.
Il 5G è al centro di questa rivoluzione industriale. Il 5G porterà alla nascita di servizi che cambieranno il modo di vivere, produrre, lavorare e muoversi delle persone.
Le stime del WEF (World Economic Forum) già nel 2018 indicavano che l'Industria delle Telecomunicazioni avrebbe creato valore per più di $ 10 trilioni abilitando la digitalizzazione in cinque settori industriali chiave per lo sviluppo economico e sociale a livello globale grazie ai miglioramenti della produttività e dei processi offerti dalle infrastrutture di telecomunicazioni.
Tutto sta cambiando nell'industria delle telecomunicazioni con un'accelerazione senza precedenti che si sta concretizzando con il 5G.[1]
La nuova rete mobile 5G aumenta le velocità di connessione integrando più modalità d'accesso, di gran lunga superiori rispetto al 4G, e garantisce tempi di latenza bassissimi, e in considerazione delle alte prestazioni consentirà la connessione di un numero elevatissimo di dispositivi wireless e dei sensori nell'architettura IoT ad alta affidabilità. La rete 5G è anche pensata per i nuovi scenari di cyber security offrendo resilienza e mitigando i tentativi di violazione della infrastruttura di telecomunicazione mobile.
Il centro di questa evoluzione tecnologica è la iper-connettività, tema del congresso mondiale WWRF (World Wide Research Forum) tenutasi in Malesia nel 2021. [2]
Ho partecipato in questo convegno come relatore presentando una memoria sul "Digital Transformation and Challenges in 5G Networks". [3]
In parallelo come membro dell'Advisory Board di IOTHINGS World ho partecipato alla definizione del frame work industriale per i mercati verticali che utilizzano le tecnologie IOT e alla valutazione di startup e proposte industriali con la premiazione delle migliori soluzioni presentate nell'edizione del 2021. Inoltre, queste attività si sono svolte durante partecipazione ad IOTHINGS World nell'edizione del 2023.

Figura 1
Partecipazione ad IOTHINGS World: Verso il 6G Digital Transformation e IOT [4]

Il ruolo delle infrastrutture di telecomunicazioni nella Transizione Digitale

L'industria delle telecomunicazioni incide sul 2,3% del PIL nazionale e rappresenta circa il 5% degli investimenti in Italia. L'interconnessione dei sistemi di smart logistics e smart mobilities, così come le smart grids energetiche sono al centro dei nuovi scenari di investimento e le opportunità per l'economia nazionale sono legate allo sviluppo delle tecnologie 5G del mobile e dell'infrastruttura in fibra ottica nazionale. Tutto il processo di trasformazione digitale dipende dall'industria delle telecomunicazioni che abilita i cambiamenti anche nell'organizzazione del lavoro come nel caso dello Smart Working. In Europa, l'Italia ha i suoi punti di forza nell'indice DESI 2022 nella connettività con le infrastrutture di telecomunicazioni e integrazione delle tecnologie digitali e spicca per lo sviluppo delle reti 5G. Infatti, l'Italia è il Paese che ha registrato il maggiore aumento della copertura 5G, passando in meno di un anno dal 40% al 99,7% contro un 74,4% della Francia e un 86,5% della Germania. La media EU27 è del 72% per la copertura della popolazione con una crescita media nel 2022 del 23% indicativo dell'accelerazione nell'istallazione delle stazioni radio base che hanno raggiunto ben 252.920 impianti. [5]
La regione Lazio è al centro di questo sviluppo della Digital Economy grazie alle infrastrutture. Il Lazio eccelle infatti con i suoi poli industriali come quello Tiburtino nelle Telecomunicazioni e nell'ICT, nelle Telecomunicazioni per la presenza dei centri direzionali dei maggiori player e nell'area ICT per gli investimenti significativi. In particolare, la provincia di Roma ospita i più importanti centri nazionali degli operatori Telco, satellitari e dell'industria elettronica, grazie anche ad una elevata presenza di startup e di poli tecnologici.
Questo si riflette nella Innovazione, dove il Lazio è nelle prime posizioni in Europa per brevetti e ricerca.
Secondo lo "European Regional Competitiveness index" la regione Lazio è tra la più attive d'Italia e tra le più avanzate in Europa. Nel grafico che rappresenta il benchmark europeo degli indici di competitività la Regione Lazio viene messa a confronto anche con una regione importante per

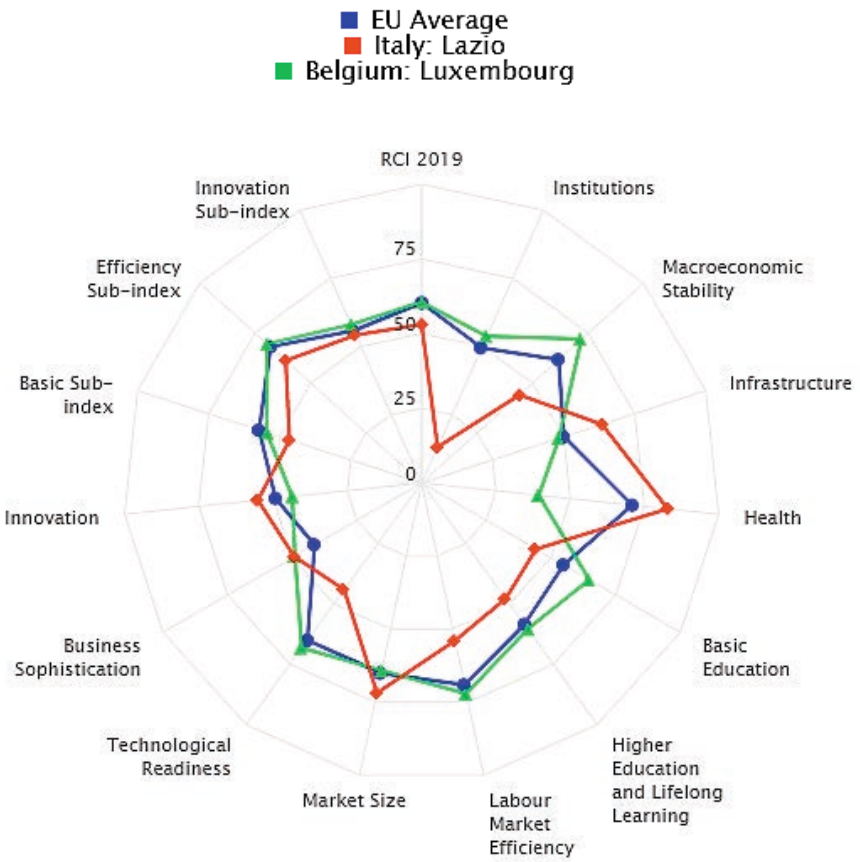
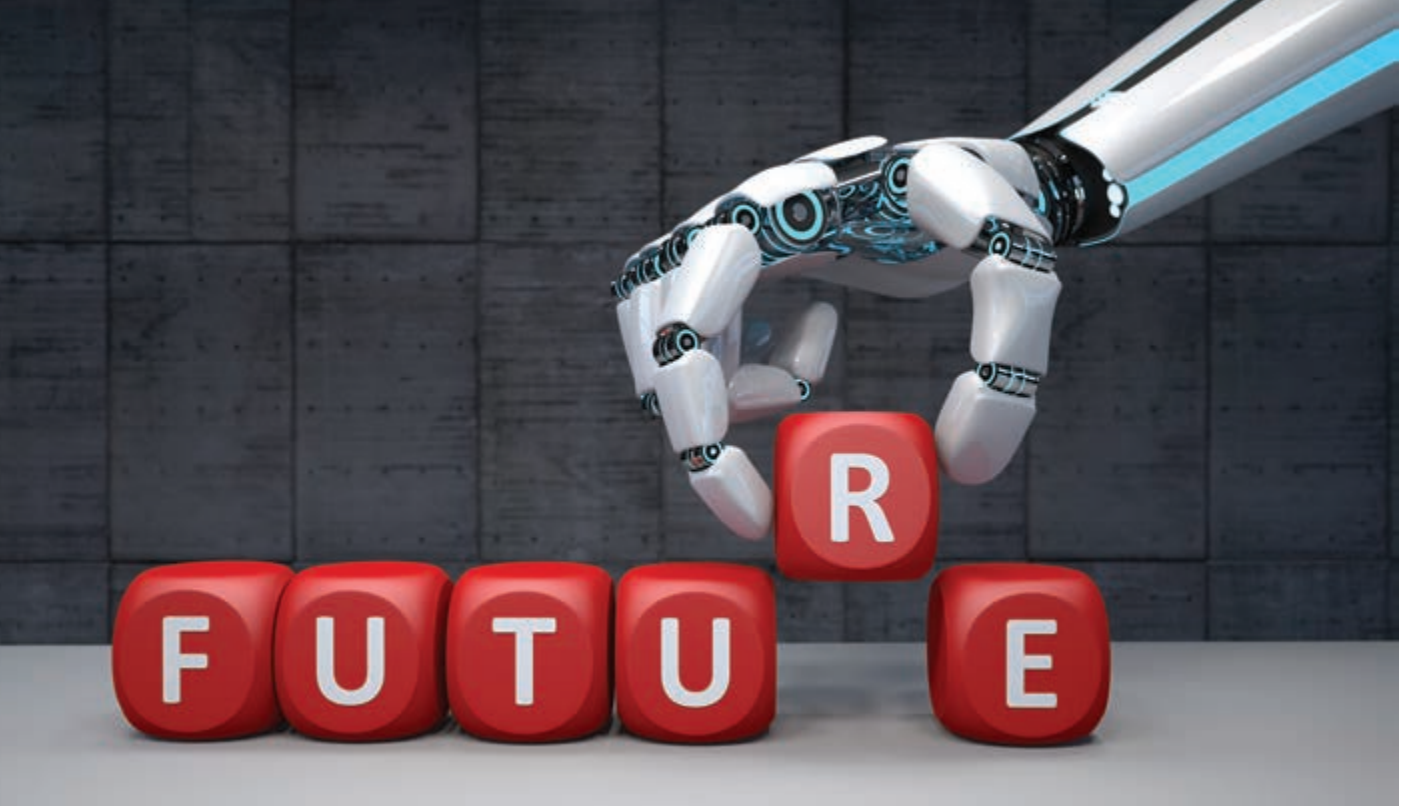


Figura 2
Benchmark di competitività regionale europea: Lazio, Belgio-Lussemburgo e media europea



sviluppo economico sociale, come Belgio-Lussemburgo. Si nota come il Lazio come dimensione di Mercato, Salute, Innovazione, infrastrutture e "business sophistication" sia sopra i parametri di benchmark europeo e sia performante in modo ottimale nei settori strategici.

Il ruolo del 5G nella "digital transformation"

Si stima che il 5G avrà un fatturato a livello mondiale di € 225 miliardi nel 2025, il 5G è quindi un asset chiave per l'Europa al fine di poter competere nel mercato globale e la sua sicurezza è fondamentale per garantire l'autonomia strategica dell'Unione Europea.
Le nuove opportunità di business saranno legate allo sviluppo delle nuove infrastrutture di rete 5G che si basano sulle architetture Software Defined Network (SDN). Lo slicing di rete nel 5G sfrutta la virtualizzazione dell'infrastruttura NFV e rappresenta una modalità di erogazione dei servizi abilitando modelli di business che si differenziano sulla base delle applicazioni nei mercati verticali oltre ad offrire una ulteriore opportunità per la sicurezza, se gestito correttamente.

Aspetti innovativi della Rete 5G

L'architettura di rete 5G è progettata intorno ai concetti di resilienza. Ad esempio, la suddivisione in sotto reti isola alcuni gruppi della rete da altre funzioni. Ad esempio, si può utilizzare una rete mobile dedicata completa in modo esclusivo. Un operatore della rete 5G può anche isolare dispositivi IoT a bassa priorità su una porzione separata per garantire che questi non interferiscano con altri utenti in caso di problemi se prevedono un uso massivo di dispositivi IoT. le reti 5G sono in grado di supportare una quantità senza precedenti di dispositivi IOT connessi: due ordini di grandezza superiori rispetto alle reti 4G riferiti ad una densità per Km^2. Si raggiungono così il milione di dispostivi connessi per Km^2.
La forte enfasi posta sulla sicurezza della rete mobile 5G è stata un fattore di differenziazione nel mercato nei confronti delle altre tecnologie wireless, alcune delle quali hanno architetture di rete intrinsecamente più vulnerabili.
L'architettura della rete 5G è integrata con le nuove funzionalità SDN/NFV (Software Defined Network/ Network Function Virtualization) copre gli aspetti architetturali e di servizio che interessano:

- device (mobili e fissi);
- le infrastrutture;
- le funzionalità di rete e quelle a valore aggiunto;
- gestione e orchestrazione del sistema.

Il Layer di business viene implementato come application layer dove sono implementati gli use case ed i Business models, e dialoga con i layer SDN/NFV (Business Enablement Layer) tramite delle API (Application Program Interface).

5G e Industria 4.0: requisiti delle applicazioni distintive

Il processo di transizione Digitale per Industria 4.0 è legato all'evoluzione delle infrastrutture di telecomunicazioni. Il fattore di trasformazione più rilevante non è quello che riguarda l'introduzione della singola tecnologia innovativa

Figura 3
Realtà virtuale e Industria 4.0

tra elementi nel processo di produzione, bensì il fatto che l'interconnessione generalizzata delle macchine e la improvvisa disponibilità di dati relativi a tutte le fasi del processo, dentro e fuori dall'azienda (ovvero progetto, produzione, vendita e utilizzo in campo) apre la porta a una completa ridefinizione delle fasi stesse, nonché alla creazione di modelli di business totalmente nuovi, non realizzabili anche solo pochi anni fa. È quindi tutta la filiera che si può ridisegnare e riorganizzare, modificando i rapporti (e a volte anche i ruoli) fra cliente, fornitore e utilizzatore finale, modificando l'offerta commerciale da vendita di prodotto a fornitura di servizio, passando da una organizzazione basata su un modello tayloristico ad una struttura flessibile che opera in modalità Lean (Lean Thinking).
In questa cornice le nuove applicazioni 5G che presentano requisiti sfidanti sono quelle legate a latenza e banda/Throughput che assicurano Quality of Experience (QoE) indispensabili per le applicazioni di Realtà aumentata, Internet tattile (applicazioni per robotica e industria 4.0) e per le applicazioni Internet of Things (IoT) ad elevate affidabilità Ultra-reliable IoT.
Ma non solo, con la velocità, latenza ed accesso alle risorse radio in modalità innovativa: anche grazie a network capability come lo "slicing" 5G, è possibile progettare servizi che si adattano alle esigenze di un'impresa o utente con specifiche esigenze di QOS come, ad esempio, riunioni video e smart working ad alta priorità o applicazioni per le smart factory di internet tattile. In questa applicazione i parametri "delay" sono di pochi millisecondi e la velocità della connessione deve essere al massimo consentendo quindi di operare da remoto in modo diretto nell'ambiente "smart factory" e in modalità virtuale con i visori che consentono una customer experience come in presenza. Le applicazioni sono molteplici in situazione d'emergenza e in ambiente non presidiato.

Transizione Digitale: Telecomunicazioni & Smart working

Nei settori produttivi in Italia sia il telelavoro che le fabbriche con un elevato grado di automazione sono soggette ad un maggior rischio cyber sia per le soluzioni di continuità operativa in fase di aggiornamento, sia per le architetture di rete d'emergenza. Il nuovo perimetro che include le reti in ambito residenziale presenta infatti un maggiore rischio per la cyber security specie se si gestiscono processi di produzione delle Smart Factory da remoto.
In questo scenario si complica l'architettura dei servizi: sarà possibile effettuare chiamate olografiche sulla rete 5G e grazie ai visori disponibili per la realtà virtuale e aumentata con gli smartphone 5G e sarà possibile partecipare alle presentazioni in 3D a distanza condividendole da tablet e smartphone. La realtà aumentata e la realtà virtuale sono le applicazioni che viaggeranno sulla rete 5G grazie alla maggiore larghezza di banda e bassissima latenza.
L'evoluzione del concetto di ambiente di lavoro collaborativo si attua quindi con il 5G attraverso la creazione di uno spazio virtuale per le riunioni in cui l'avatar dell'organizzatore interagisce con quelli dei colleghi che sono in altri sedi, condividendo contenuti multimediali nei tavoli di lavoro

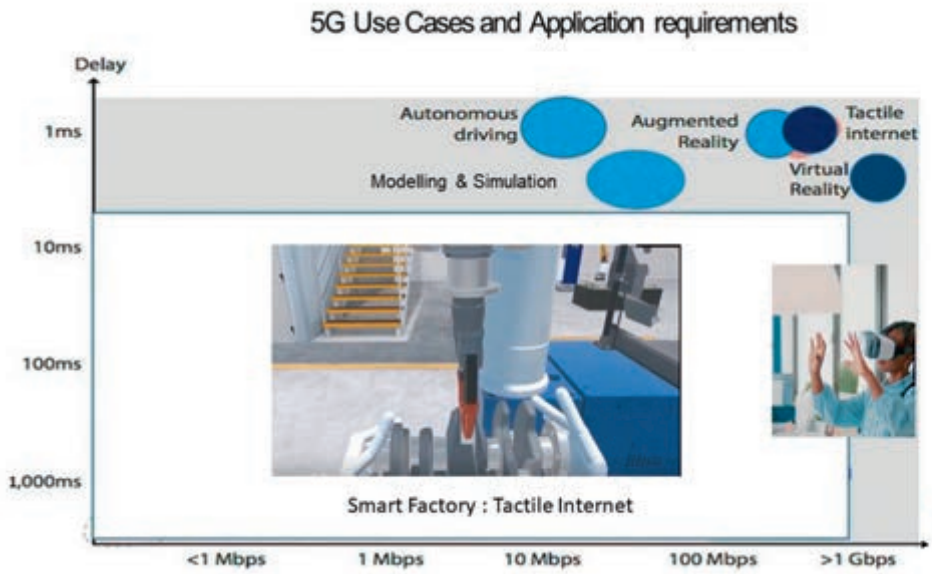


Figura 4 - Servizi distintivi abilitati dalla rete 5G

3D. Attualmente la collaborazione ai progetti e la condivisione di attività si attuano grazie alle piattaforme applicative in cloud di lavoro collaborativo a cui si accede con "device" mobili come tablet e PC. Quindi lo Smart Working in 5G rappresenta un vero salto di paradigma.
Durante il Covid abbiamo sperimentato nuove modalità di interazione e lavoro a distanza anche nel controllo delle istallazioni industriali. L'infrastruttura di telecomunicazione in Italia si è rivelata infatti fondamentale con la sua resilienza ed ha assorbito gli elevati picchi di traffico legati al lock down in ambito sociale e lavorativo.
Durante la diffusione della pandemia Covid ed a seguito del lock down i sistemi produttivi e sociali si sono dovuti adattare alle nuove necessità organizzative del mondo del lavoro attraverso lo smart working e l'evoluzione delle reti aziendali extra-net e industriali con l'automazione e controllo a distanza nella Smart factory. Passato il periodo di lock down gli spostamenti per lavoro e quelli per il tempo libero tendono a riallinearsi al periodo precedente, tuttavia permane un divario ancora significativo, segno che alcuni processi legati al lavoro con la trasformazione in rete collaborativa con postazioni casa-ufficio sono diventati irreversibili. Se osserviamo le statistiche legate agli spostamenti derivate dalle elaborazioni dei dati basati sulle applicazioni degli smartphone con le informazioni di localizzazione elaborate in modalità anonima, si scoprono interessanti fenomeni in ambito sociale e lavorativo.
Dai dati statistici disponibili si comprende come nel periodo di lock down le infrastrutture di TLC siano state sottoposte a carichi crescenti di traffico per il fenomeno del trasferimento nelle abitazioni delle attività produttive a causa dello smart working sbilanciando così i flussi di traffico voce e dati. Nel caso di Londra l'attività dell'area direzionale della City si era completamente spostata in ambito residenziale.

La resilienza delle Reti 5G

La protezione delle infrastrutture critiche industriali e legate alla fornitura dei servizi pubblici, dipende fortemente dalle reti di Telecomunicazione nell'ambito di una più ampia strategia di resilienza delle filiere produttive. Ogni interruzione o perdita del servizio di una delle infrastrutture chiave può essere seriamente invalidante per il nostro Paese e per il cittadino che ne è fruitore. Le interconnessioni tra le infrastrutture critiche possono causare un effetto domino poiché le reti elettriche, trasporti, e telecomunicazioni sono mutuamente interdipendenti, a tal punto che il grado di interconnessione ha un effetto sulla resilienza di queste infrastrutture incidendo pesantemente sulla loro operatività e piena funzionalità.
Lo scenario di sicurezza cibernetica si complica ulteriormente con l'utilizzo dell'IOT massivo (Internet of Things) abilitato dal 5G in ambito sanitario, mobilità, Smart City e Industria 4.0. Verranno esaminati alcuni scenari di cyber security legati all'evoluzione delle infrastrutture TLC e come mitigare i rischi legati alla evoluzione dello Smart Working e della Smart Factory imposti dai cambiamenti produttivi e sociali causati dal COVID.
Le reti 5G sostituiranno nella loro evoluzione

man mano che si renderanno disponibili, i meccanismi di sicurezza già in campo con misure dinamiche che vengono implementate dai sistemi basati sull'intelligenza artificiale per rispondere a una nuova generazione di attacchi "zero day" su più livelli.
Le strategie di protezione delle Reti 5G si inquadrano in una serie di controlli di visibilità di tutti gli elementi in real time, con rilevamento delle intrusioni e meccanismi di mitigazione per rendere una superficie di attacco più gestibile applicando tecniche di intelligenza artificiale.
L'introduzione della sofisticata suddivisione in sotto reti nel 5G (network slicing) tende a contrastare l'aumento della superficie di attacco attraverso la quale è possibile effettuare attacchi DDOS ed introdurre malware nelle piattaforme del cliente. Così le nuove protezioni 5G isolano queste sezioni attraverso più livelli della rete e forniscono sicurezza end-to-end attraverso un frame work di autenticazione comune.
Questa suddivisione facilita inoltre l'implementazione personalizzabile delle funzioni sensibili alla sicurezza dell'accesso alla rete 5G, come la crittografia del piano utente, in una posizione centrale sicura, mantenendo le funzioni non sensibili alla sicurezza in posizioni distribuite meno sicure.
Gli attacchi DDOS "multi vector" avvengono a vari livelli e interessano tutte le componenti architetturali secondo strategie precise che mirano a superare le difese saturandole per arrivare all'applicazione d'utente come, ad esempio, nella fabbrica fortemente automatizzata. Nella Figura 6 si esprime a livello concettuale la coesistenza degli attacchi "multi vector".
La crescita esponenziale di dispositivi IoT collegati alle reti Telco e alle infrastrutture cloud, combinato con lo sviluppo delle reti 5G necessarie per la loro diffusione, sta tuttavia creando un ambiente ricco di insidie in ambito cybersecurity. Questo panorama di minacce richiede alla industry Telco di modificare l'approccio alla sicurezza della rete, non più solo tesa a garantire quella interna legata alla resilienza delle infrastrutture agli attacchi informatici ma anche quella esterna legata alla nuova superficie di attacco DDOS generato dalla crescita incontrollata dei dispostivi IOT non tutti conformi agli standard minimi di sicurezza.

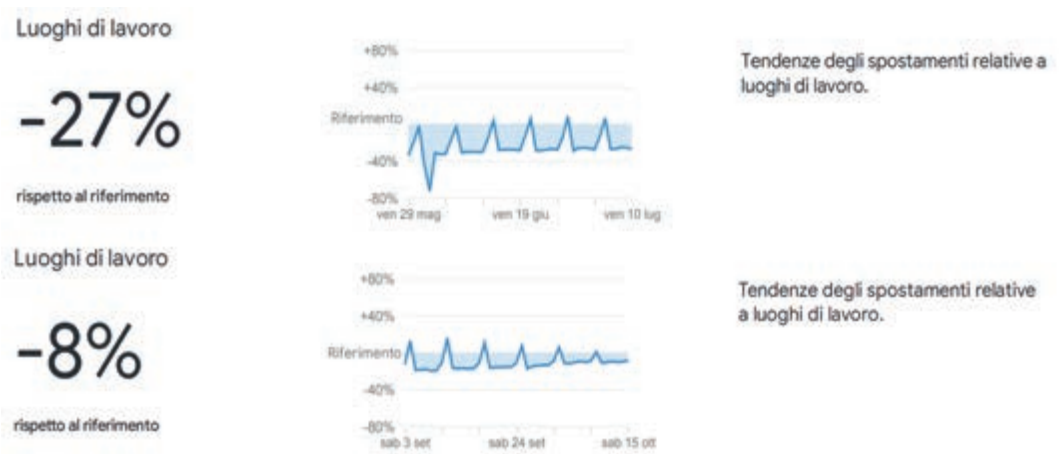


Figura 5
Analisi della mobilità verso i luoghi di lavoro in modalità aggregata (casa–ufficio) rispettivamente 2020 in alto 2022 in basso [6-7]

Su questi aspetti sono state emanate delle linee guida dall'agenzia europea ENISA per il 5G sugli aspetti di "Threat Landscape for 5G Networks". Il 5G abiliterà Massive Internet of Things (MIoT) applicazioni come sensori di traffico e servizi da veicolo a infrastruttura (V2I) che sono alla base delle città intelligenti. È fondamentale che gli hacker non possano accedere a tali dati, dirottare i dispositivi IoT o interrompere i servizi con attacchi DDoS (Distributed Denial of Service).
La resilienza del sistema 5G agli attacchi informatici è realizzata attraverso una varietà di funzioni complementari. Innanzitutto, l'accesso alla rete 5G è stato sviluppato pensando a molti use cases e predisposto per funzionalità che supportano la sicurezza, e alcuni di questi sono stati raccolti in una classe sotto il termine comunicazioni ultra-affidabili a bassa latenza (URLLC). Le funzionalità fornite da 5G NR per casi d'uso di questa classe sono ideali per il controllo industriale e le infrastrutture critiche.
Il lavoro sulla cyber-security per il 5G viene svolto nei gruppi di standardizzazione internazionali dove sono armonizzate soluzioni per evitare le minacce e rendere robuste e resilienti agli attacchi degli hacker i protocolli e le architetture 5G core e radio.
Tra questi si segnala ETSI, GSMA, 3GPPP e 5GPPP che hanno prodotto standard e raccomandazioni.
Vanno sottolineati i miglioramenti nelle tecnologie 5G che sono stati pertanto sviluppati dai costruttori secondo le raccomandazioni di questi enti di standardizzazioni per affrontare le minacce alla sicurezza informatica attuali ed emergenti nelle reti 5G.
La sicurezza rimane pertanto un tema centrale nella commercializzazione delle reti 5G in tutto il mondo. Gli standard 3GPP 5G includono miglioramenti per crittografia, autenticazione, protezione dell'integrità, privacy e disponibilità della rete Il 3GPP (3rd Generation Partnership Project), è l'organizzazione mondiale che ha lavorato allo sviluppo standardizzato di tutti i requisiti di sicurezza fondamentali che includono misure per la crittografia, l'autenticazione reciproca degli elementi di rete core e di accesso, la protezione dell'integrità, la privacy e la disponibilità della rete. Risulta così un "frame work" di autenticazione unificato che consente una mobilità senza soluzione di continuità tra le diverse tecnologie radio di accesso e di interconnessione tra gli elementi core. Particolare attenzione è stata posta nella protezione della privacy dell'utente per le informazioni sensibili che essendo potenzialmente vulnerabili potrebbero essere utilizzate per identificare e tracciare gli abbonati. È stato migliorato in ottica sicurezza i protocolli SS7 e Diameter per il roaming.

Il principale obiettivo del 3GPP Security Working Group (SA3) è garantire che le "security features" sviluppate per la rete LTE possano evolvere e svilupparsi per il 5G e che tutti i potenziamenti e sviluppi per la security nel 5G per garantire i nuovi servizi debbano anche prendere in considerazione ed armonizzarsi per l'impatto sui sistemi esistenti LTE. Questo approccio duale e simmetrico consente di risparmiare tempo ed aiuta a ridurre le possibili duplicazioni negli standard e aiuta l'impegno del gruppo nell'eliminare le minacce sulla interfaccia radio, nel piano della segnalazione, privacy e interfaccia utente.
Come deve essere quindi progettata la sicurezza per i nuovi casi d'uso abilitati dal 5G?
Le soluzioni infrastrutturali per gli "use cases" relativi ai mercati verticali devono tener conto delle nuove "network capabilities" e sfruttare tutti i meccanismi che lo standard 5G mette in campo non ultima la sua resilienza. Si possono utilizzare sotto reti virtuali con il network slicing per piattaforme IOT mission critical con la 5G Ultra-Reliable Low-Latency Communication URLLC. In tal modo si isolano le reti IOT ad alte prestazioni e critiche per i servizi di pubblica utilità e per la fabbrica intelligente, Smart Factory, dalle reti consumer IOT per applicazioni domestiche di robotica smart home. Inoltre, l'implementazione dovrà essere conforme agli standard tecnici internazionali delle reti TLC con i dispositivi IOT di ultima generazione che devono soddisfare i requisiti minimi di sicurezza (ENISA).
La crescita esponenziale di dispositivi IoT collegati alle reti di telecomunicazione e alle infrastrutture cloud, combinata con lo sviluppo delle reti 5G necessarie per il loro sviluppo, sta creando un ambiente ricco di insidie in ambito cybersecurity. Questo panorama di minacce richiede di modificare l'approccio alla sicurezza della rete, non più solo tesa a garantire quella interna legata alla resilienza delle infrastrutture agli attacchi informatici ma anche quella esterna legata alla nuova superficie di attacco DDOS generato dalla crescita incontrollata dei dispositivi IOT non tutti conformi agli standard minimi di sicurezza. Secondo il WEF (World Economic Forum) i dispositivi connessi IOT saranno di gran lunga più numerosi della popolazione mondiale.
Le nuove applicazioni 5G che presentano requisiti sfidanti sono quelle legate a latenza e banda/Throughput che assicurano Quality of Experience (QoE) necessari per la Realtà aumentata, Internet tattile (applicazioni per robotica e industria 4.0) e per le applicazioni Internet of Things (IoT) ad elevate affidabilità Ultra-reliable IoT. Ma non solo la velocità, latenza ed accesso alle risorse radio in modalità innovativa: anche grazie a network capability come lo "slicing" 5G, è

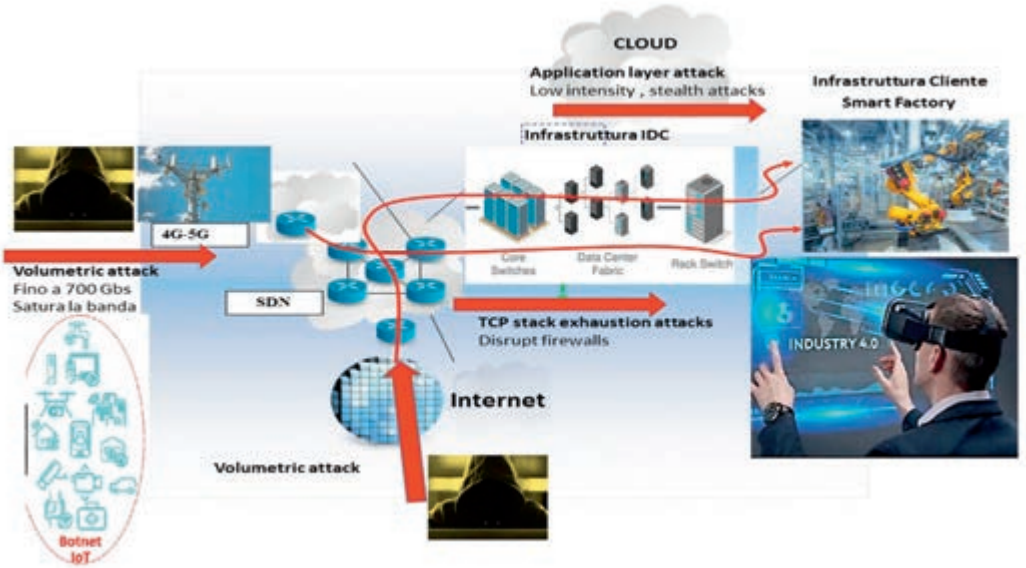


Figura 6
Attacchi multi vector (volumetrici DDOS) su rete Mobile e infrastrutture TLC

Figura 7
Specifiche ENISA per la cybersecurity della Rete 5G


WORLD MAP


/:: DFG2ER 121CVS
/:: DVB-ERQ-TL.:.L
/:: 13RTVN134 58 3
/:: 135 325 VERY2
/:: CCNRFT 2334 13
/:: 1245 34 YXDVN
/:: 124C6VBTHMY
3431
1 5 41 1 1 12310XS
GDSFTG.1 4Z1
1454///Z GFG.
45SER112231
/::RS13154 14546731/ 4113443431
/::ZRR13251 51524454 1321X 1 5 41 1 1
/::32150123 SDF3T E R VEGDSFTG.1
/::1321 1 RCDCEW HHTY Z121 1454///Z
/::VGDL.R [ ]]] ZR1223 .... 145SER11
121CV5063"--DVW 1213
-TL.:.L.-- .;LZLD.VLLL
34 56 32GF 235 SD
CVERY2 356 89
2334 135532 55551566
YXDVNMM 1346 RERY
THMY Y Y Y YRGJJ..IO
/::RS13154 14546731/ 4113443431
/::ZRR13251 51524454 1321X 1 5 41 1 1 12310XS
/::32150123 SDF3T E R VEGDSFTG.1 4Z1
/::1321 1 RCDCEW HHTY Z121 1454///Z GFG.
/::VGDL.R [ ]]] ZR122231 .... 145SER1122231
73%
64%

possibile progettare servizi che si adattano alle esigenze di un'impresa o utente con specifiche esigenze di QOS come, ad esempio, riunioni video e smart working ad alta priorità.
Questo senza subire rallentamenti e criticità della rete legate a traffici a bassa priorità (gaming e filmati video ricreativi). Questa nuova architettura che presenta innegabili vantaggi introduce nuovi tipi di minacce alla sicurezza poiché crea una superficie d'attacco aumentata. Questo impatta sul perimetro di sicurezza nazionale. In caso di "rischio grave e imminente per la sicurezza nazionale connesso alla vulnerabilità di reti, sistemi e servizi", l'art. 5 del Perimetro di Sicurezza Nazionale Cibernetica concede al Presidente del Consiglio dei Ministri il potere di disattivare, in modo parziale o totale, uno o più apparati o prodotti impiegati nelle reti e nei sistemi colpiti. Questo può riguardare porzioni di reti (ad es. Sottoreti slicing 5G, componenti reti IOT).
Il network slicing è una componente di architettura di rete fondamentale nel 5G. La suddivisione in rete E2E sfrutta le network capabilities della tecnologia di virtualizzazione nel 5G per affrontare in modo flessibile un'ampia varietà di casi d'uso con requisiti diversi.
Un operatore della rete può anche isolare i dispositivi IoT a bassa priorità su una porzione separata per garantire che questi non interferiscano con altri utenti in caso di problemi con dispositivi IoT mission critical o per servizi di sicurezza pubblica.

Ma se tutte le difese predisposte vengono superate non resta che attivare misure drastiche sulle infrastrutture di rete. Tra gli strumenti tecnologici previsti di controllo e disattivazione di elementi critici delle infrastrutture abbiamo l'architettura con la virtualizzazione di porzioni rete (slicing) nel 5G. Il "network slicing" è la capacità di poter configurare reti per diverse categorie o gruppi di clienti attivando il funzionamento simultaneo di reti virtuali/logiche per supportare operatività aziendali indipendenti (ad esempio con scenari specifici di casi d'uso verticali nel trasporto, nella sanità o servizi pubblici) utilizzando una infrastruttura fisica comune.

Wireless World Research Forum: attività "Beyond 5G", verso il 6G

Nel Wireless World Research Forum è emerso con chiarezza sin dall'inizio delle attività di ricerca che le nuove architetture dei servizi per i mercati verticali sarebbero state sempre più legate allo sviluppo di architetture Software Defined Network nel 5G, mentre per il 6G si lavora sui nuovi use cases che richiederanno il 6G, ed i business models che giustifichino gli investimenti necessari per le nuove tecnologie Radio.
Queste nuove tecnologie offrono una serie di potenzialità e vantaggi perché consentono di ottimizzare le risorse radio e gli investimenti e ottenere così una pianificazione efficiente nell'uso delle reti fisse e mobili, offrendo una mobilità glo-

bale agli utenti in una cornice in cui la sicurezza è sempre al centro dei requisiti di progettazione.
Tra le tecnologie innovative wireless, in un prossimo futuro, quelle di Software Defined Radio e Cognitive Radio saranno in grado di adattarsi alle variazioni dell'ambiente, alle interferenze e alla disponibilità delle frequenze licenziate e non, contribuendo così alla gestione del traffico nelle comunicazioni tra diversi sistemi, anche in scenari operativi che prevedano metodologie di gestione dello spettro più flessibili.
La Cognitive Radio è la tecnologia intelligente che esplora lo spettro sfruttando i buchi delle frequenze non licenziate o sottoutilizzate e la loro disponibilità spaziale. Nella rete di comunicazione 6G si prevede che i dispositivi come gli smartphone interagiscano con le stazioni radio base della rete cellulare e ricevano indicazioni sulla porzione di spettro in cui possono trovare condizioni più favorevoli in termini di maggiore disponibilità per le frequenze e bit rate.
Sia la cognitive radio (CR) che la sesta generazione di reti wireless con standards 6G abiliteranno nuovi modelli di business: mentre da un lato, la Cognitive Radio offre la possibilità di aumentare in modo significativo l'efficienza dello spettro utilizzato dagli utilizzatori finali (CR users) grazie all'utilizzo dei buchi di frequenza non licenziata e al livello di utilizzo delle bande disponibili, dall'altro lato, il 6G abiliterà l'interconnessione ultra broadband con applicazioni con Quality of Service (QoS) definite per classi d'utente differenziate per scopi e scenari con modelli di business basati sulle architetture di servizio richieste dal mercato in modalità intelligente con le reti neuronali.
Sarà pertanto possibile adattarsi ai rapidi mutamenti di mercato grazie ad una combinazione di servizi 6G che abiliteranno business model diversificati in rapida evoluzione.
Questo è il vero scopo del 6G: non la tecnologia, ma anticipare le esigenze del mercato per offrire servizi "net-centrici". Le reti 6G continueranno il percorso evolutivo basato sul 5G, che include reti sempre più "self-organizing", un'avanzata qualità del servizio e con un'architettura "edge computing" che supporta l'accesso ai servizi erogati dal 6G Core basato su piattaforme di Intelligenza Artificiale e Machine Learning. In questa architettura sarà la componente di backhaul con la CDN e la componente CORE con AI & Machine Learning a mitigare gli attacchi cyber.
La prossima decade vedrà il 6G connettere miliardi di dispositivi, sensori e veicoli connessi, in uno scenario in cui i robot e i droni genereranno Zettabyte di informazioni digitali. Il 6G migliorerà le applicazioni 5G con requisiti più stringenti, ad esempio la telepresenza olografica e la comunicazione immersiva, e soddisferà parametri ancora più severi rispetto al 5G. A partire dal 2030 potremmo assistere all'avvento dell'era in cui l'uso della robotica mobile personale interagirà con piattaforme di Intelligenza Artificiale

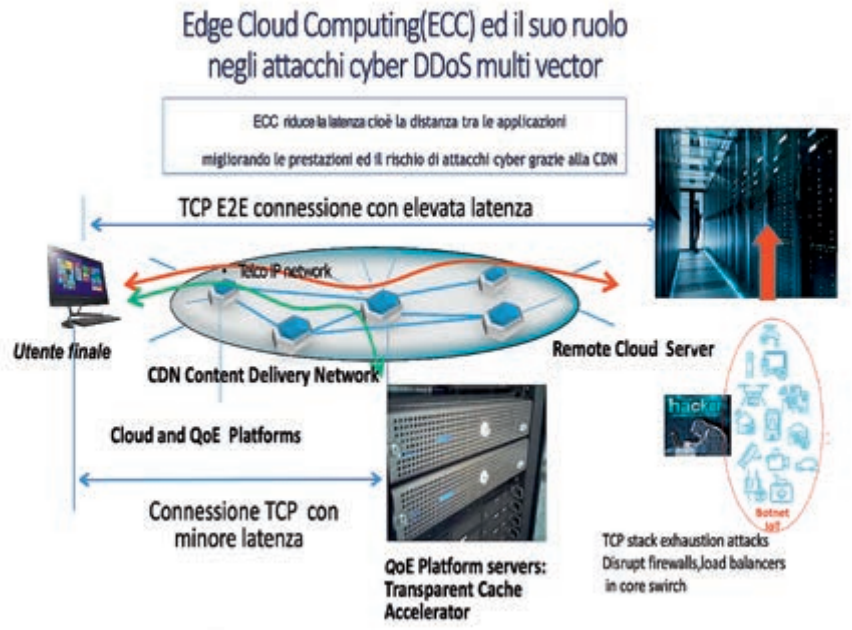


Figura 8 - Edge Cloud Computing e attacchi cyber DDOS.

di nuova generazione grazie a sistemi neuronali offerti dalla connettività della rete 6G. L'intelligenza artificiale sarà sia locale che distribuita grazie ad architetture di fog computing e capacità di quantum computing. "AI everywhere" è il mantra della nuova rete.
Il 6G è la generazione di reti mobili che ci aiuterà ad affrontare queste sfide socioeconomiche in cui il modo di vivere e lavorare farà un nuovo salto di paradigma. Si evolverà progressivamente dall'essere umano-centrico come nel 5G, ad essere sia umano che macchina-centrico. Il 6G offrirà una connettività wireless completa quasi istantanea e senza restrizioni grazie alla cognitive radio in cui l'intelligenza artificiale si cala sia nel dispositivo che nella gestione delle interfacce radio.
Un nuovo panorama emergerà anche per le industrie e le aziende coinvolte sempre dalla trasformazione digitale grazie alla convergenza che il 6G abiliterà nei campi della connettività, della robotica, del cloud. Ciò rimodellerà radicalmente il modo in cui operano le aziende cambiando anche le relazioni sociali future. Questo ci espone a rischi legati alla carenza di siti di sviluppo di microchip in Europa.

Bibliografia

[1] "5G Business Modelling" https://rivista.ording.roma.it/5g-business-modelling/
[2] "Hyperconnectivity: Beyond 5G, Opportunites & Challenges" https://wwrf45.wsconferences.com/
[3] "Speakers - WWRF" https://wwrf45.wsconferences.com/keynote-speakers/
[4] "ANUTEI all'IOTHINGS 2023" http://www.anutei.it/index.php/8-conferenze/78-anutei-all-iothings-2023
[5] "4 th 5G Observatory Stakeholder workshop" CNECT/2021/OP/0008 European 5G Observatory, Phase III https://5gobservatory.eu/wp-content/uploads/2022/11/4th-E5GO-stakeholder-workshop_consortium.pdf
[6] Variazioni negli spostamenti in Italia 10 luglio 2020 https://www.gstatic.com/covid19/mobility/2020-07-10_IT_Mobility_Report_it.pdf
[7] Variazioni negli spostamenti in Italia 15 ottobre 2022 https://www.gstatic.com/covid19/mobility/2022-10-15_IT_Mobility_Report_it.pdf
[8] "Verso il 6G: modelli e strategie per l'ecosistema italiano e Ue" https://www.agendadigitale.eu/infrastrutture/verso-il-6g-modelli-e-strategie-per-lecosistema-italiano-e-ue/
[9] "Microchip, 5G e cloud: così la Ue accelera sui pilastri della trasformazione digitale" https://www.agendadigitale.eu/industry-4-0/microchip-5g-e-cloud-cosi-la-ue-accelera-sui-pilastri-della-trasformazione-digitale/
[10] "5G e Industria 4.0, il ruolo delle telco per la quarta rivoluzione industriale" https://www.agendadigitale.eu/infrastrutture/5g-e-industria-4-0-ecco-il-ruolo-delle-telco-per-la-quarta-rivoluzione-industriale/
[11] "5G business modelling" https://rivista.ording.roma.it/5g-business-modelling/
[12] "Industry 4.0 – Come la Digital Transformation incide nella rivoluzione industriale" https://rivista.ording.roma.it/industry-4-0-come-la-digital-transformation-incide-nella-rivoluzione-industriale/
[13] "Telecommunications industry: Come le Telecomunicazioni abilitano la quarta rivoluzione industriale" http://rivista.ording.roma.it/digital-transformation/
[14] "Come lo sviluppo delle infrastrutture di Telecomunicazioni incide sulla Digital Trasformation" http://rivista.ording.roma.it/digital-transformation-2/
[15] "Cognitive Radio e Software Defined Radio per le reti di Telecomunicazione" https://rivista.ording.roma.it/cognitive-radio-e-software-defined-radio-per-le-reti-di-telecomunicazione/
[16] "Cybersecurity a prova di 5G, così nasce la "resilience by design"" https://www.agendadigitale.eu/infrastrutture/cybersecurity-a-prova-di-5g-cosi-nasce-la-resilience-by-design/
[17] "Cybersecurity per IoT e 5G, il ruolo strategico degli standard" https://www.agendadigitale.eu/sicurezza/cybersecurity-per-iot-e-5g-il-ruolo-strategico- degli-standard/
[18] "In sicurezza verso la rivoluzione 5G" http://channels.theinnovationgroup.it/cybersecurity/sicurezza-rivoluzione-5g/
[19] Tavola rotonda: "perimetro cyber e data protection nell'internet of things" http://www.anutei.it/index.php/associazione/regolamento/8-conferenze/28-tavola-rotonda-perimetro-cyber-data-protection-nell-internet-of-things
[20] "5G, cosa cambia per il mondo del lavoro" https://www.agendadigitale.eu/infrastrutture/5g-cosa-cambia-per-il-mondo-del-lavoro/
[21] "5G e IoT per gestire le reti elettriche: l'impatto sulla cybersicurezza" https://www.agendadigitale.eu/infrastrutture/5g-e-iot-per-gestire-le-reti-elettriche-limpatto-sulla-cybersicurezza-anche-delle-auto/

STORIA E VICISSITUDINI DI UN RADIOISOTOPO NATURALE: L'URANIO 238

a cura di:
Ing. Giovanni Bava

Commissione:
Gestione impianti nucleari

Rivisto da:
Ing. Alberto Taglioni
Responsabile dell'Area Nucleare

Questo articolo ha offerto all'autore ed intende offrire al lettore l'occasione per ripassare o acquisire nozioni interessanti e per riflettere su situazioni particolari della vita del nostro pianeta, anche conseguenti alle attività umane. Esso è stato reso disponibile per commenti alla Commissione Gestione Impianti Nucleari e modificato in base ai suggerimenti ricevuti (si ringraziano, in particolare, gli ingg. A. Papa e F. Zambardi). L'autore esprime gratitudine per lo stimolante contesto costituito dalla Commissione Gestione Impianti Nucleari dell'Ordine degli

Ingegneri di Roma e dai professionisti che la compongono. In allegato sono riportati specifici approfondimenti, richiamati nel testo.
Isotopi dell'Uranio con numero di massa pari a 238[1] videro la luce o, più precisamente, i fotoni a partire, presumibilmente, da una decina di miliardi di anni fa; in un primo tempo, per opera di primordiali stelle super massicce, che poterono disporre di quantità di "combustibile[2]", utile alla fusione nucleare, particolarmente elevate [1]. Successivamente si verificarono diversi processi di produzione, legati al fenomeno delle supernove. Stelle un po' meno robuste, ma comunque ancora definibili massicce[3], non più alimentate a sufficienza, cominciarono ad esaurire il combustibile più idoneo e dovettero constatare che non era possibile produrre energia continuando a fondere nuclei che, divenuti pesanti, non erano più in grado di assicurare un bilancio energetico positivo attraverso il processo di fusione (Approfondimento 1). Quelle stellone, quindi, dovettero cedere all'insistenza della gravità, che già da tempo le invitava a collassare, creando le condizioni per sviluppare, in tempi ristretti, nuove, enormi quantità di energia. La catastrofica implosione fece crescere rapidamente la temperatura trasformandole in astri esplodenti estremamente brillanti, chiamati supernove; la nuova, rilevante energia generata, in un crogiolo di protoni, neutroni, elettroni e nuclei leggeri [1]-[14], consentì loro di continuare per un po' il lavoro di produzione di nuclei sempre più pesanti, con diverse modalità, nonché di scaraventare nell'universo i nuovi prodotti. Fenomeni analoghi si ripeterono e continuano a ripetersi generando quantità enormi di atomi, distribuiti in maniera non omogenea nell'universo. Altri meccanismi di formazione di elementi pesanti, oggetto di studi particolarmente recenti, sono attribuibili alla presenza di neutroni all'interno di alcune stelle longeve (processo lento) o a fenomeni quali le violente collisioni di stelle di neutroni (processo rapido). In quei contesti hanno luogo reazioni di cattura dei neutroni con la formazione di nuclei sempre più pesanti che, decadendo con l'emissione di elettroni, pongono le premesse per la formazione di atomi con più elevato numero atomico[4] [16]-[18].

Figura 1
Immagine di una supernova [14].

L'Uranio 238 è tra gli atomi più pesanti formati in quei contesti e poi proiettati nello spazio; il suo nucleo, con il grosso carico di protoni (92) e di neutroni (146), non era stabile ma la sua struttura gli consentiva comunque di sopravvivere a lungo, portando a 4,5 miliardi di anni il tempo di dimezzamento, per decadimento radioattivo, del numero di atomi presenti. È interessante osservare, nello schema in Figura 2, come L'Uranio 238, decadendo, dia luogo ad una pluralità di isotopi di elementi diversi che, a loro volta, decadono finché non si forma un isotopo del Piombo stabile (Pb 216). Il processo che conduce al termine della catena è tutt'altro che rapido, basti pensare ad esempio che uno dei nuclei intermedi, il Protoattinio 234, ha un tempo di dimezzamento di 33000 anni. Se la famiglia costituita dal padre e dai discendenti rimane compatta ed isolata per tempi molto lunghi (cosa difficilmente realizzabile in maniera completa dati i tempi di dimezzamento così elevati), le attività di tutti i componenti tenderanno a uguagliarsi e la concentrazione di ciascuno di essi si porterà a valori inversamente proporzionali alla propria vita media.

A seguito dei fenomeni astrali, insieme all'Uranio 238, un gran numero di atomi con diverse caratteristiche prese a vagare nell'universo, aggregandosi in varie forme e contribuendo alla formazione di galassie e sistemi planetari. Destini simili, viste le comuni caratteristiche atomiche, li ebbe un altro isotopo dell'Uranio, il 235, generato in maniera indipendente, con vita media più breve[5] ma propenso a formare le medesime aggregazioni. Una marcata differenza di comportamento dei nuclei dei due suddetti isotopi riguarda l'atteggiamento nei confronti dei neutroni eventualmente incidenti su di essi; l'isotopo 238 tende prevalentemente ad assorbirli, trasformandosi, dopo un paio di decadimenti, in un "prezioso" isotopo del Plutonio, il 239, per questo viene considerato "fertile"[6] (solo in presenza di neutroni con particolari energie anche l'U238 può subire la fissione); il nucleo dell'isotopo 235 viene prevalentemente frantumato dall'impatto di neutroni a bassa[7] velocità (termici), liberando nuova energia, e viene, per questo, considerato "fissile". Attualmente, nelle zone della crosta terrestre dove è presente l'Uranio, l'isotopo 235 si presenta con una percentuale in peso pari a circa il 7 per mille. Questa percentuale, che era superiore nel passato, tende lentamente a ridursi ulteriormente a causa del più rapido decadimento dell'Uranio 235 rispetto al 238.

A partire dalla primigenia sfera fusa, che costituiva il neo pianeta terra, complessi fenomeni hanno determinato la attuale distribuzione dell'Uranio nelle varie parti della crosta oceanica e continentale, nonché nelle profondità, fino al nucleo centrale [16]. Già da molti decenni [19] gli studi e le indagini hanno portato a ritenere che la primitiva distribuzione disomogenea dell'Uranio sulla crosta terrestre persistette a lungo, fino a quando non vennero generate rocce con concentrazioni più elevate attraverso una combinazione di processi orogenetici, metamorfici e sedimentari. Da tali formazioni l'Uranio fu successivamente rimobilizzato e concentrato formando i depositi attuali contenenti suoi minerali [19].

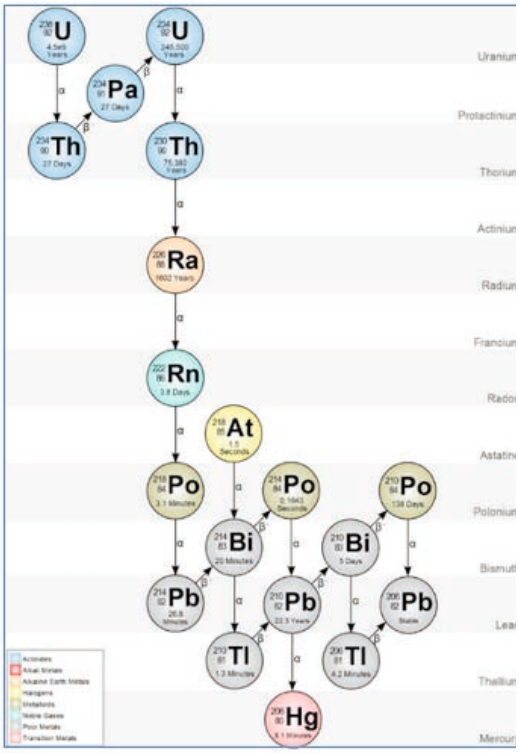


Figura 2 - catena di decadimento dell'U238 [9].

L'Uranio 238 è l'elemento più pesante presente in natura; puro, si presenta come un metallo bianco argenteo, duttile e malleabile; se finemente suddiviso è piroforico. La sua struttura atomica, contenente ben 92 elettroni, gli conferisce peculiari caratteristiche chimiche. In particolare, i suoi orbitali più esterni, 5f (che caratterizzano gli attinid) e 6d, dispongono solo di 3 e 1 elettrone rispettivamente[8], hanno pertanto una propensione a perdere o condividere elettroni, manifestando un comportamento metallico, con legami forti. La valenza che si riscontra più di frequente è la 6, ma possono presentarsi anche le valenze 5, 4 e 3; gli stati allotropici dell'Uranio metallico sono tre, in funzione essenzialmente delle temperature (ortorombico, tetragonale e cubico a facce centrate). Altre caratteristiche chimico fisiche di interesse sono l'elevata den-

Figura 3
minerale di Zircone delle Jack Hills australiane [21].

sità ed il comportamento debolmente paramagnetico; talune altre saranno evidenziate nel seguito.
Continuando a seguire le vicissitudini dei primi atomi di U238, interessa particolarmente, ai nostri fini, evidenziare che l'Uranio era presente negli aggregati che diedero luogo alla formazione della terra, circa 4,4 miliardi di anni fa. Esso, in particolare, legato in alcuni zirconi, trovati in Australia alcuni anni fa, ci ha permesso di confermare l'età del nostro pianeta. Infatti, quei minerali, formatisi nelle prime fasi di vita della terra, contengono sia l'Uranio che i suoi prodotti di decadimento; questa circostanza consente di stimare, attraverso la misura delle quantità di Uranio 238 e 235, insieme ai loro diversi prodotti di decadimento, in particolare del Piombo, il tempo trascorso dal momento in cui i minerali si sono formati. Le misure hanno collocato quel momento a circa 4,37 miliardi di anni da oggi. Nella figura 3 è riportato un minerale di Zircone delle Jack Hills australiane - nesosilicato di formula $ZrSO_4$ - l'oggetto in assoluto più lontano nel tempo reperito sul globo terrestre. Questo minerale accoglie nel suo reticolo cristallino elementi ad elevata valenza ionica, tra cui l'Uranio.
Il chimico tedesco M.H. Klaproth scoprì la presenza dell'Uranio sulla terra, in realtà di un suo ossido, in un minerale di pechblenda proveniente dalla Sassonia, nel 1789; ritenendo che quell'ossido fosse un elemento metallico, lo chiamò Uranite, desiderando ricordare il nome di un pianeta scoperto poco tempo prima. Solo dopo più di 50 anni ci si rese conto dell'equivoco isolando l'atomo di Uranio. Il nuovo metallo cominciò ad essere utilizzato, ad esempio, per colorare vetro e ceramica.
Dalla nascita della terra ad oggi, l'Uranio è stato, e continua ad essere, protagonista di diverse situazioni che hanno interessato o interessano attualmente il nostro pianeta:

- è stato scoperto, negli anni '70, che circa due miliardi di anni fa reazioni di fissione ebbero luogo, ad Oklo, nel Gabon, per centinaia di migliaia di anni in reattori[9] naturali posti in formazioni rocciose che, nel tempo, hanno mantenuto segregati soprattutto il Plutonio e gli altri elementi transuranici prodotti; la formazione di quei reattori naturali fu possibile, presumibilmente:

- in virtù della maggiore percentuale dell'isotopo fissile Uranio 235, rispetto all'attuale (circa 3,5 % contro l'attuale 0,7 %);
- grazie a possibili inneschi della reazione da parte di neutroni provenienti da fissioni spontanee dell'Uranio 238 (una sporadica modalità di decadimento);
- in presenza di acqua, in grado di portare l'energia elevata dei neutroni di sponibili, mediante urti elastici, a quei valori cui corrispondono le maggiori probabilità di indurre reazioni di fissione a catena nell'Uranio 235;

- una fonte di riscaldamento endogena della terra è legata al decadimento degli isotopi radioattivi che si trovano al suo interno: è stato stimato che il flusso di calore dalla terra verso lo spazio ammonta a circa 44 teraWatt [7] e che poco meno della metà è dovuto al decadimento degli isotopi radioattivi; il contributo dell'U238 risulterebbe essere dell'ordine 8 teraWatt[10];
- una parte del fondo naturale di radiazione che tuttora irraggia, con diverse intensità, la popolazione mondiale (il valore medio si aggira intorno ai 2 mSv/anno[11]) è dovuta proprio all'Uranio 238 ed agli altri radioisotopi naturali con i loro prodotti di decadimento.

L'abbondanza dell'Uranio è circa 500 volte superiore a quella dell'oro ed è diffuso quasi come lo stagno (Figura 4). È presente nella maggioranza delle rocce e del suolo, nei fiumi e nell'acqua di mare. È, per esempio, presente nel granito, che rappresenta il 60% della crosta terrestre, in concentrazioni di circa 4 ppm (parti per milione), 3,3 ppb (parti per bilione) nell'acqua di mare [19]. Nei depositi fosfatici può raggiungere 400 ppm, mentre in quelli carboniferi si può arrivare a 100 ppm. Esistono sulla terra aree particolari ove la concentrazione di uranio nel suolo è sufficientemente elevata[12] perché la sua estrazione per l'utilizzo come combustibile nucleare divenga economicamente conveniente.
Tali concentrazioni sono riscontrabili principalmente in minerali quali l'uraninite che, insieme alla pechblenda (varietà amorfa), è il più diffuso e contiene ossidi di uranio particolarmente stabili (numero di ossidazione - n.o. - prossimo a +4). Ci sono miniere attive di Uranio in 20 Paesi [5]. I maggiori produttori sono Kazakistan, Canada e Australia che, insieme, contribuiscono al 65% della produzione globale. Seguono Namibia, Russia, Niger, Uzbekistan, Stati Uniti ed altri.
Anche in Italia è presente Uranio in concentrazioni elevate, in quantità stimabili intorno a 7400 tonnellate [2]. In particolare, furono svolte attività minerarie esplorative in Val Vedello (Approfon-

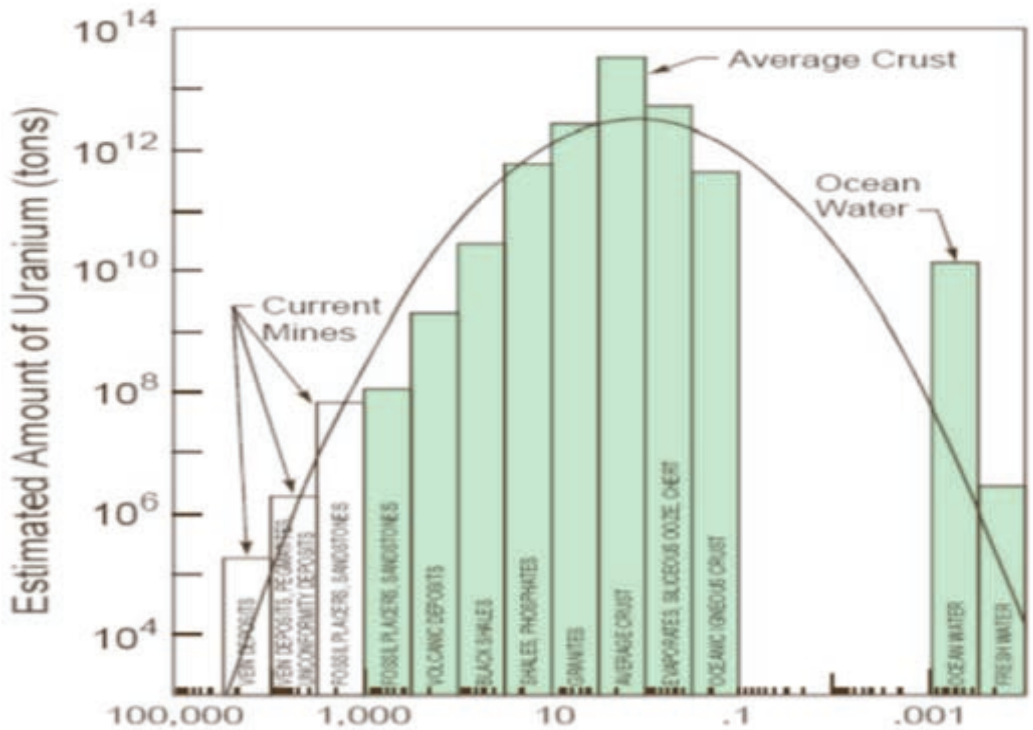


Figura 4
Distribuzione dell'Uranio nella crosta terrestre [2].

dimento 2), in provincia di Sondrio (giacimento scoperto mezzo secolo fa dall'Eni, ma in seguito al referendum del 1987 il cantiere fu chiuso), e successivamente a Novazza, In val Seriana, in provincia di Bergamo; in quest'ultimo caso fu negato, dalla Lombardia, lo sfruttamento della miniera da parte di una società australiana.
Valutazioni di massima sulla disponibilità di Uranio per i futuri utilizzi come combustibile, considerando il parco di centrali nucleari attualmente operative, hanno portato a stimare risorse residue variabili, in funzione delle ipotesi sulle relative modalità di sfruttamento, per tempi fino a 700 anni [11]; se, invece, si tiene anche conto della possibilità di fare un uso estensivo dei reattori veloci "breeder", in grado di generare nuovi isotopi fissili, se si aumenta il numero di riutilizzi del combustibile esaurito e se si ricorre anche al Torio, i tempi stimati possono essere incrementati di quantità che si collocano tra due e tre ordini di grandezza in più [12], [13]. Allo stato attuale, circa il 5 per mille dell'uranio naturale è usato nei reattori; nonostante sia utilizzata solo una frazione limitata, un chilogrammo di uranio naturale è in grado di produrre circa 500 GJ, per ottenere i quali sarebbero necessari circa 20000 chilogrammi di carbone nero [19]. Se poi si considera la possibilità di utilizzare anche il Torio, presente in natura con abbondanza 4 o 5 volte superiore all'Uranio, l'energia nucleare può estendere notevolmente le sue potenzialità.
Viene spontaneo, a questo punto, chiedersi quando l'uomo divenne per la prima volta consapevole della presenza di radioattività sulla terra. Nel 1895 il fisico William Roentghen aveva scoperto la radiazione elettromagnetica e, in particolare, i raggi X. L'anno successivo, il fisico Antoine Henri Becquerel aveva deciso di studiare il comportamento di alcuni cristalli di minerali di uranio che presentavano il fenomeno della fluorescenza[13] e dovette riporli in un cassetto insieme ad una nuova lastra fotografica. Dopo qualche giorno, controllando la lastra, si accorse che era stata impressionata anche se non era stato innescato nel minerale il fenomeno della fluorescenza; dedusse, da tutto ciò, che il minerale emetteva radiazioni spontanee, cosa che poté confermare verificando che quel minerale era in grado di ionizzare un gas.
Nel 1902 Pierre e Marie Curie, studiando un minerale dell'Uranio, la pechblenda, si accorsero che esso rimaneva radioattivo anche dopo aver rimosso l'Uranio ed isolarono per la prima volta il Radio 226, particolarmente "radio attivo", ed il Polonio (chiamato in questo modo per ricordare la terra di origine di Marie). Si cominciarono, dunque, a scoprire ed utilizzare per vari scopi diversi prodotti di decadimento dell'U238.
Tra questi ultimi vi sono anche il Piombo 210 ed il Polonio 210, che rappresentano rilevanti sorgenti di esposizione per l'uomo e l'ambiente; tuttavia, da questo punto di vista, riveste una particolare importanza soprattutto il gas Radon 222, derivante dal decadimento alfa del Radio 226. Infatti, il Radon 222, così come il suo isotopo 220, generato all'interno della catena di decadimento del Torio 232, può rendere estremamente insalubri gli ambienti in cui ha vissuto e vive l'uomo (a partire dalle caverne fino agli edifici costruiti in particolari località o con determinati materiali). Quest'ultima considerazione conduce ad un nuovo approfondimento, relativo a come le abitudini e le attività umane possano creare le condizioni per incrementare la dose da radiazione assorbita dagli individui a causa della presenza dell'Uranio 238 e degli altri radioisotopi naturali. Si è già evidenziato che esiste un fondo naturale terrestre di radiazione che accompagna l'uomo nella vita di ogni giorno; la dose che ne deriva ha effetti trascurabili sulla salute umana. Tuttavia, l'uomo, operando su particolari materiali, può creare le condizioni per cui le concentrazioni dei radioisotopi vengano incrementate, ad esempio nei residui delle lavorazioni intese a estrarre altri elementi (Approfondimento 3); inoltre, in ambienti ove si svolgono lavorazioni particolari, può aver luogo l'accumulo di polveri o gas con concentrazioni elevate di radioisotopi. Già nel sedicesimo secolo fu osservato come i lavoratori impegnati in una miniera di cobalto, in prossimità di depositi contenenti uranio, manifestassero problemi di salute rilevanti; ma solo nel 1870 si poté accertare che l'esposizione a particolari condizioni di lavoro era stata la causa di morte per tumore ai polmoni di numerosi minatori.
I settori industriali, nei quali sono impiegati materiali contenenti radionuclidi di origine naturale e nell'ambito dei quali si possono generare rischi di esposizione, segnalati e regolamentati dalla normativa italiana (D.Lvo 101/2020 mod. 203/2022), sono i seguenti:

- Centrali elettriche a carbone.
- Estrazione di minerali diversi dal minerale di uranio.
- Industria dello zircone e dello zirconio.
- Lavorazione di minerali e produzione primaria di ferro.
- Lavorazioni di minerali fosfatici e potassici.
- Produzione del pigmento TiO_2.
- Produzione di cemento.
- Produzione di composti di torio e fabbricazione di prodotti contenenti torio.
- Produzione di energia geotermica.
- Produzione di gas e petrolio.
- Impianti per la filtrazione delle acque di falda.
- Lavorazioni di taglio e sabbiatura.

Ad esempio, la concentrazione di Uranio 238 in ogni chilogrammo di ceneri volatili, disperse in atmosfera da un impianto dove viene bruciato carbone, dà luogo a circa cento disintegrazioni al secondo (100 Bq[14]/kg) [3]; nei fanghi derivanti dalla lavorazione dello stagno l'attività può arrivare a 5500 Bq/kg, nei fanghi derivanti dal processo termico di lavorazione dei minerali fosfati a circa 2300 Bq/kg. Una attività attualmente non presente nel nostro Paese, che può dar luogo ad esposizioni elevate dell'uomo e dell'ambiente, se non adeguatamente gestita, è l'estrazione dei minerali di uranio da miniera.
Il già citato Decreto Legislativo n. 101 del 2020, oltre alle attività su richiamate ed alle situazioni di esposizione da gas Radon, regolamenta anche l'utilizzo di materiali da costruzione che possono contenere radionuclidi naturali fonte di radiazioni gamma.
L'utilizzo dell'Uranio per la produzione di energia nucleare ha determinato nuove, particolari situazioni, tra cui:

- la disponibilità di grandi quantità di Uranio "impoverito" in seguito ai processi di trasferimento dell'isotopo 235 verso altre porzioni di Uranio da rendere "arricchito"[15] ; furono, di conseguenza, concepite diverse tipologie di utilizzi per questo prodotto di scarto (colorazione, gioielleria, armamenti - vedere Approfondimento 4 - , aeronautica ecc.);
- la produzione di rifiuti con concentrazioni di attività anche molto elevate. Nei reattori nucleari, infatti, si verifica la generazione di prodotti di fissione[16] particolarmente radioattivi, l'attivazione di vari materiali a causa della presenza di flussi neutronici, la generazione di elementi transuranici all'interno del combustibile; come già accennato, quest'ultima situazione può avere risvolti positivi se si pensa, ad esempio, alla generazione di nuovi isotopi fissili (ad esempio il Plutonio) che possono essere riutilizzati. I reattori "veloci" (nei quali i neutroni sono prevalentemente ad energie superiori a quella termica)

sono in grado di sfruttare le potenzialità dei nuclei fertili come l'Uranio 238;
- la produzione di rifiuti ad alta attività anche nelle attività di arricchimento e riprocessamento del combustibile utilizzato nei reattori etc.

Non tutte le attività umane che impiegano minerali contenenti l'Uranio sono indirizzate al benessere (produzione di energia, di sostanze utili all'industria etc.): ve ne sono che hanno la finalità di predisporre mezzi di distruzione. Sulla terra sono stati effettuate più di 1800 prove di ordigni nucleari, cui l'Uranio 238 ha presenziato fornendo un contributo limitato rispetto agli isotopi fissili. La Francia, ad esempio, ha effettuato poco meno di 150 prove sottoterra, negli atolli di Mururoa e Fangataufa. Le prove sono state effettuate in profondità, all'interno di rocce vulcaniche o calcaree, al fine di confinare i radioisotopi fuoriusciti dalle esplosioni. Nonostante la liberazione di enormi energie abbia dato luogo a frammentazione delle rocce e sia stato accentuato il flusso ascendente di acqua oceanica è stato osservato come isotopi quali il Plutonio siano stati efficacemente trattenuti dalla lava vetrosa generatasi a seguito delle esplosioni e, in generale, gli altri radioisotopi, tranne il trizio, siano stati rilasciati in frazioni limitate e non siano rilevabili, anche a causa della diluizione nell'oceano o nelle lagune [4].

I minerali delle rocce, i manufatti, i residui di lavorazioni immessi nell'ambiente possono reagire in varie maniere con i gas e con l'acqua, subendo processi di alterazione chimica che ne modificano le caratteristiche e che creano, in taluni casi, le condizioni per incrementarne la mobilità. Ma è soprattutto in presenza e col movimento delle acque superficiali e sotterranee, con diverse caratteristiche chimiche, che si possono da un lato generare composti che conferiscono all'Uranio una particolare mobilità, d'altro lato trasferirlo verso zone ove esso trova le condizioni più idonee per depositarsi[17] , eventualmente creando indesiderati accumuli.

È utile sapere come si comporta l'Uranio,

presente in materiali solidi, quando viene abbandonato inconsapevolmente o smaltito dopo specifici utilizzi o lavorazioni. L'approfondimento dei meccanismi di mobilizzazione e trasporto consente di fare previsioni sul possibile destino dell'Uranio reintrodotto nell'ambiente, ma risulta utile anche nello studio della storia evolutiva degli ambiti naturali che, a loro volta, sono in grado di fornire dati interessanti sui processi verificatisi nel passato; ad esempio, si è potuto constatare che minerali come l'uraninite sono particolarmente stabili in quanto non solubili nelle condizioni di pH (4 – 8) che caratterizzano i flussi freatici [17]. Ovviamente, quando si è consapevoli della sua presenza nei residui o negli scarti in quantità rilevanti e non può essere utilizzato, l'Uranio viene segregato, trattato, condizionato e smaltito in formazioni tanto più stabili quanto maggiori sono i pericoli associati ma, comunque, prima o poi dovrà fare i conti con i processi naturali. È già stato notato come la sua progenie, tranne il Radon 222, non sia gassosa. Il Radon tende a svincolarsi e si è osservato che talvolta porta con sé uno dei suoi figli, il Piombo 214 radioattivo, che successivamente può depositarsi su superfici disponibili. Anche altri membri della progenie, con diverse caratteristiche chimiche, soprattutto se posti in un ambiente naturale ed in presenza di acqua, tendono ad andare per la loro strada; l'unione familiare è altresì compromessa dai comportamenti di quei componenti che, emettendo particelle alfa, provocano urtanti rinculi.

Le situazioni che l'Uranio deve affrontare nell'ecosistema ed i processi possibili sono numerosi e complessi; nel seguito, si riportano informazioni di maggior dettaglio relative ad alcuni interessanti comportamenti dell'Uranio nell'ambiente, quali risultano dalla documentazione reperita.

La sua mobilità è funzione del numero di ossidazione nei suoi composti, essendo il n.o. +6 quello più diffuso, nel suolo superficiale o poco profondo, e che gli conferisce maggiore solubilità, nonché maggiore stabilità chimica e mobilità in soluzione [8]. In condizioni aerobiche, l'Uranio forma facilmente composti, ad esempio con materie organiche, carbonati, fosfati, solfati, che lo rendono più o meno solubile. In condizioni anerobiche può essere ridotto al n.o. +4 sotto forma di idrossido o reagire, ad esempio, con solfuri. Sono molte le situazioni in cui l'Uranio è attaccato più o meno lentamente, ma inesorabilmente, dall'acqua. In soluzioni acquose, l'Uranio non si presenta mai da solo ma, quanto meno, legato a due atomi di ossigeno a formare ioni uranile; i cationi uranile (UO_2^{2+}) e i suoi complessi acquosi costituiscono la forma chimicamente più stabile e mobile in soluzione; in funzione delle condizioni di pH, essi tendono a idrolizzare, a formare diversi complessi stabili con leganti contenenti ossigeno (ossidi, idrossidi, solfati, fosfati e carbonati) o altri leganti inorganici quali i fluoruri, in competizione o in concorso con metalli quali rame, calcio o magnesio; questi ultimi, in funzione della solubilità relativa, possono contribuire alla formazione di minerali compositi contenenti uranile [6]. Altri possibili leganti possono essere i composti organici quali citrati, sostanze umiche[18] . In presenza di Calcio lo si può trovare legato a formare il complesso $Ca_2UO_2(CO_3)_3$, frequentemente presente nell'acqua di mare ed in altre acque ricche di Calcio. I complessi carbonatici ($UO_2(CO_3)_{2/3}$), presenti in condizioni di pH elevato, sono particolarmente stabili in soluzione, data la loro carica negativa. Infatti, sono restii a posarsi su superfici di minerali che, a loro volta, presentino cariche negative (es. minerali argillosi). In condizioni di pH basso, oltre al catione uranile, dominano i complessi $(UO_2)F^+$, $(UO_2)SO_4$, $(UO_2)F_2$, $(UO_2)HPO_4$. Per pH intermedi si possono segnalare i complessi $(UO_2)(HPO4)_2^{2-}$ [17]. I complessi umici sono in grado di trattenere fortemente l'Uranio ed altri metalli; in presenza di superfici con ossido ferro ed in condizioni di basso pH, gli acidi umici sono in grado di fissare l'Uranio sulla fase solida.

In caso di presenza in eccesso di altri minerali in soluzione, durante il processo di trasporto dei composti di Uranio, può aver luogo una coprecipitazione.

Come già evidenziato, l'Uranio può essere immobilizzato all'interno di reticoli cristallini di minerali (es. zircone, monazite, apatite), ove sono presenti elementi con analoghe caratteristiche (raggio ionico, carica, elettronegatività, ecc.), quali l'Ittrio, lo Zirconio, il Torio, il Cerio, il Calcio e il Bario [17].

Sono stati osservati numerosi altri meccanismi di trasporto o immobilizzazione; tra questi:

- specifiche interazioni con gli ossidi di ferro;
- deposizione nel suolo di micro-cristalli di silicati di uranile in cavità, fratture o tra grani;
- assorbimento e desorbimento superficiale (caratterizzato attraverso il coefficiente di distribuzione sperimentale k_d, tipicamente funzione del legante e del pH);
- interazioni semplici o susseguenti di carattere chimico, comportanti scambi ionici;
- molteplici interazioni di biogeochimica microbica.

I meccanismi citati sono tra quelli che hanno determinato e determinano la distribuzione dell'Uranio nelle rocce, nel suolo, nelle acque; successivamente, attraverso specifici processi, esso può essere incorporato nei vegetali e negli animali. La dettagliata conoscenza di tutti que-

sti percorsi è fondamentale per assicurare che lo smaltimento dei residui e dei rifiuti contenenti Uranio sia tale da non perturbare gli equilibri e non indurre dosi aggiuntive rispetto a quelle che derivano all'uomo e all'ambiente dalla natura. È, infine, opportuno sottolineare che il rapporto uomo - Uranio 238 è particolarmente ostico non solo in relazione ai rischi da radiazioni ma anche poiché, ove ingerito e non totalmente espulso con le urine, l'Uranio può provocare effetti tipici di un avvelenamento da metalli pesanti e si accumula nelle ossa e soprattutto nei reni; può generare anche dermatiti, gravi degenerazioni dei reni, necrosi delle arterie.
Emerge chiaramente che l'Uranio 238 vanta una lunga storia, subisce numerose vicissitudini nell'universo e su questa terra; presenta comportamenti assai variegati, in funzione delle circostanze, e interfaccia con l'uomo in diverse situazioni. Ci sarebbe ancora tanto altro da riferire, ad esempio esaminando le diverse modalità con cui esso ha contribuito e continua a contribuire alla produzione di energia necessaria per l'uomo, descrivendo le tecniche di processamento dell'Uranio naturale per ottenere combustibili o mostrando come sono stati costruiti i modelli matematici di simulazione del trasporto nell'ambiente etc., ma ciascuna di tali tematiche richiede una trattazione specifica. Approfondire la conoscenza delle caratteristiche di questo radioisotopo è importante per una gestione consapevole di questa rilevante risorsa, in alcuni casi ospite incomodo, di cui dispone il nostro pianeta, nelle diverse circostanze in cui esso fa capolino nella nostra esistenza.

Approfondimenti

Approfondimento 1 - La massima energia di legame nel nucleo atomico (picco di stabilità) si colloca nella zona tra 50 e 60 u.m.a. (Figura 5), all'interno della quale si dispongono, ad esempio, il Ferro, il Cobalto e il Nichel (quest'ultimo ha la massima energia di legame per nucleone[19]). Nuclei di massa inferiore, fondendo, e nuclei di massa superiore, scindendosi, sono potenzialmente in grado di liberare energia dando luogo alla produzione di nuclei posti in prossimità del picco di stabilità.
Infatti, una maggiore energia di legame comporta una minore massa dei nucleoni legati; nucleoni di altra provenienza, portandosi a quelle configurazioni cui competono le massime energie di legame, perdono massa; la perdita di massa conduce ad una cessione di energia: $E= \Delta mc^2$.

Approfondimento 2 - In Figura 6 è presentato lo spettro relativo alle emissioni gamma di un minerale di pechblenda proveniente dalla Val Vedello. Si distinguono, da sinistra in successione, i picchi dovuti al decadimento del Torio 234, dell'Uranio 235, del Radio 226, del Piombo 214 (tre picchi) e del Bismuto 214.

Approfondimento 3 - I materiali che presentano concentrazioni di radionuclidi naturali superiori alla media della crosta terrestre sono generalmente chiamati NORM, acronimo inglese di Naturally Occurring Radioactive Materials; con il termine TENORM[20] sono, invece, indicati quei materiali che presentano concentrazioni di radionuclidi naturali più elevate rispetto alle

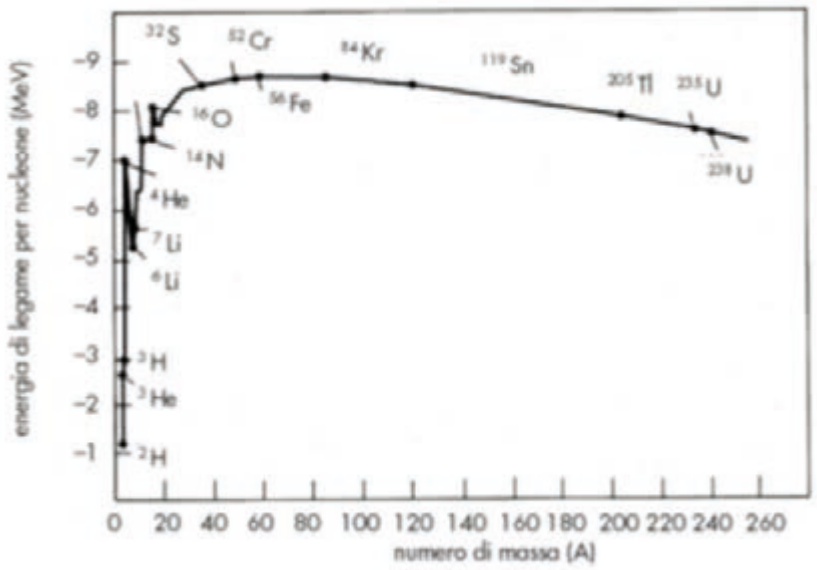


Figura 5 - andamento dell'energia di legame per nucleone in funzione del numero di massa del nucleo [22].

sostanze originarie, a seguito di specifiche lavorazioni svolte dall'uomo, anche nel passato.

Approfondimento 4 - L'uranio impoverito, utilizzato per la fabbricazione di missili, proiettili penetranti (Figura 7) e armature per il suo elevatissimo peso specifico, presenta una particolare pericolosità, legata al fatto che, principalmente a seguito delle esplosioni, parti di esso volatilizzano, permanendo in aria e successivamente ricadendo sotto forma di polvere. Diviene, pertanto facilmente inalabile, ingeribile o capace di posarsi sulle ferite e, una volta entrato nei tessuti, nei polmoni o nell'apparato digerente in quantità rilevanti, può provocare gravi malattie [20].

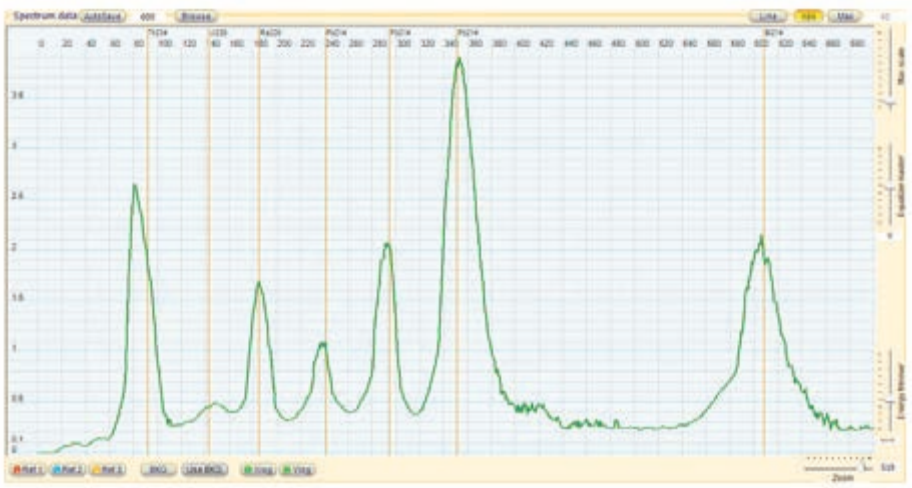


Figura 6
Emissioni gamma di un minerale di pechblenda proveniente dalla Val Vedello [9].

Note

1. Il numero di massa è la somma del numero di neutroni e protoni nel nucleo ed è approssimativamente pari al relativo peso in unità di massa atomica (u.m.a.).
2. Principalmente Idrogeno ed Elio.
3. Costituite da più di 8 masse solari, mentre le prime stelle supermassicce potevano contare su masse di centinaia o migliaia di masse solari.
4. Il numero atomico corrisponde alla quantità di protoni presenti nel nucleo.
5. Tempi di dimezzamento di circa 710 milioni di anni.
6. È considerato fertile un isotopo in grado di generale un nucleo fissile per cattura neutronica. Il Pu 239 è "fissile".
7. È compito del moderatore dei reattori nucleari far abbassare, mediante urti elastici, la velocità dei neutroni emessi dalle fissioni di più di un fattore 10000 .
8. Configurazione completa [Rn] $5f^3$ $6d^1$ $7s^2$.
9. Almeno 17 reattori [16].
10. Le alte fonti di calore endogeno da decadimento derivano soprattutto dal Torio e dal Potassio 40. Valutazioni specifiche sono state effettuate mediante la misurazione dei "geoneutrini", generati dai decadimenti ed emergenti dalla superficie terrestre.
11. Il Sievert (Sv) è l'unità di dose, che misura l'energia assorbita (Joule/kg) dal corpo, tenendo conto dell'efficacia biologica, valutata in base alla specifica radiazione e alle diverse sensibilità dei tessuti; la dose citata si riferisce al corpo intero.
12. Dallo 0.01% fino al 20% e più, come nelle riserve dell'Athabasca Basin del Canada, le più ricche al mondo [19].
13. Proprietà di alcune sostanze di riemettere radiazioni elettromagnetiche ricevute.
14. Il Becquerel, dal nome dello scopritore della radioattività, è l'unità di misura dell'attività dei radionuclidi e corrisponde a una disintegrazione al secondo.
15. Solo una limitata percentuale di impianti nucleari (≈ 12%) è in grado di produrre energia con uranio naturale non arricchito [19]. Essi utilizzano carbonio o acqua pesante come moderatori, poiché non sono avidi di neutroni.
16. Prodotti di fissione: nuclei derivanti dalla frantumazione degli isotopi fissili impattati da un neutrone.
17. Ad esempio, a contatto con materiale organico, argille, ambienti riducenti o piccole particelle.
18. Sostanze naturali, costituite da miscele complesse di acidi umici, fulvici o umine, che si formano a seguito della biodegradazione microbica di sostanza organica (vegetale o animale).

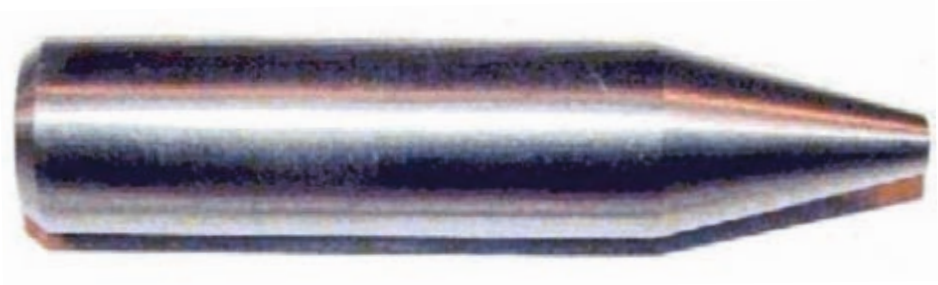


Figura 7
un proiettile penetrante
di Uranio impoverito [23].

Bibliografia

[1] N. de Grasse Tyson, D Goldsmith – ORIGINI – Quattordici miliardi di anni di evoluzione cosmica
[2] ENEA – F. Vettraino - Rapporto di sintesi su risorse e domanda mondiali di uranio con riferimenti alla situazione nazionale - 2011
[3] INAIL - Il rischio fisico nel settore della bonifica dei siti industriali di origine non nucleare contaminati da radiazioni ionizzanti – 2016 - https://www.inail.it/cs/internet/docs/alg-il-rischio-fisico-settore-bonifica-siti-industriali.pdf
[4] ROBERT FRY, DES LEVINS, AND ERNST WARNECKE - RADIOACTIVE RESIDUES FROM UNDERGROUND WEAPON TESTING: THE MURUROA ASSESSMENT- RADIONUCLIDE MIGRATION THROUGH THE GEOSPHERE - https://www.iaea.org/sites/default/files/publications/magazines/bulletin/bull40-4/40405083033.pdf
[5] FOCUS Energia – Dove si estrae l'Uranio? https://www.focus.it/scienza/energia/dove-si-estrae-uranio#:~:text=Contrasto-,A%20differenza%20di%20gas%20e%20petrolio%2C%20la%20distribuzione%20geografica%20dell,al%2065%25%20della%20produzione%20globale
[6] IAEA TRS 488 - The Environmental Behaviour of Uranium https://www.iaea.org/publications/14688/the-environmental-behaviour-of-uranium
[7] Paul Preuss – Berkley Lab – What keeps the earth cooking? - https://newscenter.lbl.gov/2011/07/17/kamland-geoneutrinos/
[8] IRSN - Natural Uranium and the environment- https://en.irsn.fr/EN/Research/publications-documentation/radionuclides-sheets/environment/Pages/Natural-uranium-environment.aspx
[9] Spettrometria gamma dell'Uranio – Physics Open Lab - https://physicsopenlab.org/2016/01/29/spettrometria-gamma-delluranio/
[10] Chimica on line - https://www.chimica-online.it/elementi/uranio.htm
[11] ENEA – F. Troiani – Ciclo del combustibile nucleare e rifiuti radioattivi – 2009
[12] Scientific American - How long will the world's uranium supplies last? - https://www.scientificamerican.com/article/how-long-will-global-uranium-deposits-last/#:~:text=Second%2C%20fuel%2Drecycling%20fast%2D,only%20the%20NEA%2Destimated%20supplies.
[13] OCSE NEA - R. Price, J.R. Blaise - Nuclear fuel resources: Enough to last? - https://www.oecd-nea.org/nea-news/2002/20-2-Nuclear_fuel_resources.pdf
[14] NATURE - Daniel M. Siegel, Jennifer Barnes Brian D. Metzger - Collapsars as a major source of r-process elements -2019 - https://www.nature.com/articles/s41586-019-1136-0
[15] Anna Frebel Timothy C. Beers - Physics today - The formation of the heaviest elements https://physicstoday.scitation.org/doi/10.1063/PT.3.3815
[16] World Nuclear Association – The cosmic origins of Uranium (Updated April 2021) - https://world-nuclear.org/information-library/nuclear-fuel-cycle/uranium-resources/the-cosmic-origins-of-uranium.aspx#:~:text=The%20Earth's%20uranium%20had%20been,of%20the%20Earth's%20heat%20flux.
[17] ENEA M. Frullini, C. Rusconi, F. Giannetti, D.V. Di Maio - Indagini conoscitive relative alle problematiche inerenti lo smaltimento geologico dei rifiuti radioattivi ad alta attività e lunga vita https://www.enea.it/it/Ricerca_sviluppo/documenti/ricerca-di-sistema-elettrico/nuovo-nucleare-fissione/lp4/rds-118-lp4.pdf
[18] Sanjana Curtis - Alchimia cosmica – Le Scienze – Marzo 2023 – www.lescienze.it
[19] Ian Hore-Lacy - World Nuclear Association, London, United Kingdom Uranium for Nuclear Power Resources, Mining and Transformation to Fuel
[20] US Department of Veteran Affairs – Depleted Uranium https://www.publichealth.va.gov/exposures/depleted_uranium/#:~:text=The%20two%20primary%20health%20concerns,of%20concern%20are%20the%20kidneys
[21] Il minerale più antico: lo Zircone delle Jack Hills https://www.trilobiti.com/forum/precambrian-area/il-minerale-piu-antico-lo-zircone-delle-jack-hills
[22] Università di Trieste – materiale per studenti – Chimica Nucleare http://www.dsch.univ.trieste.it/~kaspar/fisica/MaterialeStudenti/Lucidi2.pdf
[23] Wikipedia – Uranio https://it.wikipedia.org/wiki/Uranio
[24] Universo Astronomia – 14 aprile 2020 – una supernova da record https://www.universoastronomia.com/2020/04/14/una-supernova-da-record/

Quaderno

a cura di:
Ing. Aldo Delia e
Ing. Angela Marrelli

Commissione:
Progettazione
integrata in
ambito sanitario

ANALISI DELLA COMUNICAZIONE DI AVVENUTA INSTALLAZIONE DI UNA MACCHINA RM

CRONOGRAMMA DELLA DOCUMENTAZIONE

1 INTRODUZIONE

La **risonanza magnetica (RM)** è una tecnologia di imaging non invasiva che produce immagini anatomiche dettagliate tridimensionali. Viene utilizzata per la diagnostica ed il monitoraggio dell'andamento del trattamento.
Mentre la classica radiografia consente l'acquisizione di immagini attraverso l'impiego di radiazioni, la risonanza magnetica si basa sul campo magnetico.
Essa sfrutta le capacità magnetiche ed elettriche dell'elettrone, permettendo di studiare i tessuti biologici attraverso la valutazione dell'assorbimento di energie a RF da parte dell'elettrone sottoposto ad un campo magnetico esterno.
La caratteristica principale della RM è quella di utilizzare radiazioni elettromagnetiche a basso contenuto energetico che non modificano o distruggono le sostanze analizzate.

2 INSTALLAZIONE DI UNA RISONANZA MAGNETICA

Prima di descrivere nel dettaglio la **Comunicazione di avvenuta installazione (CAI)**, occorre fare una premessa per definire le modalità di avvio installazione, sostituzione o trasformazione da settoriale a total body di una risonanza magnetica.
Il primo documento necessario è la "Istanza per l'installazione di apparecchiatura a risonanza magnetica del gruppo A per uso diagnostico", come richiesto dal D.M. 14/01/2021 – DPR n. 542/1994, da inviare alla Regione di pertinenza.
In tale modello vengono richieste informazioni preliminari relative al sito di installazione ed alle figure responsabili precedentemente individuate, che verranno allegate al documento.
A seguito dell'invio di questo modello, la regione deve dare l'autorizzazione all'inizio lavori.
Successivamente, è possibile avviare l'inizio lavori comunicandolo tramite il modello "Comunicazione interventi edilizi e di manutenzione ordinaria o straordinaria (art. 2, comma 2 R.R 20/2019)".
Tale comunicazione deve essere trasmessa alla Regione di pertinenza ed alla ASL. Contestualmente, il direttore dei lavori dovrà aprire la CILA o la SCIA (a seconda che siano presenti interventi strutturali o meno).
Alla conclusione dei lavori il **datore di lavoro (DL)** invia la richiesta di esercizio alla Regione, tramite il modello 1 bis *Istanza di autorizzazione all'esercizio studio medico/sanitario* (L.R. n. 4/2003; art. 8 R.R. n. 20/2019).
Parallelamente, il direttore dei lavori chiude la CILA o SCIA consegnando il nuovo accatastamento all'ufficio catasti. Entro 15 giorni dal termine dei lavori, emette una dichiarazione di conformità alla Regione e alla ASL asseverata dal tecnico abilitato.
In questo lasso di tempo, il sito in cui è stata installata la risonanza magnetica, può essere soggetto ad ispezione e l'ER ha a disposizione 60 giorni di tempo per consegnare la CAI, come descritto nel successivo capitolo.

3 COMUNICAZIONE DI AVVENUTA INSTALLAZIONE

La comunicazione di avvenuta installazione di una apparecchiatura RM è la notifica obbligatoria con cui il legale rappresentante della struttura sanitaria che ha installato una apparecchiatura RM comunica, entro sessanta giorni dall'installazione, il soddisfacimento dei requisiti previsti dagli standard di sicurezza e impiego a tutte le amministrazioni interessate.
La CAI permette di stabilire se il tomografo sia stato installato in sicurezza e se il centro diagnostico abbia avviato le proprie attività secondo procedure consone e consente di uniformare le modalità di comunicazione nei confronti delle

amministrazioni interessate dalla comunicazione:

- Regione o provincia autonoma;
- ASL territorialmente competente;
- Ministero della salute;
- Istituto superiore di sanità o ISS;
- Istituto nazionale per l'assicurazione contro gli infortuni sul lavoro o INAIL.

3.1 ALLEGATI

Il compito dell'ingegnere è analizzare e raccogliere la documentazione necessaria in fase di progettazione per realizzare una struttura in sicurezza e avere a disposizione i documenti richiesti dalla CAI:

1. Relazione tecnica di garanzia degli standard di sicurezza;
2. Caratteristiche tecniche dell'apparecchiatura RM;
3. Lettera di conferimento dell'incarico e quella di accettazione dei responsabili della sicurezza;
4. Planimetria del presidio/piano ove giace l'apparecchiatura RM;
5. Planimetria del sito RM;
6. Mappa delle linee isomagnetiche teoriche a campo contenuto e le misure del campo magnetico statico disperso;
7. Documentazione tecnica relativa all'impianto di ventilazione/condizionamento della sala RM;
8. Certificato di taratura della cella ossigeno;
9. Documentazione tecnica relativa al tubo di quench;
10. Regolamento di sicurezza;
11. Questionario anamnestico preliminare all'esecuzione dell'esame RM;
12. Scheda di accesso in ZC;
13. Percorso del dewar;
14. Controlli di qualità;
15. Documentazione tecnica relativa alla gabbia di Faraday;
16. Benestare all'uso del tomografo;
17. Protocollo di sorveglianza sanitaria rilasciato dal medico competente per la formulazione del giudizio di idoneità alla mansione specifica dei lavoratori esposti ai fattori di rischio presenti in ambiente RM.

Analizziamo, per ogni documento, i dati da riportare, l'attore responsabile della sua produzione, il ciclo di vita del documento ed eventuali criticità.

3.1.1 Relazione tecnica di garanzia degli standard di sicurezza

Rappresenta il documento introduttivo che riporta in allegato tutte le informazioni richieste a corredo della w. Si tratta di una dichiarazione, firmata dall'esercente della struttura sanitaria sulla base di indicazioni fornite dal MRR e dall'ER, in cui viene:

- Garantita la presenza di un accesso controllato e regolamentato da idonea cartellonistica;
- Garantita la presenza di un regolamento di sicurezza, in cui vengono codificate le misure di sicurezza e protocolli comportamentali;
- Elencata la lista dei dispositivi di sicurezza presenti nel sito RM;
- Definito il protocollo di controlli di sicurezza;
- Elencata la lista degli allegati della CAI.

Nella parte introduttiva è possibile inserire anche una breve descrizione della macchina, i riferimenti normativi e la delibera della regione con il parere favorevole alla realizzazione dei locali ed alla installazione della RM.

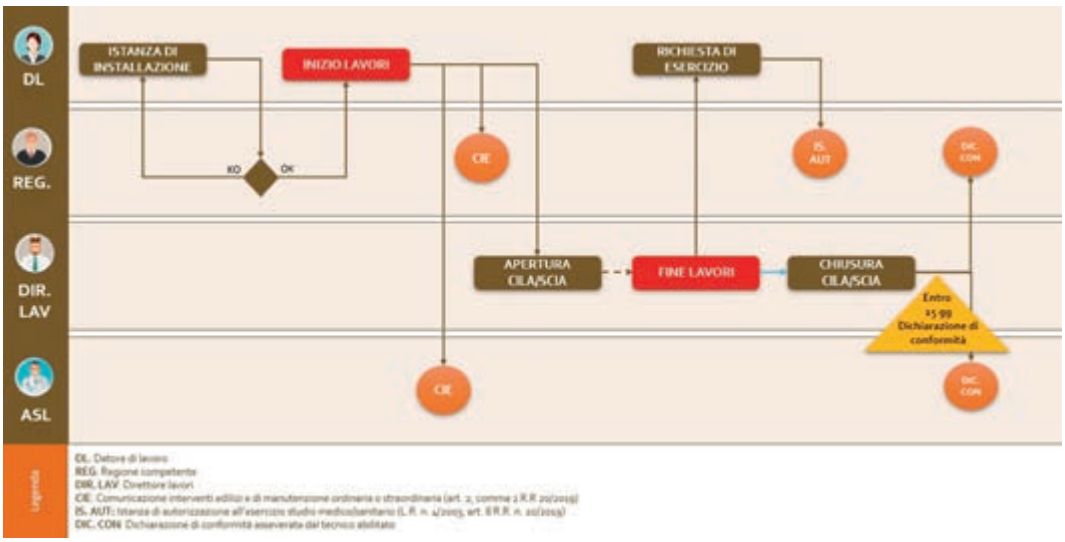


Figura 1
Flusso documentale preliminare

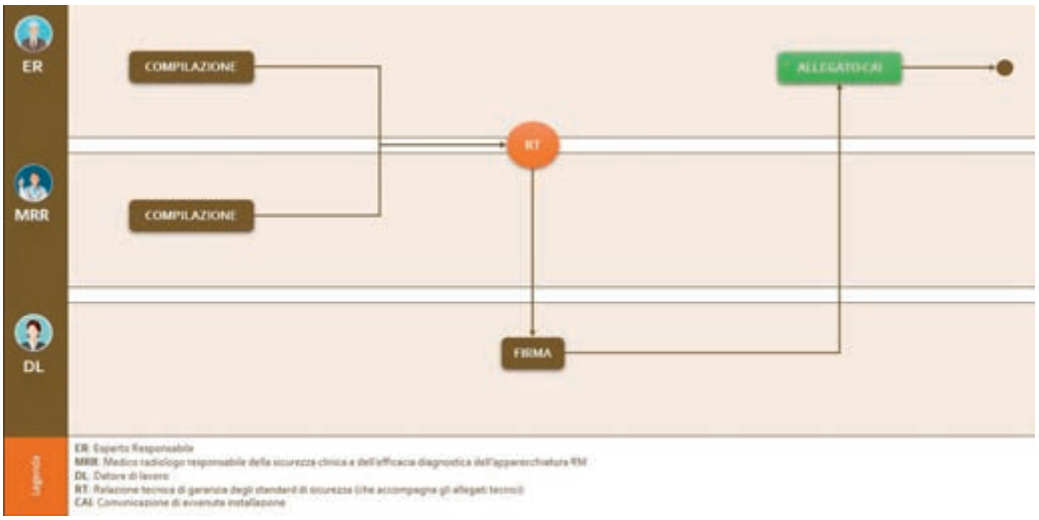


Figura 2
Flusso del documento "Relazione tecnica di garanzia degli standard di sicurezza"

3.1.2 Caratteristiche tecniche dell'apparecchiatura RM

Riporta una breve descrizione tecnica della macchina RM. Per ogni tomografo RM devono essere trasmessi:

- Marca;
- Modello;
- Numero di serie;
- Tipo di magnete;
- Intensità del campo magnetico statico caratteristico;
- Descrizione tecnica dettagliata dell'apparecchiatura e sue componenti;
- Data di installazione del tomografo;
- Data di inizio attività del tomografo.

Tutte le informazioni vengono fornite dalla ditta produttrice del tomografo RM e sono reperibili dalla scheda tecnica che accompagna il macchinario installato.

3.1.3 Lettera di conferimento dell'incarico e accettazione dei responsabili della sicurezza

Il DL ha il compito di individuare due responsabili per la sicurezza e la qualità dell'impianto, ovvero il **medico radiologo responsabile** della sicurezza clinica e dell'efficacia diagnostica dell'apparecchiatura RM (**MRR**) e l'**esperto responsabile** per la sicurezza in RM (ER).
Risulta necessario trasmettere i seguenti documenti e la data della loro redazione:

- Lettera di conferimento dell'incarico da parte del DL per il MRR;
- Lettera di conferimento dell'incarico da parte del DL per il ER;
- Lettera di accettazione dell'incarico da parte del MRR;
- Lettera di accettazione dell'incarico da parte del ER;
- Curriculum vitae del MRR, dove è possibile verificare l'aderenza del professionista ai

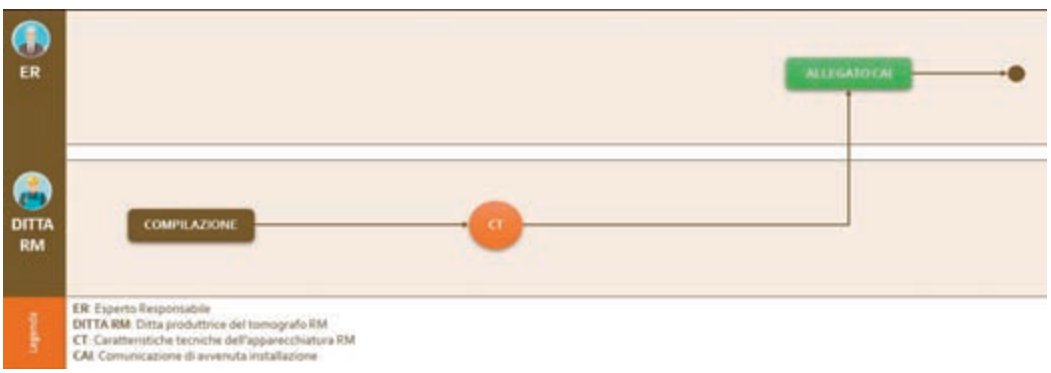


Figura 3
Flusso del documento "Caratteristiche tecniche dell'apparecchiatura RM"

requisiti necessari previsti dalla normativa vigente;
- Curriculum vitae del ER, dove è possibile verificare l'aderenza del professionista ai requisiti necessari previsti dalla normativa vigente.

È possibile unificare la lettera di conferimento e accettazione in un unico documento, per ogni responsabile, in cui viene riportata la lettera di conferimento e l'accettazione del responsabile tramite controfirma del documento stesso.
Per ogni tomografo RM deve essere individuato un unico MRR ed un unico ER.
Questo documento viene prodotto dal DL ed inviato ai responsabili che la controfirmeranno per accettazione dell'incarico.

3.1.4 Planimetria del presidio/piano ove giace l'apparecchiatura RM

Riporta la planimetria generale di tutta la zona del presidio, da cui devono essere specificate la localizzazione del sito e l'indicazione delle proprietà confinanti con il presidio, se presenti, per valutare l'eventuale debordo del campo magnetico statico disperso o esposizione a gas criogeno.
L'area che la planimetria deve mostrare è quella del reparto o del piano ove giace il tomografo RM e i locali esterni al sito subordinati alla macchina.
La planimetria deve essere in scala e avere l'unità di scala planimetrica rappresentata. Devono, inoltre, essere evidenziati:

- Il sito RM;
- La destinazione d'uso dei locali;
- La **zona ad accesso controllato (ZAC);**
- La **zona controllata (ZC);**
- La **zona di rispetto (ZR).**

In particolare, dalla documentazione deve rilevarsi:

- Se il presidio è pubblico o se è privato;
- La ragione sociale del presidio e l'esatto indirizzo;
- L'azienda sanitaria locale territorialmente competente nel luogo dove sorge il presidio;
- Il nominativo del direttore sanitario del presidio con la direzione sanitaria.

La planimetria del presidio viene prodotta da colui che ha effettuato il progetto (progettista). Poiché viene effettuata precedentemente alla costruzione del sito e alla installazione della RM, tale documento risulta essere già disponibile al ER, in quanto persona coinvolta sia nella progettazione che nella validazione di tale documento.

3.1.5 Planimetria del sito RM

La planimetria del sito RM deve mostrare i seguenti locali:

- La sala magnete, con la rappresentazione della sagoma del tomografo;
- La sala comandi;
- La sala per la preparazione del paziente;
- La sala per la gestione delle emergenze;
- Lo spogliatoio;
- Il locale tecnico;
- La sala anamnesi, se interna al sito;
- I servizi igienici, specificando la destinazione ad uso esclusivo del personale o anche per i pazienti e se adatti all'uso per persone diversamente abili;
- Le sale di attesa, se presenti nel sito, con indicazione della tipologia di pazienti che possono accogliere (esterni, interni o barellati);
- La sala refertazione.

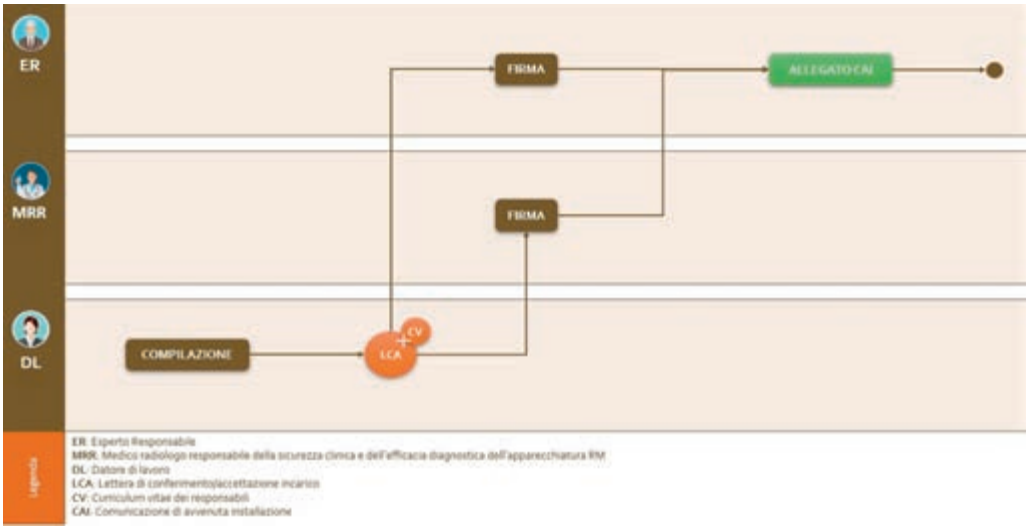


Figura 4
Flusso del documento "Lettera di conferimento dell'incarico e quella di accettazione dei responsabili della sicurezza"

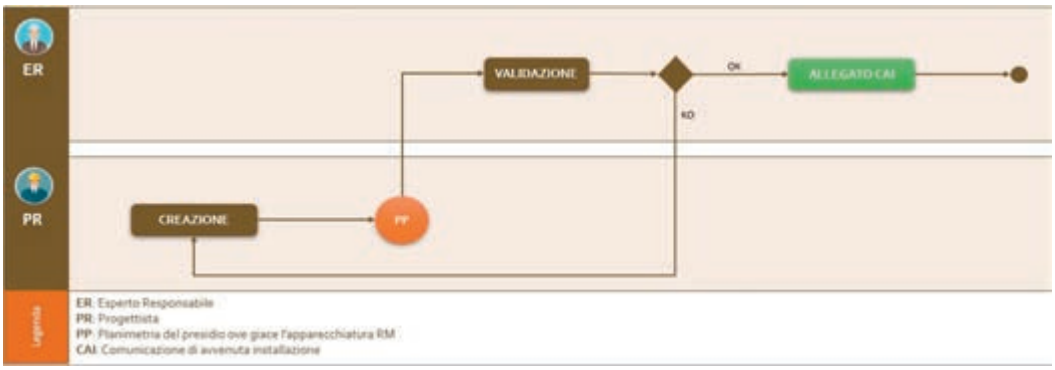


Figura 5
Flusso del documento "Planimetria del presidio ove giace l'apparecchiatura RM"

La planimetria del sito RM deve essere in scala, con l'unità di scala planimetrica in evidenza e deve mostrare la destinazione d'uso di tutti i locali subordinati al tomografo. Qualora sia presente più di una macchina RM, tutti i locali devono avere anche l'indicazione di quale sia il tomografo a cui afferiscano.
Nel caso in cui un locale abbia più di una destinazione d'uso (ad esempio il locale preparazione che può essere utilizzato anche come locale emergenze) queste devono essere indicate entrambe.
Nella planimetria deve essere indicata l'esatta collocazione del sito RM, ovvero indirizzo, piano, la destinazione d'uso dei locali adiacenti al sito e alla sala magnete, identificare il reparto dove si trova il tomografo RM.
Occorrerà anche quantificare il numero massimo di pazienti che è possibile gestire nel sito RM.
Qualora, nel corso della costruzione del sito e dell'installazione della macchina RM, si sia resa necessaria qualsiasi modifica rispetto alla planimetria progettata, questa deve essere riportata sul progetto e validata dall'ER.

3.1.6 Mappa delle linee isomagnetiche teoriche a campo contenuto e le misure del campo magnetico statico disperso

La mappa delle linee isomagnetiche rappresenta le linee di forza del campo magnetico statico e disperso del tomografo. Deve:

- Essere in scala (1:100 o 1:50), con unità di scala rappresentata;
- Riportare la sagoma del tomografo;
- Rappresentare nei tre piani cartesiani le linee isomagnetiche pari a 0,5 mT (interna alla ZAC) e 0,1 mT (interna alla ZR).

La mappa delle linee isomagnetiche teoriche in campo contenuto viene rilasciata dalla ditta installatrice delle barriere di contenimento.
A seguito dell'installazione del tomografo RM, vengono effettuate le misure dell'intensità del campo magnetico disperso. Tali misure sperimentali devono essere validate dall'ER nel caso in cui lui stesso non abbia effettuato le misure.

3.1.7 Documentazione tecnica relativa all'impianto di ventilazione o condizionamento della sala RM

L'impianto di ventilazione/condizionamento della sala RM garantisce, nella sala magnete, le seguenti condizioni:

- Il corretto microclima necessario per il benessere del paziente in esame;
- Uno stato barico positivo, per impedire l'ingresso di pulviscolo che potrebbe inficiare i risultati degli esami;

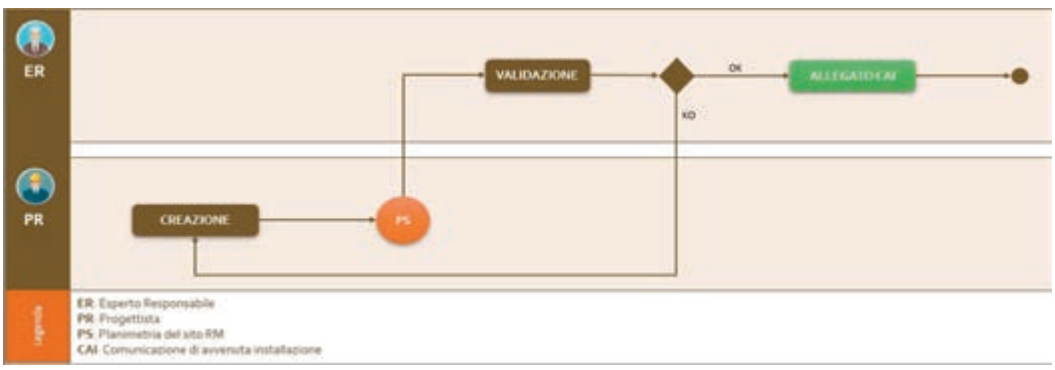


Figura 6
Flusso del documento "Planimetria del sito RM"

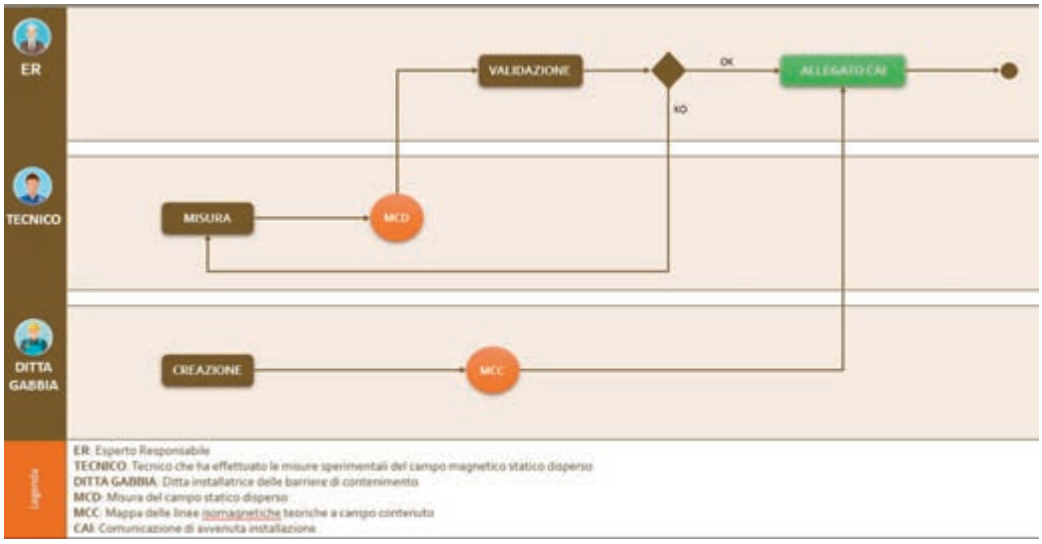


Figura 7
Flusso del documento "Mappa delle linee isomagnetiche teoriche a campo contenuto e le misure del campo magnetico statico disperso"

- La sicurezza, nel caso di tomografi a magnete a superconduttore. In caso di quench, infatti, l'impianto di condizionamento/ventilazione opera in regime di emergenza aumentando il numero orario di ricambi d'aria e portando la sala RM ad uno stato barico negativo per espellere gas criogeno e introdurre aria pulita.

Tale impianto deve essere verificato con periodicità almeno semestrale.
I documenti da accludere alla CAI, per i magneti a superconduttore sono i seguenti:

- Una relazione tecnica descrittiva del funzionamento dell'impianto, in cui viene riportato:
  - Lo schema dell'impianto nella sala magnete;
  - Il numero di ricambi d'aria/ora, in situazione normale e di emergenza;
  - Il volume della sala magnete.
- La dichiarazione di conformità a regola d'arte.

Il documento in questione viene realizzato dalla ditta installatrice dell'impianto di ventilazione.

In aggiunta allo schema dell'impianto è necessario allegare anche il report con le verifiche della ventilazione della sala effettuate dall'ER, nel quale viene indicata, per ogni bocchetta, il valore della portata d'aria in condizioni normali e di emergenza e in cui viene dimostrato che la sala sia in leggera sovrappressione in condizioni normali e in depressione in condizioni emergenziali.

3.1.8 Certificato di taratura della cella ossigeno

Nel caso di apparecchiature RM a magnete a superconduttore, è obbligatoria l'installazione di un sistema per la rilevazione dell'ossigeno, che

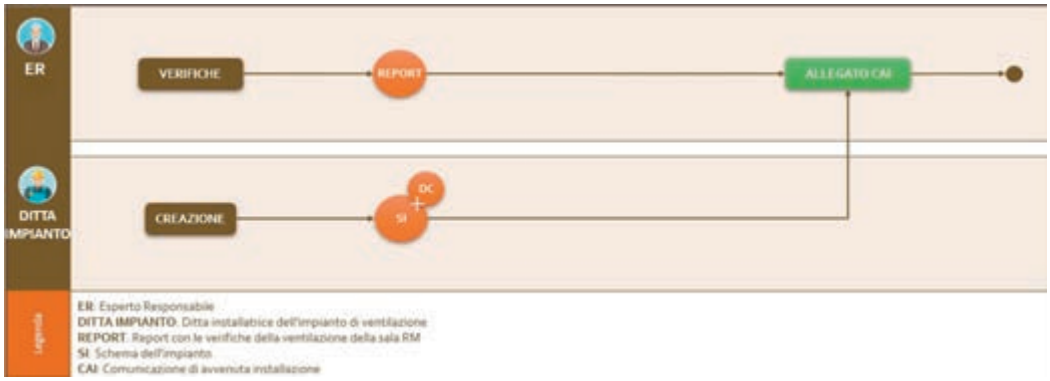


Figura 8
Flusso del documento "Documentazione tecnica relativa all'impianto di ventilazione o condizionamento della sala RM"

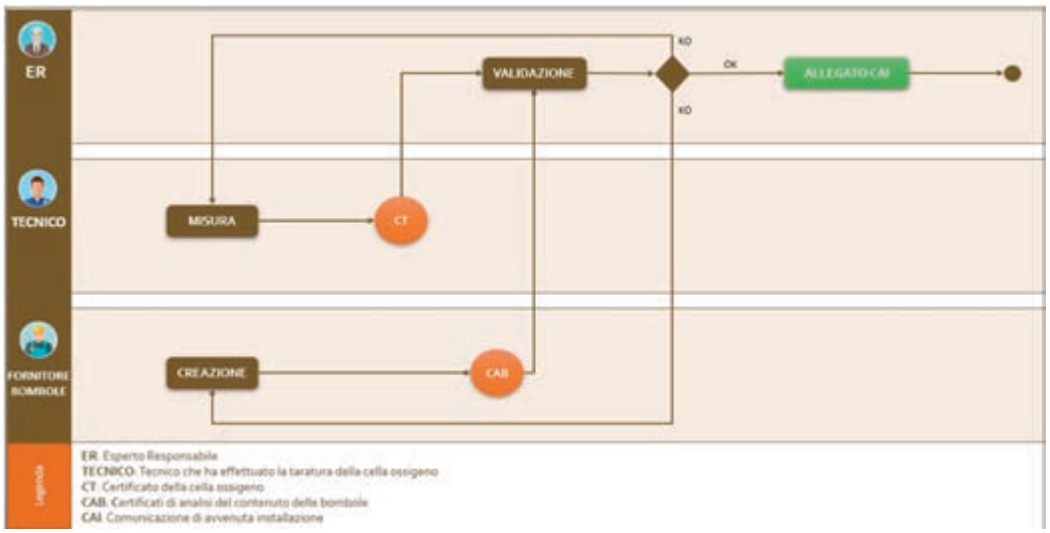


Figura 9
Flusso del documento "Certificato di taratura della cella ossigeno"

monitori costantemente il livello di O_2 nella sala magnete.
Il sistema di rilevazione deve essere tarato con cadenza semestrale e, ad ogni taratura, viene prodotto un certificato in cui viene garantita la taratura della cella a quattro punti ed in cui vengono inseriti anche i certificati del contenuto gassoso delle bombole con cui la cella O_2 è stata tarata.
Nel certificato deve essere indicato:

- Che la taratura sia stata effettuata esponendo la cella a 4 gas di prova con frazione di ossigeno certificata:
  - Taratura di zero, la frazione di O_2 è pari al valore minimo di sensibilità della cella stessa (0%);
  - La frazione di O_2 è pari al valore soglia di allarme fissata dal D.M. salute 10/08/2018 (18%);
  - La frazione di O_2 è pari al valore soglia di preallarme fissata dal D.M. salute 10/08/2018 (19%);
  - La frazione di O_2 è pari al valore ambiente (20,9%).
- La data di scadenza del sensore di O_2;
- La data in cui è stata effettuata la taratura;
- Il nome del tecnico che ha effettuato la taratura e la firma dello stesso;
- L'identificazione delle bombole utilizzate per la taratura;
- La validazione del certificato di taratura da parte dell'ER.
- In aggiunta al certificato di taratura devono essere allegati i certificati di analisi del contenuto gassoso delle bombole utilizzate per la taratura (rilasciati dal fornitore delle bombole) e l'ER dovrà verificare:
- Data di scadenza delle bombole;

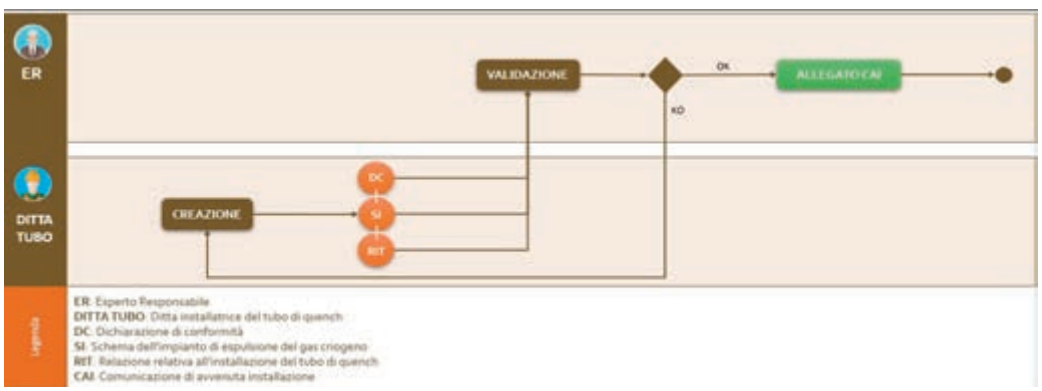


Figura 10
Flusso del documento "Documentazione tecnica relativa al tubo di quench"

- Rispondenza con quanto riportato nel certificato di taratura.
- Il certificato di taratura viene fornito da un tecnico e validato dall'ER. I certificati di analisi del contenuto delle bombole vengono rilasciati dal fornitore e validati dall'ER.

3.1.9 Documentazione tecnica relativa al tubo di quench

L'impianto di espulsione del gas criogeno è un dispositivo di sicurezza obbligatorio per tutti i tomografi RM a superconduttore. Tale impianto consente l'espulsione, in caso di quenching, del gas criogeno in ambiente esterno.
La documentazione tecnica relativa comprende:

- Lo schema dell'impianto (in scala e che riporti il terminale del tubo di quench per dimostrare il rispetto delle distanze cautelative con il contesto circostante);
- Le specifiche tecniche richieste del tubo di quench in relazione al tomografo RM;
- La relazione relativa all'installazione del tubo con il calcolo della caduta barica lungo il medesimo;
- La dichiarazione di conformità alla regola dell'arte.

Lo schema dell'impianto, la relazione relativa all'installazione del tubo e la dichiarazione di conformità vengono prodotte dalla ditta installatrice del tubo e validate dall'ER.
I requisiti relativi al tubo di quench vengono rilasciati dalla ditta fornitrice del tomografo RM.

3.1.10 Regolamento di sicurezza

Rappresenta le norme interne, redatte dal MRR e dall'ER e portate alla conoscenza di tutti coloro che hanno la possibilità di accedere al sito RM.
Tale documento deve essere trasmesso in allegato alla CAI, datato e firmato da entrambi i responsabili e deve contenere le seguenti informazioni:

- Le aree di rischio del sito RM (ZAC, ZC, ZR);
- Modalità di sorveglianza fisica e medica per tutta la popolazione coinvolta;
- Procedure di accesso, gestionali e di emergenza;
- Protocolli comportamentali per i lavoratori che possiedono l'autorizzazione ad accedere;
- Viene redatto e prodotto dai responsabili per la sicurezza e dal DL.

3.1.11 Questionario anamnestico e consenso informato

Viene proposto al paziente prima dell'esecuzione dell'esame, dal MRP, per verificarne l'idoneità ad accedere all'esame diagnostico.
Il documento riporta una serie di quesiti diagnostici che il MRP propone al paziente prima dell'esame e riporta la firma del medico.
In aggiunta al questionario viene fornito al paziente il consenso informato (l'atto autorizzativo del paziente) in cui viene informato sugli eventuali rischi e controindicazioni dell'esame.
Il Questionario anamnestico viene redatto dal MRR.

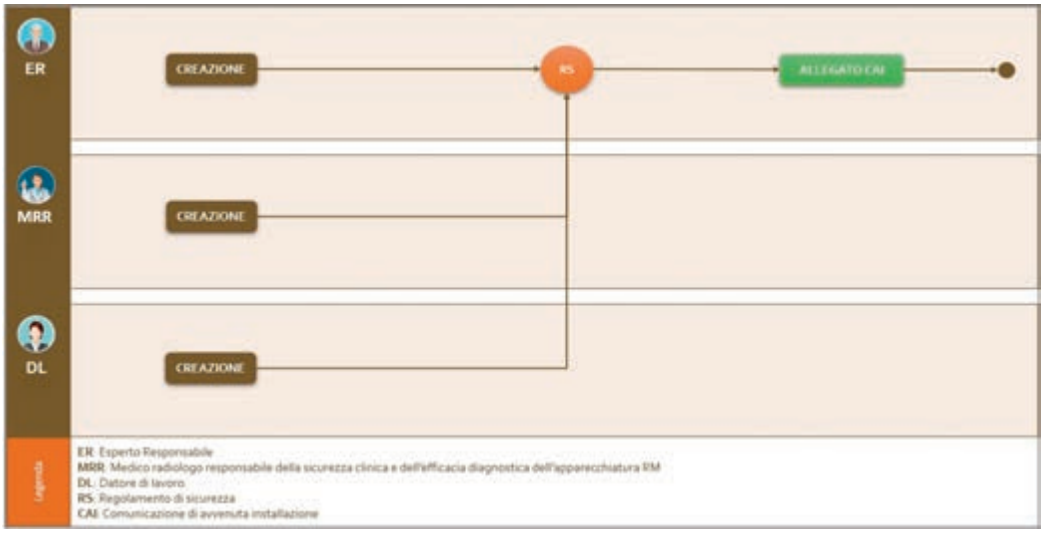


Figura 11
Flusso del documento "Regolamento di sicurezza"

3.1.12 Scheda di accesso in zona controllata

Analogamente al questionario anamnestico ed al consenso informato che sono dedicati alla verifica di idoneità del paziente allo svolgimento dell'esame, anche per visitatori e accompagnatori, viene effettuato un questionario preliminare. A seguito di questo, nella scheda di accesso viene richiesta la firma di un consenso informato da parte dei visitatori o di chi accede alla zona. La scheda di accesso in zona controllata viene redatta dal MRR.

3.1.13 Il percorso del Dewar

Il percorso del Dewar è il tragitto che gli operatori addetti al rabbocco del gas criogeno nei magneti a superconduttore devono effettuare per portare la bombola di gas dall'esterno della struttura alla sala RM.
Il percorso (più breve) viene stabilito dall'ER sulla base della planimetria della struttura.

3.1.14 Controlli di qualità

I controlli di qualità sono controlli periodici effettuati sul tomografo RM che hanno il fine di verificare la qualità delle sue prestazioni e delle immagini prodotte. Il primo controllo di qualità viene effettuato all'accettazione della macchina RM e, in seguito, con cadenza almeno semestrale.
In allegato alla CAI viene richiesto un rapporto tecnico delle misure di accettazione e nel caso in cui la CAI fosse trasmessa nel semestre successivo all'accettazione, anche gli ultimi controlli effettuati.
Il D.M. salute 10/08/2018 stabilisce che ***è compito del MRR e dell'ER predisporre e mantenere attivo sotto la propria responsabilità un programma di garanzia della qualità.*** La scelta del protocollo da usare spetta esclusivamente all'ER, ma il giudizio di idoneità all'uso clinico dell'apparecchiatura deve essere sottoscritto sia dal MRR che dall'ER.

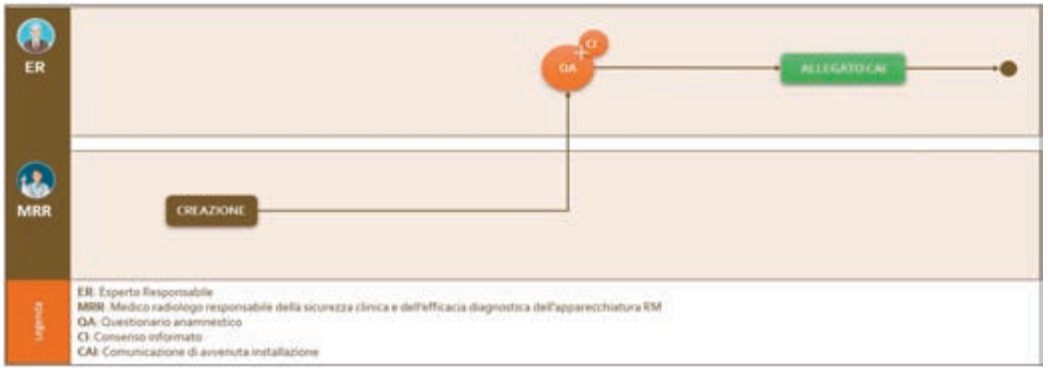


Figura 12
Flusso del documento "Questionario anamnestico e consenso informato"

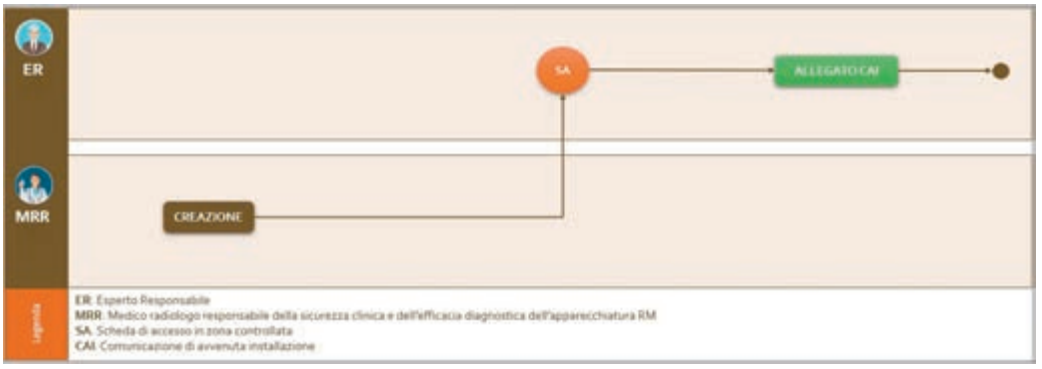


Figura 13
Flusso del documento "Scheda di accesso in zona controllata"

Figura 14
Flusso del documento "Percorso del Dewar"

3.1.15 Documentazione tecnica relativa alla gabbia di Faraday

Per isolare la macchina RM da onde elettromagnetiche esterne, viene costruita una schermatura per i campi elettromagnetici a radiofrequenza, definita gabbia di Faraday.
Relativamente alla gabbia di Faraday, occorre allegare:

- Documentazione tecnica descrittiva della gabbia in cui viene incluso:
  - progetto della gabbia di Faraday;
  - costruzione del collegamento a terra;
  - modalità di manutenzione, pulizia e sostituzione.
- Rapporto di collaudo, in cui è indicata:
  - la strumentazione utilizzata per la verifica della tenuta della gabbia;
  - la modalità di esecuzione delle prove;
  - i punti della gabbia dove è stata effettuata la prova;
  - la tabella dei valori sperimentali di attenuazione della stessa RF in ogni punto di prova.

La documentazione tecnica viene fornita dalla ditta installatrice della gabbia di Faraday, mentre il rapporto di collaudo deve essere datato e validato dall'ER.

3.1.16 Benestare all'uso del tomografo

A seguito dei controlli periodici di sicurezza e qualità, viene rilasciato il benestare all'uso del tomografo, contestualmente al collaudo.
Questo deve essere periodicamente confermato a seguito di successivi controlli di sicurezza e qualità (con cadenza almeno annuale).
Il benestare all'uso del tomografo viene rilasciato dall'ER e dal MRR.

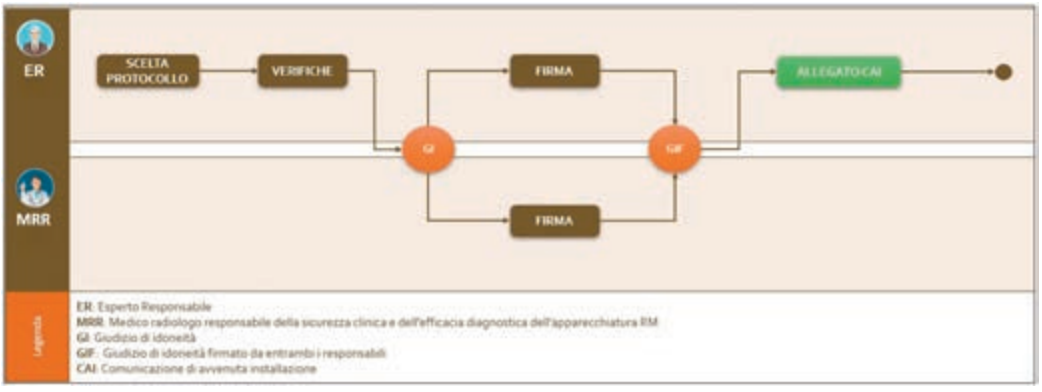


Figura 15
Flusso del documento "Controlli di qualità"

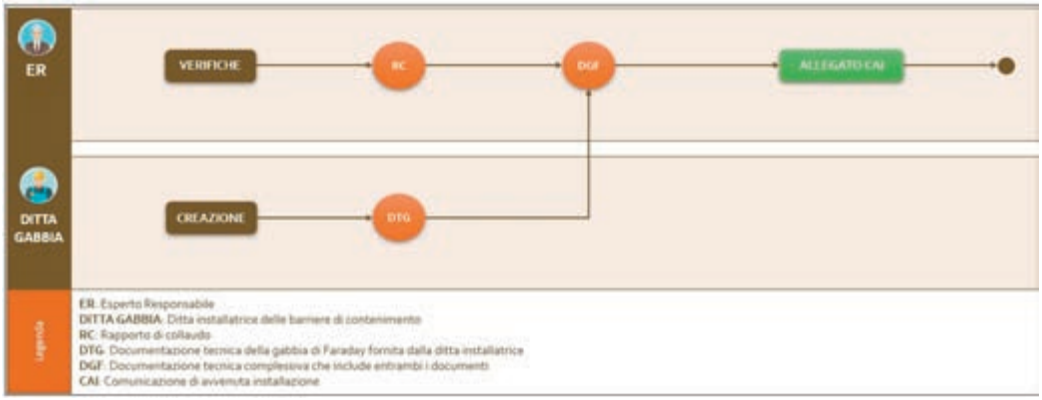


Figura 16
Flusso del documento "Documentazione tecnica relativa alla gabbia di Faraday"

3.1.17 Idoneità alla mansione specifica dei lavoratori esposti

Il Protocollo di sorveglianza sanitaria per la formulazione del giudizio di idoneità alla mansione specifica dei lavoratori esposti ai fattori di rischio presenti in ambiente RM viene prodotto dal Medico Competente (MC) che si occupa della sorveglianza sanitaria dei lavoratori che hanno accesso alla ZAC o alla ZC.
Sono previsti due documenti da trasmettere in allegato alla CAI:

- Protocollo medico, con cui il MC ha verificato l'idoneità del lavoratore;
- Format per il rilascio dell'idoneità alla mansione.

Devono essere individuati in modo specifico senza ambiguità gli agenti di rischio su cui è stata effettuata la valutazione.

3.1.18 Altri documenti

- Cartellonistica ed etichettatura presente all'interno del sito;
- Posizionamento della cella O_2 sopra la macchina;
- Presenza delle linee isogauss a terra;
- Terminale del tubo di quench, per mostrare il rispetto delle distanze di sicurezza.

Figura 17
Flusso del documento "Benestare all'uso del tomografo"

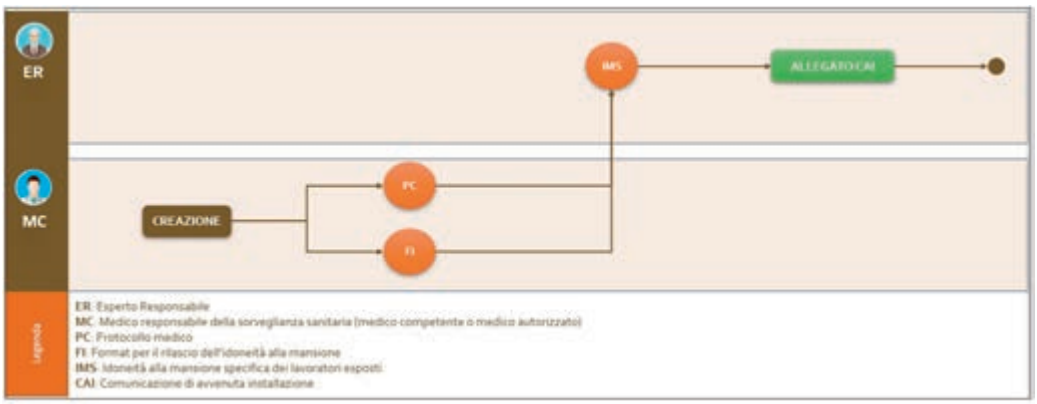
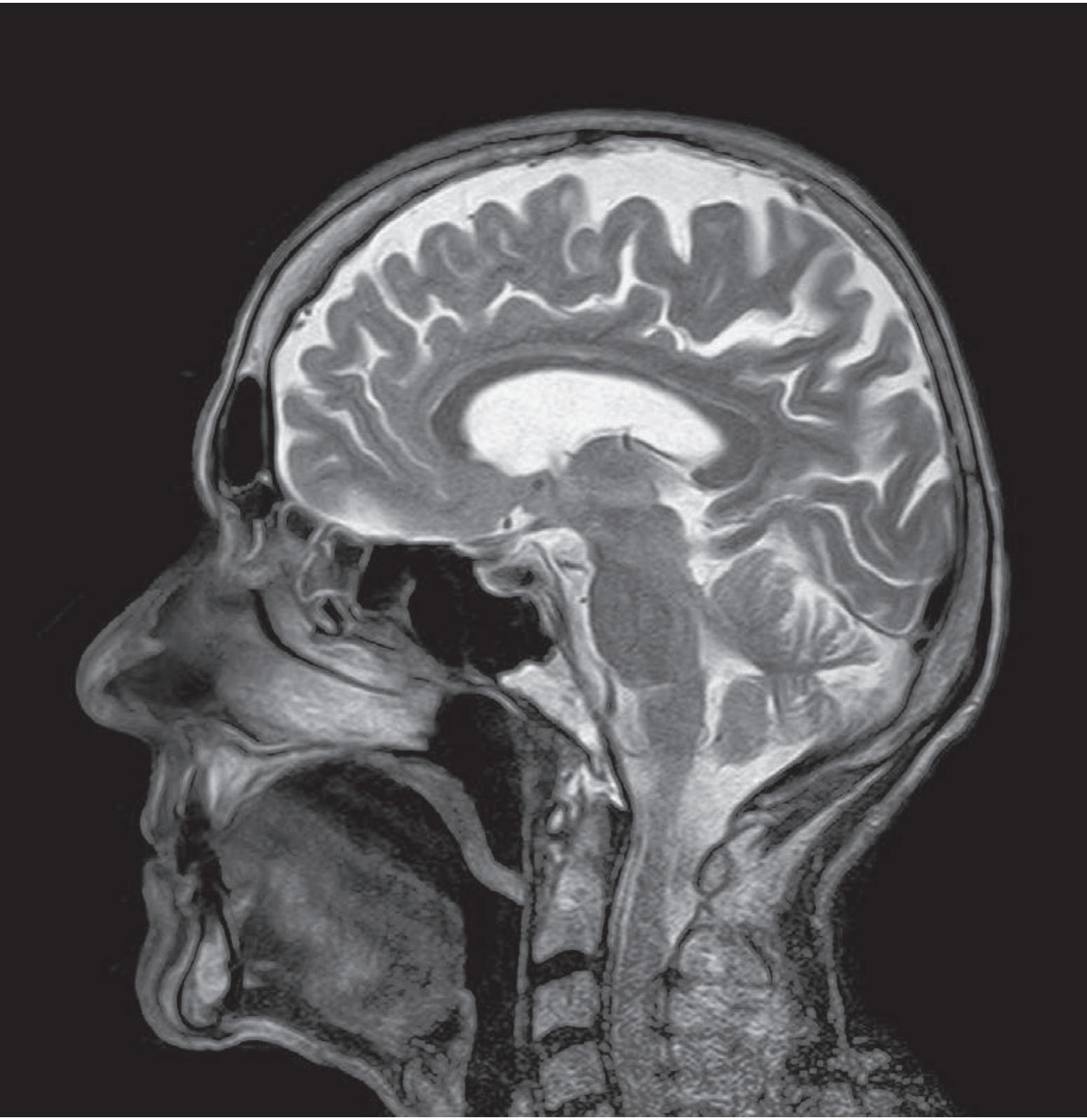


Figura 18
Flusso del documento "Idoneità alla mansione specifica dei lavoratori esposti"

io roma



ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI ROMA

4 CRONOGRAMMA DELLA GESTIONE DOCUMENTALE

La Tabella 1 riporta in ordine tutti i documenti che vengono raccolti nel corso dell'installazione di una RM. Vengono riportati, inoltre, i responsabili della produzione o consegna del documento ed eventuali criticità.

Ordine	Descrizione attività cardine	Responsabile	Note	Criticità
1	Lettera di conferimento dell'incarico e accettazione		Quando il cliente decide di cambiare/acquistare una nuova apparecchiatura, il DL produce la lettera di conferimento e la invia ai responsabili individuati che la controfirmeranno per accettazione.	Finché la lettera non viene inviata e firmata, l'ER non può essere individuato come "responsabile" dell'installazione della RM.
2	Curriculum Vitae	ER		
3	Curriculum Vitae	MRR		
4	Compilazione Lettera	DL		
5	Firma	MRR		
6	Firma	ER		
7	Caratteristiche tecniche dell'apparecchiatura RM		Fornito alla struttura al momento del preventivo.	
8	Compilazione	Ditta RM		
9	Mappa delle linee isomagnetiche			
10	Mappa delle linee isomagnetiche in campo statico disperso	Ditta RM	Rilasciate dal costruttore del tomografo con le caratteristiche del tomografo.	Un'errata indicazione porterebbe poi un errore su tutte le successive valutazioni di contenimento del campo.
11	Planimetria del presidio		Rilasciata dalla struttura in quanto già in suo possesso.	Sulla base delle planimetrie vengono effettuate tutte le successive valutazioni, dunque è un documento indispensabile per procedere con i lavori e con la produzione della CAI.
12	Creazione/consegna	PR		

Ordine	Descrizione attività cardine	Responsabile	Note	Criticità
13	Validazione della planimetria del presidio	ER	Al termine dei lavori l'ER verifica che la planimetria su carta combaci con la struttura	
14	Planimetria del sito RM			Come per la planimetria del presidio
15	Creazione/consegna	PR		
16	Validazione	ER		
17	Percorso del dewar		Stabilito dall'ER in fase di progettazione del sito. Spesso si sfruttano entrate/uscite di emergenza o normali già presenti.	
18	Percorso del dewar	ER		
19	Mappa delle linee isomagnetiche			
20	Mappa in campo contenuto	Ditta Gabbia		Nel corso del collaudo, l'ER valida le misure e verifica la corretta installazione delle barriere. Nel caso di misure errate, si dovrebbe rimettere mano alla struttura delle barriere di contenimento.
INSTALLAZIONE IMPIANTO VENTILAZIONE				
INSTALLAZIONE RM				
INSTALLAZIONE GABBIA				
21	Documentazione tecnica relativa all'impianto di ventilazione e condizionamento			
22	Schema impianto	Ditta Impianto		
23	Documentazione tecnica relativa al tubo di quench			
24	Schema impianto	Ditta Tubo		
25	Relazione installazione tubo	Ditta Tubo		


SIGNA
Creator

Ordine	Descrizione attività cardine	Responsabile	Note	Criticità
26	Dichiarazione di conformità	Ditta Tubo	Fornita all'ER al termine delle opere sull'impianto.	
27	Validazione documenti	ER		
28	Documentazione tecnica relativa alla gabbia di Faraday			
29	Documentazione tecnica gabbia	Ditta Gabbia		
30	Certificato di taratura della cella ossigeno			
31	Misure cella O2	Tecnico		
32	Produzione certificato	Tecnico		
33	Analisi contenuto bombole	Fornitore delle bombole		
COLLAUDO				
34	Documentazione tecnica relativa all'impianto di ventilazione e condizionamento			
35	Verifiche ventilazione	ER	Effettuate dall'ER prima che si innalzi il campo	Sono di importanza cruciale, in quanto l'impianto di ventilazione è il principale sistema di sicurezza in caso di emergenze.
36	Report verifiche	ER		
37	Documentazione tecnica relativa alla gabbia di Faraday			
38	Rapporto di collaudo	ER		
39	Mappa delle linee isomagnetiche			
40	Validazione misure del campo statico disperso	ER		

Ordine	Descrizione attività cardine	Responsabile	Note	Criticità
41	Certificato di taratura della cella ossigeno			
42	Validazione misure cella O2	ER		
43	Validazione analisi bombole	ER		
44	Controlli di qualità			
45	Scelta protocollo	ER		
46	Verifiche	ER		
47	Creazione giudizio di idoneità	ER		
48	Firma documento	ER		
49	Firma documento	MRR		
50	Benestare all'uso del tomografo			Rilasciato a condizione che tutte le precedenti verifiche abbiano avuto esito positivo.
51	Benestare all'uso del tomografo	ER		Sarebbe auspicabile che l'ER acquisisse la planimetria catastale da parte del direttore dei lavori e la dichiarazione di conformità dei requisiti minimi, così da non doversi assumere responsabilità al di là della sua competenza
52	Benestare all'uso del tomografo	MRR		
53	Regolamento di sicurezza			Prima dell'inizio delle attività cliniche viene stilata una prima versione. Ci possono essere continue revisioni nel corso del tempo. Agli organi competenti va comunicata la versione definitiva.
54	Creazione	ER		
55	Creazione	MRR		
56	Creazione	DL		
57	Questionario anamnestico preliminare		Prima dell'inizio delle attività cliniche	
58	Questionario anamnestico	MRR		

Ordine	Descrizione attività cardine	Responsabile	Note	Criticità
59	Consenso informato	MRR		
60	Scheda di accesso in zona controllata		Prima dell'inizio delle attività cliniche	
61	Scheda di accesso in zona controllata	MRR		
62	Idoneità alla mansione specifica dei lavoratori esposti			
63	Protocollo di sorveglianza sanitaria	MC		
64	Format rilascio idoneità	MC		
INIZIO ATTIVITA' CLINICHE				
65	Relazione tecnica degli standard di sicurezza			
66	Compilazione	ER		
67	Compilazione	MRR		
68	Firma	DL		
INVIO CAI				

Tabella 1 - Cronogramma della gestione documentale dell'installazione di una macchina RM

5 CONCLUSIONI

L'ER ha il compito di raccogliere la documentazione richiesta a corredo della CAI nel corso dei 60 giorni a disposizione dal termine dell'installazione della RM, interfacciandosi con tutti gli attori coinvolti nella produzione documentale. Suo compito è, inoltre, verificare la validità dei documenti ricevuti effettuando anche un'analisi ed eventualmente verifiche sul campo delle informazioni recepite.

L'ER, dunque, assume un ruolo non dissimile da quello di un ufficio tecnico per stabilire e valutare l'esattezza delle informazioni recepite da ciascun documento, dopo averne effettuato la raccolta.

Di seguito si propone la lista delle attività associate ad ogni attore coinvolto nella produzione della CAI.

Responsabile	Attività
Esperto Responsabile	Stesura relazione tecnica degli standard di sicurezza
	Firma accettazione incarico
	Validazione planimetria presidio e sito
	Validazione misure del campo statico disperso
	Stesura report verifiche di ventilazione sala
	Validazione certificato cella ossigeno
	Validazione certificato analisi contenuto bombole
	Validazione documentazione del tubo di quench
	Stesura regolamento di sicurezza
	Progettazione percorso Dewar
	Controlli di qualità
	Stesura rapporto di collaudo della gabbia
	Benestare all'uso del tomografo RM
Medico Responsabile	Stesura relazione tecnica degli standard di sicurezza
	Firma accettazione incarico
	Stesura regolamento di sicurezza
	Stesura questionario anamnestico e consenso informato
	Firma giudizio di idoneità
	Benestare all'uso del tomografo RM
	Stesura scheda di accesso in ZC
Datore di lavoro	Stesura lettera di conferimento/accettazione incarico
	Raccolta CV dei responsabili per la sicurezza
	Firma relazione tecnica degli standard di sicurezza
	Stesura regolamento di sicurezza
Medico competente	Stesura documento di idoneità alla mansione specifica per i lavoratori esposti
Ditta produttrice del tomografo	Caratteristiche tecniche dell'apparecchiatura RM
Ditta produttrice della gabbia di Faraday	Documentazione gabbia di Faraday
	Mappa linee isomagnetiche in campo contenuto
Ditta installatrice del tubo di quench	Documentazione tubo di quench
Ditta dell'impianto di ventilazione	Schema impianto di ventilazione e condizionamento
Progettista	Planimetria presidio con l'apparecchiatura RM
	Planimetria del sito RM
Fornitore delle bombole	Certificato analisi del contenuto delle bombole
Tecnico	Misure campo statico disperso
	Taratura celle O_2

Tabella 2 – Compiti svolti dai responsabili per installare una macchina RM.

Analizzando i cicli di vita di ciascun documento e accorpando tutti i flussi derivati da tale analisi viene riportato il flusso complessivo, ovvero, il ciclo di vita totale della CAI.

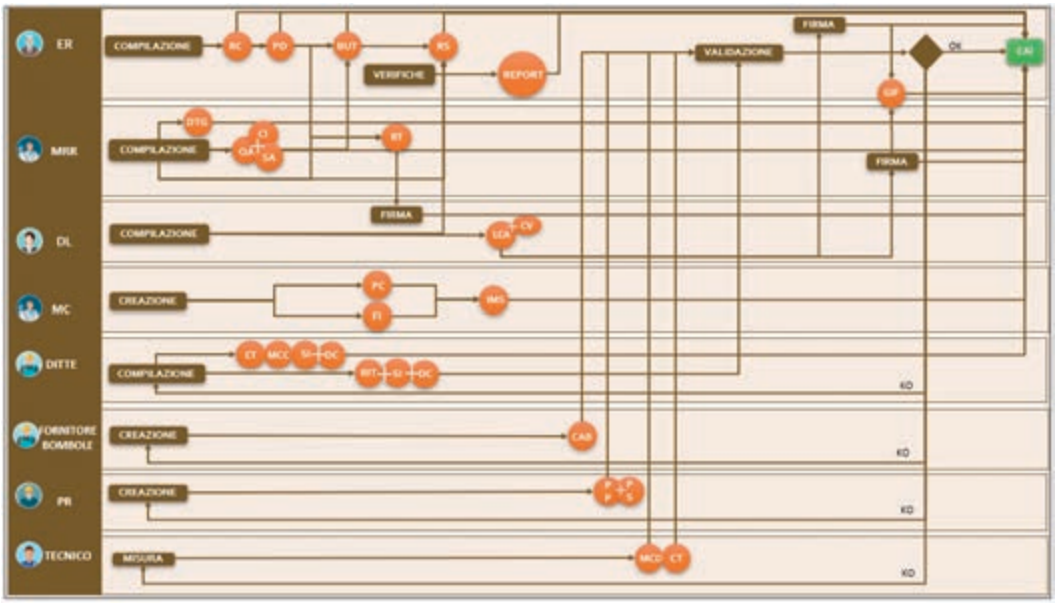


Figura 19
Flusso complessivo della CAI.

Nel corso dell'analisi del flusso documentale legato all'installazione di una nuova macchina RM, a partire dalla istanza di installazione fino alla produzione e consegna della CAI, sono state evidenziate alcune criticità:

- La produzione della CAI, viene effettuata con un limite di tempo di 60 giorni a partire dalla sua installazione, quindi parallelamente alle eventuali ispezioni da parte di ASL;
- personaggi che partecipano in qualche modo alla produzione della CAI sono molti e l'ER ha il compito di interagire con essi per raccogliere la documentazione richiesta, può presentarsi il problema che alcuni di questi non siano collaborativi, rallentando, così, la raccolta documentale e il proseguimento delle attività.

Lista Acronimi

ER Esperto Responsabile della Sicurezza
MA Medico Autorizzato
MRR Medico Radiologo Responsabile per la sicurezza clinica
MRP Medico Responsabile della Prestazione Diagnostica
DL Datore di lavoro
CAI Comunicazione di Avvenuta Installazione
RM Risonanza Magnetica
ZAC Zona ad Accesso Controllato
ZC Zona Controllata
ZR Zona di Rispetto

Bibliografia

[1] Canese, R., & Podo, F. (1994). Introduzione alla risonanza magnetica ad uso clinico. Principi fisici e strumentazione.

[2] DOMENICI, V., & VERACINI, C. A. (2008). RISONANZA MAGNETICA NUCLEARE: passato, presente e futuro di una tecnica spettroscopica che ha cambiato la chimica e non solo. CnS, La chimica nella scuola, 70-89.

[3] INAIL. (2018). Attuazione dei nuovi standard di sicurezza in risonanza magnetica - La comunicazione di avvenuta installazione da inviare all'INAIL (2018).

[4] INAIL. (2022). Aggiornamento. Obbligo di comunicazione di avvenuta installazione delle apparecchiature a risonanza magnetica: Aggiornamento ai sensi del DM Salute 14/01/2022 e indicazioni all'utenza.

[5] REPUBBLICA, P. D. (1994, 08 08). DPR 542 del 08/08/1994. DPR 8 agosto 1994, n. 542 - Regolamento recante norme per la semplificazione del procedimento di autorizzazione all'uso diagnostico di apparecchiature a risonanza magnetica nucleare sul territorio nazionale.

[6] Salute, M. d. (s.d.). D.M. 14/01/2021. Determinazione degli standard di sicurezza e impiego per le apparecchiature a risonanza magnetica e individuazione di altre tipologie di apparecchiature a risonanza magnetica settoriali non soggette ad autorizzazione.

SFIDE DI CYBERSECURITY NELLA SICUREZZA FERROVIARIA

Quaderno

a cura di:
Ing. Mennato Catillo

ABSTRACT

Il trasporto ferroviario è un sistema molto complesso, che per funzionare ed essere efficiente ha bisogno di elementi strutturali e di figure professionali che lo gestiscano.
Oggi, il sistema europeo di controllo del traffico ferroviario, o più specificamente della marcia treni, si basa sull'applicazione di nuove tecnologie per l'interazione e lo scambio di informazioni treno/terra, allo scopo di incrementare l'automazione della guida, della sicurezza di circolazione e della potenzialità di una linea ferroviaria. Stiamo parlando di ETCS. Il funzionamento dell'ETCS si basa su componenti che scambiano informazioni, rispettivamente posti a terra e a bordo del mezzo di trazione.
L'evoluzione tecnologica e il processo di standardizzazione dei componenti elettronici e delle tecnologie dell'informazione e della comunicazione, sia a livello di infrastruttura che di materiale rotabile, ha generato nuovi rischi all'interno del settore ferroviario: la sicurezza dell'esercizio ferroviario è oramai correlata al concetto di sicurezza informatica. Si introduce così il rischio "cyber" nel settore ferroviario. Negli ultimi anni il sistema ferroviario ha subito diversi attacchi che hanno sostanzialmente influito i sistemi di informazione.
La cyber security è sempre più cruciale in un mondo che fa affidamento a infrastrutture e a dispositivi connessi. Il crescente grado di connettività delle infrastrutture e del materiale rotabile sta creando un notevole aumento della loro superficie di attacco. Ovviamente, questa connettività offre livelli di prestazioni più elevate in termini di affidabilità, disponibilità, sicurezza e aggiornamento.
Il fattore tempo è un altro punto da considerare: il tempo "cyber" richiede misure rapide per l'applicazione di correzioni al sistema (segnalazione, manutenzione, ecc.) al fine di affrontare eventuali vulnerabilità; ma i tempi di sicurezza ferroviaria richiedono un'analisi di non regressione del sistema, e la garanzia che l'aggiornamento effettuato non renda l'infrastruttura incompatibile con il materiale rotabile che circola su di essa, o addirittura degradi il livello di sicurezza.
Tra il grande entusiasmo per la digitalizzazione, molti hanno sollevato la domanda su quanto sia sicuro il ricorso a queste tecnologie. La sicurezza informatica è stata definita come il "rovescio della medaglia" della digitalizzazione ferroviaria e una vera minaccia in un contesto in rapida evoluzione. La maggiore dipendenza dai sistemi digitali ha esposto il settore al mondo esterno. A differenza del passato, la struttura ferroviaria è oggi conosciuta anche al di fuori del settore ferroviario, il che significa che i sistemi potrebbero essere più facilmente penetrati da chiunque.

Quali sono i rischi? Quanto sono resilienti i nostri sistemi e quanto velocemente possono essere ripristinati? Inoltre, quanto è complesso proteggere reti estese come quelle in Europa? Le soluzioni devono includere valutazioni e aggiornamenti regolari, poiché le minacce evolvono anno dopo anno, e devono essere concepite in stretta collaborazione tra i protagonisti del settore.
ENISA (European Union Agency for Cybersecurity), a novembre del 2021, ha pubblicato un Report dal titolo "Railway Cybersecurity – Good Practices in Cyber Risk Management" con il proposito di fornire buone pratiche per gli approcci di gestione del rischio informatico applicabili al settore ferroviario.

1 Background

Il punto di partenza è l'attuale stato della normativa e dell'indicazione di parametri di conformità relativi alla sicurezza informatica nel settore ferroviario.
Da diversi anni, la Commissione Europea sta promuovendo lo sviluppo del trasporto ferroviario Europeo attraverso:

- Omologazione dei sottosistemi di terra e di bordo.
- Integrazione sistemi CCS – Sistemi che comandano e controllano il segnalamento ferroviario.
- Armonizzazione dei sistemi normativi e dei processi.

Il progresso tecnologico scientifico, la mitigazione dell'impatto del fattore umano come elemento di sicurezza intrinseco e lo sviluppo delle normative ferroviarie sono i principali inputs dell'evoluzione del Sistema Ferroviario Europeo. Sistemi, che in passato erano elettromeccanici, oggi sono basati su calcolatori programmabili e controllori digitali. L'obiettivo principale è l'aumento della velocità, della sicurezza, della disponibilità, dell'affidabilità e manutenibilità del sistema trasporto ferroviario.
Futuri progetti sono focalizzati sulle tecnologie Internet, rete 5G e sistemi ad intelligenza artificiale: un esempio è la progettazione di sistemi in grado di monitorare, in tempo reale, la costanza geometrica e l'integrità strutturale della rete ferroviaria.
Questo processo di automazione e digitalizzazione produrrà un aumento di dispositivi e dati generati connessi alla rete, che comporterà a sua volta una crescita esponenziale delle "superfici di attacco" vulnerabili per svariati fini: carpire informazioni, creare reti per la diffusione

di programmi dannosi (dispositivi asserviti per attacchi finalizzati a paralizzare il servizio), o con il solo scopo di compromettere la funzionalità del dispositivo stesso.
In definitiva, il sistema ferroviario oggi si ritrova a dover fronteggiare la nuova sfida derivata dai problemi di sicurezza che le nuove tecnologie comportano.
Nel 2016, l'Unione Europea con la Direttiva NIS 1148/2016 (Network and Information Security), ha iniziato ad identificare e caratterizzare gli attori dello spazio digitale, riconoscendo al trasporto ferroviario la natura di Servizio Essenziale. Un Operatore di Servizi Essenziali è tale se un suo danneggiamento potrebbe intaccare la sicurezza Nazionale del Paese; da ciò segue la necessità per gli Operatori di Servizi Essenziali di essere resilienti, anche ad attacchi informatici.

2 "Cyber Risk" nel sistema ferroviario

Il punto di partenza per le imprese ferroviarie e di conseguenza per i gestori delle infrastrutture ferroviarie è l'identificazione delle risorse e dei servizi ferroviari che sono sottoposti a rischi informatici. Il sistema ferroviario è composto da diverse unità, ognuna responsabile delle proprie infrastrutture, risorse e servizi. Tali unità sono inevitabilmente interconnesse ed interagiscono per fornire servizi.
Il passo successivo è sviluppare indicatori per valutare l'impatto del rischio informatico sulla disponibilità, integrità e riservatezza di tali risorse e servizi.
Diversi studi sono in corso. ENISA (European Union Agency for Cybersecurity), nell'attività dal tema "Railway Cybersecurity - Good Practices in Cyber Risk Management", ha individuato i seguenti principali servizi ferroviari:

- Garantire la sicurezza e l'incolumità dei passeggeri e delle merci.
- Manutenzione dell'infrastruttura ferroviaria e dei treni.
- Gestione delle finanze.
- Pianificazione delle operazioni e gestione delle risorse.
- Informazione ai clienti.
- Trasporto di merci e passeggeri.
- Vendita e distribuzione di biglietti.

Da tale studio è emersa la necessità per gli stakeholder ferroviari di utilizzare varie tassonomie come base per identificare le loro principali risorse e servizi informatici. Inoltre, come già detto, devono essere considerate l'interdipendenza tra i sistemi.

L'identificazione di tutte le interdipendenze dei sistemi può essere una vera sfida. I sistemi si evolvono rapidamente e la digitalizzazione di tutti i processi aggiunge sempre più sistemi che devono essere presi in considerazione.
Nell'attività condotta da ENISA, sono stati individuati gli asset e i servizi da includere nella valutazione del rischio informatico. In particolare, sono state individuate 5 aree da analizzare: i servizi forniti, i dispositivi (sistemi tecnologici) che supportano questi servizi, le apparecchiature utilizzate per fornire tali servizi, le persone che li utilizzano e i dati utilizzati. Di seguito i dettagli:

1. Individuate le seguenti categorie di servizi:
   - Segnalamento ferroviario ETCS/ERTMS (sistema OT);
   - Servizi ausiliari (sistema OT);
   - Controllo e comando (sistema OT);
   - Network allocation system (sistema IT);
   - Gestione delle risorse (sistema IT);
   - Sviluppo (sistema IT);
   - Manutenzione (sistema IT);
   - Servizi passeggeri (sistema IT);
   - Supporto aziendale (sistema IT);
   - Sicurezza "Security" (sistema OT e IT);
   - Sicurezza "Safety" (sistema OT).
2. Individuate le seguenti categorie di dispositivi che supportano i servizi:
   - Telecom.
   - Infrastrutture terra/bordo IT e OT.
3. Individuate le apparecchiature utilizzate per fornire i servizi.
4. Individuate le persone che utilizzano i suddetti servizi.
5. Individuati i dati utilizzati.

Prima di analizzare gli scenari di rischio infomatico occorre fare delle ultime considerazioni.
I sistemi OT sono generalmente più vulnerabili dei sistemi IT, in parte a causa della mancanza di consapevolezza della sicurezza informatica nel personale OT, in parte perché non sono stati progettati pensando alla sicurezza informatica (lunghi cicli di vita di 30 anni, presenza di sistemi ereditati) e perché sono meno controllati e decentralizzati rispetto ai sistemi IT. Mentre in passato rimanevano meno esposti, spesso isolati da internet e da altre reti IT, ora sono sempre più interconnesse con i classici sistemi IT, il che li rende ancora più vulnerabili ed esposti alle minacce informatiche.Le RU (imprese ferroviarie) e gli IM (gestori dell'infrastruttura) devono quindi identificare e valutare:

- quali minacce informatiche sono applicabili alle loro risorse e servizi. Una delle domande più comuni è se le minacce, come disastri, attacchi fisici o interruzioni, devono essere incluse o considerate come fuori dallo scopo dell'ecosistema "cyber";
- la probabilità di uno scenario di minaccia: il livello di attacco, il livello di esposizione della risorsa. Di seguito alcuni metodi proposti:

- X2Rail-314 propone il Common Vulnerability Scoring System (CVSS). Si selezionano quattro metriche di sfruttamento CVSS: vettore di attacco (esposizione del sistema), complessità dell'attacco, privilegi richiesti e interazione dell'utente. I livelli per queste metriche sono stati definiti, calcolando matematicamente la probabilità risultante.
- ISO27005 combina la probabilità di accadimento della minaccia (bassa, media, alta), la facilità di esposizione (bassa, media, alta) e il valore dell'asset (da 0 a 4) per calcolare la probabilità di uno scenario incidente. È difficile gestire queste informazioni perché cambiano nel tempo man mano che il panorama delle minacce si evolve.

3 Scenari di rischio informatico "Cyber Risk" nel settore ferroviario

Le principali minacce da considerare sono:

- Disastri naturali: terremoti, inondazioni, frane, tsunami, forti piogge, forti nevicate, forti venti, eruzioni, tuoni, inquinamento, polvere, corrosione, esplosioni, danni causati da animali (ratti, scoiattoli, ecc.).
- Danni/perdite involontari di informazioni o risorse IT.
- Accesso ai locali da parte di persona non autorizzata, vandalismo, furto, ed altro.
- Guasti e/o malfunzionamenti dei dispositivi e sistemi di comunicazione.
- Interruzioni. Indisponibilità delle risorse necessarie, compreso assenza di personale (sciopero, pandemia, ecc.) o bassa competenza/maturità del personale.
- Minacce Software e Hardware.

ENISA (European Union Agency for Cybersecurity), nell'attività dal tema "Railway Cybersecurity - Good Practices in Cyber Risk Management", ha individuato i seguenti principali scenari di rischio informatico.

Scenario 1:
Compromissione del sistema di segnalamento o del sistema di controllo automatico del treno, con conseguente incidente ferroviario

Lo scenario potrebbe essere il seguente:

1. Un utente malintenzionato raccoglie informazioni (violazione fisica, dipendente malintenzionato, ecc.).
2. Costruzione di un dispositivo o un software per comandare e controllare la marcia dei treni.
3. Presa di controllo della marcia dei treni.
4. False informazioni di segnalazione vengono iniettate e portano a una grave interruzione o a un incidente ferroviario.

Gli impatti sono:

- Sicurezza dei treni e quindi dei passeggeri.
- Interruzione dell'attività.
- Perdita di reputazione del gestore delle infrastrutture/veicoli.

Misure di sicurezza:

- Sicurezza fisica e ambientale: l'operatore impedisce l'accesso fisico non autorizzato e il danneggiamento e l'interferenza con le informazioni dell'organizzazione e le strutture di elaborazione delle informazioni.
- Sicurezza delle risorse umane: programma di sensibilizzazione alla sicurezza CIS "Critical Information System" per il personale e un programma di formazione sulla sicurezza per i dipendenti con responsabilità relative al CIS.
- Crittografia: politica e procedure relative alla crittografia, al fine di garantire un uso adeguato ed efficace della crittografia per proteggere la riservatezza, l'autenticità e/o l'integrità delle informazioni nel suo CIS "Critical Information System".
- Diritto di accesso: l'operatore concede diritti di accesso a un utente o/a un processo automatizzato solo quando tale accesso è strettamente necessario all'utente per svolgere la sua missione o al processo automatizzato per svolgere le sue operazioni tecniche.
- Correlazione e analisi dei log: l'operatore crea un sistema di correlazione e analisi dei log che estrae gli eventi registrati dal sistema di registrazione installato su ciascuno dei CIS "Critical Information System" per rilevare gli eventi che incidono sulla sicurezza del CIS "Critical Information System".
- Rilevamento: l'operatore predispone un sistema di rilevazione degli incidenti di sicurezza del tipo "indagine di analisi per file e protocolli". Le indagini di analisi per file e protocolli analizzano i flussi di dati per cercare eventi che potrebbero influire sulla sicurezza del CIS "Critical Information System".

Scenario 2: Sabotaggio dei sistemi di supervisione della circolazione ferroviaria, con conseguente blocco del traffico ferroviario

Lo scenario potrebbe essere il seguente:

1. Un utente malintenzionato introduce un malware ICS, tramite e-mail phishing inviate a dipendenti o dispositivi utilizzati su sistemi OT.
2. Il malware ICS si propaga, prende il controllo del sistema e ottiene l'accesso remoto.
3. Il malware consente agli aggressori di comunicare facilmente con i sistemi di supervisione del traffico e manipolare in remoto la memoria del sistema per iniettare "shellcodes", iniettando infine un payload che interrompe i sistemi di supervisione.
4. I sistemi di supervisione si arrestano, impedendone la supervisione e determinando un arresto urgente della circolazione ferroviaria.

Gli impatti sono:
- Interruzione dell'attività.
- Perdita di reputazione del gestore delle infrastrutture/veicoli.

Misure di sicurezza:
- Sicurezza delle risorse umane: programma di sensibilizzazione alla sicurezza CIS "Critical Information System" per il personale e un programma di formazione sulla sicurezza per i dipendenti con responsabilità relative al CIS.
- Procedura di mantenimento della sicurezza informatica: l'operatore sviluppa e implementa una procedura per il mantenimento della sicurezza in conformità con il proprio ISSP "Information System Security Policy". A tal fine, la procedura definisce le condizioni che consentono il mantenimento del livello minimo di sicurezza delle risorse CIS "Critical Information System".
- Audit di sicurezza: l'operatore definisce le procedure per l'esecuzione di valutazioni di sicurezza del sistema informativo e audit di risorse critiche e CIS, tenendo conto dell'analisi dei rischi regolarmente aggiornata.
- Rilevamento: l'operatore predispone un sistema di rilevazione degli incidenti di sicurezza del tipo "indagine di analisi per file e protocolli". Le indagini di analisi per file e protocolli analizzano i flussi di dati per cercare eventi che potrebbero influire sulla sicurezza del CIS "Critical Information System".
- Correlazione e analisi dei log: l'operatore crea un sistema di correlazione e analisi dei log che estrae gli eventi registrati dal sistema di registrazione installato su ciascuno dei CIS "Critical Information System" per rilevare gli eventi che incidono sulla sicurezza del CIS "Critical Information System".

Scenario 3: Attacco ransomware e conseguente interruzione delle attività

Lo scenario potrebbe essere il seguente:

1. Un utente malintenzionato si infiltra nel sistema informatico tramite phishing o rubando le credenziali.
2. Scansionano la rete alla ricerca di vulnerabilità, per sfruttarle e raccogliere informazioni.
3. Scoprono vulnerabilità sui sistemi (ad esempio a causa di una gestione inadeguata delle patch).
4. Distribuiscono un ransomware che crittografa i dati su tutti i sistemi vulnerabili.
5. I sistemi e i dispositivi infetti non possono più essere utilizzati.
6. Chiedono un riscatto in bitcoin in un periodo di tempo limitato in cambio della decrittazione dei dati.
7. Estorcono ulteriormente dipendenti e clienti minacciando di esporre dati personali o riservati.

Gli impatti sono:

- Interruzione dell'attività.
- Perdita di dati e informazioni.
- Perdita di reputazione.
- Perdita finanziaria.

Misure di sicurezza:

- Procedura di mantenimento della sicurezza informatica: l'operatore sviluppa e implementa una procedura per il mantenimento della sicurezza in conformità con il proprio ISSP "Information System Security Policy". A tal fine, la procedura definisce le condizioni che consentono il mantenimento del livello minimo di sicurezza delle risorse CIS "Critical Information System".
- L'operatore segrega i propri sistemi al fine di limitare la propagazione di incidenti di sicurezza informatica all'interno dei propri sistemi o sottosistemi.
- L'operatore filtra i flussi di traffico che circolano nel proprio CIS. L'operatore vieta quindi i flussi di traffico che non sono necessari per il funzionamento dei suoi sistemi e che possono facilitare un attacco.
- Sicurezza delle risorse umane: programma di sensibilizzazione alla sicurezza CIS "Critical Information System" per il personale e un programma di formazione sulla sicurezza per i dipendenti con responsabilità relative al CIS.
- Rilevamento: l'operatore predispone un sistema di rilevazione degli incidenti di sicurezza del tipo "indagine di analisi per file e protocolli". Le indagini di analisi per file e protocolli analizzano i flussi di dati per cercare eventi che potrebbero influire sulla sicurezza del CIS "Critical Information System".
- Correlazione e analisi dei log: l'operatore crea un sistema di correlazione e analisi dei log che estrae gli eventi registrati dal sistema di registrazione installato su ciascuno dei CIS "Critical Information System" per rilevare gli eventi che incidono sulla sicurezza del CIS "Critical Information System".

Scenario 4: Furto dei dati personali dei clienti dal sistema di gestione delle prenotazioni

Lo scenario potrebbe essere il seguente:

1. Gli aggressori identificano e recuperano i dati di autenticazione (credenziali) per ottenere l'accesso a sistemi utili:
   a. o raccogliendo informazioni sui sistemi ferroviari attraverso;
   b. o individuando i sistemi mirati utilizzati per la gestione delle prenotazioni e recuperando l'identità delle persone che li utilizzano;
   c. o una volta identificati i sistemi e i loro operatori/utenti, gli aggressori lanciano attacchi di phishing per recuperare le credenziali di accesso a tali sistemi.
2. L'aggressore ottiene l'accesso diretto, accede al sistema utilizzando le credenziali di amministratore.
3. Ottengono l'accesso non autorizzato ai dati dei clienti e li recuperano.
4. Trapelano i dati o li vendono.

Gli impatti sono:

- Reputazione offuscata.
- Sanzione normativa (GDPR).

Misure di sicurezza:

- Audit di sicurezza: l'operatore definisce le procedure per l'esecuzione di valutazioni di sicurezza del sistema informativo e audit di

risorse critiche e CIS, tenendo conto dell'analisi dei rischi regolarmente aggiornata.
- L'operatore segrega i propri sistemi al fine di limitare la propagazione di incidenti di sicurezza informatica all'interno dei propri sistemi o sottosistemi.
- L'operatore filtra i flussi di traffico che circolano nel proprio CIS. L'operatore vieta quindi i flussi di traffico che non sono necessari per il funzionamento dei suoi sistemi e che possono facilitare un attacco.
- Per l'identificazione, l'operatore imposta account univoci per gli utenti o per i processi automatizzati che devono accedere alle risorse del suo Critical Information System (CIS). Gli account inutilizzati o non più necessari devono essere disattivati. Dovrebbe essere istituito un processo di revisione regolare.
- Tra le regole definite nella sua politica di sicurezza dei sistemi, l'operatore concede i diritti di accesso a un utente o a un processo automatizzato solo quando tale accesso è strettamente necessario all'utente per svolgere la sua missione o al processo automatizzato per svolgere le sue operazioni tecniche.

Scenario 5: Fuga di dati sensibili a causa di un database esposto e non protetto

Lo scenario potrebbe essere il seguente:

1. Un fornitore che fornisce servizi memorizza dati sensibili in un database non protetto, esposto su Internet, senza password e senza crittografare le informazioni.
2. Gli hacker si connettono al database ed esfiltrano le informazioni.
3. Il database contiene informazioni personali, come indirizzi e-mail, data di nascita, nome, motivo del viaggio e organizzazione del viaggio.
4. Gli hacker utilizzano le informazioni per attacchi di estorsione rivolti a dipendenti e clienti.

Gli impatti sono:

- Perdita dei dati degli utenti.
- Sanzione normativa (GDPR).
- Reputazione offuscata.

Misure di sicurezza:

- Audit di sicurezza: l'operatore definisce le procedure per l'esecuzione di valutazioni di sicurezza del sistema informativo e audit di risorse critiche e CIS, tenendo conto dell'analisi dei rischi regolarmente aggiornata.
- L'operatore stabilisce una mappatura del proprio ecosistema, inclusi gli stakeholder interni ed esterni. Questa mappatura può includere i fornitori, in particolare quelli che hanno accesso o gestiscono le risorse critiche dell'operatore.
- L'operatore stabilisce una policy per le sue relazioni con il proprio ecosistema al fine di mitigare i potenziali rischi individuati. Ciò include ma non è limitato alle interfacce condivise tra il CIS e terze parti.

Scenario 6: Attacco DDoS, impedendo ai viaggiatori di acquistare i biglietti

Lo scenario potrebbe essere il seguente:

1. Un utente malintenzionato ha precedentemente infettato un certo numero di computer, creando una botnet (un insieme di dispositivi compromessi controllati da un hacker per eseguire i propri attacchi).
2. La botnet viene utilizzata per lanciare un attacco DDoS alle reti ferroviarie: le reti ed

i server esposti a internet vengono inondati di richieste e tentativi di connessione e quindi spenti, incapaci di sostenere il flusso.

3. Tutti i servizi e le azioni che richiedono i dispositivi esposti a Internet non sono ora disponibili: distributori automatici di biglietti, siti o applicazioni e siti Web commerciali. I passeggeri non possono prenotare i biglietti.

Gli impatti sono:

- Reputazione offuscata.
- Perdita di entrate.
- Interruzione delle attività.
- Onere amministrativo e delle risorse.

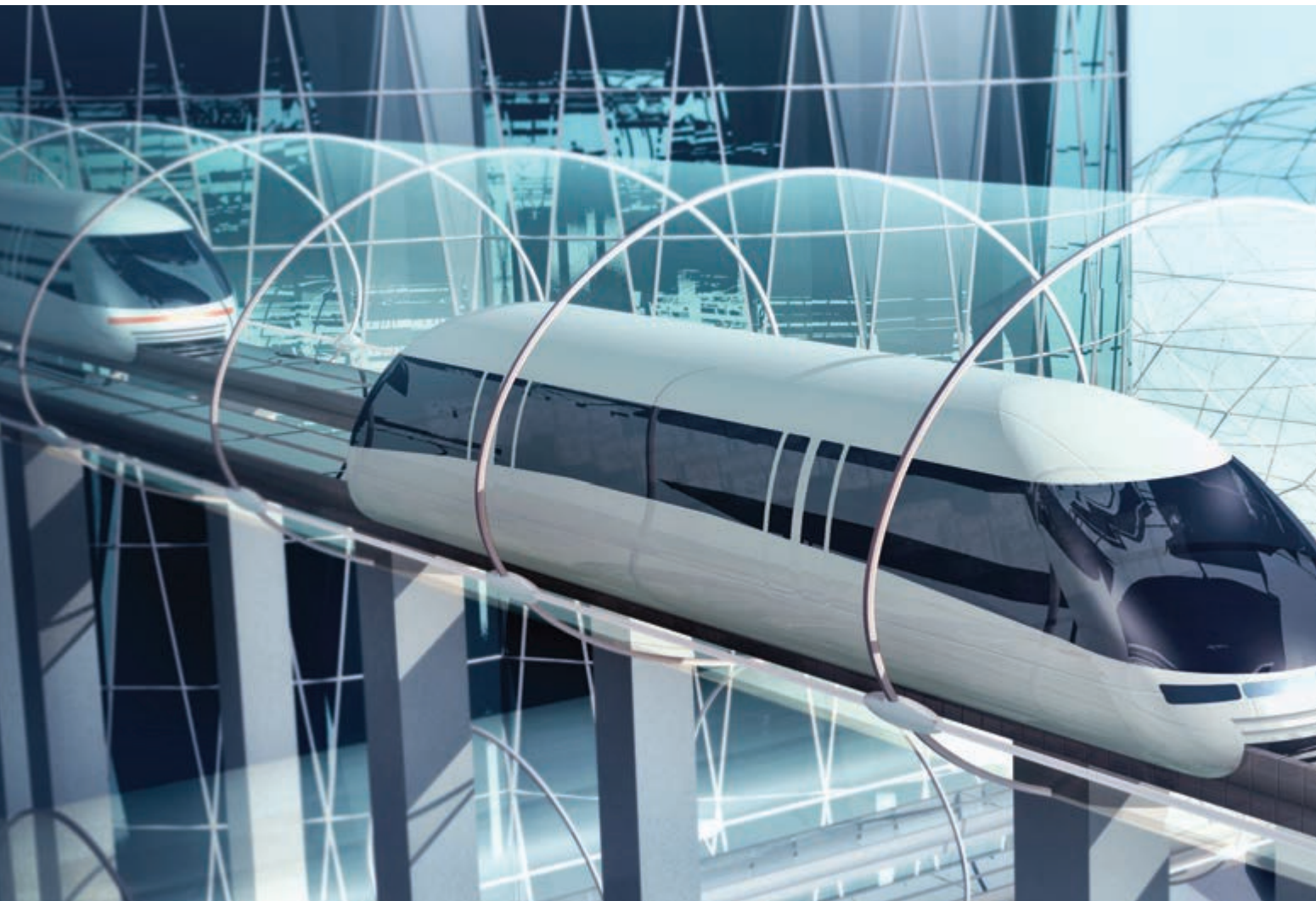
Misure di sicurezza:

- Rilevamento: l'operatore predispone un sistema di rilevazione degli incidenti di sicurezza del tipo "indagine di analisi per file e protocolli". Le indagini di analisi per file e protocolli analizzano i flussi di dati per cercare eventi che potrebbero influire sulla sicurezza del CIS "Critical Information System".
- Correlazione e analisi dei log: l'operatore crea un sistema di correlazione e analisi dei log che estrae gli eventi registrati dal sistema di registrazione installato su ciascuno dei CIS "Critical Information System" per rilevare gli eventi che incidono sulla sicurezza del CIS "Critical Information System".
- In accordo con il proprio ISSP, l'operatore definisce obiettivi e linee guida strategiche in merito alla gestione della continuità operativa, in caso di incidente di sicurezza informatica.
- In accordo con il proprio ISSP, l'operatore definisce obiettivi e linee guida strategiche per la gestione del disaster recovery, in caso di grave incidente di sicurezza informatica.

Scenario 7: Evento disastroso che distrugge il datacenter, causando l'interruzione dei servizi IT

Lo scenario potrebbe essere il seguente:

1. Un evento disastroso colpisce i datacenter e ne distrugge una parte; può trattarsi sia di



una calamità naturale (terremoto, alluvione, tempesta, ecc.) sia di un incendio dovuto a un malfunzionamento fisico.
2. I server ferroviari a supporto dei sistemi informatici vengono fisicamente distrutti.
3. I principali sistemi informatici non sono disponibili, con conseguente interruzione di tutti i servizi supportati dall'IT.
4. I back-up archiviati nei datacenter vengono distrutti anche fisicamente; i dati vengono così persi, prolungando l'interruzione.

Gli impatti sono:

- Perdita di informazioni.
- Interruzione delle attività.
- Perdita di entrate.

Misure di sicurezza:

- In accordo con il proprio ISSP, l'operatore definisce obiettivi e linee guida strategiche in merito alla gestione della continuità operativa, in caso di incidente di sicurezza informatica.
- In accordo con il proprio ISSP, l'operatore definisce obiettivi e linee guida strategiche per la gestione del disaster recovery, in caso di grave incidente di sicurezza informatica.
- Sicurezza fisica e ambientale: l'operatore impedisce l'accesso fisico non autorizzato e il danneggiamento e l'interferenza con le informazioni dell'organizzazione e le strutture di elaborazione delle informazioni.

4 Considerazione sulle misure di sicurezza informativa

Una volta che i rischi sono stati identificati e classificati in ordine di priorità in base ai criteri di valutazione del rischio, dovrebbero essere trattati mediante un piano di trattamento del rischio. In accordo alla normativa ISO 27005 (capitolo 9 "Information security risk treatment"), si possono proporre quattro opzioni per quanto riguarda il trattamento del rischio:

- Modifica del rischio: modificare il livello di rischio introducendo, rimuovendo o alterando i controlli in modo che il rischio residuo possa essere rivalutato come accettabile (vedi norma ISO 27005, 9.2 "Risk modification").
- Conservazione del rischio: accettare il rischio senza ulteriori azioni, se il livello di rischio soddisfa i criteri di accettazione dei rischi (vedi norma ISO 27005, 9.3 "Risk retention").
- Evitare il rischio: evitare l'attività o la condizione che aumenta il rischio particolare "vedi norma ISO 27005, 9.4 "Risk avoidance").
- Condivisione del rischio: condivide il rischio con un'altra parte che può gestire più efficacemente il rischio specifico vedi norma ISO 27005, 9.5 "Risk sharing").

Come descritto nello standard ISO 27005, queste opzioni devono essere selezionate in base all'esito della valutazione del rischio, al costo previsto per l'implementazione di queste opzioni e ai benefici attesi da queste opzioni.

5 Cybersecurity ed il ruolo della certificazione accreditata

Con lo sviluppo della società digitale e dei servizi ICT, il tema della cybersecurity ha assunto un ruolo strategico.
Nello studio dell'Osservatorio Accredia "Cybersecurity e protezione dei dati: il ruolo della certificazione accreditata" si è dimostrato l'importanza delle valutazioni della conformità alle norme tecniche come fattori abilitanti per la cybersecurity, esercitando un ruolo determinante nell'attuale processo di trasformazione digitale della società.
In Europa, la Direttiva sulla sicurezza delle reti e delle informazioni (Direttiva EU 2016/1148) nota

come NIS (Network and Information Security) è stata il primo passo di legislazione sulla cybersecurity a livello UE, con l'obiettivo di migliorare la sicurezza informatica e delle informazioni in tutta l'Unione. Con questa Direttiva si faceva obbligo agli Stati membri di designare Autorità nazionali competenti, Computer Security Incident Response Team (CSIRT) con compiti connessi alla cybersecurity.
Più recente è il Regolamento UE 2019/881, Cybersecurity Act, che costituisce una parte fondamentale della nuova strategia dell'UE per la sicurezza cibernetica, mirando a rafforzare la resilienza dell'Unione agli attacchi informatici e a creare un mercato unico della sicurezza cibernetica in termini di prodotti, servizi e processi ICT.
In Italia, l'architettura nazionale di cybersecurity è stata definita nel DL 82/2021, con l'istituzione del Sistema nazionale di sicurezza cibernetica e l'Agenzia per la Cybersicurezza Nazionale (ACN). All'ACN è attribuita la funzione di Autorità nazionale di certificazione della cybersecurity (National Cybersecurity Certification Authority - NCCA). Successivamente, con il D.Lgs. 123/2022 viene adeguato l'ordinamento nazionale alle disposizioni contenute nel titolo III "Quadro di certificazione della cybersecurity" del Regolamento UE 2019/881.
Infine, la Strategia Nazionale di Cybersicurezza 2022-2026 emanata a maggio 2022 dall'ACN promuove lo sviluppo di un quadro omogeneo e coerente degli standard europei per la cybersecurity. La Strategia individua tre obiettivi da perseguire: protezione, risposta e sviluppo.
È possibile indicare una misura del beneficio con l'utilizzo dei servizi accreditati per la cybersecurity?
Per rispondere a questa domanda, nell'analisi contenute nello studio dell'Osservatorio Accredia "Cybersecurity e protezione dei dati: il ruolo della certificazione accreditata" sono state adottate due metodologie complementari:

- la prima metodologia si è basata sull'analisi di casi di studio selezionati che ha condotto alla definizione di una serie di indicazioni qualitative legate al beneficio derivante dall'ottenimento e mantenimento di una certificazione accreditata per la norma UNI CEI EN ISO/IEC 27001.
- la seconda metodologia si è basata su attività di analisi delle vulnerabilità dei servizi web esposti da un vasto campione di organizzazioni, con la messa in relazione degli esiti di tale analisi rispetto al possesso (o meno) di una certificazione accreditata per la UNI CEI EN ISO/IEC 27001. Questa seconda metodologia di analisi ha consentito di ottenere indicatori di carattere quantitativo circa il livello di esposizione al rischio delle aziende certificate.

Tutte le esperienze raccolte con i casi di studio hanno permesso di capire come solo con il tempo le organizzazioni certificate riescano a comprendere quanto il percorso seguito abbia cambiato profondamente la loro organizzazione, con un miglioramento tangibile in molti contesti, non necessariamente limitati alla migliore gestione del rischio cibernetico.
Per la seconda metodologia di analisi dei potenziali benefici derivanti dall'utilizzo dei servizi accreditati si è approfondito uno studio tecnico su due tipi di organizzazioni: una dotata di certificazione per la sicurezza UNI CEI EN ISO/IEC 27001 e una dotata di certificazione per la qualità UNI EN ISO 9001:2015. Le attività di analisi quantitativa hanno confermato un migliore livello di sicurezza delle organizzazioni con una certificazione accreditata per la UNI CEI EN ISO/IEC 27001.
Quali sono le prospettive future sul contributo dei servizi accreditati per la cybersecurity?
I servizi accreditati di cybersecurity hanno un ruolo centrale nel costruire relazioni di "fiducia" tra produttori e consumatori di prodotti e servizi digitali. Tale ruolo è destinato a crescere alla luce delle iniziative nazionali e comunitarie tese a rafforzare le difese e la resilienza dei servizi digitali.
Va osservato che gli attuali schemi di certificazione non sempre soddisfino le esigenze di mercato. L'implementazione di schemi di certificazione capaci di offrire un livello di sicurezza adeguato a contesti operativi caratterizzati da un livello di rischio non elevato, senza incorrere in tempi e costi gravosi, consentirebbe di aumentare l'interesse.
Infine, è importante considerare anche la certificazione delle competenze professionali in materia di cybersecurity, aspetto già al centro della produzione normativa europea e nazionale. L'attenzione nasce dall'esigenza di personale qualificato su competenze specialistiche e in continua evoluzione. In questo contesto sono state intraprese diverse iniziative come i programmi CyberChallenge.it, OlyCyber.it e CyberTrials promossi, nel contesto italiano, dal Cybersecurity National Lab del CINI.

6 Conclusioni

Nel presente articolo si è cercato di raccogliere buone pratiche, approcci e standard per eseguire la gestione del rischio informatico nel settore ferroviario, riportando esempi di materiale di riferimento, scenari di minacce e misure di mitigazione del rischio informatico.
La differenziazione tra IT e OT nel settore ferroviario è sempre più difficile. In molti casi è complesso identificare quale approccio è più adatto, se un dispositivo può essere conside-

rato IT o OT o quali misure di sicurezza e quale standard dovrebbero essere applicati. Occorre un approccio strutturato e unificato rispetto alla gestione del rischio informatico per aiutare ad armonizzare il settore, facilitando così le discussioni sui rischi tra le diverse entità dell'ecosistema ferroviario. In definita, il focus è:

- Maggiore armonizzazione e allineamento delle buone pratiche.
- Mantenere aggiornati i sistemi ferroviari e le valutazioni del rischio informatico.

Bibliografia

- Railway cybersecurity. Good practices in cyber risk management – ENISA, November 2021
- https://www.rfi.it/it/Sicurezza-e-tecnologie/tecnologie/ccs.html#:~:text=I%20sistemi%20ferroviari%20che%20permettono,e%20controllano%20il%20segnalamento%20ferroviario.
- https://wikirail.it/glossario/automatic-train-control/
- X2Rail-3 Deliverable D8.1 Guidelines for railway cybersecurity
- ISO 27005, annex E, E.2 Detailed information security risk assessment
- ISO 27005, annex E, E.2 Detailed information security risk assessment
- https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view
- ISO/IEC 27005 "Information security risk management"
- Cybersecurity e protezione dei dati: il ruolo della certificazione accreditata - Osservatorio Accredia – 2022
- https://www.accredia.it/comunicazione/osservatorio-accredia/

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI ROMA
Piazza della Repubblica, 59 - 00185 - Roma

Tel. 06.487.93.11 - Fax: 06.487.931.223
Cod. Fisc. 80201950583
Orari di apertura al pubblico degli uffici

Lunedì	09:30-12:30	14:30-17.30
Martedì	09:30-12:30	14:30-17.30
Mercoledì	09:30-12:30	14:30-17.30
Giovedì	09:30-12:30	14:30-17.30
Venerdì	09:30-12:30	
Sabato	09:30-12:30	

La Segreteria dell'ordine chiude alle 16.00

AREE DEL SITO WEB DEL QUADERNO

AREA CIVILE AMBIENTALE
https://rivista.ording.roma.it/civile/

AREA INDUSTRIALE
https://rivista.ording.roma.it/industriale/

AREA DELL'INFORMAZIONE
https://rivista.ording.roma.it/informazione/

AREA INTERSETTORIALE
https://rivista.ording.roma.it/intersettoriale/

È possibile consultare tutti i numeri
all'indirizzo Internet
ioroma.info

Ordine degli Ingegneri della Provincia di Roma
Piazza della Repubblica, 59 - 00185 Roma
www.ording.roma.it

Quaderno dell'Ordine degli Ingegneri della Provincia di Roma
N 2/2023 Trimestrale Anno X