Tecnologie emergenti per la sicurezza della circolazione ferroviaria e relative vulnerabilità informatiche

Christian Lusi

29 giugno 2021

Argomenti

- Principi di sicurezza della circolazione
- Ricadute tecnologiche
- Nuovi requisiti di sicurezza
- Tecnologie emergenti per garantire il rispetto dei nuovi requisiti
- Relative vulnerabilità informatiche

Principi di sicurezza della circolazione

Fissati dal **Regolamento per la Circolazione Ferroviaria** (decreto ANSF n. 4/2012)

- Vincoli di sicurezza da rispettare
- Funzioni tecnologiche per garantire automaticamente il rispetto dei vincoli
- Operatività del personale di sicurezza (macchinista, capotreno, capostazione, manutentore, ecc.)

Vincoli di sicurezza

Derivanti da:

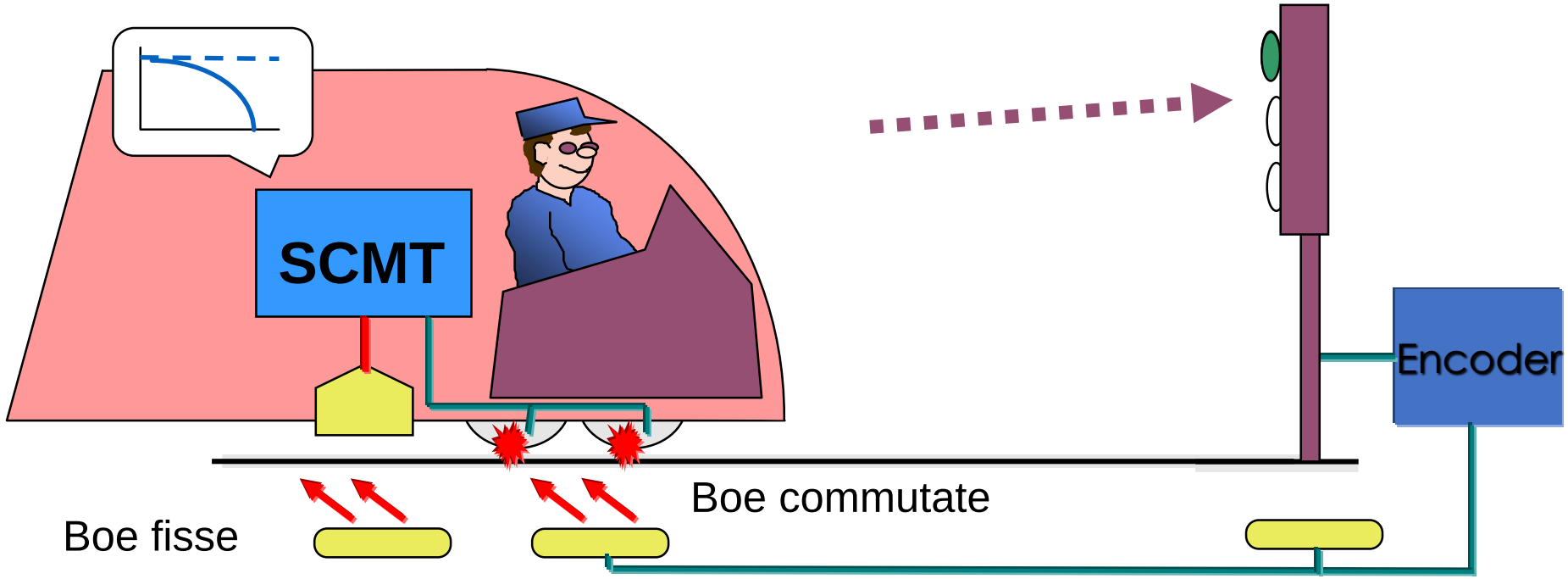
- **Caratteristiche infrastruttura, convogli e loro interazione** (velocità massima della linea, velocità massima del convoglio, peso assiale, ecc.)
- **Stato enti incontrati dal convoglio** (deviatoi, PL, circuiti occupazione, ecc.)
- **Contemporanea circolazione di più convogli** (garantire per ogni convoglio un tratto libero protetto da accesso di altri veicoli, garantire una velocità massima per rispettare spazi arresto)

Tecnologie consolidate per garantire rispetto vincoli sicurezza

- **Sistemi di protezione della marcia** (neutralizzano errori del macchinista)
- **Impianti IS** (neutralizzano errori capostazione)
- **Apparati di blocco automatico** (neutralizzano errori capostazione)

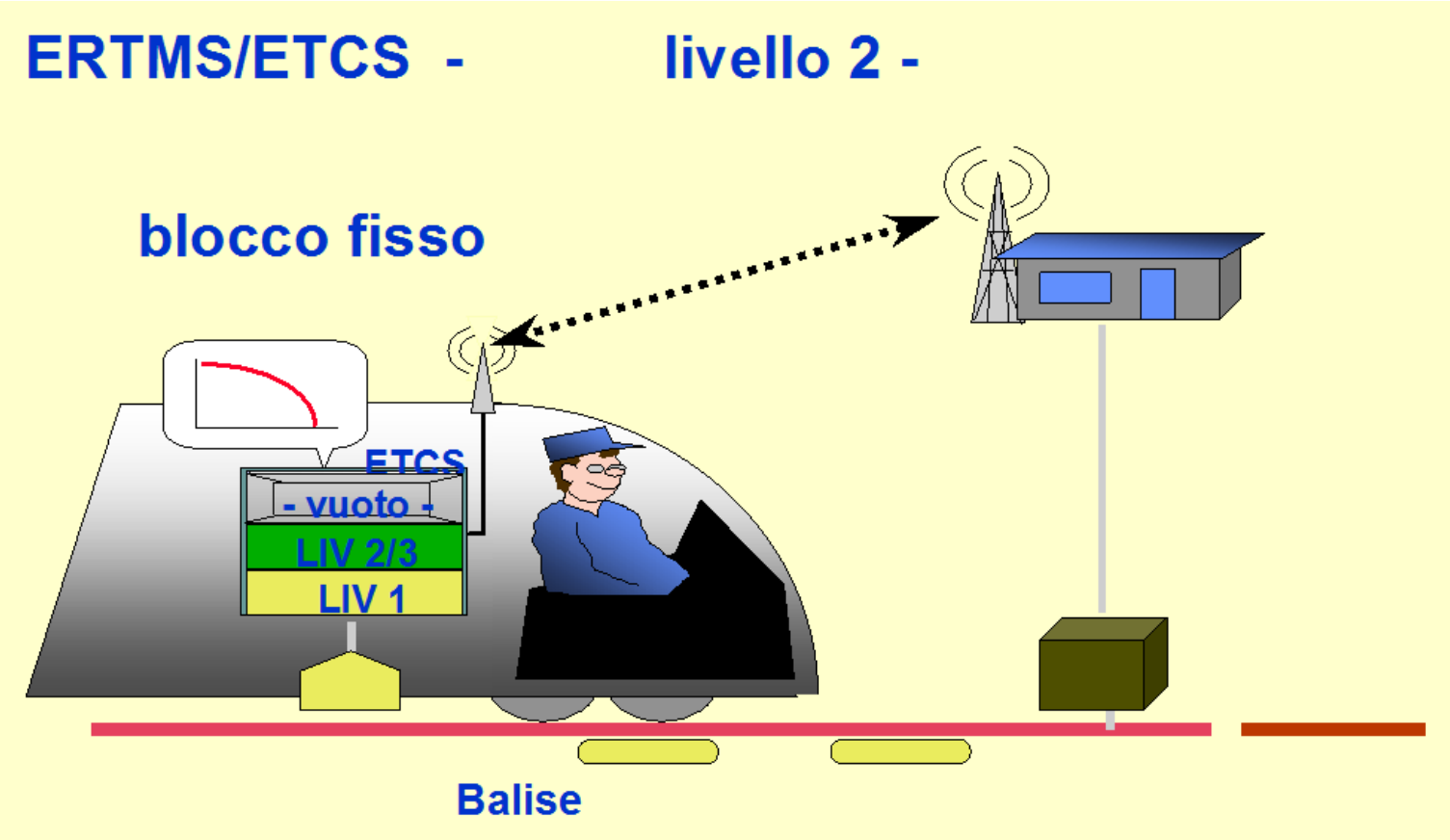
Tecnologie per garantire rispetto vincoli sicurezza

- Sistemi di protezione della marcia (neutralizzano errori del macchinista)
- SCMT



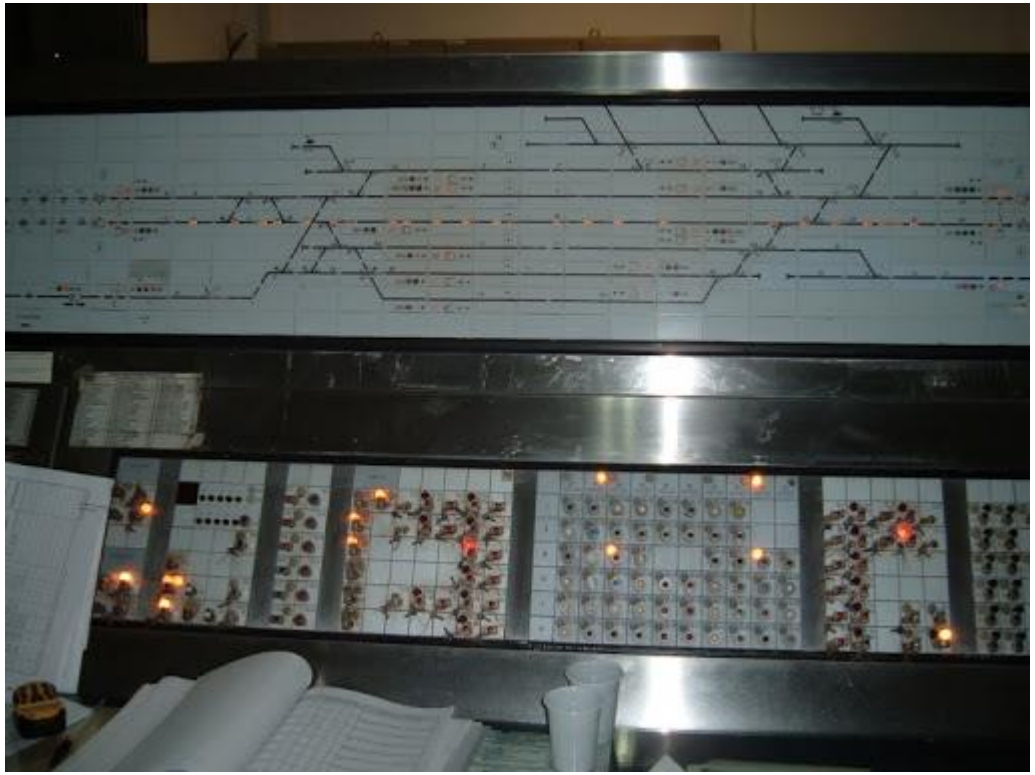
Tecnologie per garantire rispetto vincoli sicurezza

Sistemi di protezione della marcia (neutralizzano errori del macchinista)



Tecnologie per garantire rispetto vincoli sicurezza

Impianti IS (neutralizzano errori capostazione)

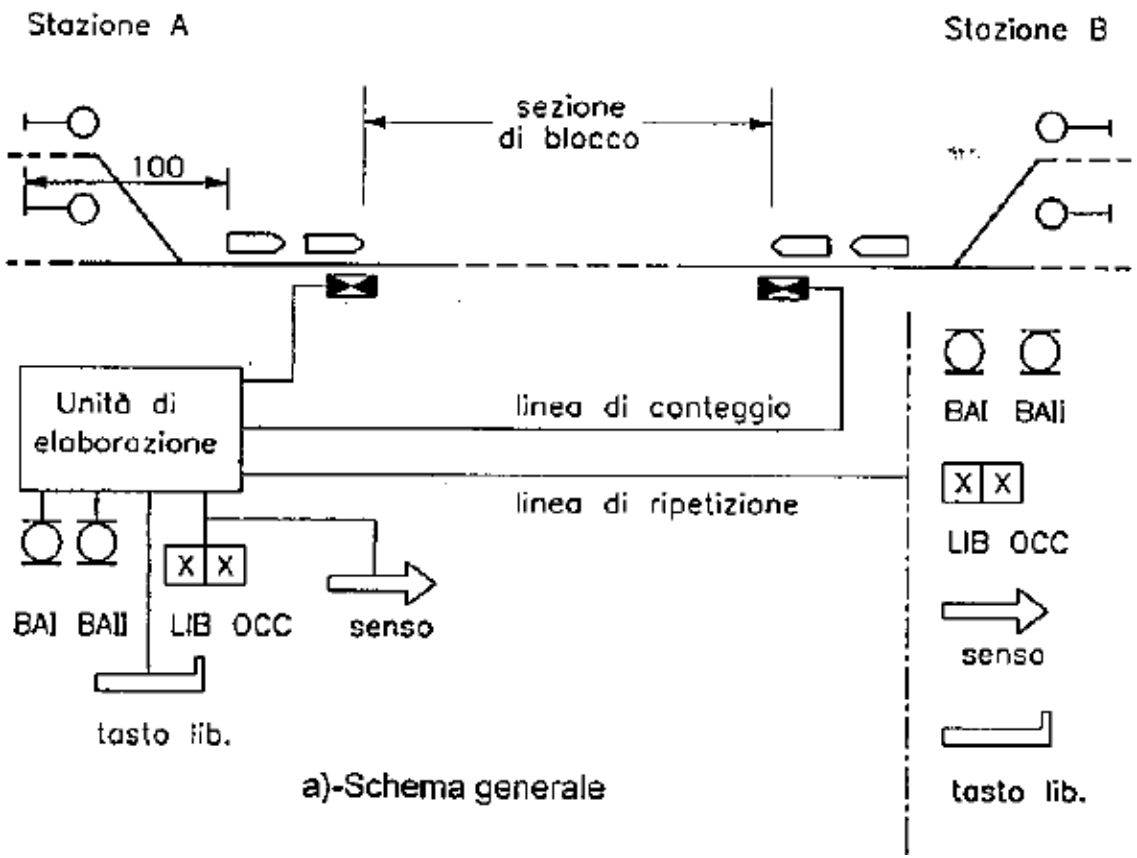


(ACEI Rosarno)

(ACC Padova)

Tecnologie per garantire rispetto vincoli sicurezza

Apparati di blocco automatico (neutralizzano errori capostazione)



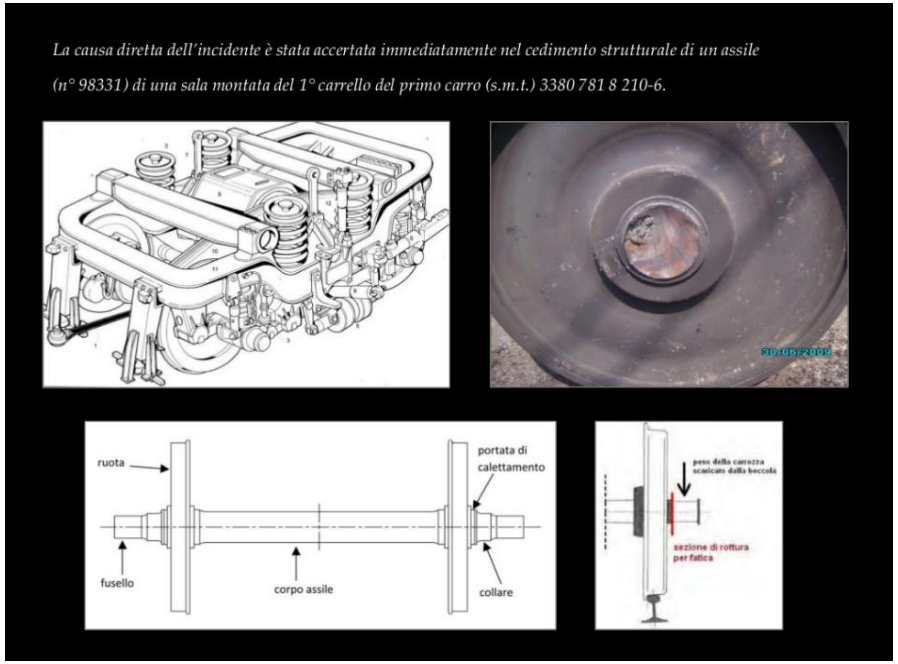
a)-Schema generale

(Blocco Conta-Assi)

Nuovi requisiti tecnologici (revisione RCF di prossima emanazione)

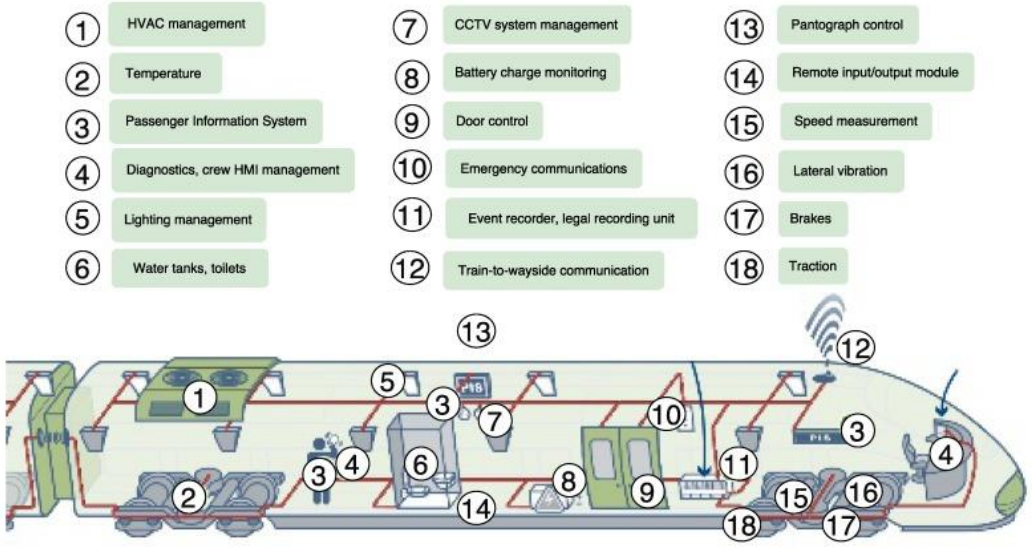
Necessari sistemi automatici per:

- monitorare automaticamente infrastruttura e veicoli in modo continuo nello spazio e nel tempo
- rilevarne le anormalità
- imporre le restrizioni di esercizio necessarie



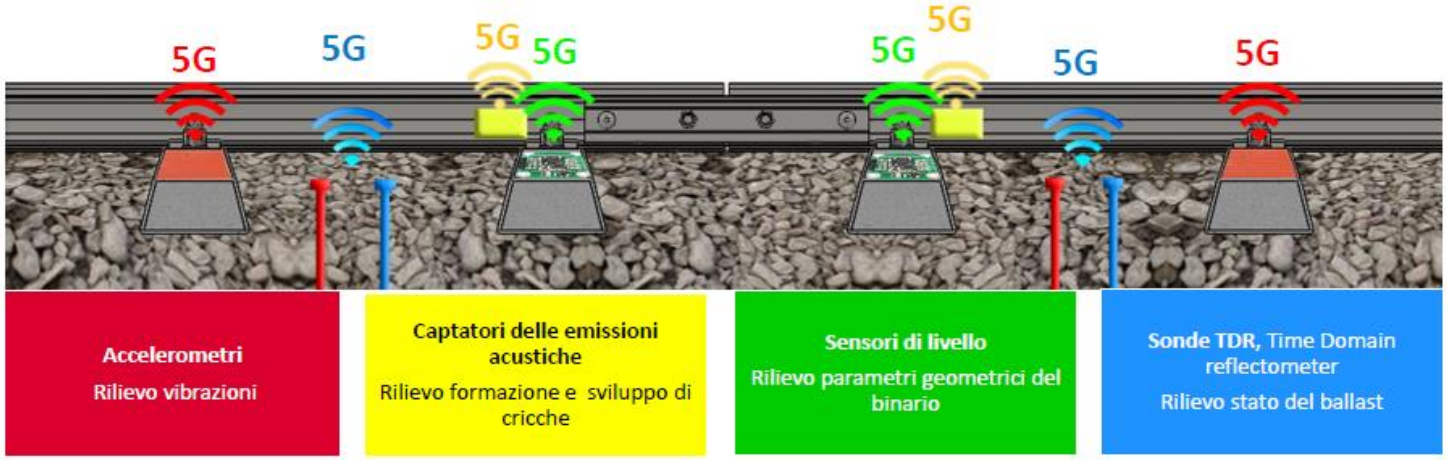
Tecnologie emergenti

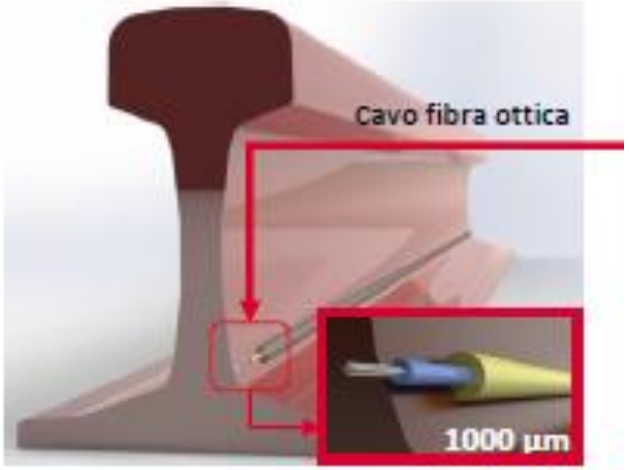
- Sensori **IoT** capillarmente diffusi su infrastruttura e veicoli
- Copertura radio **5G** per invio dati a centri di elaborazione



Supervisione della sede ferroviaria e del binario

- **Monitoraggio continuo** degli elementi base dell'infrastruttura attraverso nodi sensoriali
- **Analisi predittiva** dell'evoluzione nel tempo
- Sensori multipli intelligenti e auto-alimentati
- I dati raccolti vengono **trasmessi in tempo reale** ad un punto di raccolta per la formazione di un database con cui operare attività di diagnostica in remoto.

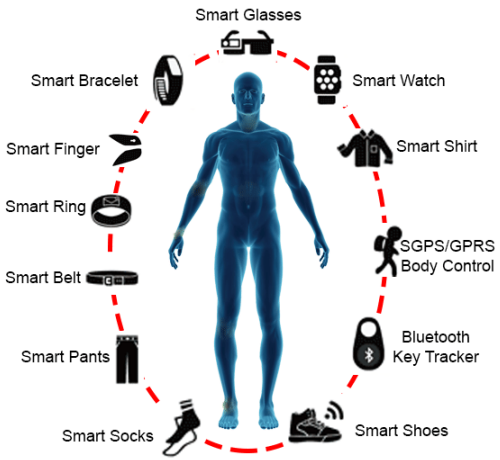




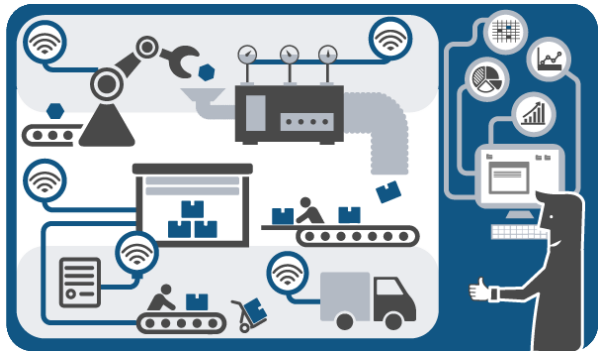
Internet of Things

Interconnessione di oggetti all'infrastruttura internet attraverso dispositivi informatici incorporati

Dispositivi indossabili



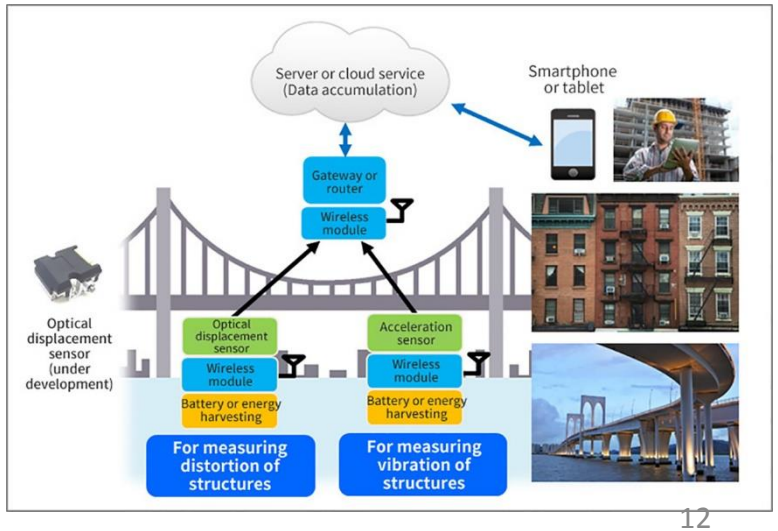
Applicazioni aziendali



Case intelligenti

Città intelligenti

Sensori ambientali



IoT: un po’ di storia

1982 - Carnegie Mellon University
Alcuni studenti del Computer Science Department installano un fotosensore su un distributore di coca cola e lo collegano a Internet. Ciò permetteva a chiunque avesse accesso a internet di sapere quante lattine erano state erogate e quante ne rimanevano.

1999 – Massachussets Institute of Technology
K. Ashton conia il termine «**Internet of things**» e teorizza la connessione di Internet al mondo fisico mediante un sistema di sensori:

«Se avessimo computer in grado di conoscere tutto ciò che c’è da sapere sulle cose, utilizzando dati raccolti senza alcun aiuto da parte nostra, saremmo in grado di monitorare e di ridurre notevolmente sprechi, perdite e costi. Potremmo sapere quando le cose devono essere sostituite, riparate o richiamate, e se sono fresche o hanno superato il loro momento migliore»

1990 – conferenza INTEROP
J. Romkey e S. Hackett presentano un tostapane Sunbeam Deluxe collegato a Internet. Il tostapane era connesso tramite TCP/IP e disponeva di un controller la cui unica funzione era di accendere o spegnere l’alimentazione.

IoT: un po’ di numeri

- 50 miliardi di dispositivi e oggetti collegati a internet entro la fine del 2020
- Oltre un miliardo di dispositivi domestici *Smart* in USA entro il 2023
- 725 dollari a famiglia spesi in dispositivi smart in USA entro il 2023, per un totale di 90 miliardi di dollari
- 6 milioni di sistemi robotici industriali basati su IoT installati entro il 2023
- 450 miliardi di dollari spesi annualmente a livello mondiale nei prossimi anni per sviluppo e produzione di soluzioni IoT

IoT: un po’ di problemi

- Entro il 2024 il numero di dispositivi connessi supererà di 4 volte quello della popolazione mondiale.
- nuova superficie di attacco DDoS generato dalla crescita incontrollata dei dispositivi IoT non tutti conformi agli standard minimi di sicurezza
- i dispositivi IoT sono potenzialmente capaci di lanciare attacchi DDoS di elevato grado di complessità, inclusi quelli a livello di applicazione
- ottenendo l’accesso a un dispositivo IoT, un cyber criminale può ricattare e spiare il suo proprietario allo scopo di estorcere denaro

Ricerca Kaspersky Lab del 2017

Su 8 dispositivi IoT selezionati casualmente:

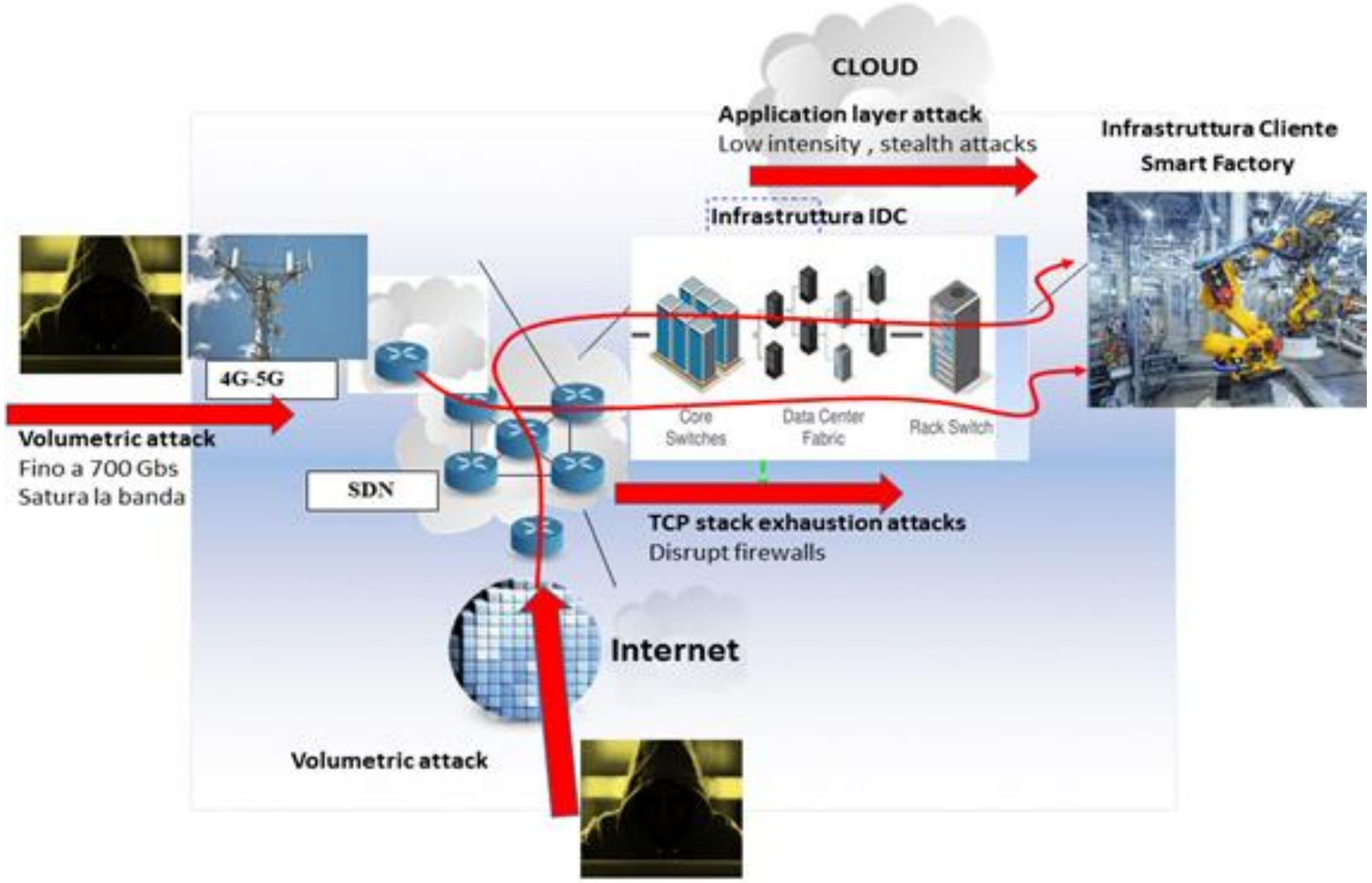
- caricatore smart
- macchinina giocattolo controllata via app
- bilancia smart utilizzabile via app
- aspirapolvere smart
- ferro da stiro smart
- telecamera IP
- smartwatch
- centralina di un sistema di smart home

→ metà dei dispositivi hackerabile a causa di password deboli:

- password di default che non poteva essere cambiata
- medesima password per tutti i dispositivi della stessa linea di prodotto

→ solo un dispositivo soddisfaceva requisiti di sicurezza adeguati

IoT: un po' di problemi



attacchi DDoS "<u>multi vector"</u> a vari livelli che interessano tutte le componenti architetturali

Interruzione del servizio: attacchi DoS

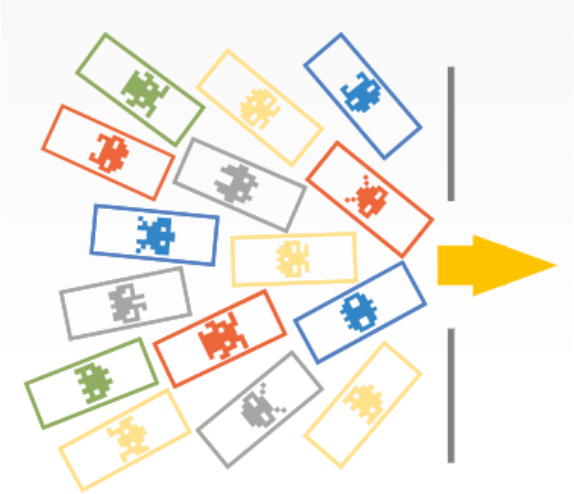
- Un attacco di negazione del servizio o un attacco DoS è un tentativo di compromettere la disponibilità, la terza delle tre proprietà fondamentali da conservare in ambito della sicurezza dei computer (Riservatezza, Integrità, Disponibilità).

- Denial of service significa proprio ciò che implica il nome: ad un utente è negato l'accesso autorizzato a servizi o dati.

- La negazione del servizio spazia dalla completa perdita di accesso a un rallentamento evidente e inaccettabile.

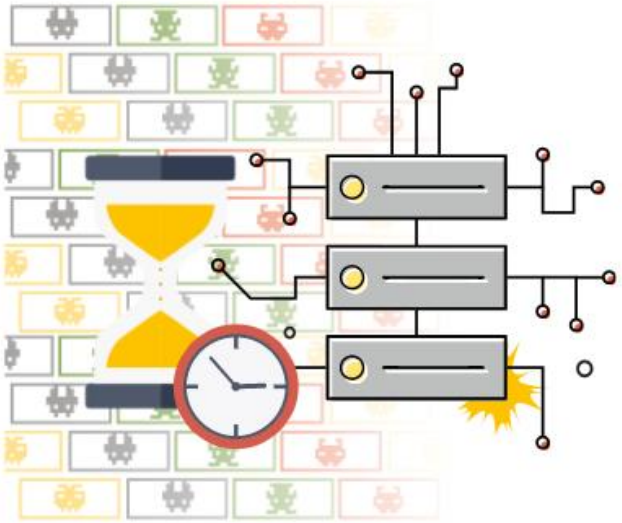
- DoS può verificarsi a causa di un volume eccessivo, di un'applicazione andata in errore, di un collegamento interrotto o di un guasto hardware o software.

Attacchi DoS: Tipologie



ATTACCO VOLUMETRICO

- saturazione dell'accesso ad internet veicolando enormi quantità di traffico che l'infrastruttura fisica non è in grado di gestire.
- attacchi di gran lunga più frequenti



ATTACCO APPLICATIVO

- saturazione delle risorse dei Server (CPU, RAM) senza necessariamente saturare la banda del link di accesso
- Si realizzano attraverso richieste di operazioni artificiosamente complesse che impiegano molto tempo per essere svolte e che rallentano o bloccano totalmente il normale flusso delle attività.

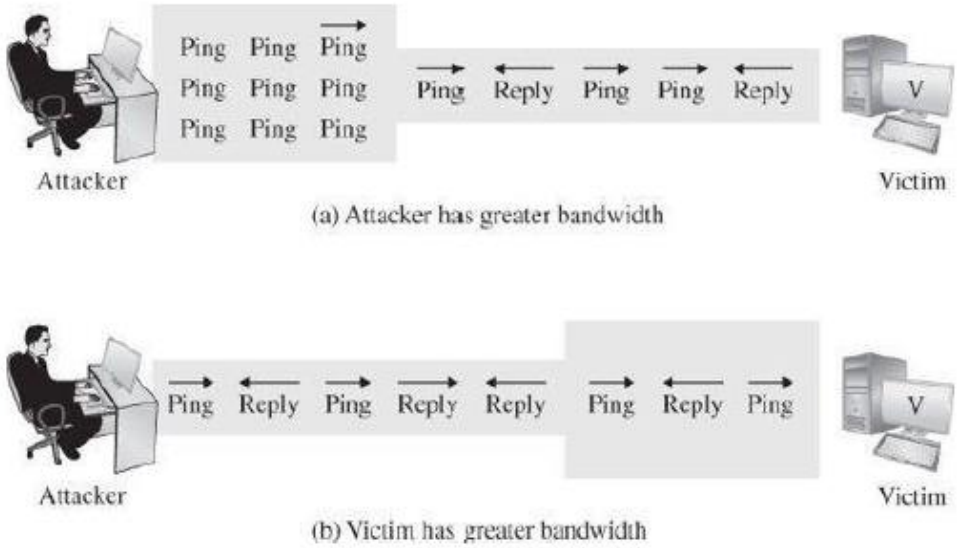
La distinzione tra attacchi Volumetrici e Applicativi risulta negli ultimi anni sempre meno netta, in quanto nella stessa campagna possono essere utilizzate entrambe le tecniche: in questo caso si parla di **strategia Multi-Vector**

Attacchi DoS: esempio di attacco volumetrico

Ping of Death

- Un **ping della morte** è un attacco semplice che usa il comando ping che è comunemente usato per testare il tempo di risposta da un host.
- Dal momento che ping richiede al destinatario di rispondere al pacchetto, tutto ciò che gli attaccanti devono fare è inviare un diluvio di ping alla vittima prevista.
- L'attacco è limitato dalla larghezza di banda più piccola sul percorso di attacco, come mostrato in figura
- Se l'attaccante è in una connessione di 10 megabyte (MB) e il percorso verso la vittima è di 100 MB o più, matematicamente l'attaccante da solo non può inondare la vittima. Ma l'attacco riesce se i numeri sono invertiti:

  l'attaccante su una connessione da 100 MB può certamente inondare una vittima da 10 MB. I pacchetti ping satureranno la larghezza di banda della vittima.



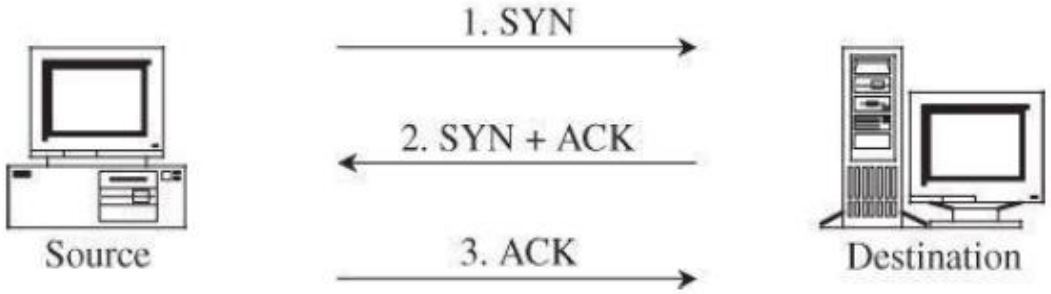
(a) Attacker has greater bandwidth

(b) Victim has greater bandwidth

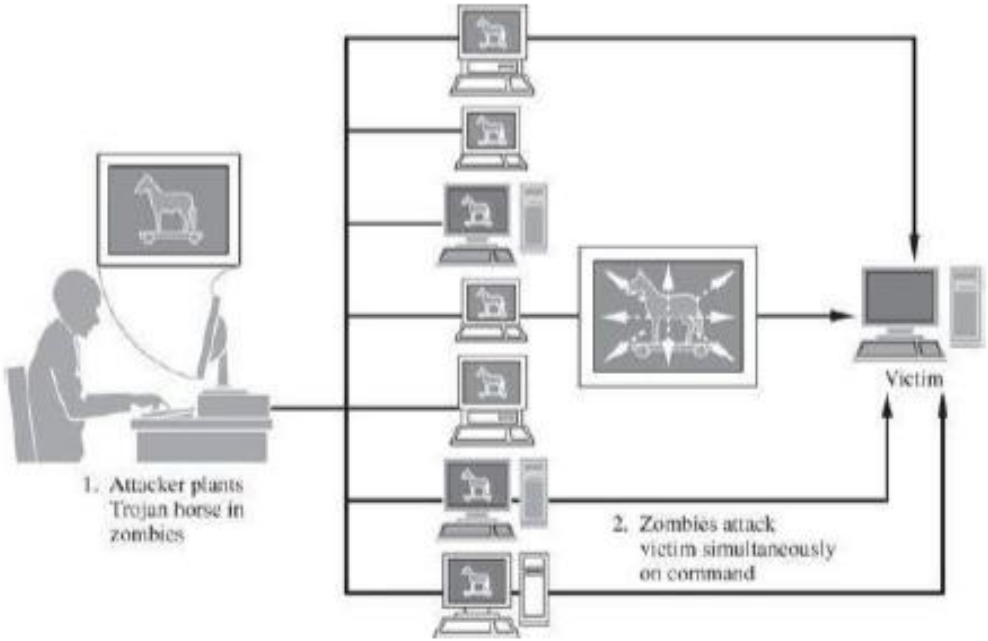
Attacchi DoS: esempio di attacco applicativo

«SYN Flooding» o «a saturazione di stack»

- Viene stabilita una sessione con un handshake TCP a tre fasi.
- In primo luogo, per avviare una connessione TCP, l'originatore invia un pacchetto con il bit SYN attivato. In secondo luogo, se il destinatario è pronto a stabilire una connessione, risponde con un pacchetto con entrambi i bit SYN e ACK. Infine, la prima parte completa lo scambio per dimostrare che il canale di comunicazione è efficiente inviando un pacchetto con il bit ACK
- Il destinatario mantiene una coda denominata “connessioni SYN_RECV”, tracciando quelle voci per cui è stato inviato un SYN-ACK ma non è stato ancora ricevuto alcun ACK corrispondente
- L'attaccante può negare il servizio al destinatario inviando molte richieste SYN, a cui il destinatario risponde correttamente con SYN-ACK; tuttavia l'attaccante non risponde mai con gli ACK per completare le connessioni, riempiendo così la coda SYN_RECV della vittima. Tipicamente, la coda SYN_RECV è abbastanza piccola, contenente 10 o 20 voci. A causa dei ritardi di routing potenziali su Internet, i tempi di attesa tipici per la coda SYN_RECV possono essere minuti. Quindi l'attaccante deve solo inviare una nuova richiesta SYN ogni pochi secondi e la coda verrà riempita.



Attacchi DoS: noleggiare una botnet



- per fare un po' di soldi, i botmaster a volte affittano le loro botnet ad altri. Il ricercatore Dancho Danchev ha riferito che, nel 2013, una botnet di 1000 host è stata affittata per $ 25 - $ 120 US, mentre una da 10.000 host per $ 200 - $ 500 US per 24 ore.
- *"Hai una causa preferita? Vuoi protestare contro …., ma temi che la tua voce solitaria non si sentirà? Partecipa con un gruppo di persone con mentalità simile a lanciare un attacco di denial-of-service distribuito contro l'oltraggio"*
  Sì, ora ci sono post di questo tipo per gruppi di persone affini che si uniscono in protesta. È possibile scaricare e installare uno script di attacco e presentarsi ad esempio un martedì alle 11:00 (GMT) per protestare facendo attaccare il tuo computer contro un certo sito

Attacchi DDoS da botnet di telecamere

- Le **IP-camera** sono tra i dispositivi IoT attualmente più diffusi
- Ottobre 2015: sferrato da una botnet di IP-camera un attacco DDoS con una potenza di fuoco di picco di **20 mila richieste al secondo**
- **900** telecamere coinvolte sparse in tutto il mondo e tutte tranquillamente accessibili da remoto tramite le **credenziali di accesso impostate all'uscita di fabbrica** del dispositivo
- Attacco basato su **flooding**
- Attaccato grande provider di servizi cloud con milioni di utenti in tutto il mondo

Conseguenze di un attacco DoS

- **Calo diretto di ricavi e profitti** dovuto al tempo di inattività.
- **Perdita dei Clienti** per indisponibilità dei servizi, con probabile migrazione del potenziale utente e della customer base verso altro fornitore.
- **Danni all'immagine o al brand** per notizie relative ad interruzione di servizio o violazioni della sicurezza e conseguenti impatti sul livello di competition nel mercato.
- **Possibili sanzioni** legate alla non compliance alle normative che prevedono la disponibilità della raggiungibilità dei dati (Availability).
- **Diminuzione della Produttività**. Quando i servizi online non funzionano, la produttività dei dipendenti e delle aziende che si affidano a tali servizi diminuisce notevolmente.
- **Penali.** Il mancato soddisfacimento di determinati requisiti di disponibilità potrebbe implicare il pagamento di penali verso Clienti e Fornitori.
- **Costi di ripristino del servizio**. La gestione non strutturata di attacchi di tipo DDoS comporta l'utilizzo di personale ed infrastrutture in emergenza con evidente dispendio di risorse ed un allungamento dei tempi necessari per le attività di ripristino.

Attacchi DoS: contromisure generali

- Gli attacchi DDoS non sono difficili da prevenire, almeno in teoria. La maggior parte dei bot sono reclutati utilizzando vulnerabilità ben note, per le quali le patch sono state distribuite per un certo tempo. Quindi, se l'intero mondo installasse le patch in modo tempestivo, la minaccia DDoS diminuirebbe.
- Alcuni utenti di computer, tuttavia, non dispongono di copie legali dei loro sistemi operativi e di altri software, pertanto non possono sottoscrivere e ottenere patch attraverso le vie normali dei produttori software.
- Gli amministratori possono affrontare gli attacchi ordinari di DoS mediante tecniche come
  - ❑ il tuning (regolazione del numero di server attivi),
  - ❑ il bilanciamento del carico (distribuendo in modo equo il carico di calcolo sui server disponibili),
  - ❑ lo shunning (riduzione del servizio fornito al traffico da determinati intervalli di indirizzi)
  - ❑ le blacklist (rifiutare le connessioni da determinati indirizzi).

Attacchi DoS: contromisure in ambito IoT

- il vero problema è la **componente legacy dei dispostivi IOT** già in campo o in produzione per la quale i meccanismi implementati di sicurezza sono di basso livello e spesso non è possibile effettuare aggiornamenti firmware dei prodotti.
- il **codice di condotta del governo britannico** (*Government's Code of Practice for Consumer Internet of Things (IoT) Security for manufacturers, with guidance for consumers on smart devices at home***)** suggerisce un approccio basato sui seguenti punti:
  - Nessuna password predefinita;
  - Attuare una politica di divulgazione delle vulnerabilità;
  - Mantieni aggiornato il software;
  - Archiviazione sicura di credenziali e dati sensibili alla sicurezza;
  - Garantire l'integrità del software;
  - Garantire che i dati personali siano protetti;
  - Rendere i sistemi resistenti alle interruzioni;
  - Rendere facile per i consumatori eliminare i dati personali;
  - Convalidare dati di input.
- Tali regole si devono calare negli standard, e nelle linee guida pubblicate da organizzazioni come l'Industrial Internet Consortium (IIC), Cloud Security Alliance (CSA), il National Institute of Standards and Technology (NIST), e l'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA)

5G: caratteristiche principali

- Frequenze rete accesso radio: 700 MHz, 3600-3800 MHz, 26 GHz
- Velocità di picco: 20 Gb/s (LTE attuale circa 100 Mbs)
- Consumo energetico: basso consumo energetico sia a livello di rete d'accesso sia di trasporto
- Tempo di latenza: da 30 a 50 volte inferiore al 4G
- Densità: fino a un milione di oggetti collegati alla rete per km^2 (100 volte di più che il 4G) senza impattare sulla velocità di connessione
- Posizionamento ad alta precisione: vantaggio del posizionamento su base cellulare è che funziona bene sia in ambienti indoor che outdoor. Risoluzione inferiore ad 1 m.

comandare a distanza e in tempo reale veicoli a guida autonoma, strumenti chirurgici, apparati di gestione traffico stradale, navale, aereo

monitorare in tempo reale lo stato delle infrastrutture e dei veicoli (IoT)

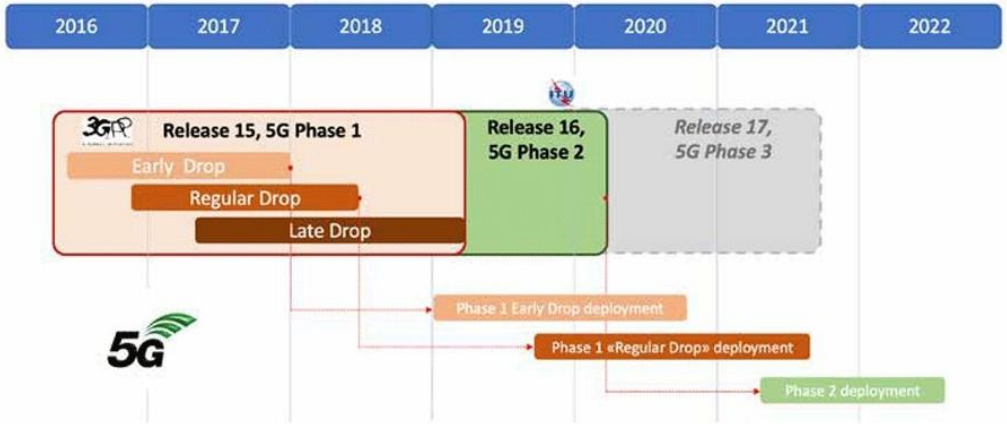
5G: specificazione e diffusione

Release 16: rilasciata a luglio 2020

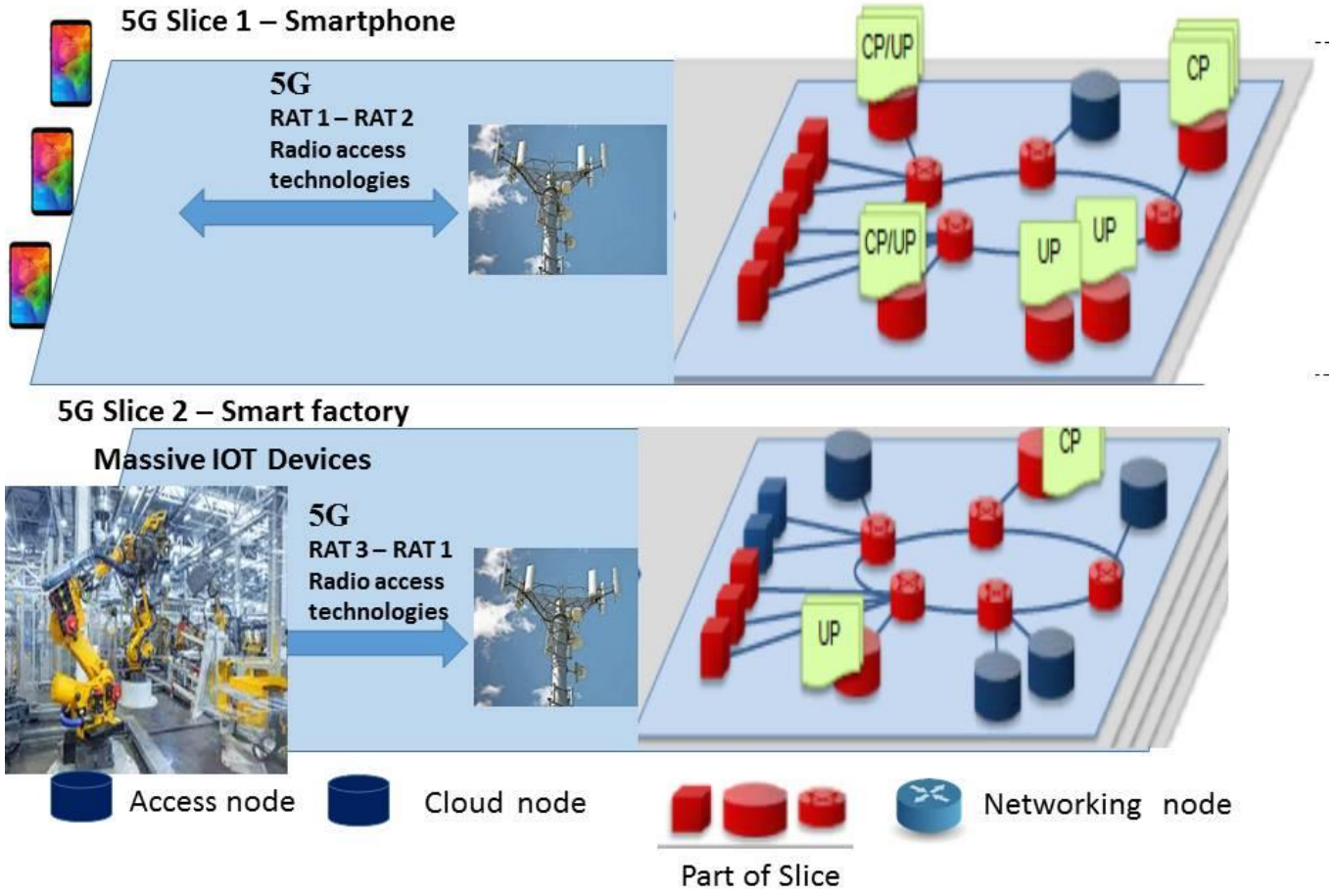
Release 17: da rilasciare entro 2022

Entro 2024:

- Raggiunto 40% popolazione mondiale
- 1,5 miliardi di abbonamenti



5G: network slicing e vulnerabilità



- realizza reti virtuali con caratteristiche diverse che condividono la medesima infrastruttura fisica di accesso e trasporto
- ogni particolare tipo di applicazione (trasporti, sanità, pubblica sicurezza, ecc.) vede una rete configurata nella maniera ottimale per gestire il suo traffico
- Aumento consistente dei nodi di rete

↓

- **superficie d'attacco aumentata** per effettuare attacchi DDOS ed introdurre malware nelle piattaforme del cliente
- possibilità di avere **molte più backdoor** di accesso da parte di chi ha configurato il sistema, attraverso cui trafugare i dati trasportati

5G: network slicing da problema a opportunità

- 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

- isolare i dispositivi più vulnerabili (come gli IoT) su una porzione separata per garantire che questi non interferiscano con altri utenti in caso di attacco

- implementare le funzioni sensibili alla sicurezza, come la crittografia utente, in una posizione centrale sicura, mantenendo le funzioni non critiche per la sicurezza in posizioni distribuite meno sicure

Grazie dell’attenzione!

Christian Lusi

christian_lusi@hotmail.com

christian.lusi@ansfisa.gov.it