E SE PARLASSIMO DI CYBER-SAFETY ?

Ing. Giorgio Pizzi

Ordine Ingegneri Napoli – Comitato italiano ingegneria dell'informazione
CONVEGNO 29 GIUGNO 2021, LA CYBER SECURITY NEL SETTORE FERROVIARIO
"Stato dell'arte e prospettive future"

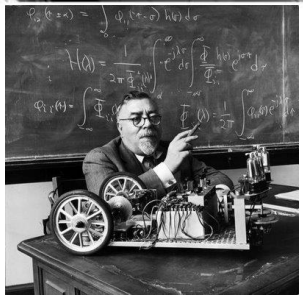
Sommario

- Non c’è nulla di “cyber” nell’IT-security
- Vulnerabilità dei sistemi embedded
- Esempi di sistemi cyber-fisici nei trasporti
- Lo studio di un caso ferroviario

Gli attacchi al settore dei trasporti

- La maggior parte dei report riguardanti minacce, vulnerabilità ed attacchi nel settore dei trasporti riguardano **l'information technology.**
- Ransomware, esposizione o furto di dati degli utenti, DoS nei sistemi di business o nei servizi ai passeggeri.
- Si tratta di attacchi **a-specifici** che di fatto riguardano tutti i settori.
- Ma quali sono le specificità?

Cosa significa «cyber»?



- Cibernetica – 1947 – Norbert Wiener
- «kubernetes» -> «guidare» -> «governare»
- I veicoli sono guidati ed il loro movimento è governato (controllato) da sistemi che devono assicurare l'incolumità dei passeggeri
- Nei sistemi di trasporto odierni questo è il ruolo della tecnologia

Definizioni a confronto

CYBERsecurity

Il preservare l'affidabilità, la disponibilità, la manutenibilità e la *safety* di un sistema di controllo ferroviario.

(fonte: UIC – International Union of Railways)

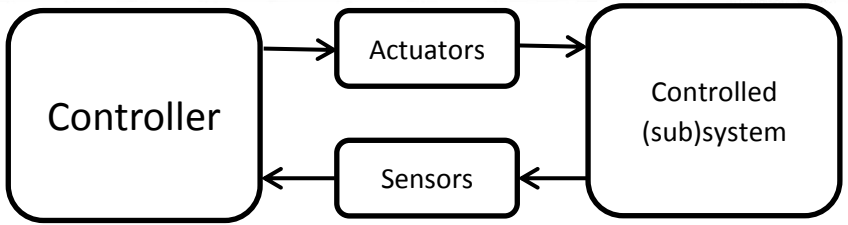
IT security

"Un insieme di strategie che previene l'accesso non autorizzato a beni dell'organizzazione quali computers, reti e dati.

Mantiene l'integrità e la confidenzialità delle informazioni sensibili, impedendo l'accesso ai malintenzionati.

(adattamento da sito web CISCO)

Un (sotto)sistema di trasporto è un sistema di controllo



Per la "**sicurezza funzionale**" sono cruciali

- Le comunicazioni tra sensori e controllore e tra controllore ed attuatori.
- La security delle operazioni del controllore

In mancanza di questi requisiti i messaggi possono essere alterati e la logica del controller può essere sovvertita. Ne risulta una compromissione della safety:

1) Il controllore non può costruire correttamente il modello del sistema o conoscerne lo stato.

2) Pur conoscendone lo stato, il controllore può non essere in grado di modificarlo se la sua logica, in quanto modificata, non può implementare l'azione di controllo appropriata.

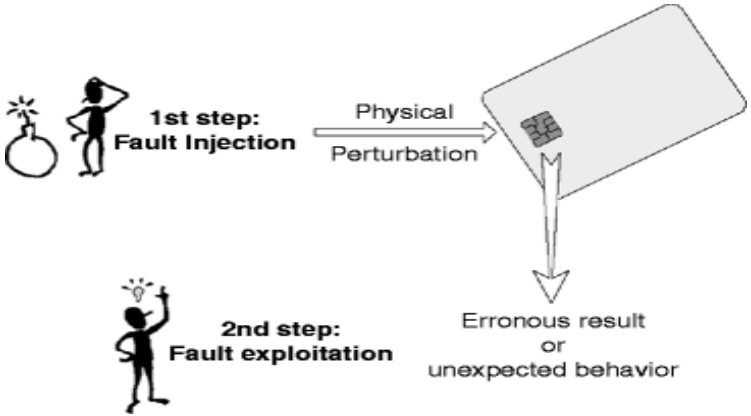
3) A causa della compromissione dei canali di comunicazione tra attuatori e sistema controllato, l'azione di controllo fallisce e non viene attuata.

Sommario

- Non c’è nulla di “cyber” nell’IT-security
- Vulnerabilità dei sistemi embedded
- Esempi di sistemi cyber-fisici nei trasporti
- Lo studio di un caso ferroviario

Unità di controllo elettronico (ECU) nei TCMS

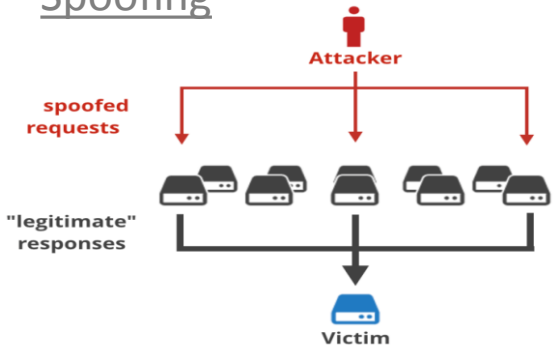
- Riprogrammazione
- Exploits di buffer overflows
- Caricamento alternativo di sistema al boot (Alternate boot loader)
- Fault injection (guasti hardware indotti da cicli software o “glitch”)



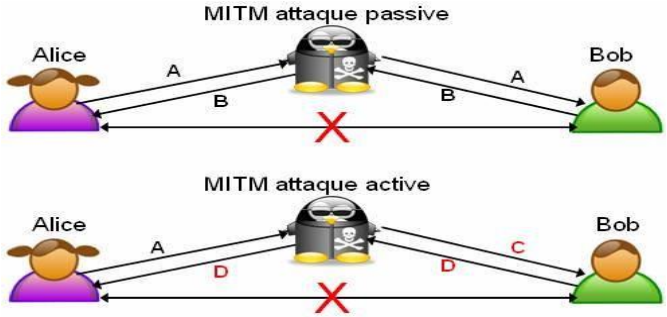
Bus di veicolo

- Assenza di requisiti di security nei protocolli di bus (esempio: CAN Bus)
  - Confidenzialità
  - Integrità
  - Disponibilità (availability)
  - Autenticità

Spoofing

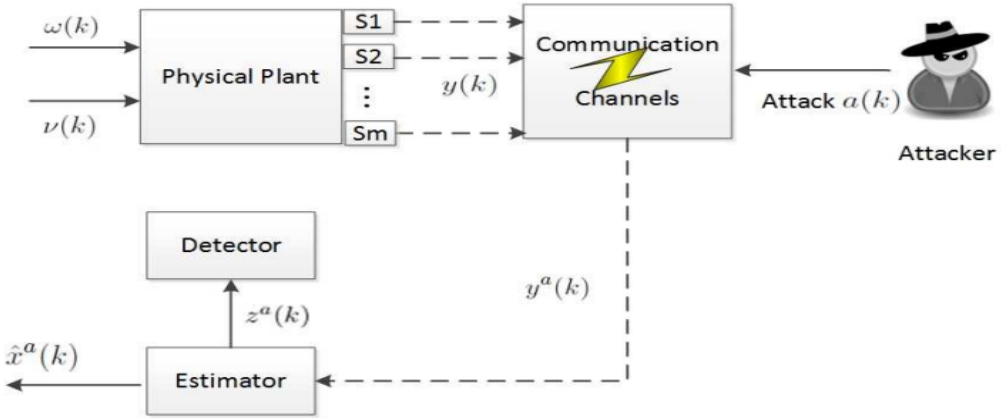


Man in the middle

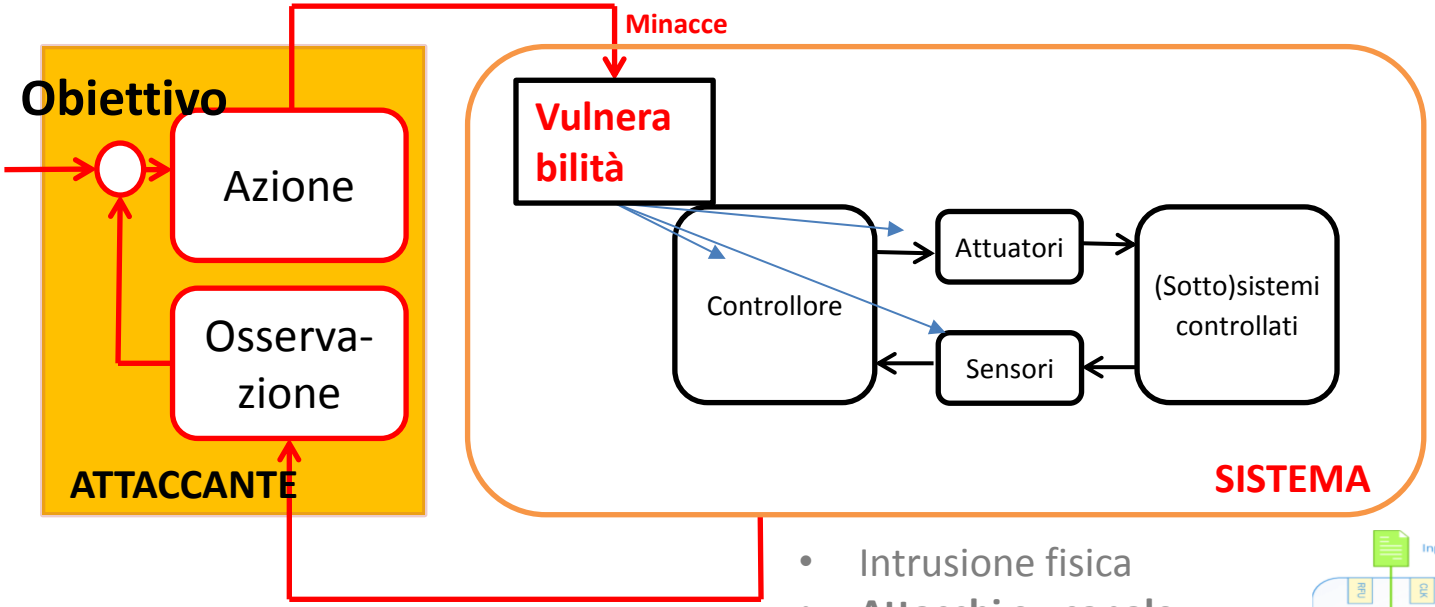


Sensori

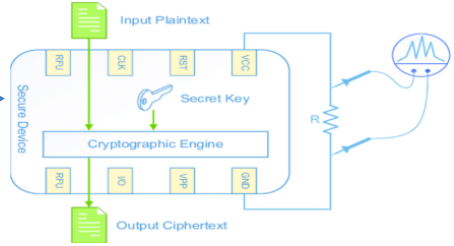
- Compromissione dei dati mediante interferenze elettromagnetiche (jamming)
- Iniezione di dati falsificati (false data injection) nei canali di comunicazione tra i sensori e le unità di elaborazione



Un modello cibernetico di attaccante



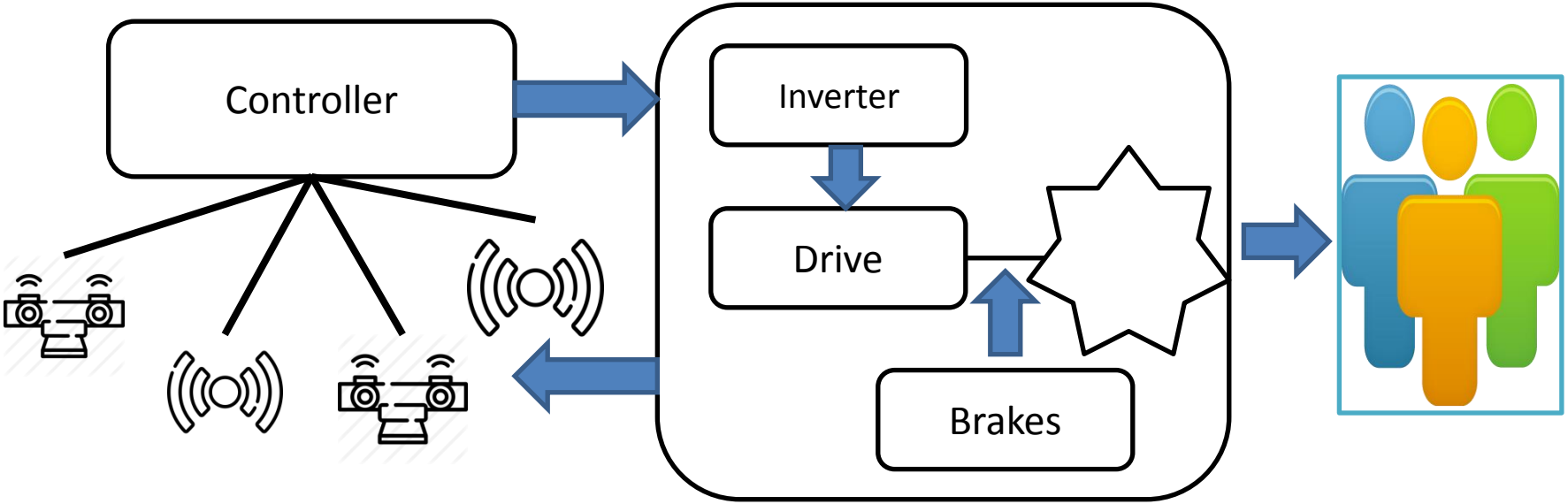
- Intrusione fisica
- **Attacchi su canale laterale (side channel)**
- Monitoraggio remoto
- Sniffing



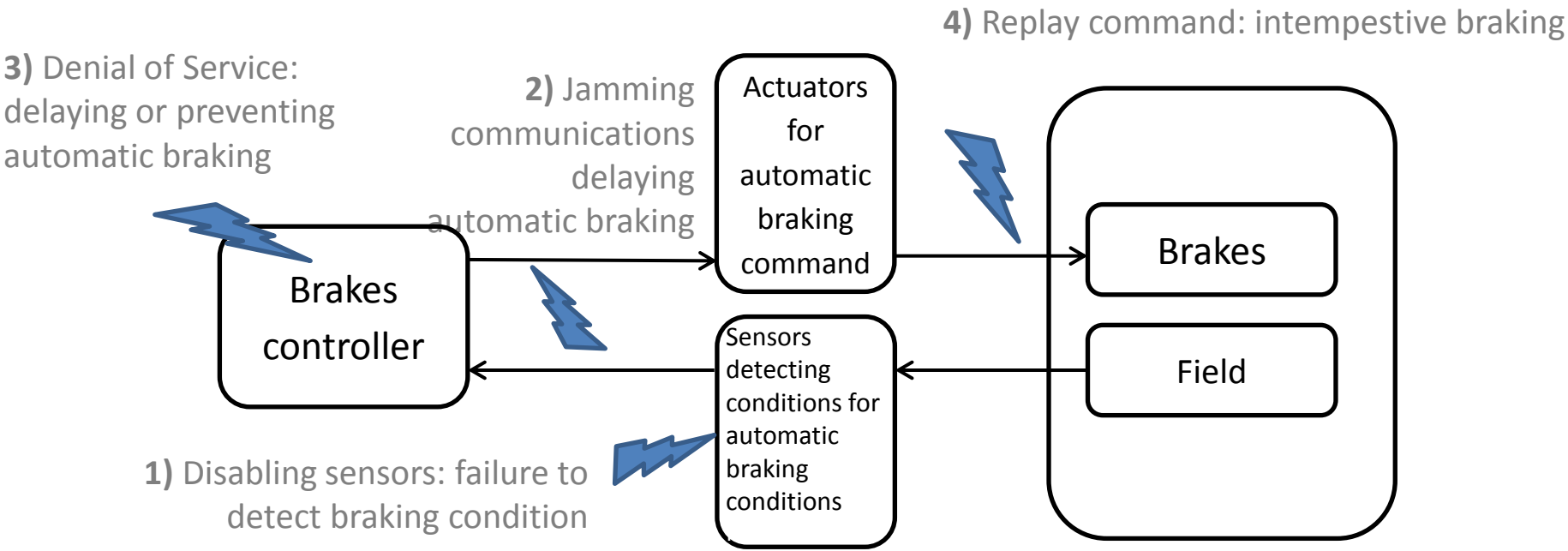
Sommario

- Non c’è nulla di “cyber” nell’IT-security
- Vulnerabilità dei sistemi embedded
- Esempi di sistemi cyber-fisici nei trasporti
- Lo studio di un caso ferroviario

Modello cyber-fisico di un impianto di traslazione



Automotive: sistema di frenatura automatica

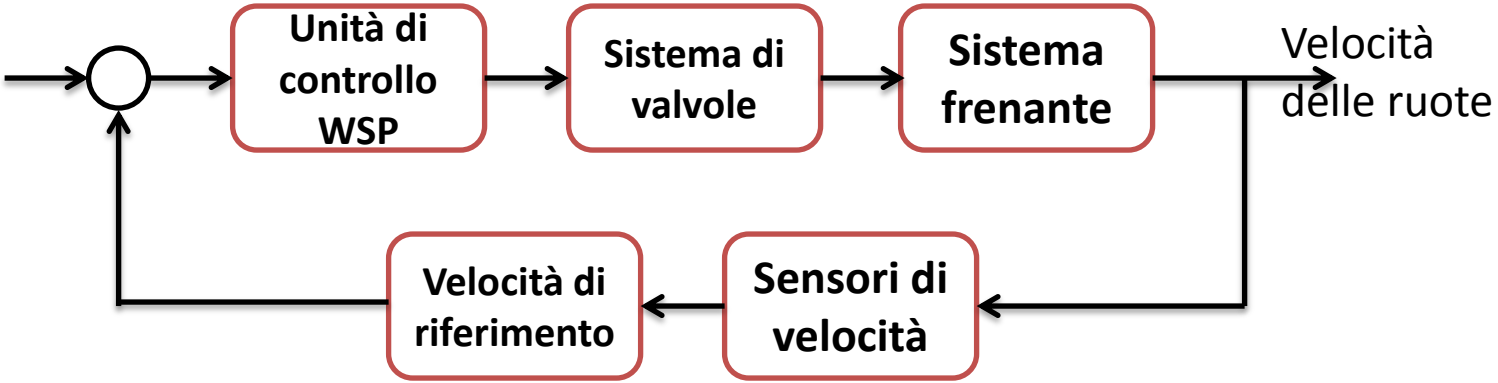


Sommario

- Non c’è nulla di “cyber” nell’IT-security
- Vulnerabilità dei sistemi embedded
- Esempi di sistemi cyber-fisici nei trasporti
- Lo studio di un caso ferroviario

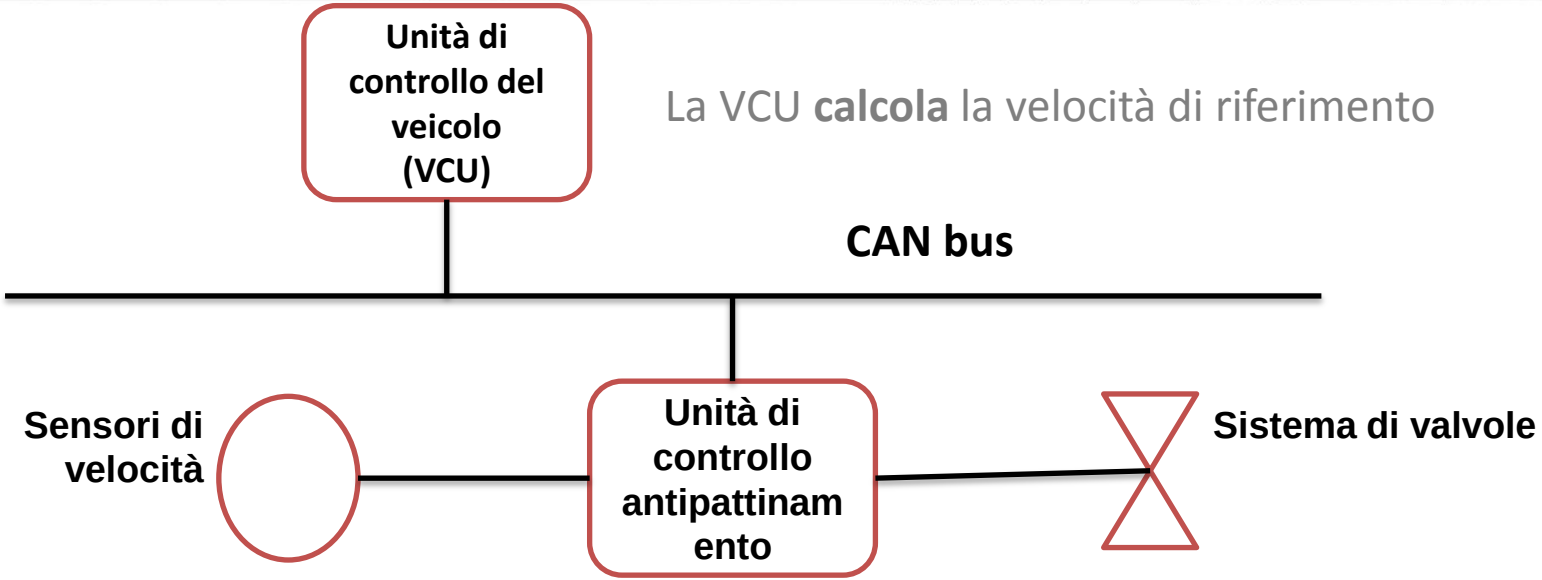
Il sistema antipattinamento (WSP): architettura e descrizione funzionale

- Wheel Slide Protection (WSP): sistema di controllo in catena chiusa della coppia frenante



- Mantiene l'aderenza tra ruote e rotaie prevenendo il blocco delle ruote durante la frenata ed il conseguente pattinamento
- La coppia frenante viene controllata regolando la pressione dell'aria nei cilindri freno, inviando comandi elettrici a valvole di trattenuta e scarico.

Architettura semplificata del WSP



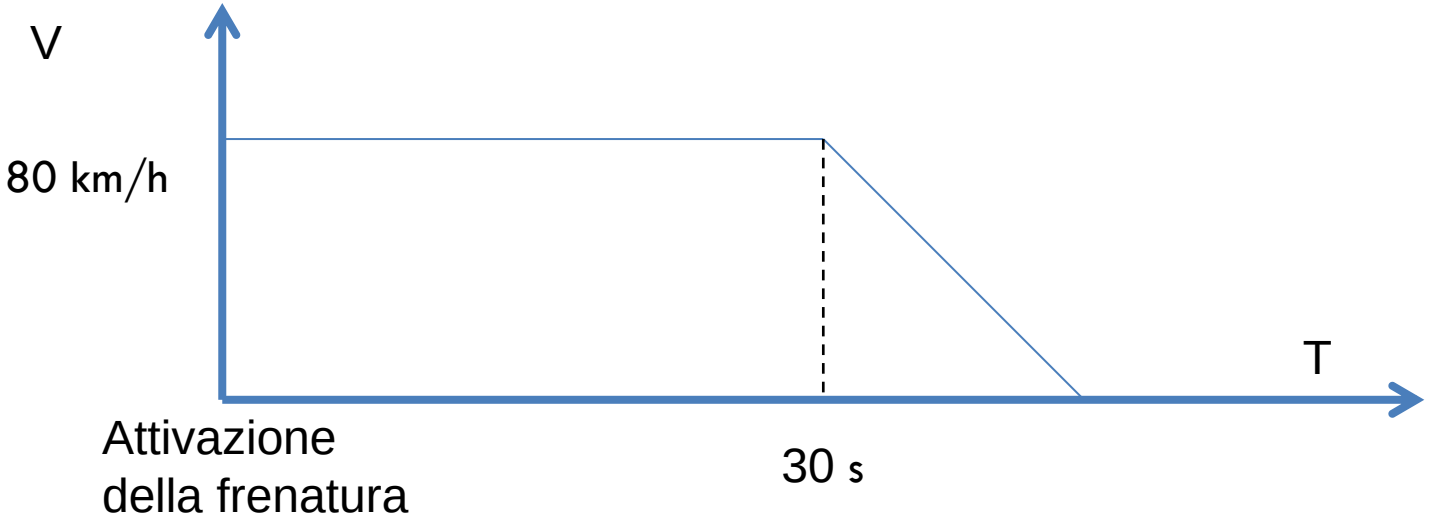
La VCU **calcola** la velocità di riferimento

L'unità di controllo antipattinamento calcola la velocità degli assili

L'unità di controllo antipattinamento **confronta la velocità di riferimento calcolata** con la velocità degli assili (**rilevazione del pattinamento**) e controlla le valvole.

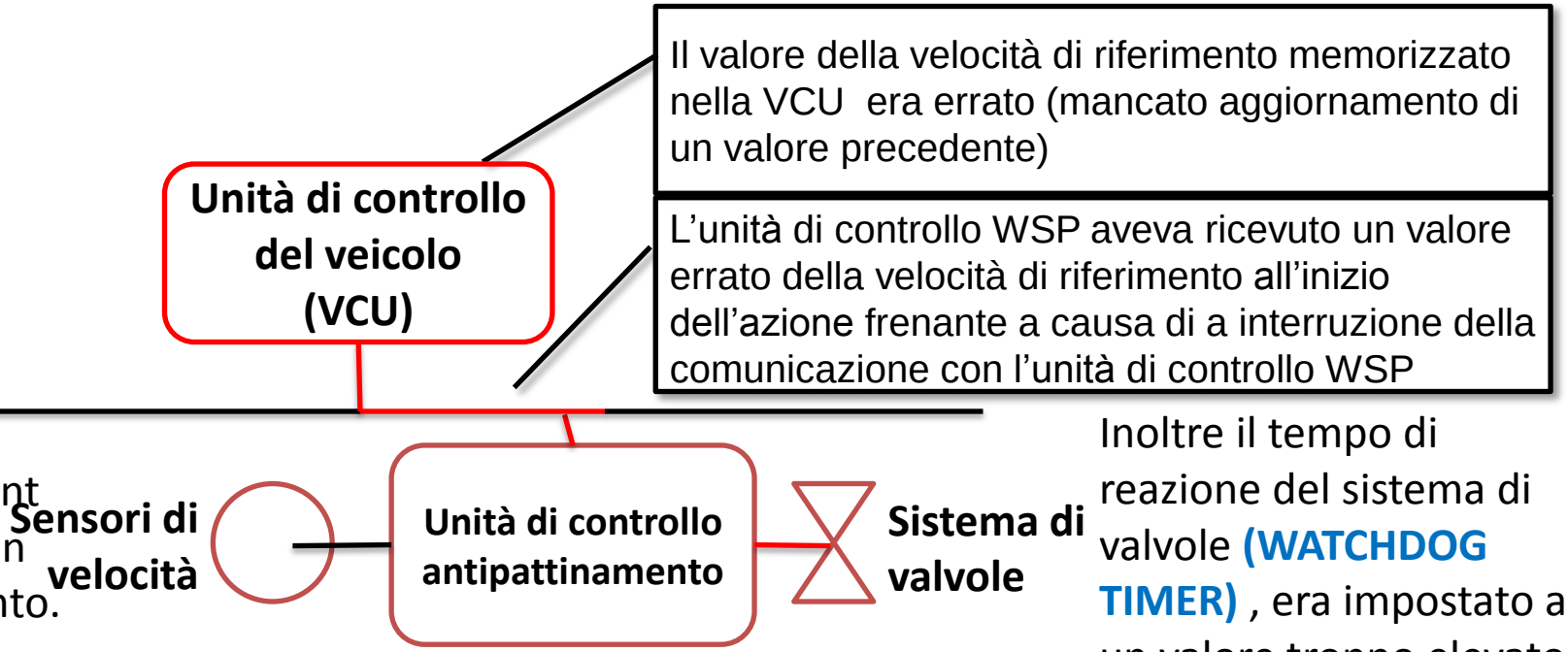
“Quasi-incidente” causato dall’assenza di azione frenante

- Treno in corsa alla velocità di 80 km/h
- Inizio dell’azione frenante ritardate di 30 s dopo la sua attivazione da parte del macchinista.



Analisi delle causes: comportamento anomalo del WSP

La coppia frenante è stata mantenuta nulla in quanto il sistema ha erroneamente rilevato un pattinamento.



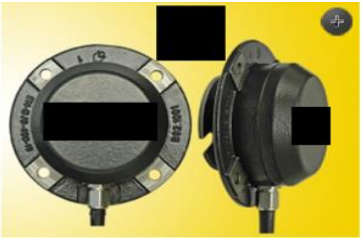
Inoltre il tempo di reazione del sistema di valvole **(WATCHDOG TIMER)** , era impostato ad un valore troppo elevato (30 s) sebbene **ammesso dalla UIC 541-05.**

Analisi dei dispositivi WSP e valutazione delle vulnerabilità

Sensori di velocità

Trad. dai data sheets: Il sensore di velocità (…omissis…) è un sensore di prossimità di tipo magnetico.

I segnali dall'encoder di sicurezza, certificato, sono acquisiti dal dal modulo (WSP) e vengono valutati ed elaborati dall'applicazione eseguita nella CPU di sicurezza certificata.



Dalla letteratura si evincono vulnerabilità dei sensori di velocità dello stesso tipo agli attacchi «false data injection» ed il loro sfruttamento (sperimentale) nella compromissione dell'ABS e dei sistemi di frenatura nel settore automotive.

WSP ECU:

Dai data sheets: conformità IEC 61508, EN 50128, EN 50129.

CPU: architettura tricore

Dalla letteratura: Possibili buffer overflows nell'architettura TRICORE e loro sfruttamento sulle ECU automotive.

Analisi dei dispositivi WSP e valutazione delle vulnerabilità

	Speed sensors	ECU (WSP cu or VCU)	Communication network
Tipo	Magnetico	L'architettura del microcontrollore è di un tipo specifico….	Il TCMS è basato su CAN bus
Fonte informativa	Come si evince dai data sheet del costruttore	Documento di certificazione che cita il tipo di complilatore	Documenti di progetto
Risultati dell'analisi della letteratura	La ricerca nel settore automotive ha evidenziato la possibilità di sfruttare questo tipo di sensori per attacchi al sistema ABS.	The automotive research has demonstrated the feasibility of an attack against microcontrollers with the same architecture	CAN bus non ha requisiti di «security»
Minacce/vulnerabilità	False data injection nella comunicazione tra sensori e centraline, utilizzo di interferenze elettromagnetiche per alterare I dati provenenti dai sensori.	Buffer overflow, alternate boot loader, fault injection	Spoofing, man-in-the-middle, replay, drop, modify, message injection

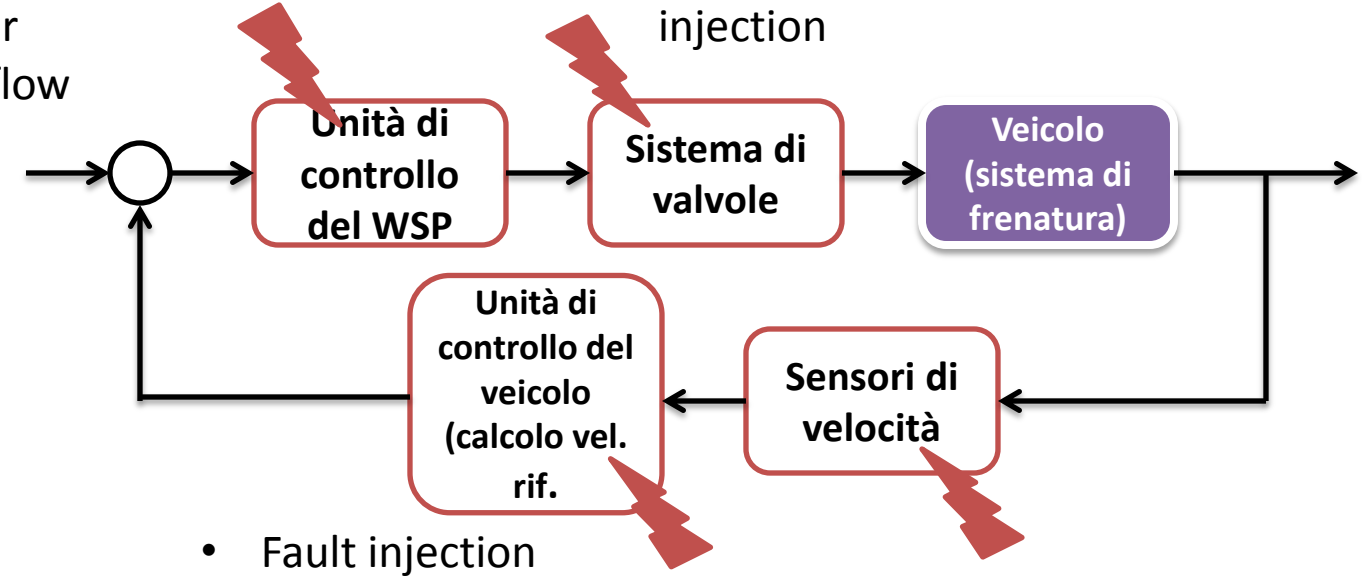
Vettori di attacco al WSP

- Unità di controllo WSP (sia di tipo hardware che software)
- Comunicazione tra VCU e unità di controllo WSP
- Comunicazione tra unità di controllo WSP e sistema di valvole
- Comunicazione tra sensori di velocità e unità di controllo WSP: può essere attaccata via “false data injection” portando a discrepanze tra velocità “di riferimento” e velocità effettiva.
- Controllo delle valvole di scarico: fault data injection

Superficie di attacco del WSP

- Fault injection
- Buffer overflow

False data injection



- Fault injection
- Buffer overflow

False data injection

Considerazioni

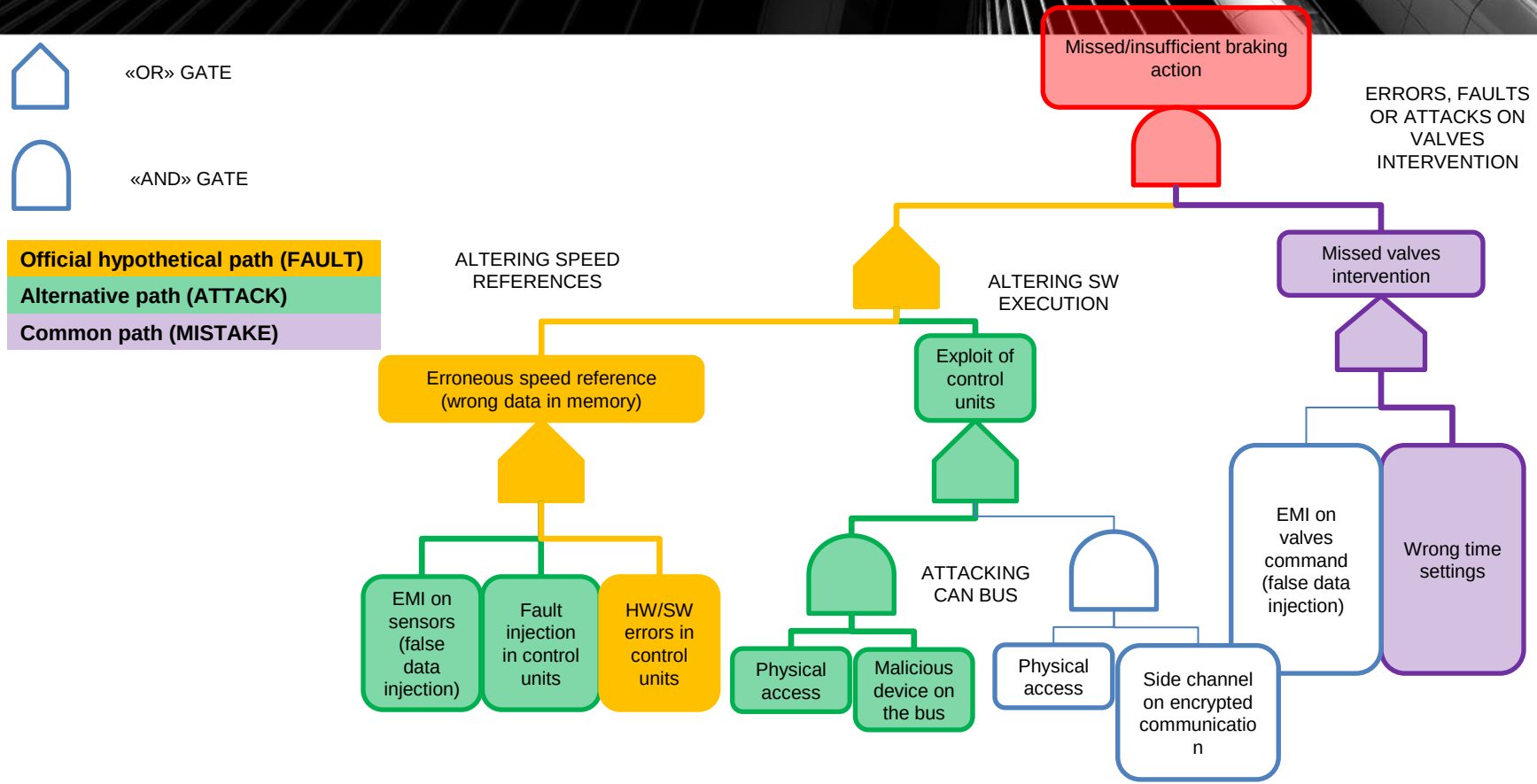
Dal punto di vista della cybersecurity, almeno due attacchi possono causare l'incidente sopra descritto:

- Un attacco alla comunicazione tra sensori di velocità ed unità di controllo WSP, mediante false data injection, che porta ad incongruenze tra velocità di riferimento e velocità effettiva;
- un attacco all'unità di controllo WSP, con lo scopo di corrompere dati in memoria, mediante una fault injection o lo sfruttamento di un buffer overflow.

In evidenza

- La cybersecurity non riguarda solo vulnerabilità software, ma anche minacce e vulnerabilità hardware ed elettromagnetiche.
- L’analisi mediante albero dei guasti è un metodo in grado di rappresentare l’interazione tra sistemi, sottosistemi e componenti, e quindi le conseguenze dei loro guasti (o errori di configurazione)
- L’albero degli attacchi è una tecnica di rappresentazione (e di valutazione del rischio) di un cyberattacco mediante una struttura ad albero, in cui ogni nodo rappresenta una fase dell’attacco.
- Combinando l’albero dei guasti e degli attacchi si può ottenere uno strumento di analisi integrata che tiene conto di
  - Guasti
  - Errori di configurazione
  - Minacce

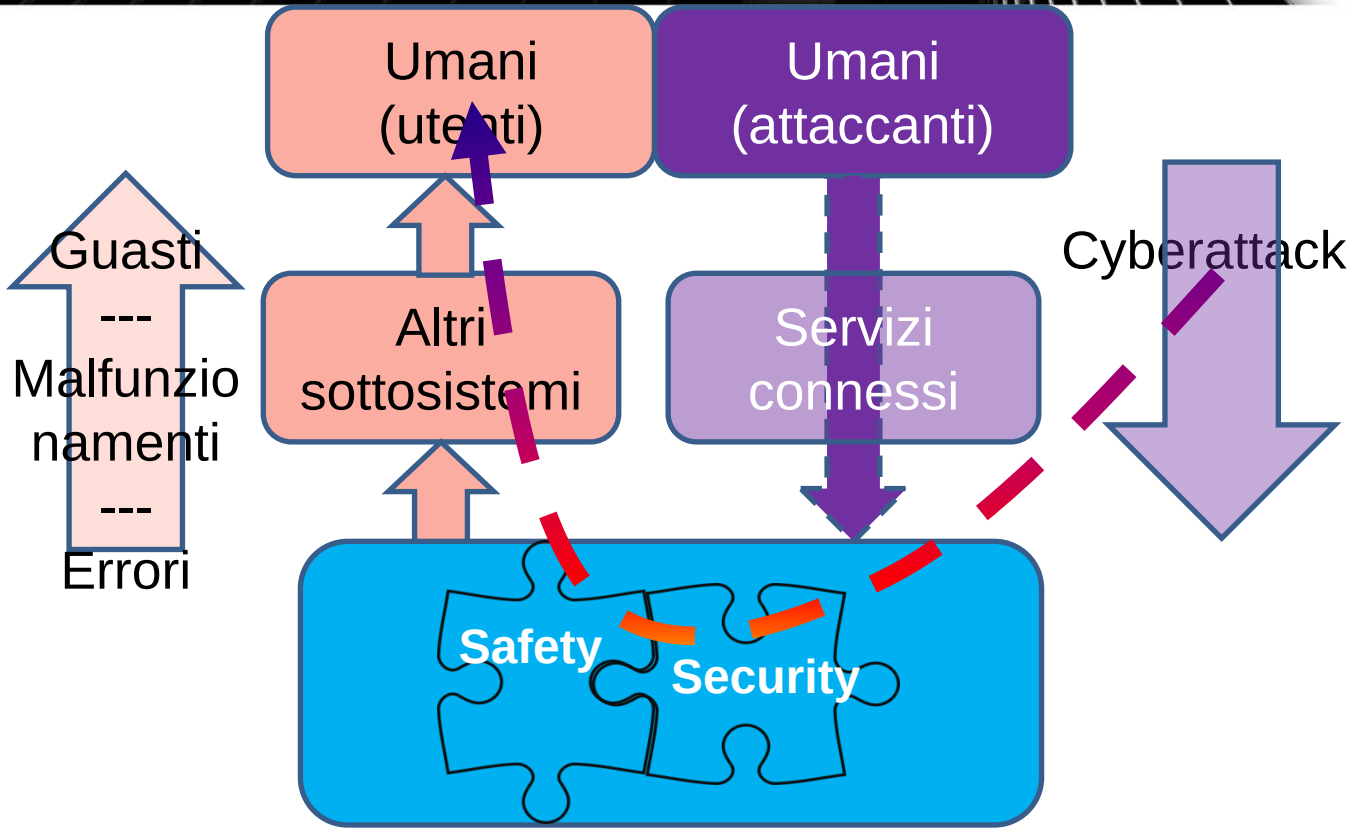
Il “fault-attack tree” del sistema WSP



Conclusioni (cybersecurity+safety=“cybersafety”)

- I singoli componenti del sistema antipattinamento sono conformi a specifiche norme o linee guida, tuttavia l’assenza di un’analisi integrata che tenga conto di aspetti di safety e cybersecurity di questo sistema di controllo può portare a risultati inattesi.
- L’albero “attack-fault” può (o dovrebbe) essere utilizzato nell’ingegnerizzazione di safety e cybersecurity attraverso un approccio integrato.
- Nei sistemi di trasporto cyber-fisici i “pericoli”, gi “errori” e le “vulnerabilità” portano allo stesso risultato: un rischio (safety).

Visione integrata tra sicurezza funzionale (safety) e cybersecurity



Riferimenti

Pizzi, Giorgio. (2020). “***Cybersecurity and its integration with safety for transport systems: not a formal fulfillment but an actual commitment.***” Transportation Research Procedia. 45. 250-257.

Grazie

Giorgio Pizzi
giorgio.pizzi@mit.gov.it

Il contenuto di questa presentazione rispecchia esclusivamente le opinioni dell’autore e non costituisce la posizione ufficiale né pegna in alcun modo la politica dell’ente per cui egli presta servizio.
Questa presentazione usa un modello disponibile su FPPT.com