Associazione Italiana esperti in Infrastrutture Critiche

29/3/2022 - Webinar

SICUREZZA DELLE FUNIVIE E SICUREZZA CIBERNETICA

IL PERCHÉ DI UN APPROCCIO INTEGRATO

Ing. Giorgio Pizzi

Programma

- Trasporto a fune e tipologie di impianti
- Infrastruttura e sottosistemi
- Progettazione della sicurezza funzionale
- Sistemi ciberfisici (cyber-fisici)
- Il sistema di comando e controllo
- Potenziali vulnerabilità
- Integrazione tra sicurezza funzionale e cybersecurity

Il trasporto a fune

- Impianti aerei: tipicamente utilizzato in montagna
- Impianti terrestri anche utilizzati in ambito urbano
- Entrambi hanno la caratteristica di essere in grado di superare pendenze elevate

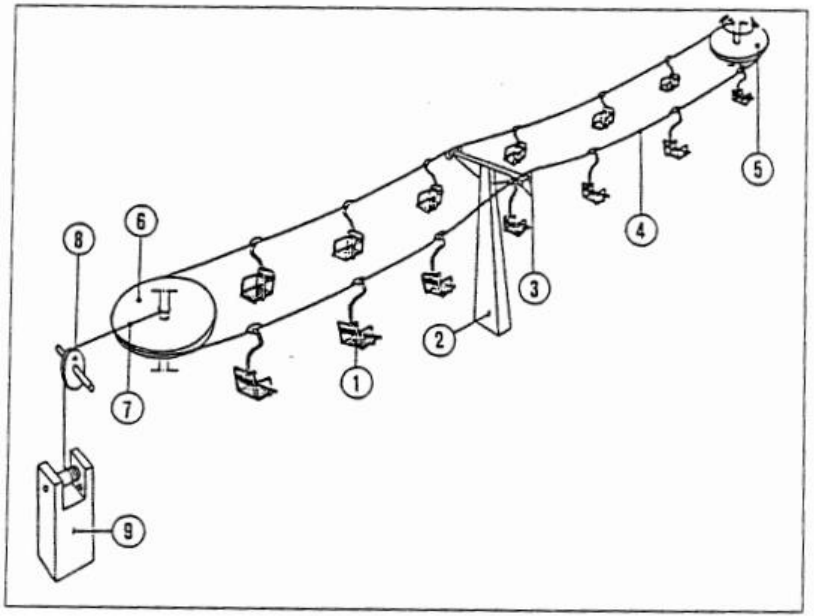
Principali tipologie di impianti aerei

- Monofune
  - A collegamento permanente (ammorsamento fisso)
    - es. seggiovie
    - Movimento
      - Unidirezionale continuo
      - Unidirezionale intermittente (pulsé, grappoli)
  - A collegamento temporaneo (ammorsamento automatico)
    - Seggiovie, cabinovie
    - Movimento unidirezionale continuo
- Bifune (movimento a va e vieni)

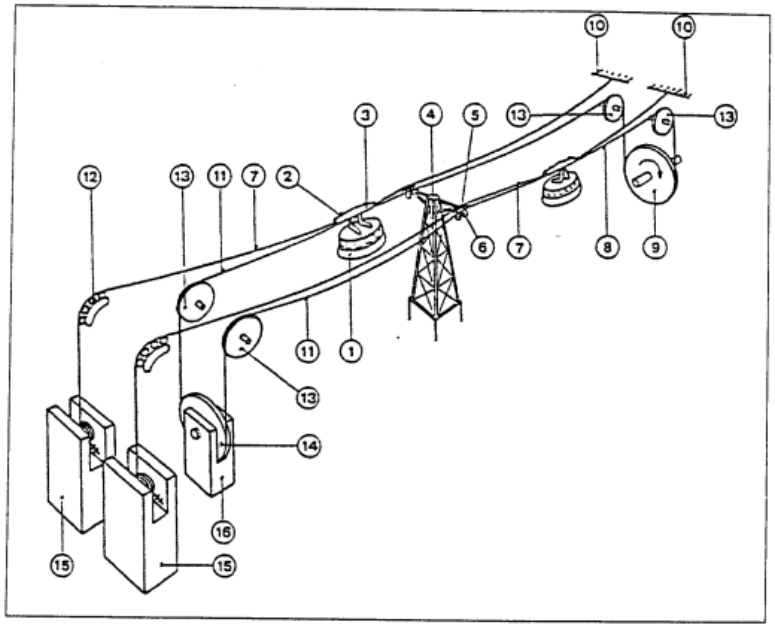
Principali tipologie di impianti terrestri

- Sciovia (skilift)
  - Traini a collegamento permanente
  - Movimento unidirezionale continuo
  - Viaggiatore con sci ai piedi
  - Per sport invernali
- Funicolare classica,
  - sede sulla quale scorrono i veicoli costituita da un binario
- People mover
  - Funicolari automatiche ad ammorsamento automatico (collegamento temporaneo) o fisso su sede «ferroviaria»
  - Tipico utilizzo in ambito urbano ed in pianura (Perugia, Pisa, Venezia,…)

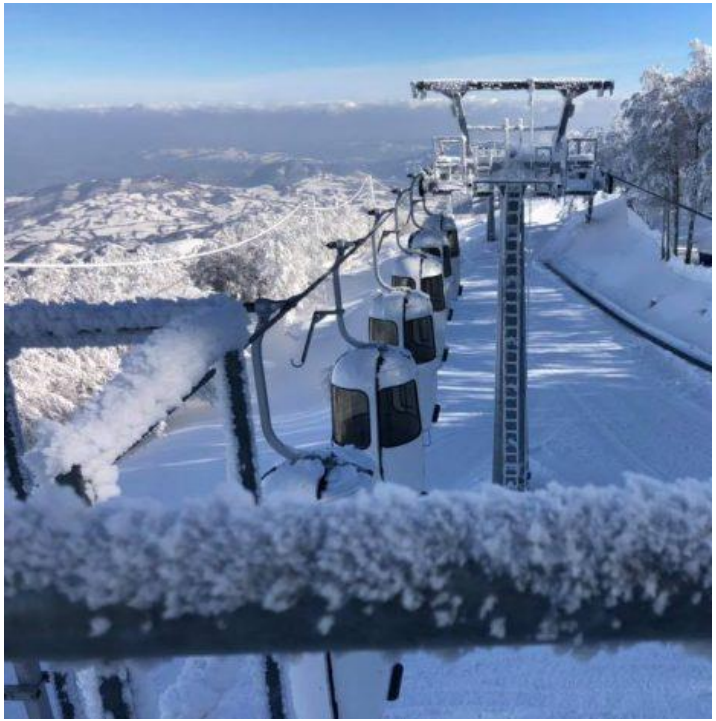
Schemi generali



Seggiovia



Funivia a va e vieni



Pulsé

Telecabina

Es. people mover

Perugia

Pisa

Impianti urbani

- Vantaggi
  - Realizzazione rapida
  - Investimenti relativamente bassi
  - Elevata compatibilità ambientale (emissioni)
  - Bassa invasività
  - Connessione alla rete di trasporto
  - Attraversamento di ostacoli / altre infrastrutture

Impianti urbani

- Caratteristiche
  - Capacità oraria:

Modalità	Capacità oraria
Bus	3500 p/h
Trasporto a fune	Fino a 8000 p/h
Tram	10000 p/h

Cable cars

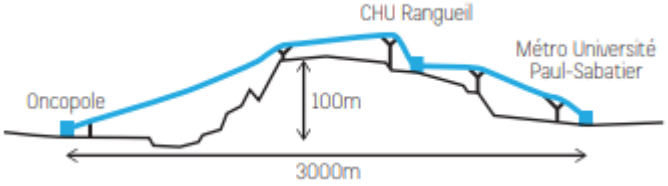
- Cabine da 8 o 10 persone
- Velocità fino a 6 m/s (21 km/h)
- Capacità: 7200 persone/h

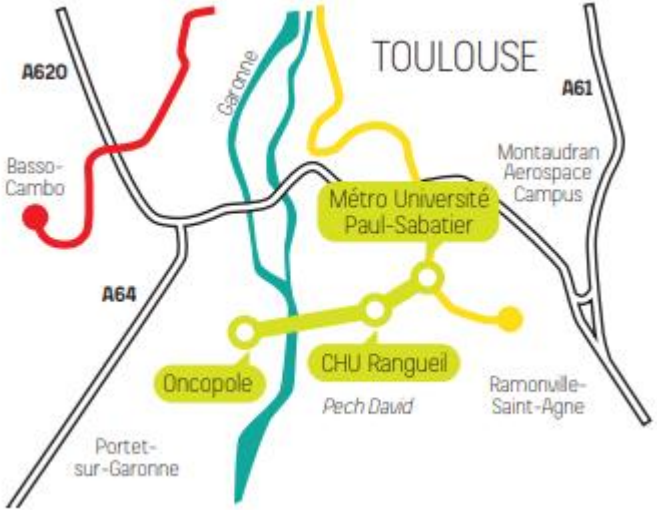
Aerial tramways

- Capacità fino a 4000 persone/h
- Cabine da circa 200 persone
- Velocità fino a 12 m/s (42 km/h)

Fonte: brochure costruttore

Toulouse





V commerciale : 20 km/h
Tempo di viaggio 10 min (30 min in auto)
Frequenza : 1 veicolo ogni 1’30’’.
Capacità :
15 cabine da 34 persone
1 500 pax/ h/direzione
Previsione 8000 pax/giorno

Fonte: https://tisseo-collectivites.fr/projets/teleo

Medellin

Fonte: wikipedia

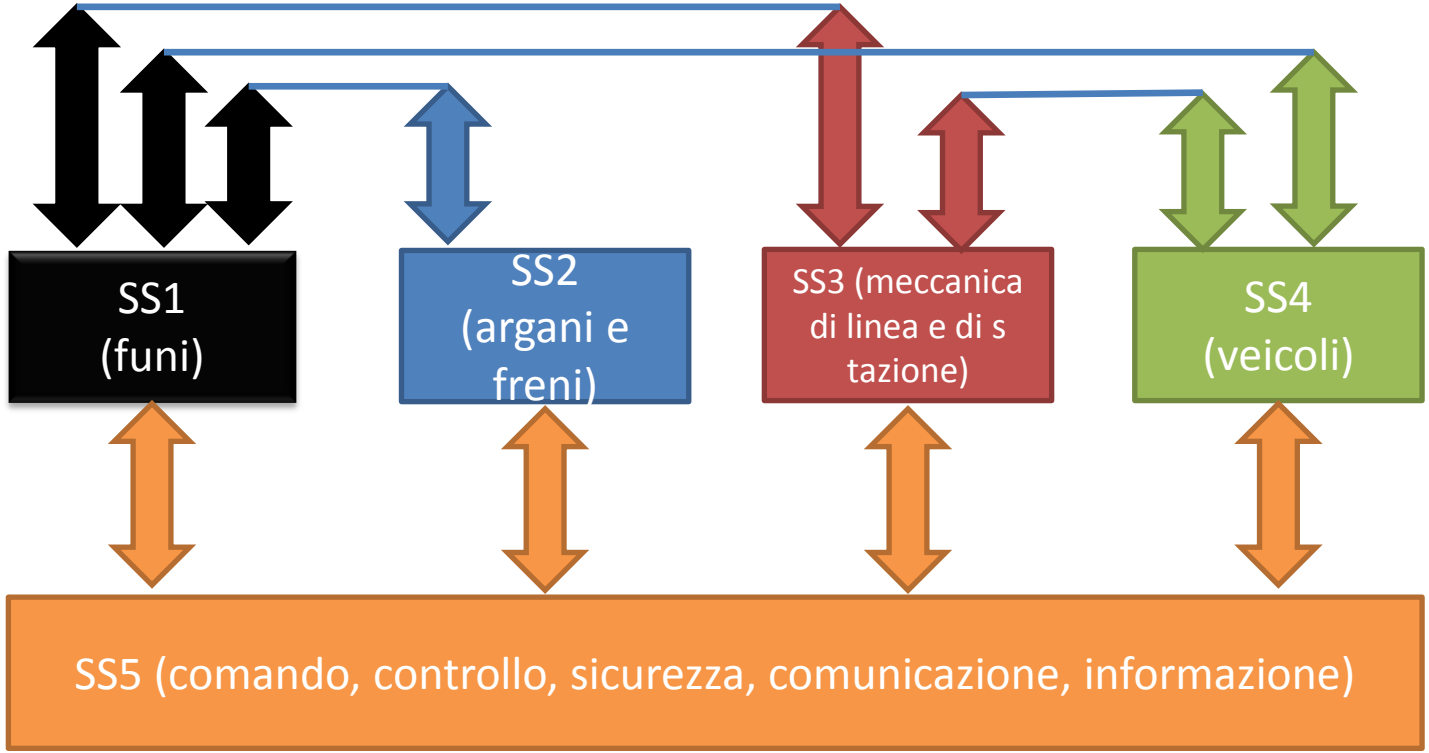
Sottosistemi

Reg. UE 424/2016: Un impianto a fune si compone delle infrastrutture e dei sottosistemi elencati di seguito:

- **1. Funi e attacchi di funi.**
- **2. Argani e freni.**
- **3. Dispositivi meccanici: 3.1. Dispositivi di tensione delle funi.3.2. Meccanismi delle stazioni. 3.3. Meccanica di linea.**
- **4. Veicoli: 4.1. Cabine, sedili o dispositivi di traino.4.2. Sospensione.4.3. Carrelli. 4.4. Collegamenti con la fune.**
- **5. Dispositivi elettrotecnici: 5.1. Dispositivi di comando, di controllo e di sicurezza. 5.2. Dispositivi di comunicazione e di informazione. 5.3. Dispositivi parafulmini.**
- **6. Dispositivi di soccorso: 6.1. Dispositivi di soccorso fissi.6.2. Dispositivi di soccorso mobili.**

+ Infrastruttura

Interfacce tra sottosistemi



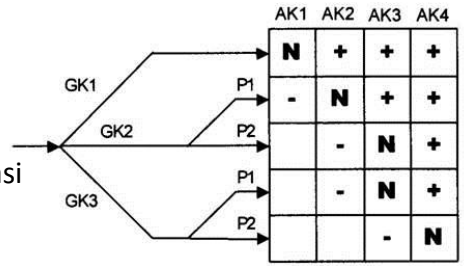
Analisi di sicurezza (es.)

Evento pericoloso	SS	Conseguenze	Dispositivo di protezione	(AK)(*)
Mancato ammorsamento	SS3. 2 SS5	…GKi	Dispositivi meccanici che garantiscano l'ammorsamento forzato in uscita stazione Sorveglianza elettrica della fase di Ammorsamento	
Inefficienza dei sistemi frenanti Mancato coordinamento dei sistemi frenanti	SS2 SS5	….GKi	Sorveglianza elettrica di mancata decelerazione per ogni sistema frenante Sorveglianza elettrica di eccesso velocità …	

(*) Classe di sicurezza: Le caratteristiche intrinseche del dispositivo si determinano in funzione della categoria di rischio (conseguenze dell'evento) e della possibilità di prevenirle, secondo EN 13243.

Safety Integrity Level (**SIL**) viene definito come il livello di riduzione del rischio garantito da una Safety Instrumented Function (SIF). **SIL <-> AK**

GK1: nessun rischio per le persone;
GK2: lesioni reversibili alle persone;
GK3: lesioni irreversibili, compreso la morte, alle persone.
Parametro P (possibilità di evitare il pericolo)
P1: possibilità di riduzione del rischio (si applica solo nei casi eccezionali);
P2: nessuna possibilità di ridurre il rischio.

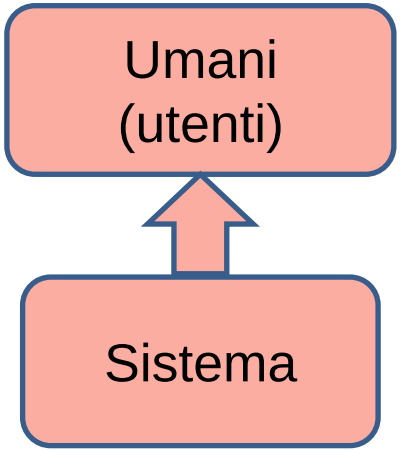


Sicurezza funzionale (functional safety)

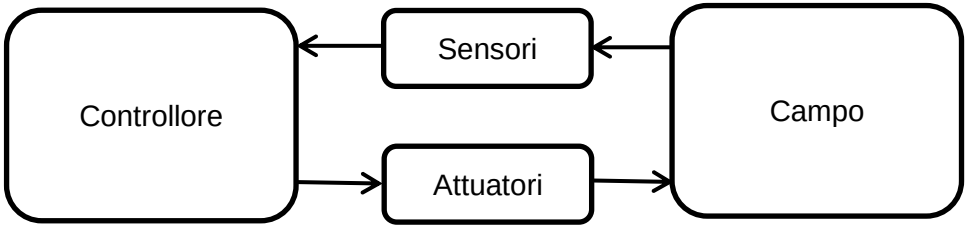
- Sistemi e dispositivi elettrici, elettronici ed elettronici programmabili (E/E/EP*)* per applicazioni di *safety,* dispositivi
- EN IEC 61508 - SIL
- Norma specifica per impianti a fune EN 13243
- Safety Instrumented Sytems: hanno il compito di assicurare la «safety» durante la fase di esercizio (impianto, processo) ed assicurare il raggiungimento di uno stato sicuro (es. arresto) quando vengono superate alcune soglie.
- Le funzioni di un SIS nel settore funiviario si chiamano «sorveglianze»
- Esempi: Sorveglianza dell'azionamento principale, del riduttore e della puleggia, dei freni, della velocità, del tensionamento, della posizione della fune

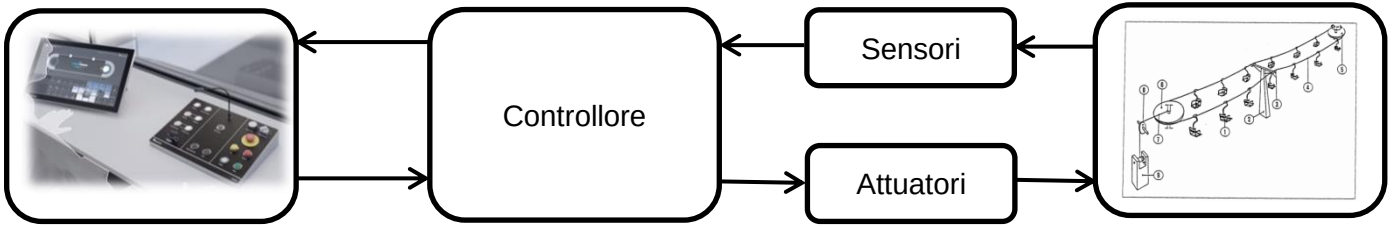
Faults

Failures
---
errors



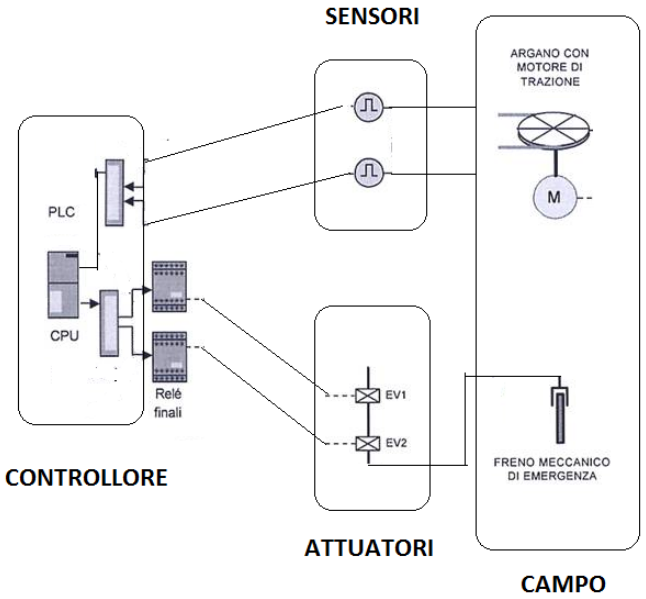
Cibernetica dal gr. Kubernetes: governo, comando e controllo





Supervisione
Comando

Esempio di funzione di sicurezza



Sensori: trasduttori di velocità posizionati in modo tale da rilevare sia il movimento della fune che la rotazione del motore.
Nel PLC viene eseguito costantemente il confronto tra i segnali elettrici provenienti dai trasduttori di velocità.
In caso di discrepanza viene eseguito il comando di chiusura del freno di emergenza sulla puleggia motrice con conseguente arresto dell'impianto tramite la diseccitazione dei relè finali.

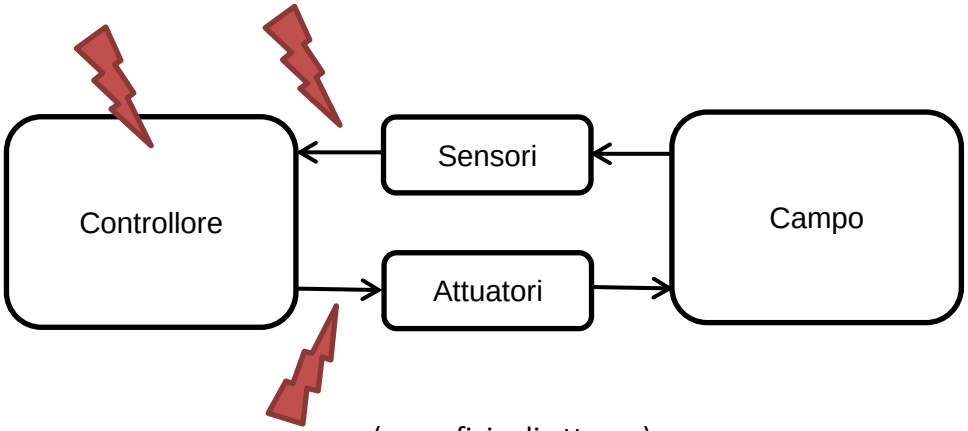
Cybersecurity

Per il funzionamento del sistema, che persegue la sicurezza funzionale, sono determinanti

- **protezione delle comunicazioni tra i sensori ed il controller e tra gli attuatori ed il controller**
- **protezione della stessa** logica di funzionamento del controller**. In assenza di tale protezione**

Infatti, il contenuto delle comunicazioni potrebbe essere alterato e la logica di funzionamento del controller potrebbe essere sovvertita. Quindi verrebbe meno anche la sicurezza, in quanto

- **Il controller non potrebbe costruire correttamente il modello del sistema (ovvero conoscerne lo stato)**
- **Il controller, pur conoscendo lo stato del sistema, potrebbe non essere in grado di correggerlo nel caso la sua logica, in seguito ad alterazione, non è in grado di implementare la corretta azione di controllo**
- **Gli attuatori, per alterazioni della comunicazione con l'oggetto del controllo, potrebbero fallire nell'implementare l'azione di controllo.**



(superficie di attacco)

Non c'è nulla di "cyber" nell'IT security!

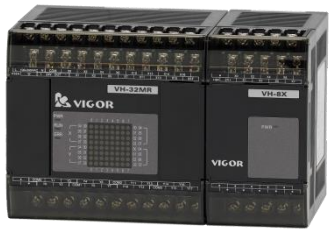
Def (UIC) - the preservation of reliability, availability, maintenability and **safety** (RAMS) of the system

Sistemi IT e sistemi embedded

Sistemi IT raccolgono ed elaborano dati per fornire conoscenza agli umani

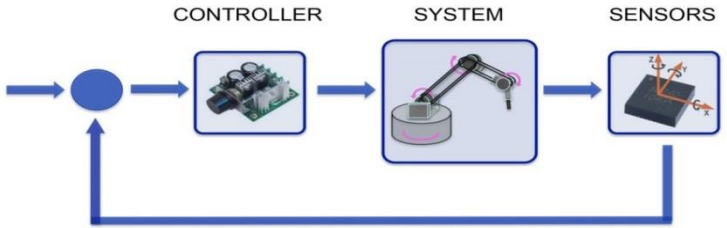
Gestionali aziendali per i servizi commerciali o per le informazioni ai passeggeri o agli operatori

Sistema «embedded»: sistema di calcolo che realizza una specifica funzione in un sistema più complesso, che esso controlla (es. firmware, PLC)



Sistemi cyber-fisici

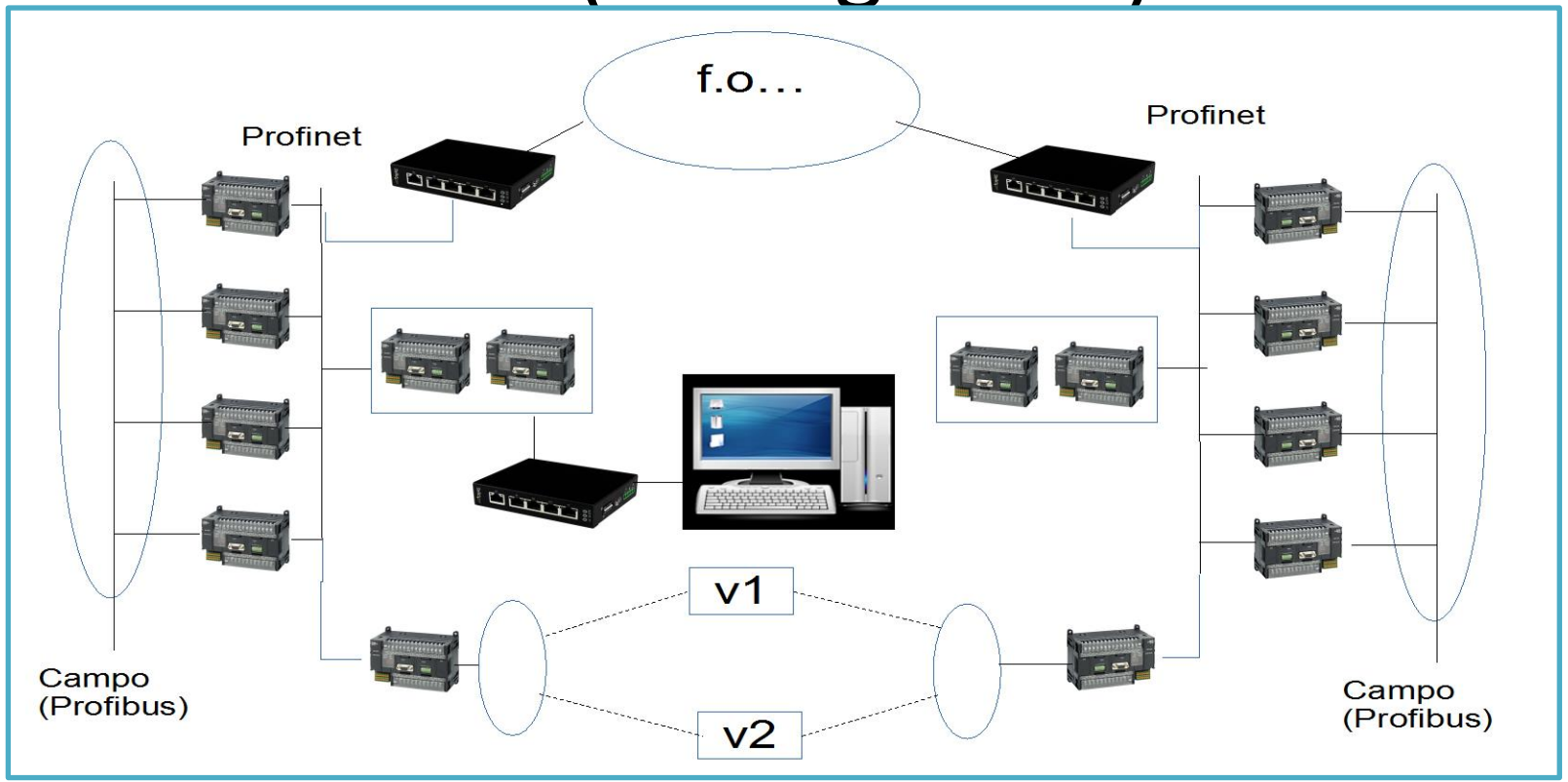
- I sistemi embedded integrati in una rete all'interno di un sistema complesso che interagisce con l'ambiente e con gli operatori o utenti umani danno vita ai sistemi "cyber-fisici" (CPS, cyber-physical systems)



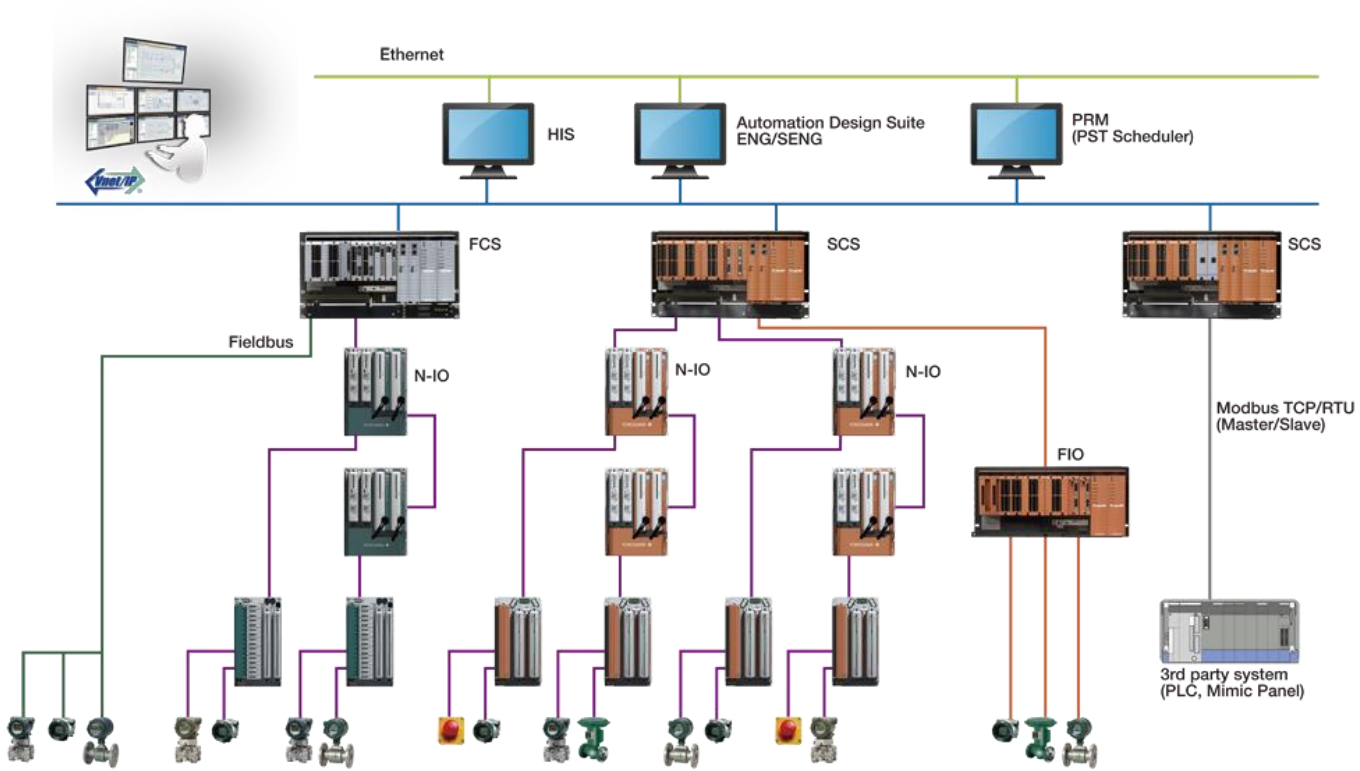
Sistemi IT vs CPS

- Per i sistemi cyber-fisici
  - Maggiore importanza della protezione fisica
  - Maggiori difficoltà nel rilevare un attacco in corso
  - Ciclo di vita più lungo dei sistemi embedded più lungo, a volte anni, con il rischio di introdurre nuove vulnerabilità negli aggiornamenti
- Mentre le vulnerabilità dei sistemi IT possono essere usate contro i sistemi stessi, **quelle dei sistemi cyber-fisici possono essere sfruttare per mettere a repentaglio l'incolumità delle persone.**

Il sistema di comando e controllo funiviario (sorveglianza)



SCADA



Monitoraggio del processo

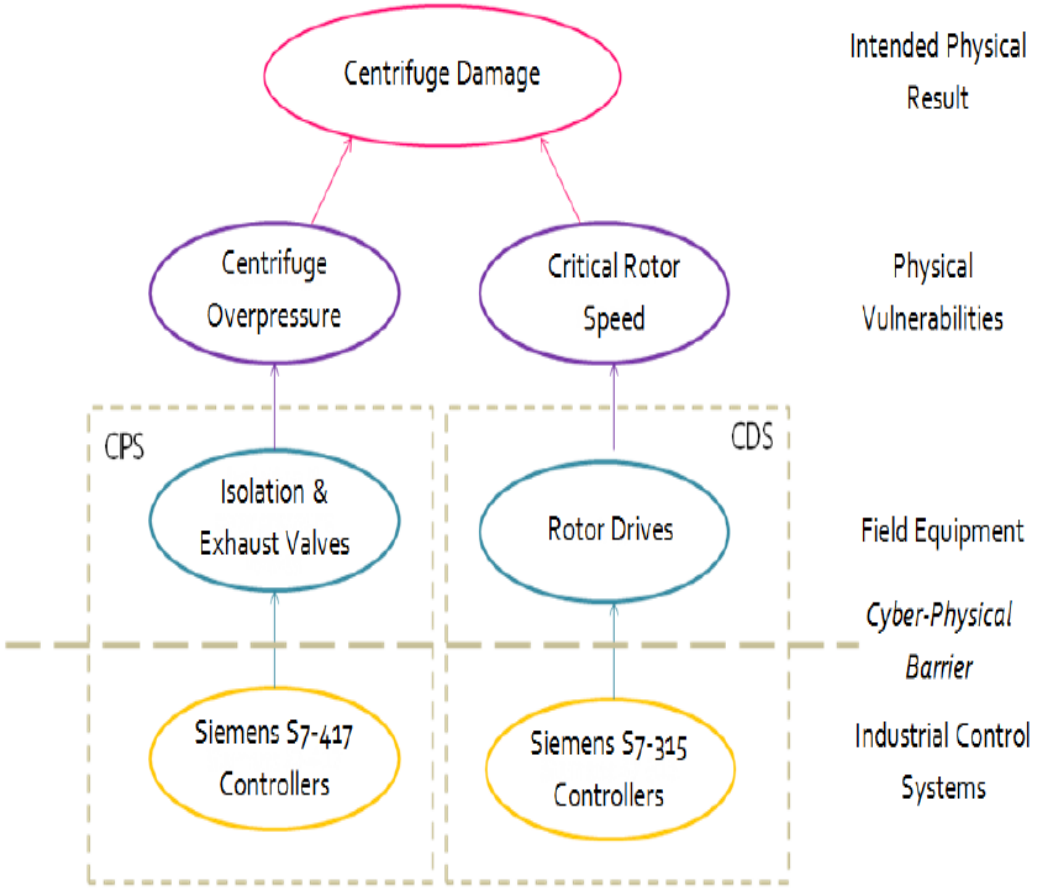
Rete di controllo

Controllo di campo

Apparecchiature di campo

Stuxnet

- Primo attacco (2009) ad un sistema **cyber-fisico**
- Richiedeva una conoscenza della parte fisica del sistema
- E’ stato apportato alle centrifughe di UF6 (uranium hexafluoride) di un impianto nucleare in Iran
- La tattica e la tecnologia utilizzata per l’attacco possono essere estese anche ad altri sistemi
- Comprende, in realtà, due attacchi



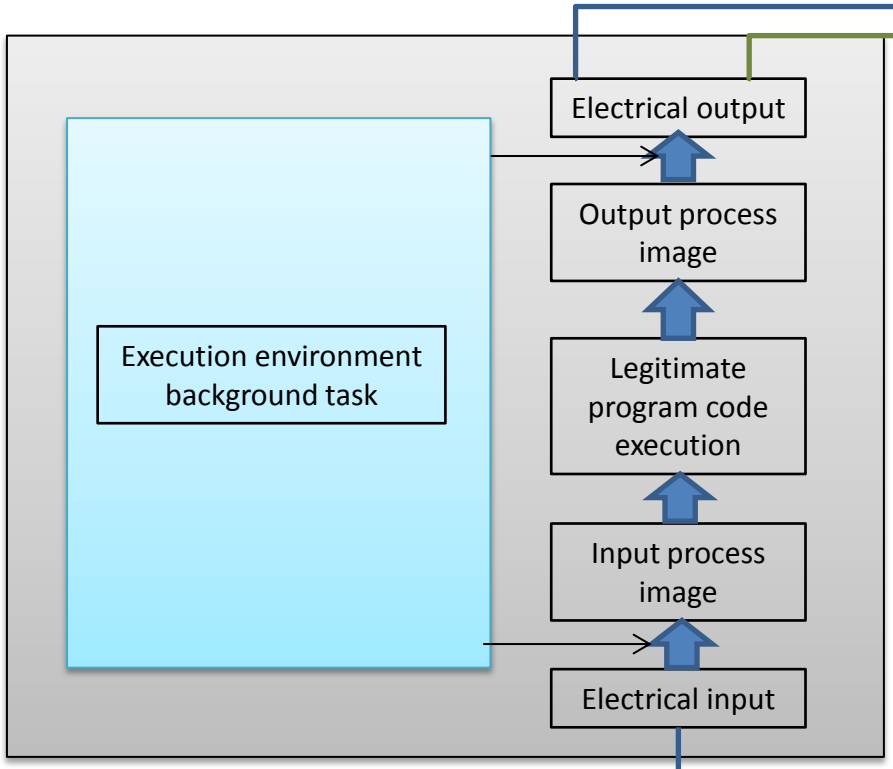
- Il primo attacco provoca una sovrapressione nelle centrifughe
- il secondo una sovravelocità nei rotori oltre la soglia massima

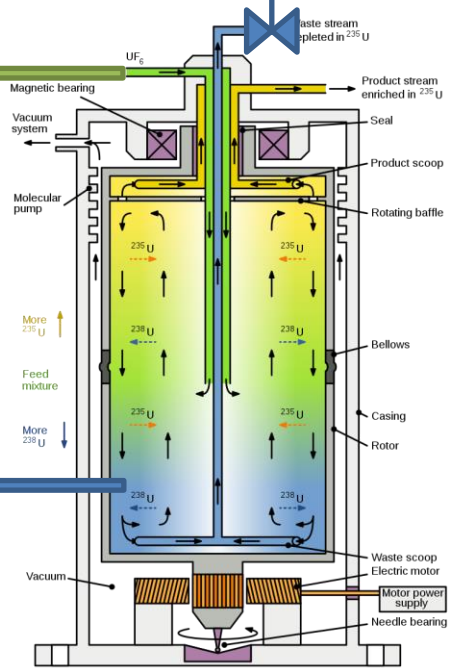
- Sovrapressione: la pressione nella centrifuga (variabile di controllo) è monitorata da un sensore. Se supera una soglia, viene comandata l’apertura di una valvola di scarico (variabile controllata) (SIS)
- Velocità rotore – Aumento della velocità agendo sul convertitore di frequenza. L’effetto è quello di aumentare la pressione.

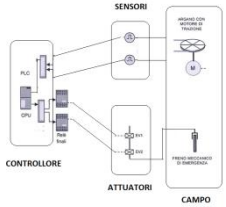
Azione del malware (v1)

- VETTORE DI ATTACCO: per la prima versione di Stuxnet è **una chiavetta USB** contenente un file di configurazione del controller Siemens preparato ad hoc, utilizzata su un **portatile in dotazione ad un tecnico.**
- TRIGGER: è costituito dalla combinazione di specifiche condizioni del processo che vengono individuate dal malware.
- PAYLOAD: **vengono manipolati I valori che definiscono il processo all'interno del controller ed il malware prende il controllo del sistema**
- Alla postazione di controllo vengono invece presentati I valori provenienti dai sensori precedenti all'attivazione dell'attacco.
- **Durante l'attacco il codice legittimo continua ad essere eseguito ma riceve valori di input falsi ed ogni azione sugli attuatori viene disattivata**.
- Il malware si pone tra la periferia (input, output) ed il codice legittimo attuando un attacco ***man-in-the-middle.***
- I segnali di ingresso dele valvole non pervengono direttamente al S7-417 ma attraverso sensori di pressione dedicati che hanno un valore di soglia configurabile che, una volta superato, attiva S7-417 che a sua volta comanda le valvole di scarico. **L'azione del malware agisce sulla conversione del segnale di pressione, in modo che pressioni superiori alla soglia vengano interpretate come pressioni ancora normali**. **In questo modo non viene comandata la necessaria apertura delle valvole di scarico.**

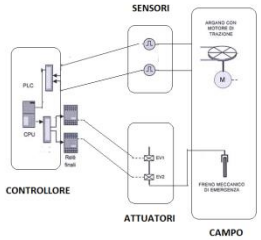
Funzionamento ordinario







Man in the middle (pass-through)



Electrical output

Output process image

Malicious output data

Stuxnet injected rogue code – Pass through mode

Legitimate program code execution

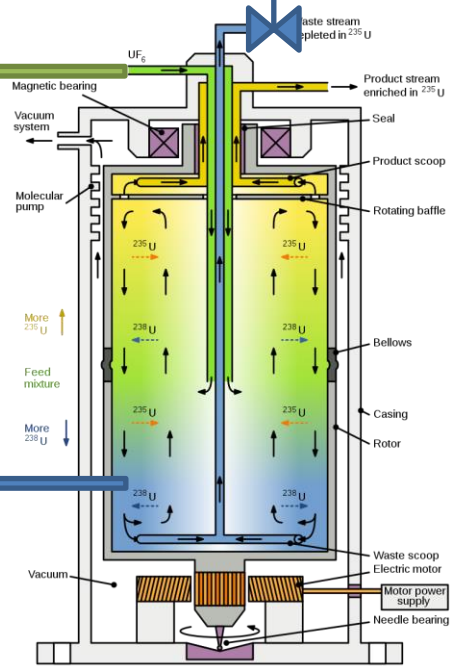
Fake input data

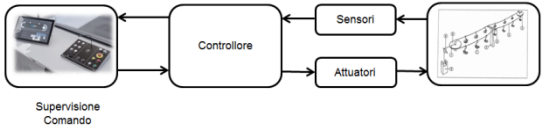
Input process image

Electrical input

Supervisore : OK!

P





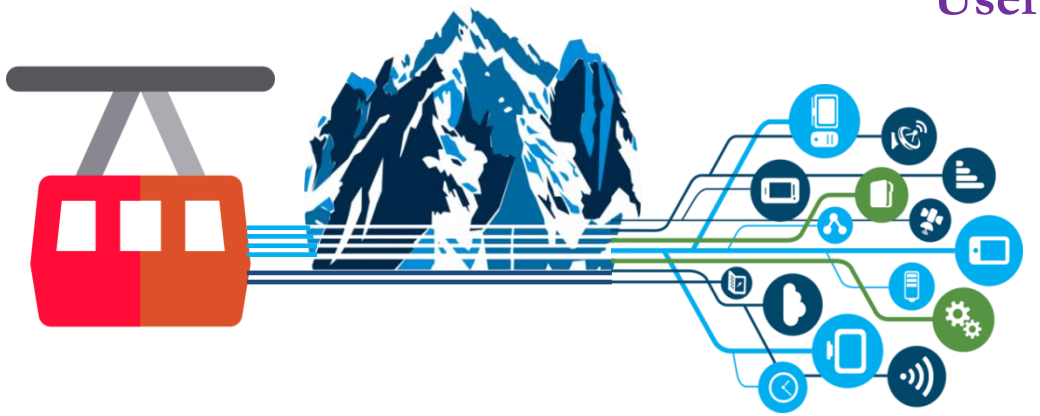
Azione del malware (v2)

- VETTORE DI ATTACCO: nella seconda versione il malware si propaga in rete attraverso un exploit di Windows
- Come nella precedente versione:
  - Il controllo da parte del codice legittimo viene sospeso.
  - La sequenza del malware viene reiterata dall'ambiente operativa del PLC.

La funivia connessa…..

AUGMENTED REALITY
Smartphone
Sensors
APPs

Predictive Maintenance
User Experience
Usability



WLAN
DEVICES
Remote assistance
Mountain Management

HMI
SCADA
Smart Ropeway
CONNECTED ROPEWAY

..e il paradigma della IoT

Avere tutto quello che si può immaginare connesso in rete in modo che l'informazione proveniente da tutte queste "cose" connesse possa essere memorizzata, trasferita, analizzata, **trasformata in "azione"** (*"acted upon"*) con modalità nuove e **tipicamente automatiche**, **attraverso connessioni di rete con tutto il resto**.

https://www.automationworld.com/article/technologies/networking-connectivity/wireless/manufacturing-and-internet-things

Il paradosso del progresso

- In un tempo in cui facciamo sempre più affidamento sull'infrastruttura digitale per la memorizzazione dei dati e l'erogazione di servizi fondamentali, questi stessi elementi diventano il principale obiettivo di un attacco
- Da una maggiore digitalizzazione deriva una maggiore fragilità

EU Cybersecurity and the Paradox of Progress Lorenzo Pupillo – CEPS policy insights – n. 2018/06, february 2018

Nuove minacce per nuove vulnerabilità

- La connessione «supera» la protezione fisica
- Gli attacchi sono complessi, mirati e portati per fasi
- Gli air-gap possono essere superati (vedi Stuxnet,
- Il fattore umano e quello gestionale sono un anello debole della catena

Supervisione-comando-controllo

- Postazione di controllo per l’esercizio dell’impianto
- Viste sinottiche, allarmi e funzioni di test

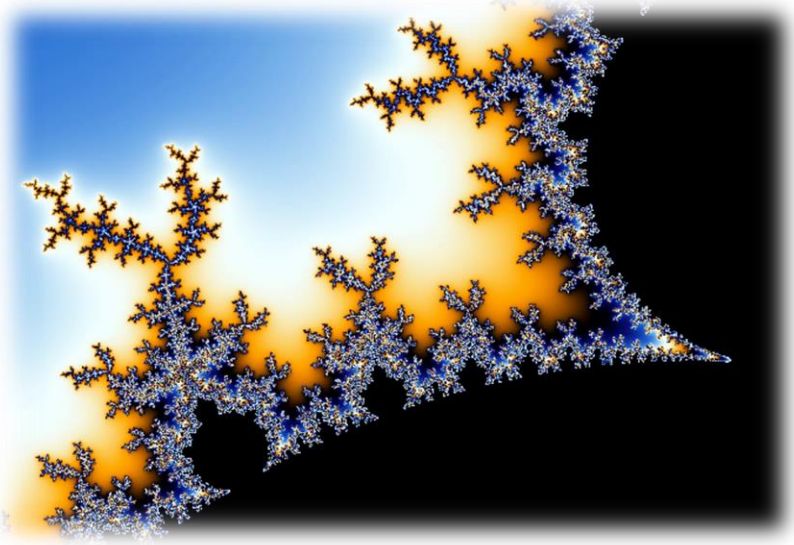
- Postazioni SCADA
- Disponibilità su palmari
- Telecomandi

Impianti non presidiati

- Non sono previsti operatori nelle stazioni
  - Controllo degli accessi
  - Rilevamento di ostacoli
  - Controllo del piano di imbarco
- Postazione centrale di controllo, anche per più impianti

Aumenta la
SUPERFICIE DI ATTACCO

- Aumento della complessità tecnologica
- Insieme dei differenti VETTORI DI ATTACCO che un utente non autorizzato (ATTACCANTE) può sfruttare per violare un SISTEMA
- Vettore di attacco: qualsiasi protocollo o sistema di comunicazione, servizio, interfaccia o parti di essa che potenzialmente presenta vulnerabilità



USB RUBBER DUCKY

$49.99

Imagine you could walk up to a computer, plug in a seemingly innocent USB drive, and have it install a backdoor, exfiltrate documents, steal passwords or any number of pentest tasks.

All of these things can be done with many well crafted keystrokes. If you could just sit in front of this computer, with photographic memory and perfect typing accuracy, you could do all of these things in just a few minutes.

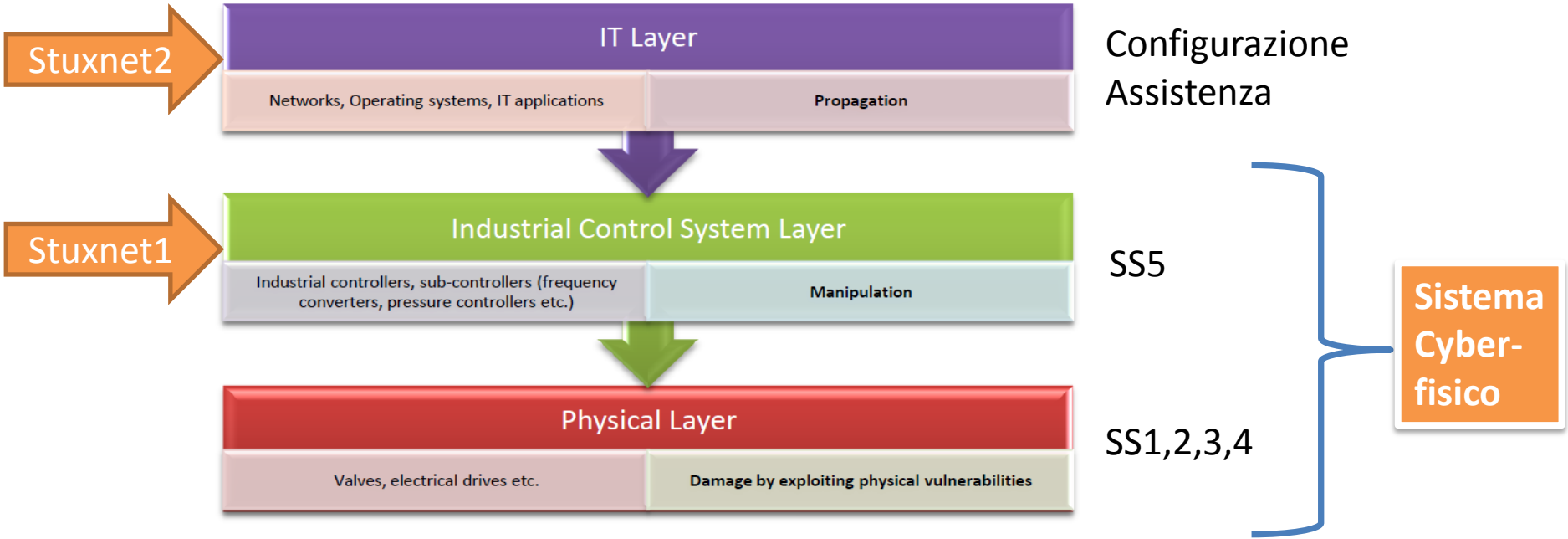
The USB Rubber Ducky does this in seconds. It violates the inherent trust computers have in humans by posing as a keyboard - and injecting keystrokes at superhuman speeds.

Since 2010 the USB Rubber Ducky has been a favorite among hackers, pentesters and IT pros. With its debut, keystroke injection attacks were invented – and since it has captured the imagination with its simple scripting language, formidable hardware, and covert design.

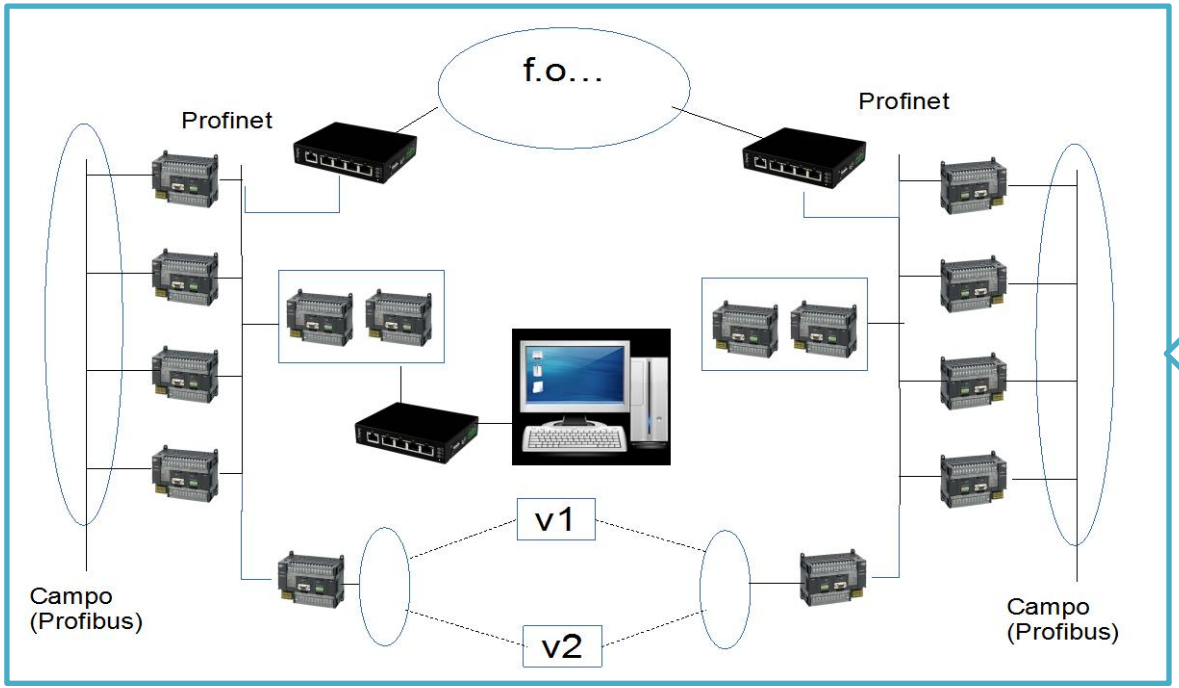
QTY

— 1 +

La funivia “connessa” non è come un sistema informatico !



Impianto a fune: sistema CYBER-FISICO

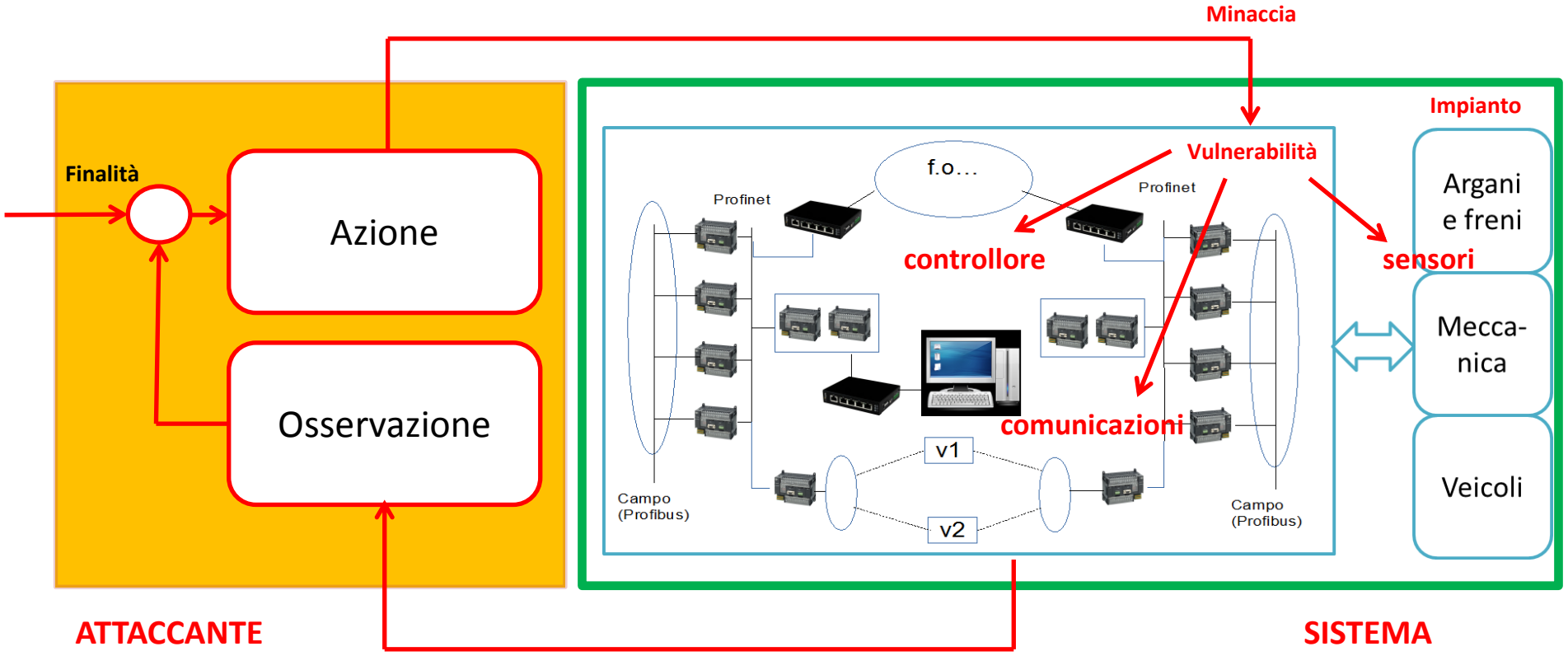


Argani e freni

Mecca-nica

Veicoli

Modello dell'attacco al sistema CYBER-FISICO



La tecnologia per l'automazione funiviaria è attaccabile?

- Tutti i sistemi che fanno uso di tecnologia elettronica, non solo digitale, sono un possibile bersaglio di un cyberattacco
  - Sistemi informativi
  - Sistemi di controllo industriale (CPS)
  - Automotive (CPS)
- Come gli altri sistemi di trasporto, anche quelli a fune sono un possibile obiettivo

The Moscow Times
INDEPENDENT NEWS FROM RUSSIA

Moscow's First Cable Car Shuts Down After Opening in Suspected Cyberattack

Nov. 29, 2018

An unnamed source told the state-run RIA Novosti news agency Thursday that the alleged hacker had demanded a Bitcoin ransom.

Forbes Innovation Leadership Money Business Small Business

42,183 views | Jan 15, 2019, 08:00am

Exclusive: Hackers Take Control Of Giant Construction Cranes

Quindi: ATTENZIONE AI TELECOMANDI!!!!)

Telecrane F25 Series CVE-2018-17935 Authentication Bypass Vulnerability

Telecrane F25 Series is prone to an authentication-bypass vulnerability.

An attacker can exploit this issue to bypass the authentication mechanism and perform unauthorized actions. This may lead to further attacks.

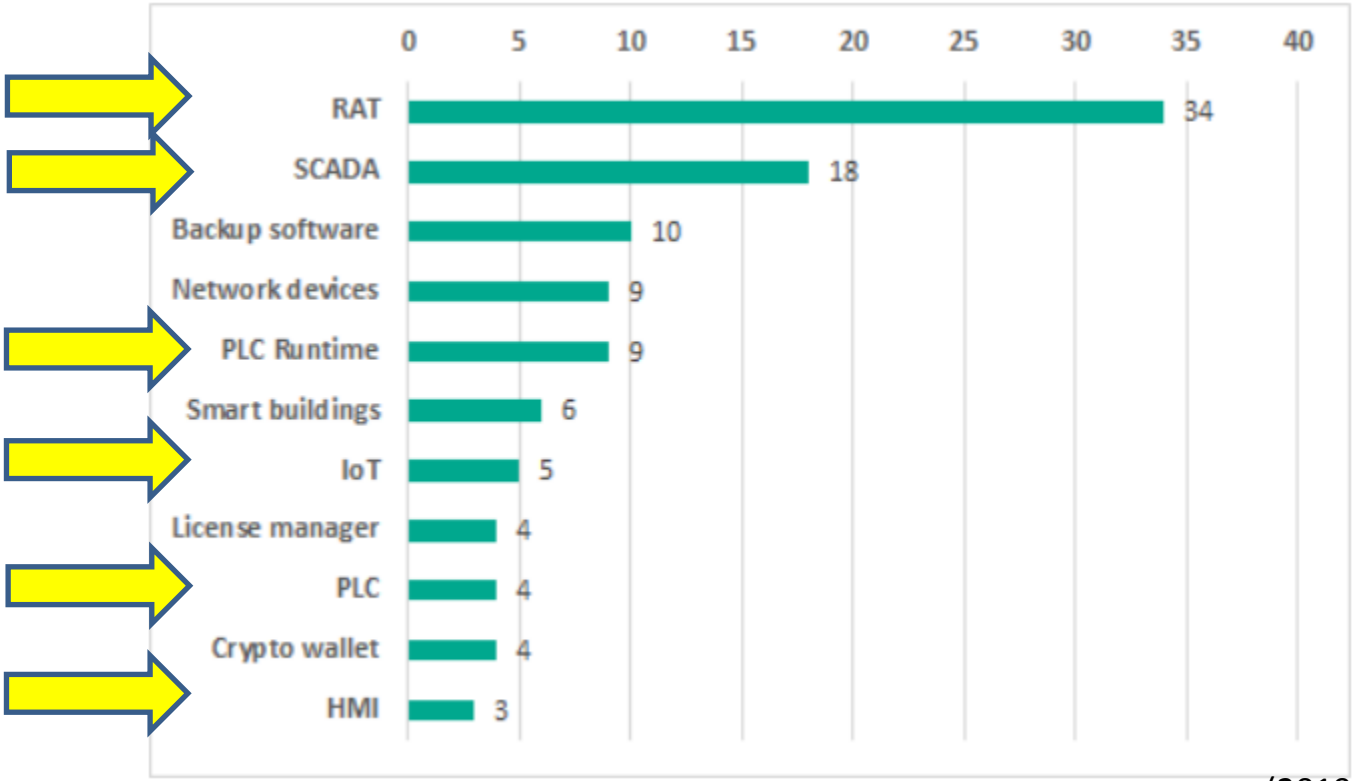
APRIL 24TH, 2018

Serious Vulnerabilities Identified in Austrian Ski Lifts Control System Can Disrupt its Operations- Researchers Claim.

The researcher duo managed to remotely access the ski lift system's control unit. They identified that it was possible to start/stop/reverse the lifts because they could access the control unit. It was also possible to make changes in the safety distance parameters between lifts.

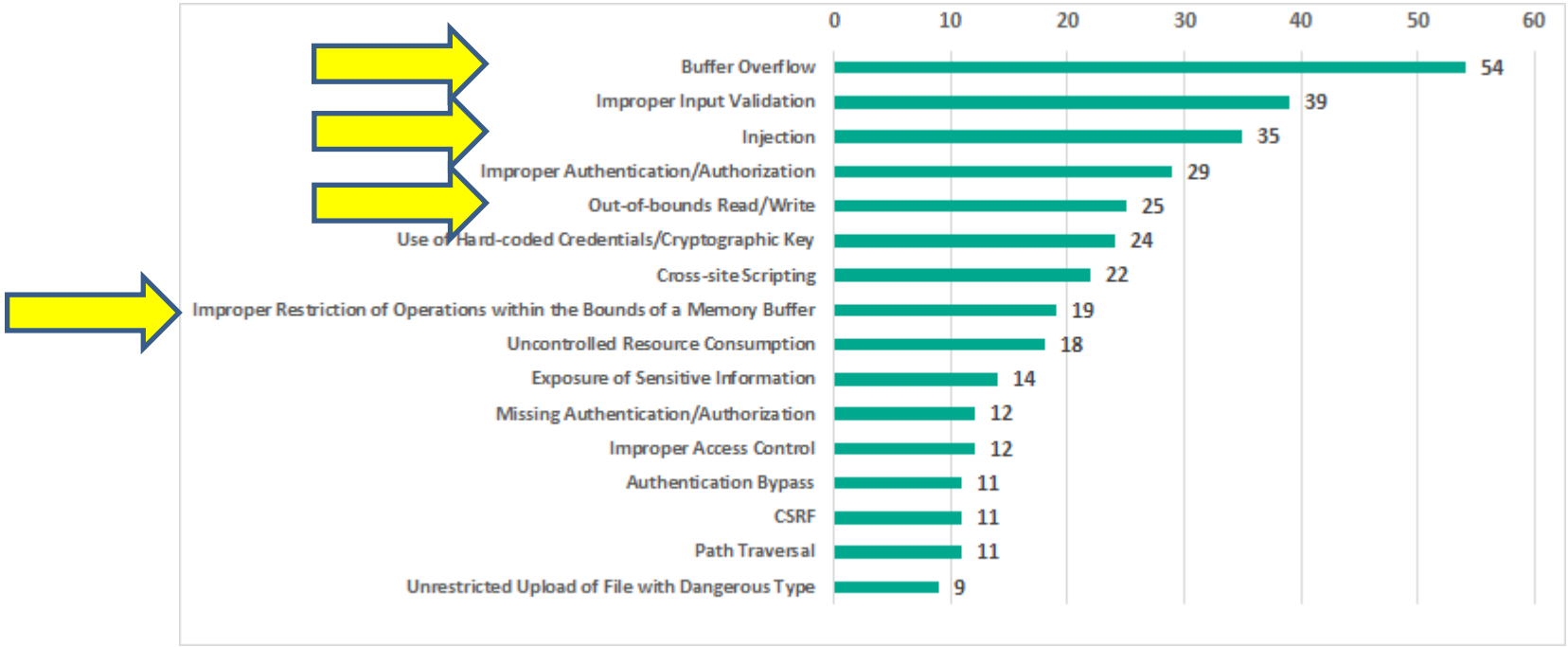
- Control panel also ran outdated firmware (previously found HTTP Header Injection and cross-site scripting (XSS) flaws in an earlier version of the ski lift's HMI software)
- "We have done Internet-wide scanning for human-machine interfaces (HMIs) several times in the past…looking for specific vendor IDs."

Vulnerabilità ICS da considerare per il settore funiviario



(2019, Kaspersky ICS CERT)

Tipologia di vulnerabilità ICS da considerare per il settore funiviario



(2019, Kaspersky ICS CERT)

Protocols

The following protocols are some of the languages that the industrial control systems use to communicate across the Internet. Many of them were developed before the Internet became widely used, which is why Internet-accessible ICS devices dont always require authentication - it isnt part of the protocol!

Modbus

Modbus is a popular protocol for industrial control systems (ICS). It provides easy, raw access to the control system without requiring any authentication.

Explore Modbus

SIEMENS

S7 (S7 Communication) is a Siemens proprietary protocol that runs between programmable logic controllers (PLCs) of the Siemens S7 family.

Explore Siemens S7

dnp

DNP3 (Distributed Network Protocol) is a set of communications protocols used between components in process automation systems. Its main use is in utilities such as electric and water companies.

Explore DNP3

TOTAL RESULTS

434

TOP COUNTRIES

Italy	434

TOP CITIES

Ruoti	21
Rome	12
Catania	11
Turin	8
Valduggia	4

TOP ORGANIZATIONS

Telecom Italia Business	53
Wind Tre	28
Vodafone Italia DSL	22
Telecom Italia	22

89.189.44.160

ip.89.189.44.160.telemar.it

Telemar s.p.a.

Added on 2019-09-08 04:25:22 GMT

Italy, Piovene Rocchette

ics

```
Copyright: Original Siemens Equipment
PLC name: SIMATIC 300(1)
Module type: CPU 315-2 DP
Unknown (129): Boot Loader           A
Module: 6ES7 315-2AH14-0AB0  v.0.3
Basic Firmware: v.3.3.2
Module name: CPU 315-2 DP
Serial number of module: S C-B9TM15582011
Plant identification:
Basic Hardware: 6ES...
```

94.85.246.46

host46-246-static.85-94-b.business.telecomitalia.it

Telecom Italia Business

Added on 2019-09-08 02:23:21 GMT

Italy

ics

```
Copyright: Original Siemens Equipment
PLC name: S7300/ET200M station_1
Module type: CPU 314
Unknown (129): Boot Loader           A%
Module: 6ES7 314-1AG14-0AB0  v.0.5
Basic Firmware: v.3.3.10
Module name: PLC_1
Serial number of module: S C-ENUK40702014
Plant identification:
Basic Hardware: 6ES7 ...
```

SHODAN | Exploits

port:102 country:it simatic s7-300

TOTAL RESULTS

1

Siemens *Simatic S7-300*/400 - CPU START/STOP Module (Metasploit)

Dillon Beresford

remote 102

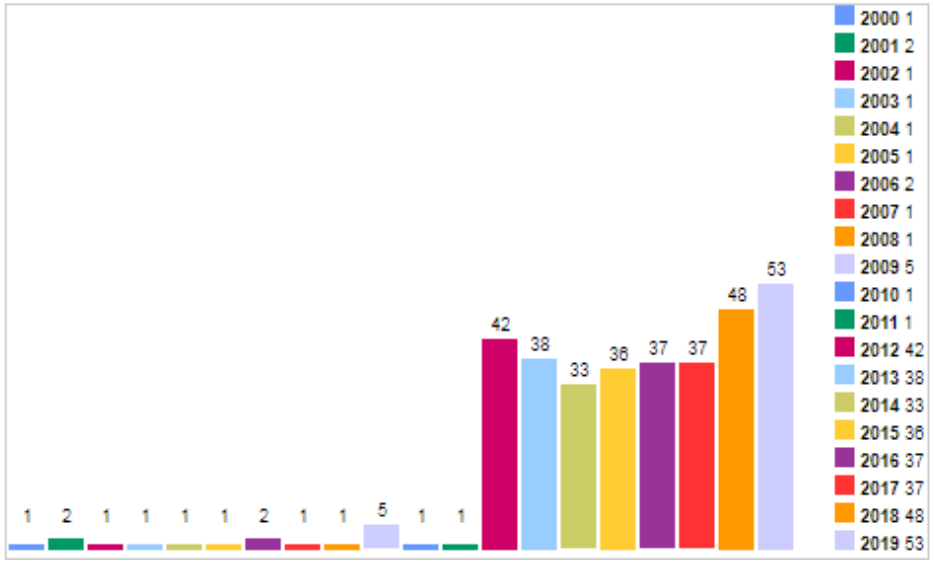
```
... # Exploit Title: Siemens Simatic S7 300/400 CPU command module
# Date: 7-13-2012
# Exploit Author: Dillon Beresford
# Vendor Homepage: http://www.siemens.com/
# Tested on: Siemens Simatic S7-300 PLC
# CVE : None

require 'msf/core'

class Metasploit3 < Msf::Auxiliary

        include Msf ...
```

CVE Details

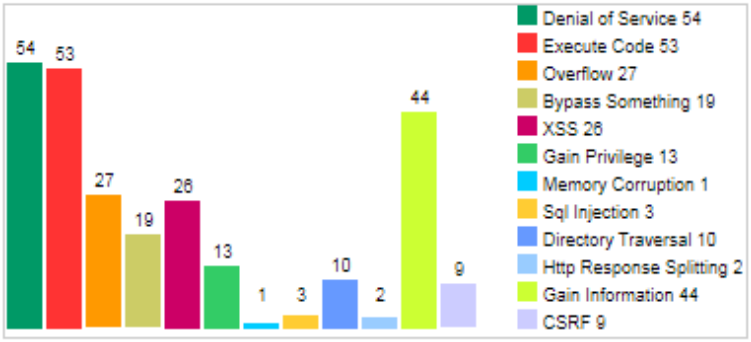
The ultimate security vulnerability datasource

Produttore leader del settore Vulnerabilità sistemi/prodotti ICS

Vulnerabilities By Year



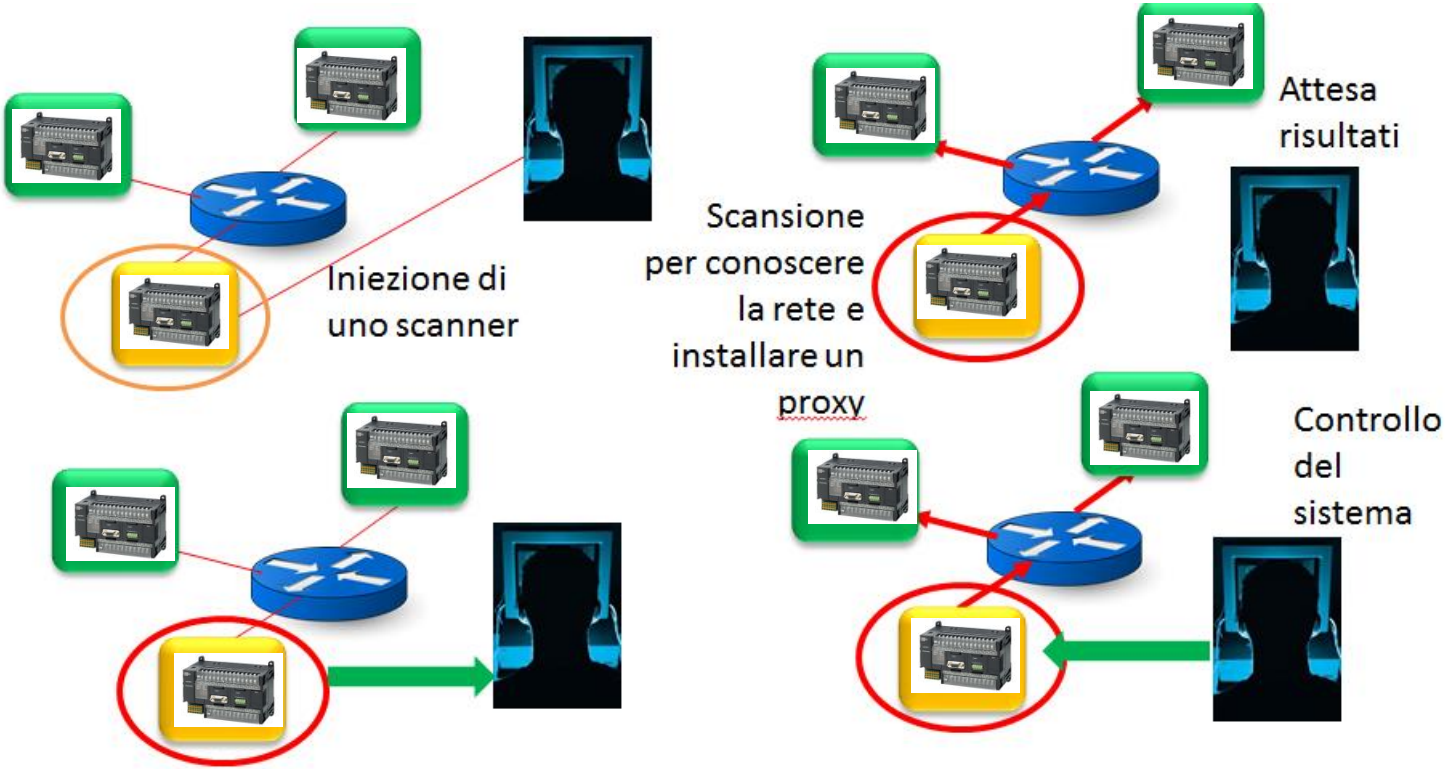
Vulnerabilities By Type



Vulnerabilità di una famiglia di PLC molto diffusa

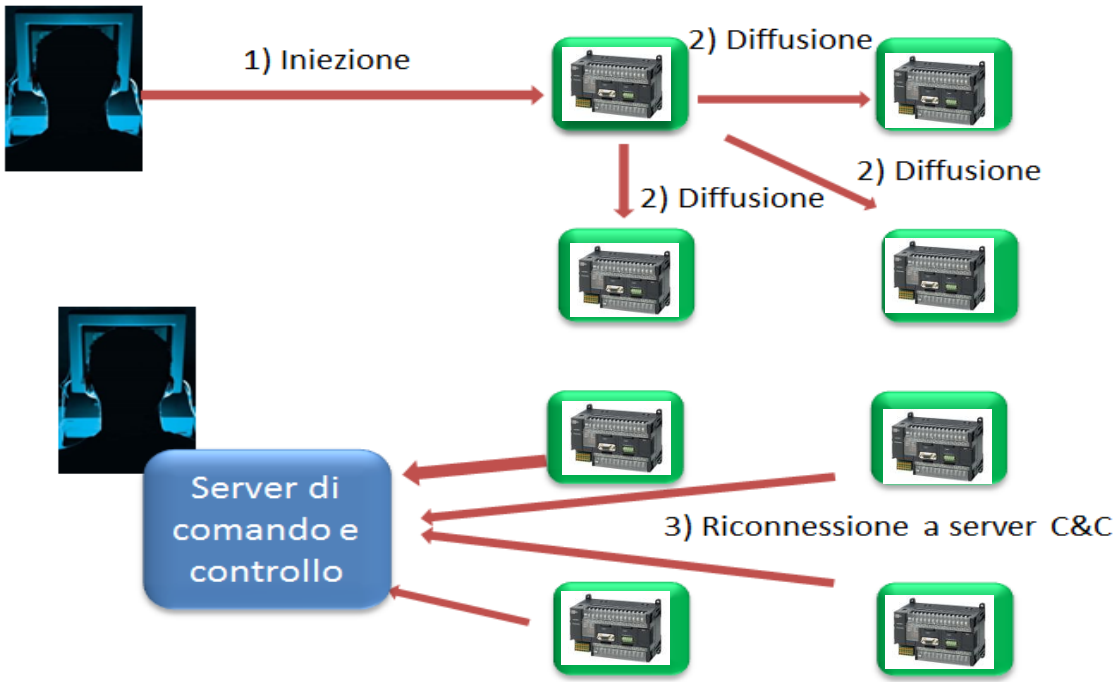
CVE-2018-4843	A vulnerability has been identified in SIMATIC CP 343-1 Advanced (All versions), SIM
CVE-2018-16561	A vulnerability has been identified in SIMATIC S7-300 CPUs (All versions < V3.X.16).
CVE-2017-2680	SIEMENS SIMATIC CP 343-1 Std, CP 343-1 Lean (All versions), SIMATIC CP 343-1 .
CVE-2016-8673	Cross-site request forgery (CSRF) vulnerability in the integrated web server on Sier
CVE-2016-8672	The integrated web server on Siemens SIMATIC CP 343-1 Advanced prior to versio
CVE-2016-3949	Siemens SIMATIC S7-300 Profinet-enabled CPU devices with firmware before 3.2.1
CVE-2015-2177	Siemens SIMATIC S7-300 CPU devices allow remote attackers to cause a denial of

PLC Back-Orifice



Johannes Klick, Stephan Lau, Daniel Marzin, Jan-Ole Malchow, Volker Roth - Internet-facing PLCs as a Network Backdoor – Freie Universitat Berlin - http://www.inf.fu-berlin.de/groups/ag-si/pub/plc_backdoor_spicy.pdf

«PLC Blaster» worm



Ralf Spenneberg, Maik Brüggemann, Hendrik Schwartke -PLC Blaster A Worm Living in PLC - https://www.blackhat.com/docs/us-16/materials/us-16-Spenneberg-PLC-Blaster-A-Worm-Living-Solely-In-The-PLC-wp.pdf

Attacco a PROFInet

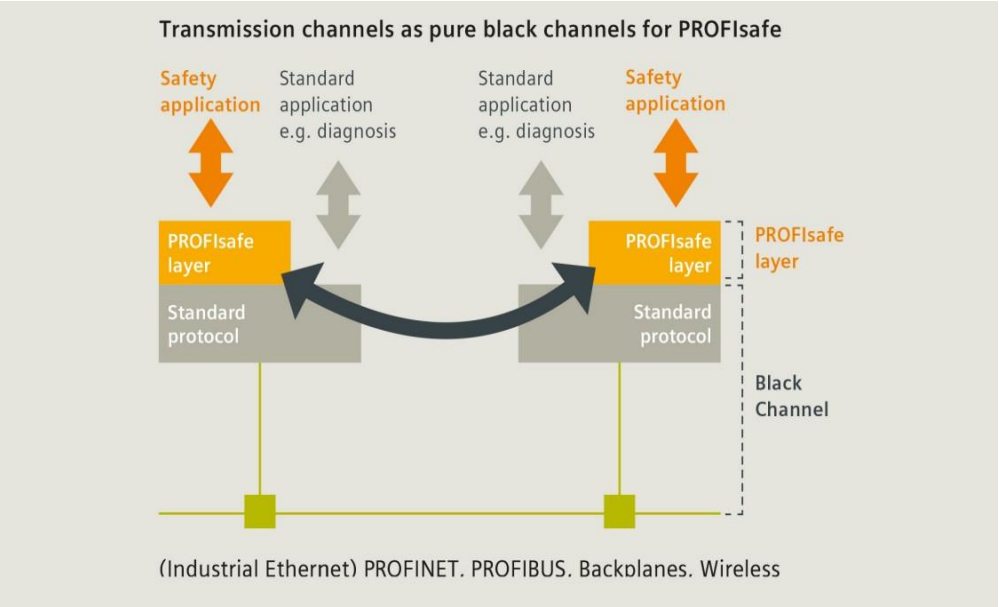
- Man-in-the-middle su reti “switched”
- Tecnica di attacco “storica” (v. ettercap)
- MAC address spoofing e corruzione della tabella “porta-mac address” dello switch.

- Invio di un frame con il MAC del dispositivo che si vuole impersonare connesso su un’altra porta per ottenere quelli a lui diretti ed instaurare una Application Relation “fasulla” tra controller e field device.

Baud, Michel & Felser, Max. (2006). Profinet IO-Device Emulator based on the Man-in-the-middle Attack. 437 - 440. 10.1109/ETFA.2006.355228.

ProfiSAFE

Basato sul principio del *black channel*, ampiamente diffuso in ambito industriale per l'implementazione di funzioni di sicurezza fino alla classe AK4 secondo EN 13243 e soddisfa i principi di confidentiality, integrity, authentication, availability . I terminali della comunicazione sono costituiti da PLC di sicurezza che le funzioni di sicurezza.



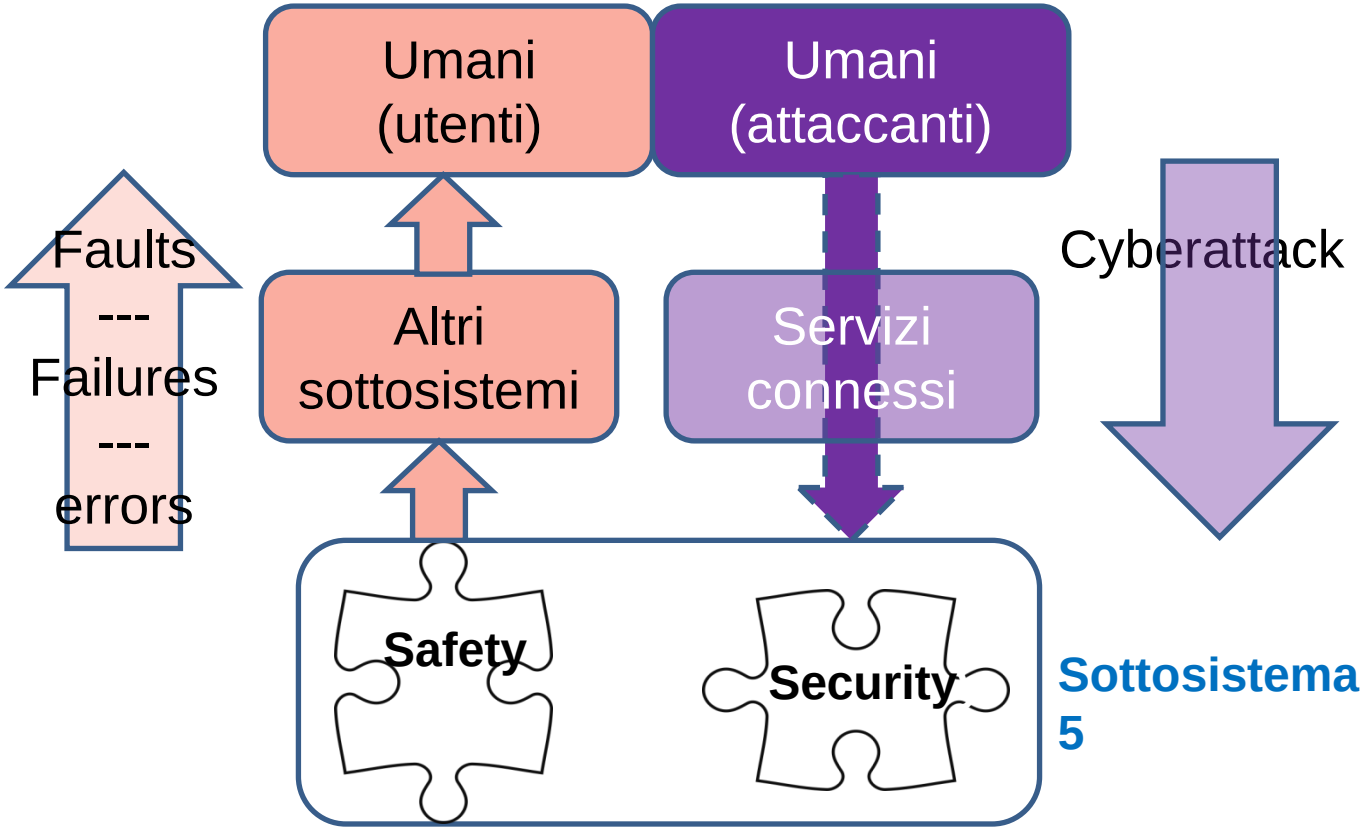
Attacco a ProfiSAFE

- Man-in-the-middle su “black channel”
- Modifica di dati “safety-related” non rilevata né dal trasmettitore né dal ricevitore, basata sulla possibilità di ricalcolare un codice di integrità di un pacchetto (“safety container”).
- Possibilità di attaccare implementazioni di PROFIsafe certificate SIL3 senza possibilità di rilevare l’attacco

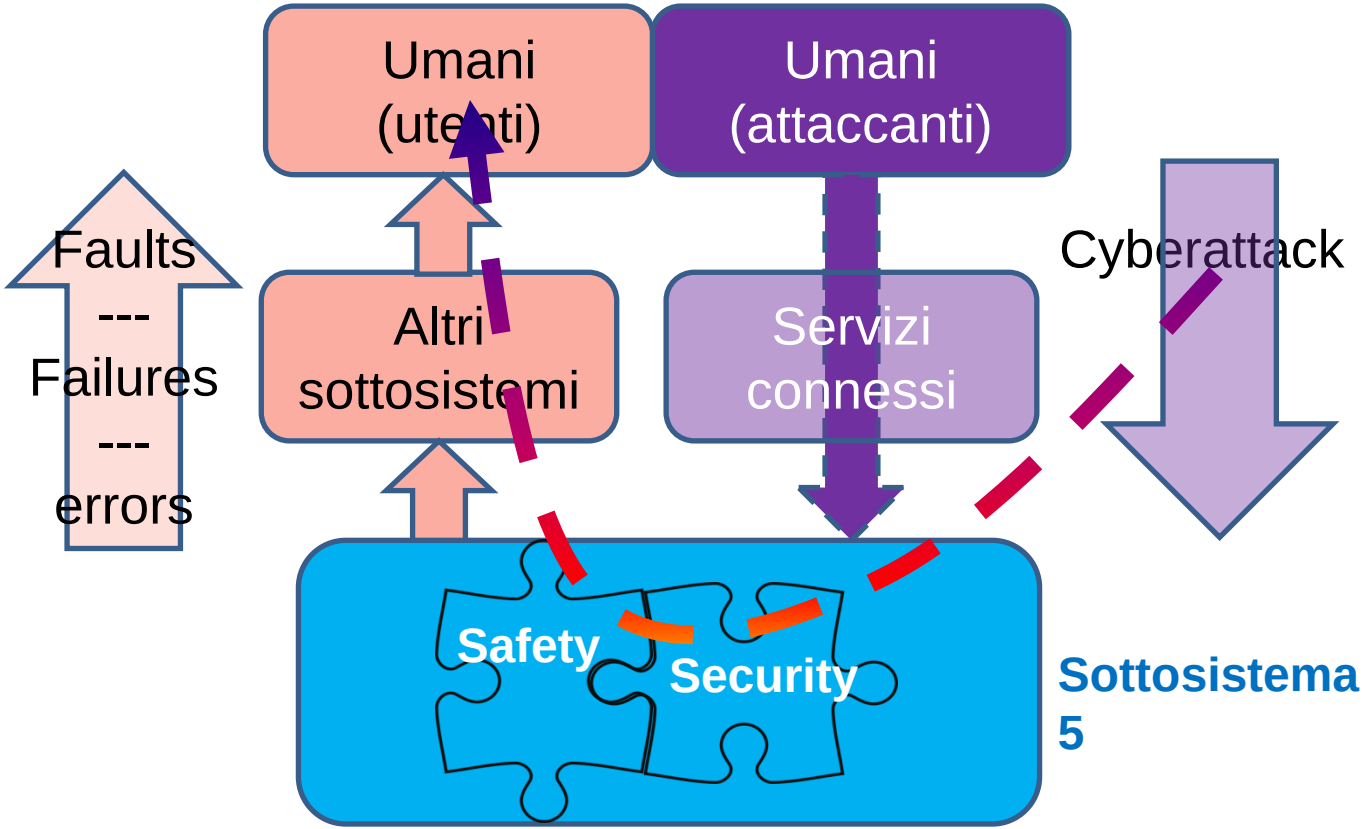
Akerberg, Johan & Björkman, Mats. (2009). Exploring network security in PROFIsafe. Proceedings of the 28th International Conference on Computer Safety, Reliability, and Security (SAFECOMP '09). 5775. 67-80. 10.1007/978-3-642-04468-7_7.

If it’s not SECURE it’s not SAFE!
(sicurezza delle funivie e sicurezza cibernetica: il perché di un approccio integrato)

Visione tradizionale di sicurezza funzionale e cybersecurity



Visione integrata tra sicurezza funzionale e cybersecurity



Per progettisti e systems integrators

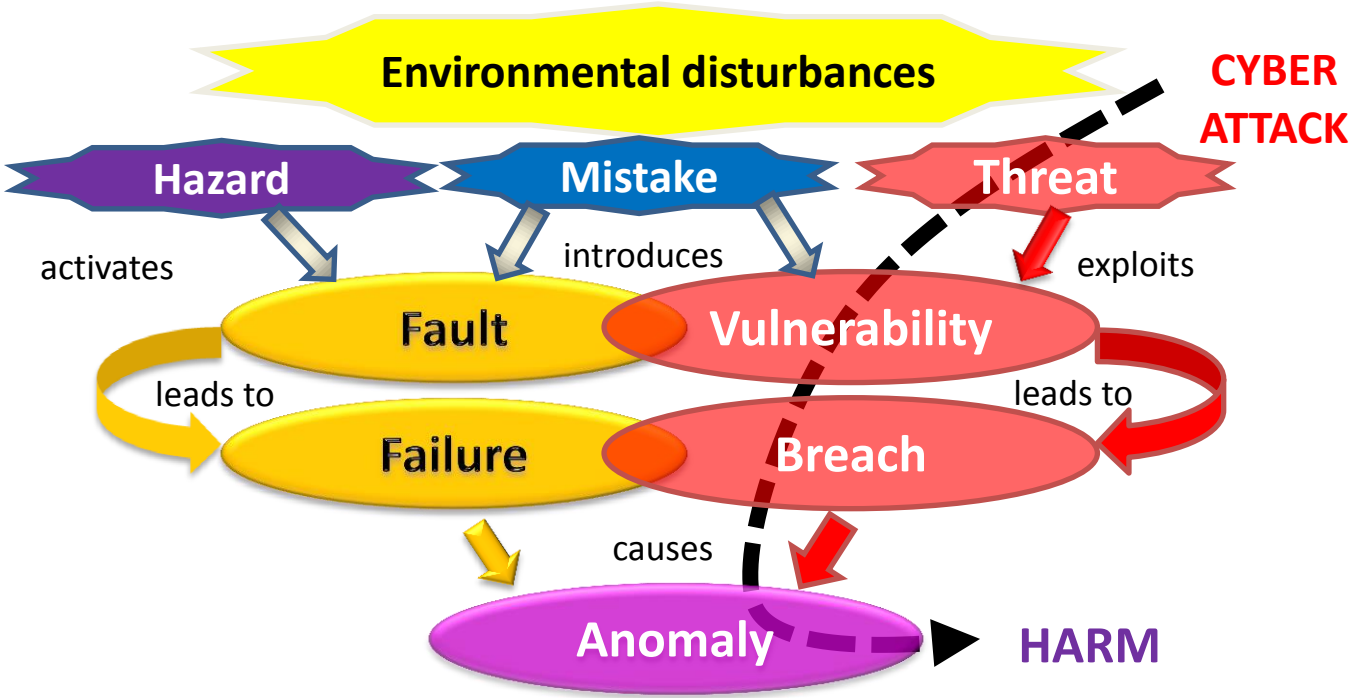
Analisi di “sicurezza” integrata: safety + cybersecurity

EN 13243:2015

4.2.1.1 The following events may lead to hazardous situations which can be avoided or limited by the safety requirements (*) of this standard:
a) accidental contact of a person with a live metallic component;
b) failure of electrical safety functions;
c) voltage drop or total loss of voltage;
d) occurrence of a short-circuit, earth fault or break;
e) failure of electrical or electronic components;
f) **foreseeable external influences,** in particular, environmental conditions and electromagnetic fields.

(*) non sono più sufficienti!

Uno scenario “aumentato”



Zalewski, J.; Buckley, I.A.; Czejdo, B.; Drager, S.; Kornecki, A.J.; Subramanian, N. A Framework for Measuring Security as a System Property in Cyberphysical Systems. Information 2016, 7, 33.

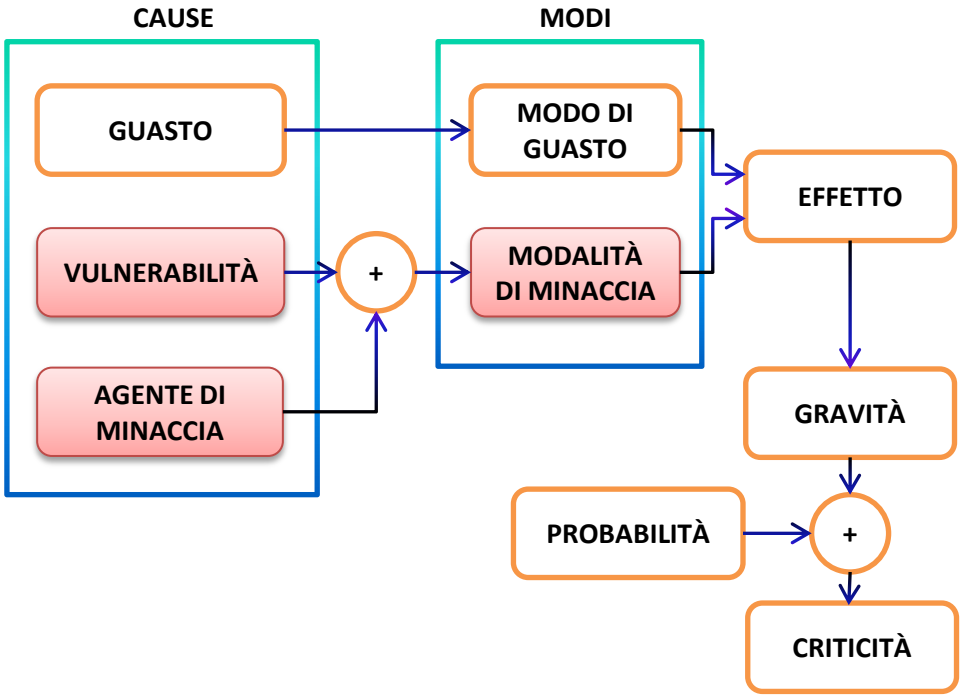
IEC 61508:2010

Subclause 7.4 Hazard and Risk Analysis Subclause 7.4.2.3

The hazards, hazardous events and hazardous situations of the EUC and the EUC control system shall be determined under all **reasonably foreseeable circumstances** (including fault conditions, reasonably foreseeable misuse and **malevolent or unauthorised action**). This shall include all relevant human factor issues, and shall give particular attention to abnormal or infrequent modes of operation of the EUC. If the hazard analysis identifies that malevolent or unauthorised action, constituting a **security threat, as being reasonably foreseeable, then a security threats analysis should be carried out**.

FMVEA

failure mode and vulnerability effect analysis



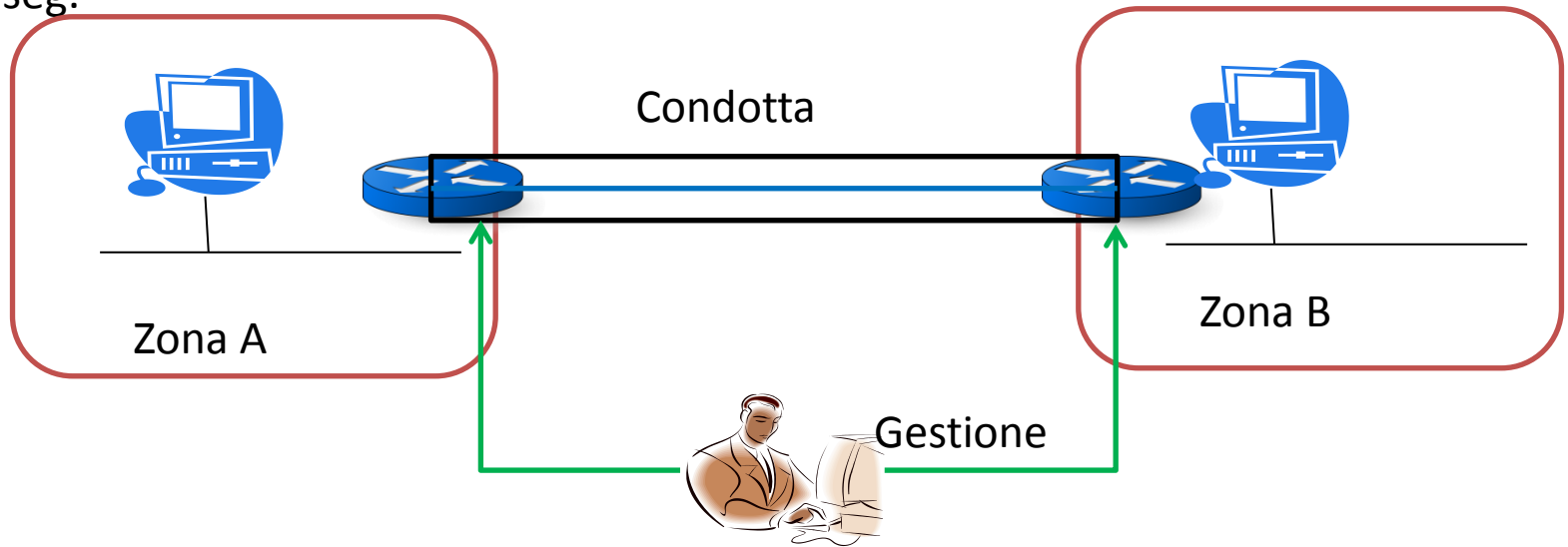
C.Schmittner, T, Gruber, P Puschner, E. Schoitsch – Security application of failure mode and effect analysis (FMEA) –SAFECOMP 2014 – Lecture notes on computer science 8666 – Settembre 2014 – ed. Springer.

IEC 62433

- Cybersecurity for operational technology in automation and control systems
- **Part 3-2** Security risk assessment for system design
- **Part 3-3** System security requirements and security levels

Procedura

- Si identificano nel sistema delle zone e dei “condotti” di collegamento tra esse;
- Le zone sono insiemi di dispositivi e sottosistemi attribuiti ad una stessa «funzione», mentre i condotti sono i canali di comunicazione tra le zone.
- Si analizzano per ciascuna zona e per ciascun condotto i rischi e le minacce (vulnerabiliy assessment)
- Scopo: per ogni zona/condotta devono essere valorizzati i requisiti fondamentali (FR) – pag. seg.



Requisiti fondamentali (FR)

1) IAC – Unauthorized access –Accesso non autorizzato
2) UC – Unauthorized use – Uso non autorizzato
3) SI – Manipulation of the system – Manipolazione del sistema
4) DC – Unauthorized disclosure of data – Pubblicazione non autorizzata di dati
5) RDF – Unwanted data flow – Flusso di dati indesiderato
6) TRE – No timely reaction to an event – Reazioni intempestive ad un evento
7) RA – Unavailability of resources- Indisponibilità di risorse

Confidentiality
Integrity
Availability

Procedura

Si verifica quali siano le caratteristiche (risorse, conoscenza, motivazione) che deve avere l'attaccante per poterle sfruttare. Quindi per ogni zona o condotto, il livello di protezione è **funzione delle caratteristiche dell'attaccante** ed è determinato utilizzando la tabella seguente.

Valore	2	3	4
Risorse (R)	Bassa	Media	Estesa
Conoscenza (K)	Comune	Specifica	Estesa
Motivazione (M)	Bassa	Media	Elevata

conseguentemente gli si assegna un "livello di protezione" (v. pag. seguente)

- PSL=f(R,K,M)
- SL = max(1, PSL – max (ORT, NAC, POT))
  - ORT – la locazione dell'attacco (locale 1, remoto 0)
  - NAC – la tracciabilità dell'attacco (no 0, si 1)
  - POT – il danno potenziale (grave 0, critico 1)

Livelli di protezione (security levels SL)

Misura il livello di confidenza che il sistema esente da vulnerabilità e funzioni secondo il comportamento atteso.

IEC 62443-3-3 (Industrial communication networks - Network and system security -Part 3-3: System security requirements and security levels) elenca, per ogni livello di protezione, quali siano i requisiti di protezione da adottare per conseguirlo.

Determinazione SL

- In funzione del livello di protezione si determina, sulla base della IEC 62443-3-3, l'insieme dei requisiti fondamentali che devono essere soddisfatti per ottenerlo;
- Sono vettori, costituiti da valori convenzionali di ogni FR
  - SL1 = (1,1,1,1,1,1,1)
  - SL2 = (2,2,2,1,2,2,1)
  - SL3 = (3,3,3,1,3,3,1)
  - SL4 = (4,4,4,1,4,4,1)
- si implementano i requisiti determinati al passo precedente secondo modalità specifiche per ogni requisito

Riepilogo

- Le potenzialità offerte dalla tecnologia per la gestione e l'esercizio degli impianti a fune costituiscono un elemento di complessità e presentano **un'altra faccia: nuove vulnerabilità**.
- L'approccio non è quello dell'IT-security in quanto un sistema di trasporto a fune è un **sistema cyber-fisico ed un eventuale attacco può compromettere l'incolumità degli utenti e degli operatori.**
- **A livello di progetto, di integrazione dei sistemi e di analisi di sicurezza è necessario tener conto *solidalmente* degli aspetti riguardanti la safety con quelli riguardanti la cybersecurity.**

Grazie per l’attenzione

Ing. Giorgio Pizzi

giorgio.pizzi@mit.gov.it