Immagine: Siemens

L'altra faccia della **FUNIVIA CONNESSA**

Ing. Giorgio Pizzi
USTIF di Roma

GIORNATA DI FORMAZIONE SIF VDA
Aosta , 20 settembre 2019

INNOVAZIONE DIGITALE E AUTOMAZIONE DELLE FUNIVIE

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, park-lot attack)
- Il fattore umano e quello gestionale sono un anello debole della catena

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.

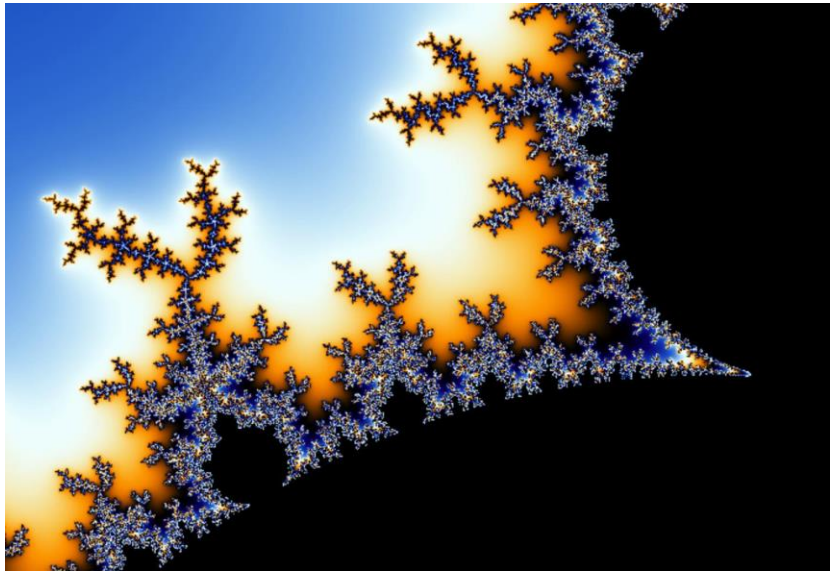
Since 2010 the USB Rubber Ducky has been a favorite among hackers, pentesters and IT pros. With its debut, keystroke injection attacks were invented – and since it has captured the imagination with its simple scripting language, formidable hardware, and covert design.

QTY

— 1 +

Aumenta la **SUPERFICIE DI ATTACCO**

- 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



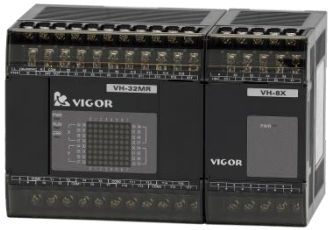
La funivia “connessa” è come un sistema informatico ?

Sistemi IT e sistemi embedded

Sistemi IT raccolgono ed elaborano dati per fornire conoscenza agli umani

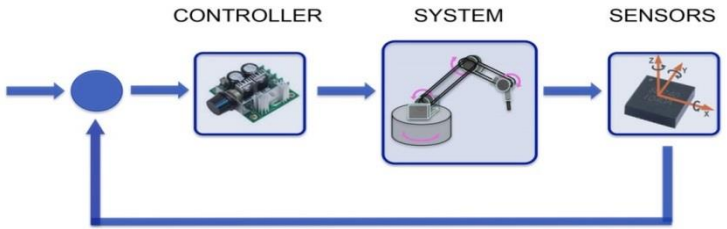
Gestionali aziendali per i servizi commerciali o per le informazioni ai passeggeri o agli operatori

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



Sistemi cyber-fisici

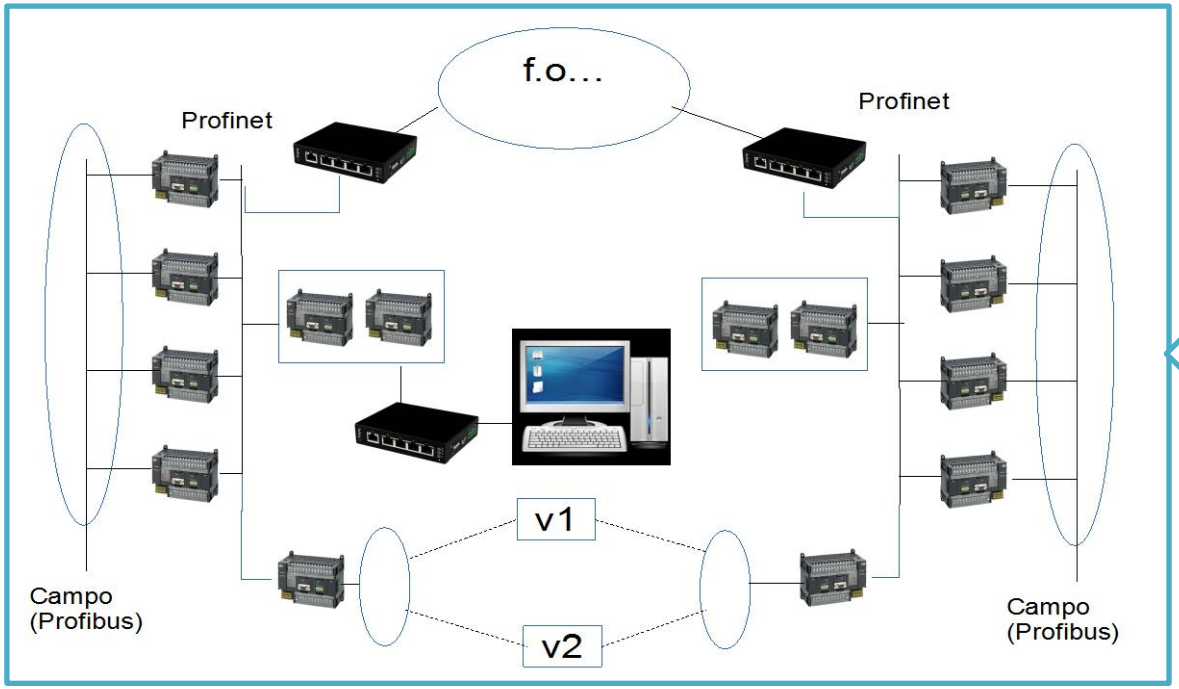
- I sistemi embedded integrati in una rete all'interno di un sistema complesso che interagisce con l'ambiente e con gli operatori o utenti umani danno vita ai sistemi "cyber-fisici" (CPS, cyber-physical systems)



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.**

Impianto a fune: sistema CYBER-FISICO

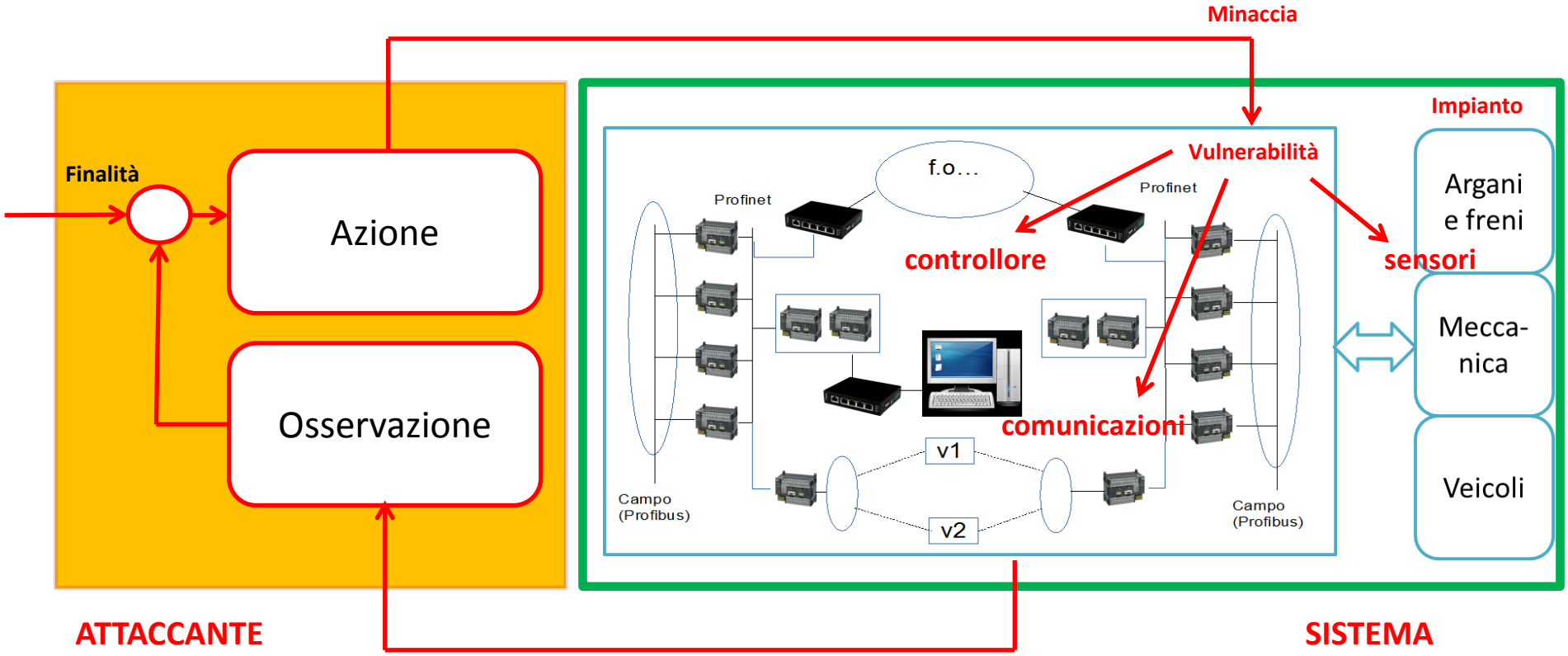


Argani e freni

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."

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 ...
```

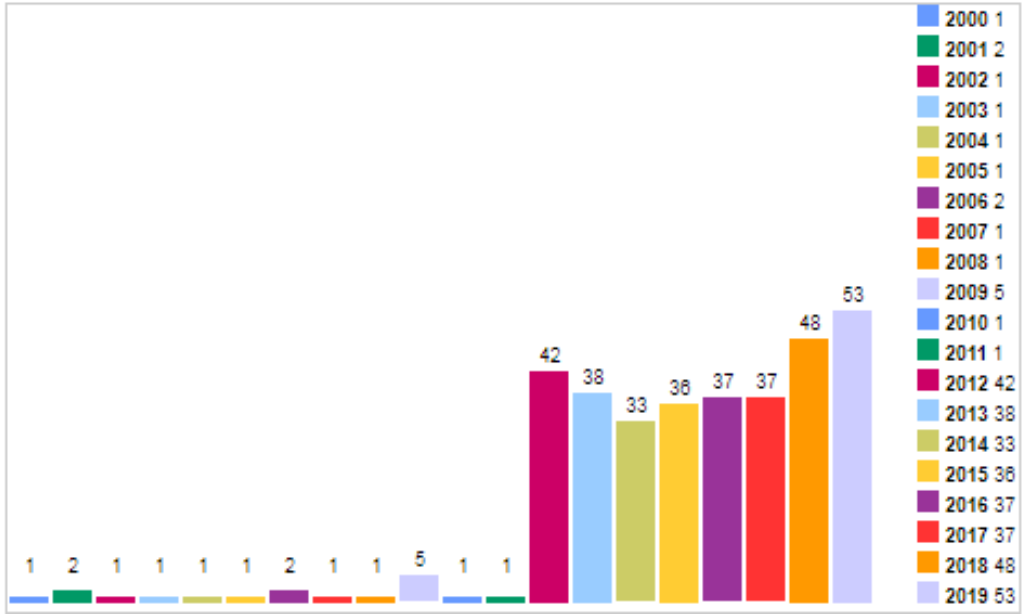
Fonte:

CVE Details

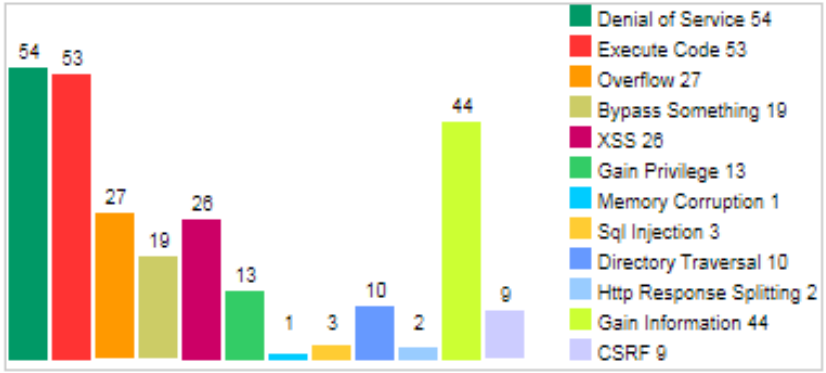
The ultimate security vulnerability datasource

Produttore leader del settore
Vulnerabilità sistemi/prodotti ICS

Vulnerabilities By Year



Vulnerabilities By Type



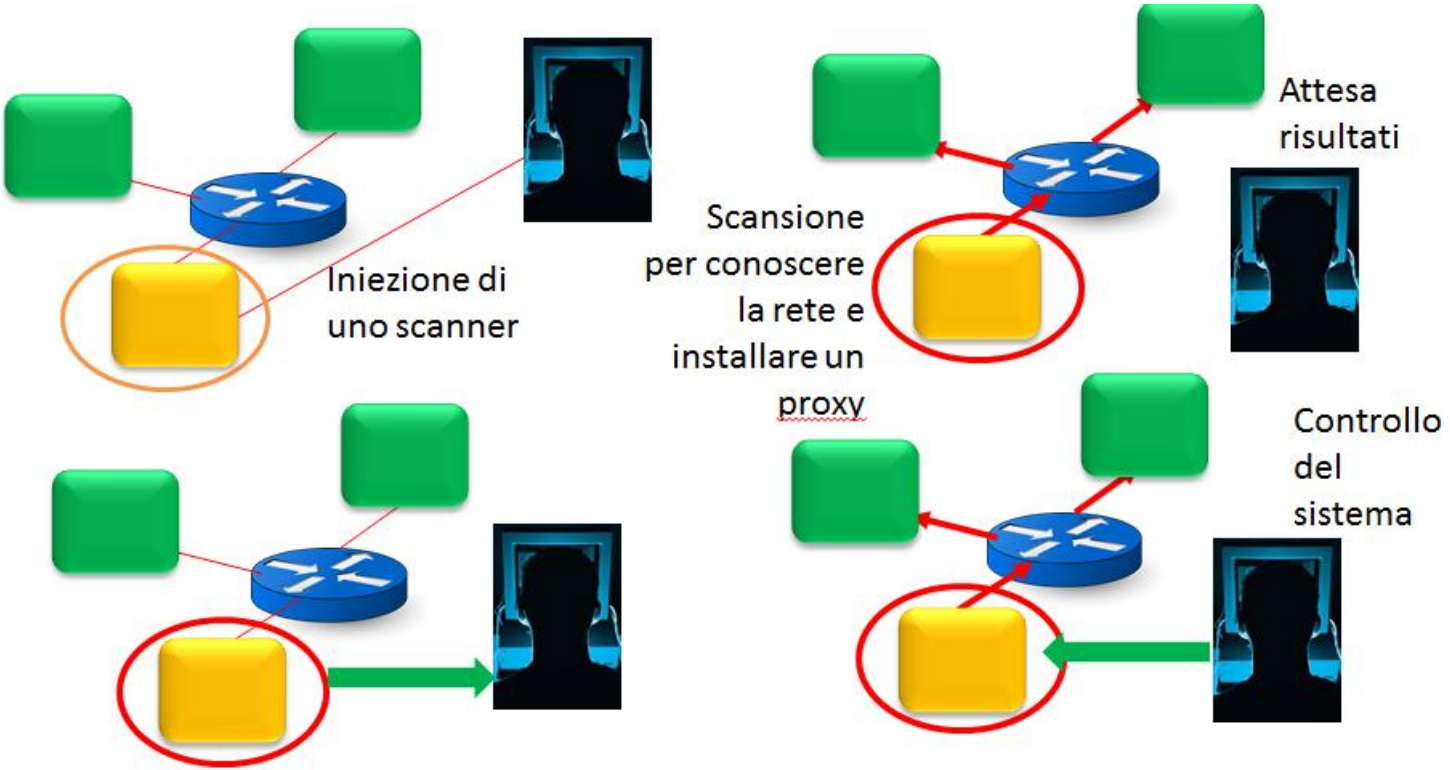
Fonte:

Common Vulnerabilities and Exposures

Vulnerabilità di una famiglia di PLC molto diffusa

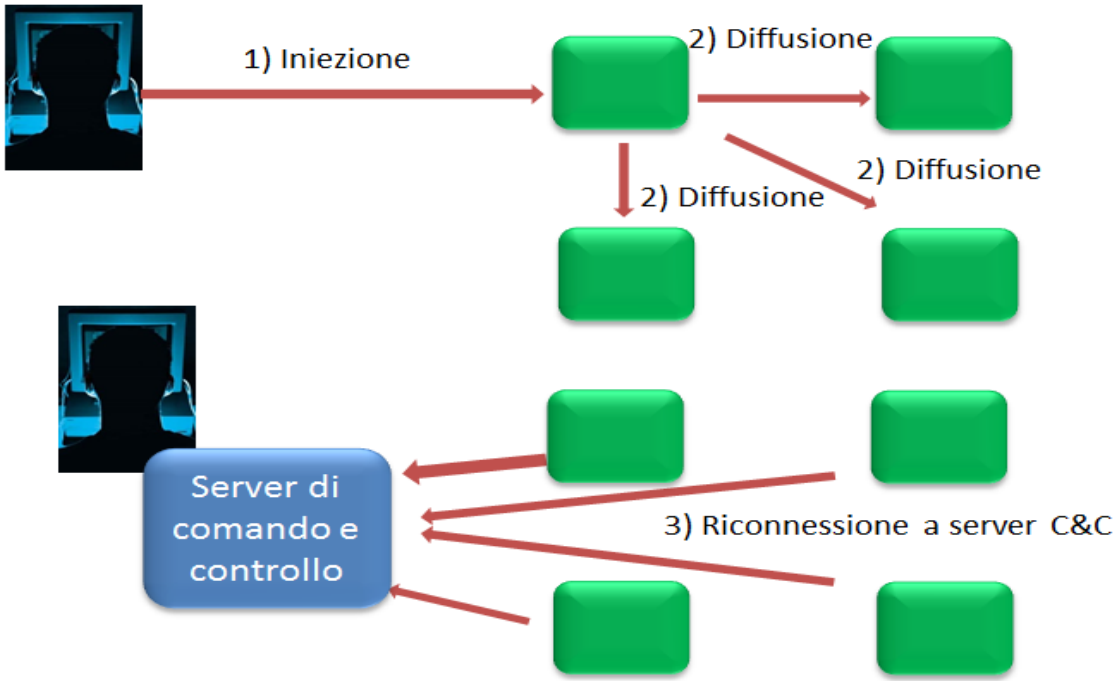
CVE-2018-4843	A vulnerability has been identified in SIMATIC CP 343-1 Advanced (All versions), SIM
CVE-2018-16561	A vulnerability has been identified in SIMATIC S7-300 CPUs (All versions < V3.X.16).
CVE-2017-2680	SIEMENS SIMATIC CP 343-1 Std, CP 343-1 Lean (All versions), SIMATIC CP 343-1 .
CVE-2016-8673	Cross-site request forgery (CSRF) vulnerability in the integrated web server on Sien
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.

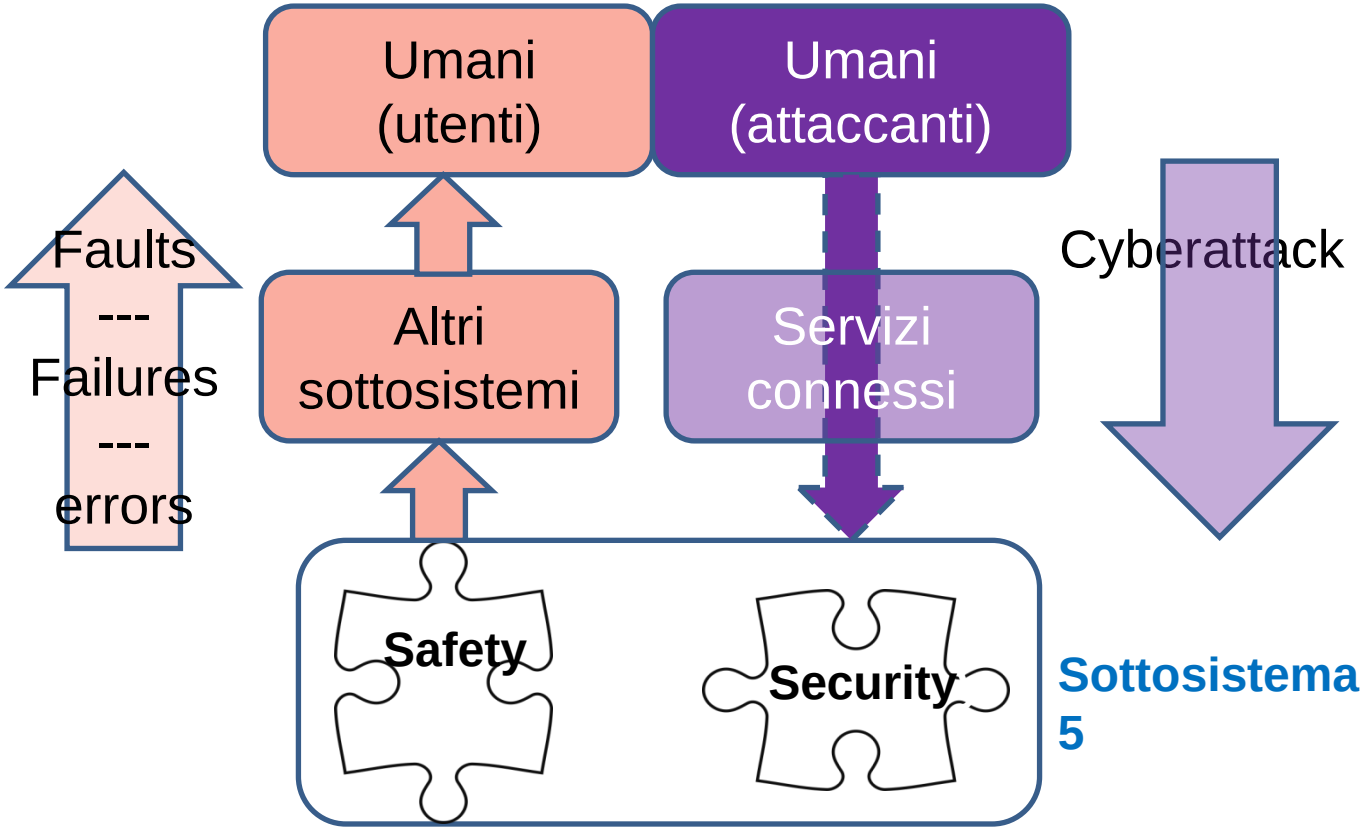
Attacco a PROFIsafe

- 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 detezione dell’attacco

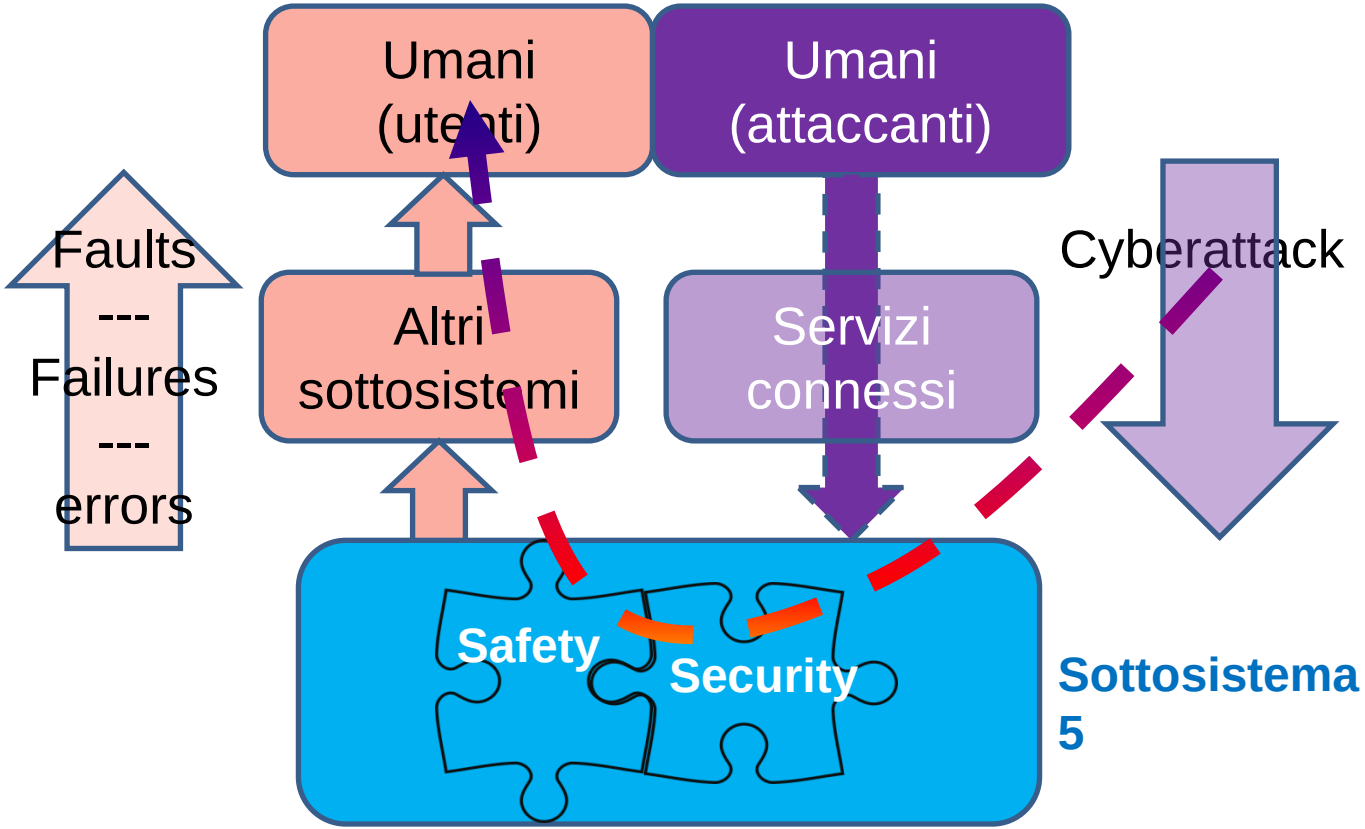
Akerberg, Johan & Björkman, Mats. (2009). Exploring network security in PROFIsafe. Proceedings of the 28th International Conference on Computer Safety, Reliability, and Security (SAFECOMP '09). 5775. 67-80. 10.1007/978-3-642-04468-7_7.

If it’s not SECURE it’s not SAFE!

Visione tradizionale di sicurezza funzionale e cybersecurity



Visione integrata tra sicurezza funzionale e cybersecurity



Cybersecurity is….

…the preservation of reliability, availability, maintenability and **safety** (RAMS) of the system

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;

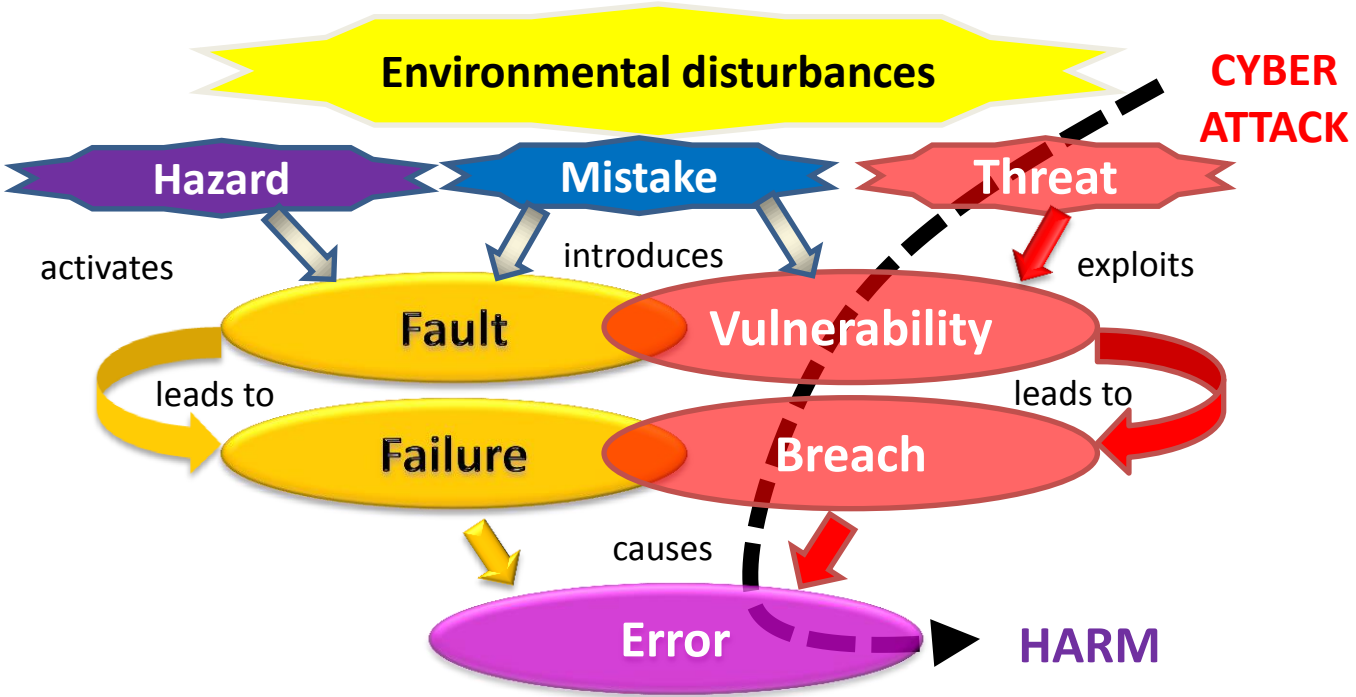
d) occurrence of a short-circuit, earth fault or break;

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.

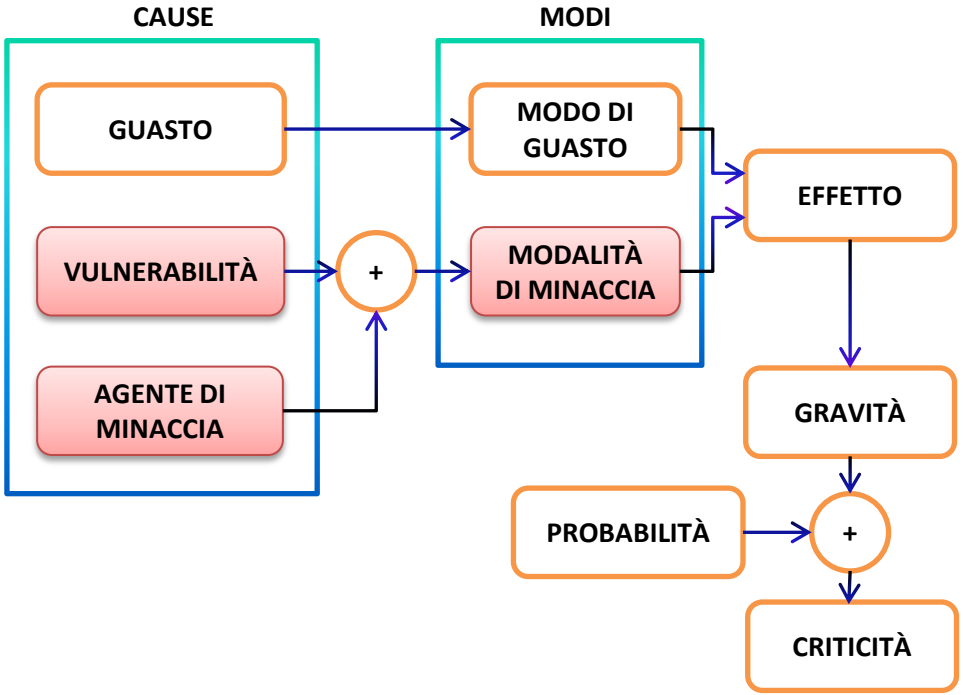
IEC 61508:2010

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.

Requisiti fondamentali (FR)

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

IEC 62433-3-3

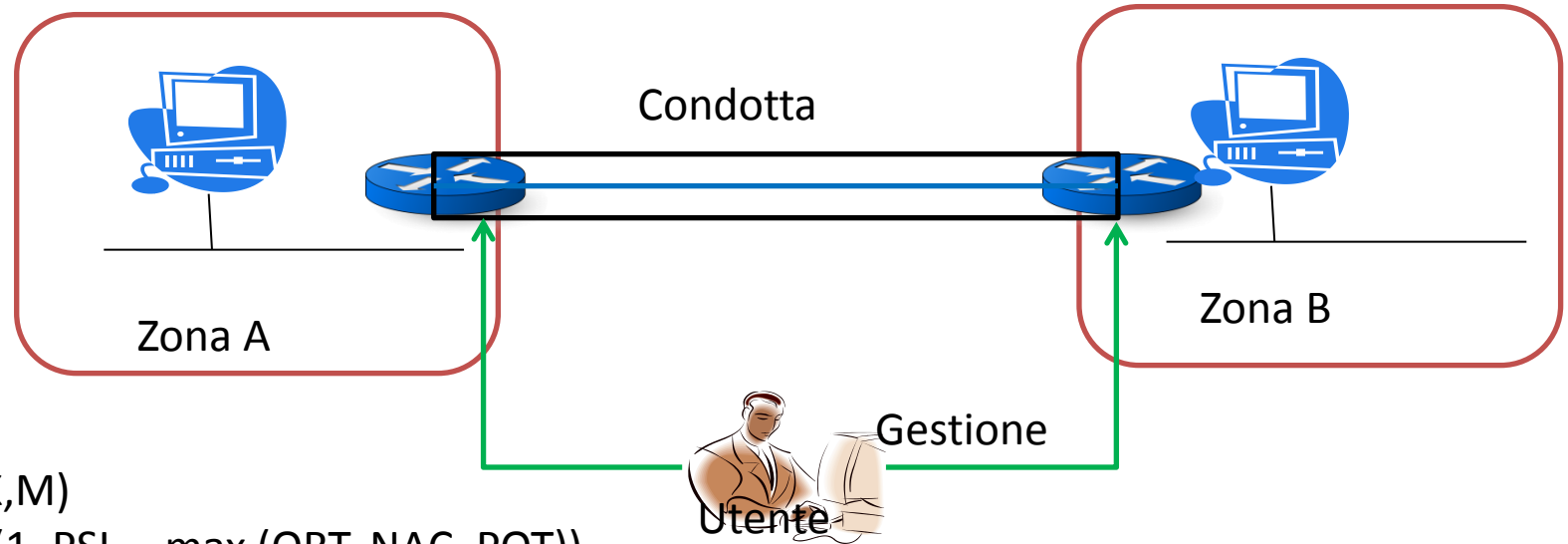
Livelli di protezione (security levels SL)

Misura livello confidenza su sistema esente da vulnerabilità e funzioni secondo il comportamento atteso. analogo a SIL. 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.

IEC 62433-3-3

Zone e condotti

La parte IT di un sistema viene suddivisa in zone e condotti (conduit). Le zone sono insiemi di dispositivi e sottosistemi che richiedono gli stessi requisiti di sicurezza, mentre i condotti sono i canali protetti di comunicazione tra le zone.



PSL=f(R,K,M)

SL = max(1, PSL – max (ORT, NAC, POT))

Riepilogo

- La funivia «connessa» rientra a pieno titolo nel paradigma dell'Internet of Things. Per questo è soggetta al paradosso del progresso, all'aumentare dei servizi offerti (digitali) presenta **un'altra faccia: nuove vulnerabilità**.
- Si sono già verificati attacchi «informatici» verso sistemi di trasporto a fune, ma una funivia non è un sistema informatico. E' prettamente un **sistema cyber-fisico ed un eventuale attacco può compromettere l'incolumità degli utenti e degli operatori.**
- Per le tecnologie (dispositivi, protocolli) utilizzati sono note numerose vulnerabilità, pertanto **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.**

Giorgio Pizzi
gpizzi@libero.it
giorgio.pizzi@mit.gov.it