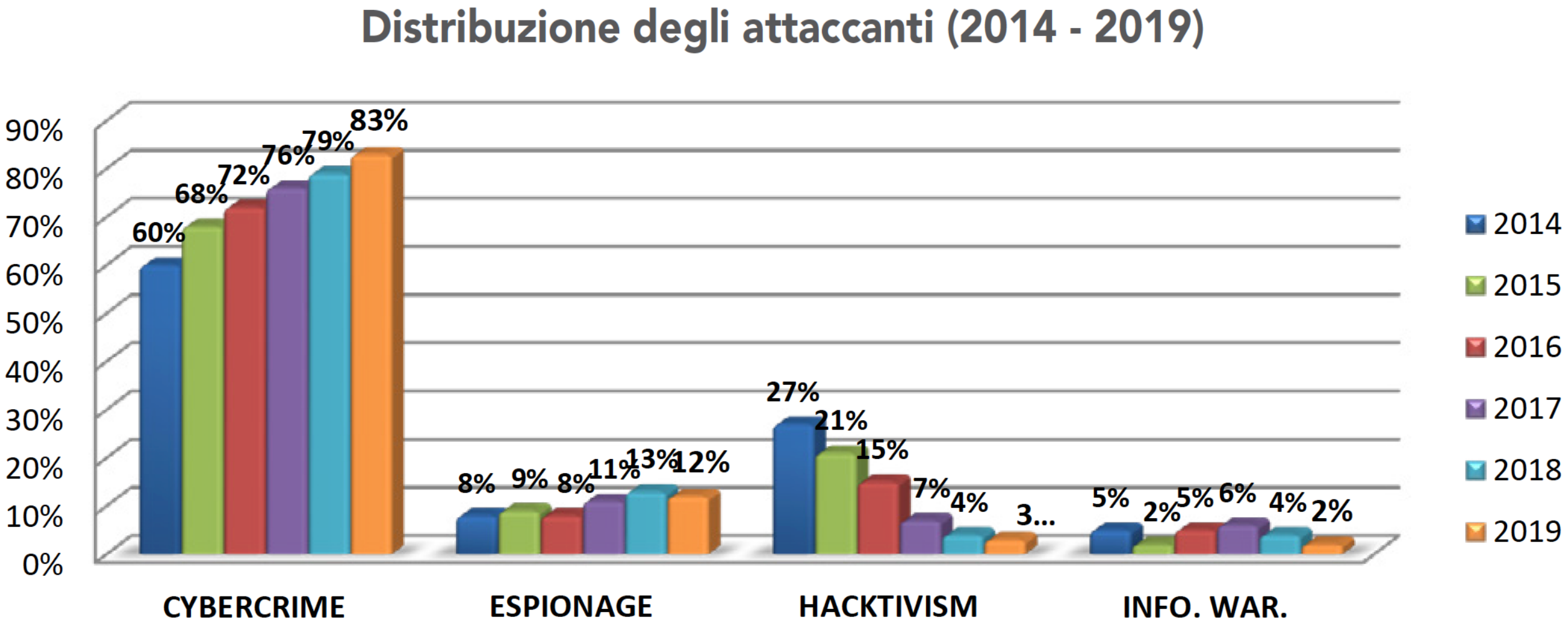
GLI EFFETTI DELLA EPIDEMIA COVID-19 SUL MERCATO DEL SOFTWARE INDUSTRIALE E DELL'AUTOMAZIONE (DALLE ANALISI DI ARC ADVISORY GROUP)

PROF. STEFANO PANZIERI

STEFANO.PANZIERI@UNIROMA3.IT



© Clusit - Rapporto 2020 sulla Sicurezza ICT in Italia

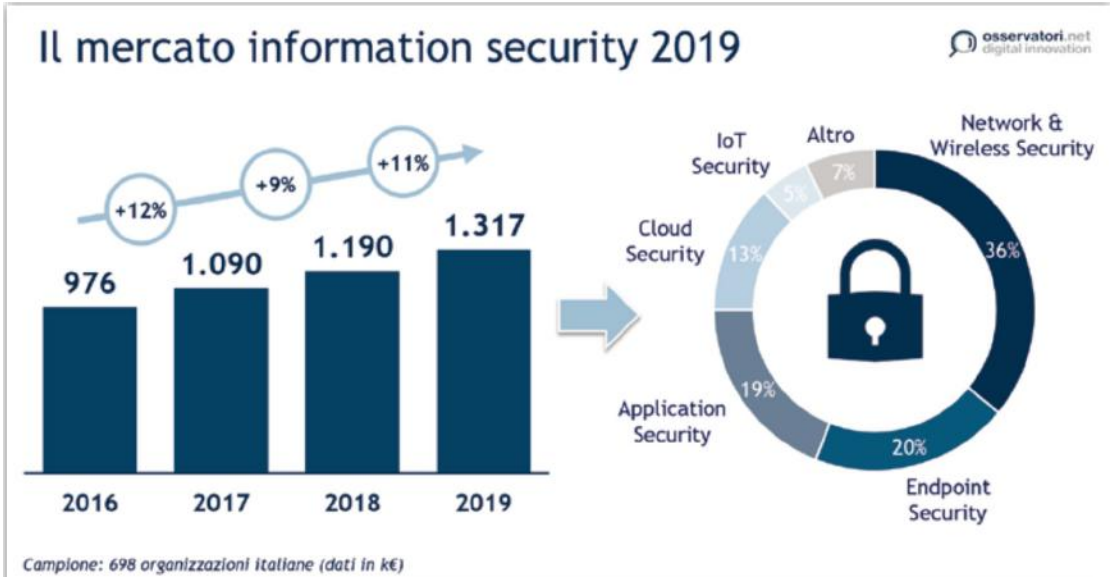
QUALI VITTIME?

VITTIME PER TIPOLOGIA	2014	2015	2016	2017	2018	2019	2019 su 2018	Trend
Gov - Mil - LEAs - Intel	213	223	220	179	252	203	-19.4%	↓
Multiple targets	-	-	49	222	304	395	29.9%	↑
Healthcare	32	36	73	80	159	186	17.0%	↑
Banking / Finance	50	64	105	117	156	141	-10.2%	↘
Online Services / Cloud	103	187	179	95	129	247	91.5%	↑
Research - Education	54	82	55	71	110	100	-8.3%	↘
Software / Hardware Vendor	44	55	56	68	109	83	-23.9%	↓
Entertainment / News	77	138	131	115	102	70	-31.4%	↓
Critical Infrastructures	13	33	38	40	57	37	-35.1%	↓
Hospitability	-	39	33	34	45	27	-40.0%	↓
GDO / Retail	20	17	29	24	39	50	28.2%	↑
Others	172	51	38	40	30	53	76.7%	↑

MA COME ANDAVA LA SPESA IN ITALIA FINO AL 2019?

- In Italia la spesa destinata alla cybersecurity ammontava nel 2017 a circa un miliardo di Euro, pari appena allo 0.05% [1] del PIL.
- Questo dato così basso era dovuto a diversi fattori quali: la mancanza di consapevolezza dei rischi e la carenza di competenza.
- L'introduzione di GDPR/NIS ha portato enti pubblici e società private a un maggiore investimento in questo delicato settore.

- Nel solo 2018 gli investimenti nella cyber security sono incrementati del 10,3% 2, facendo balzare l'Italia al quarto posto in Europa per spesa complessiva nella sicurezza dei dati.

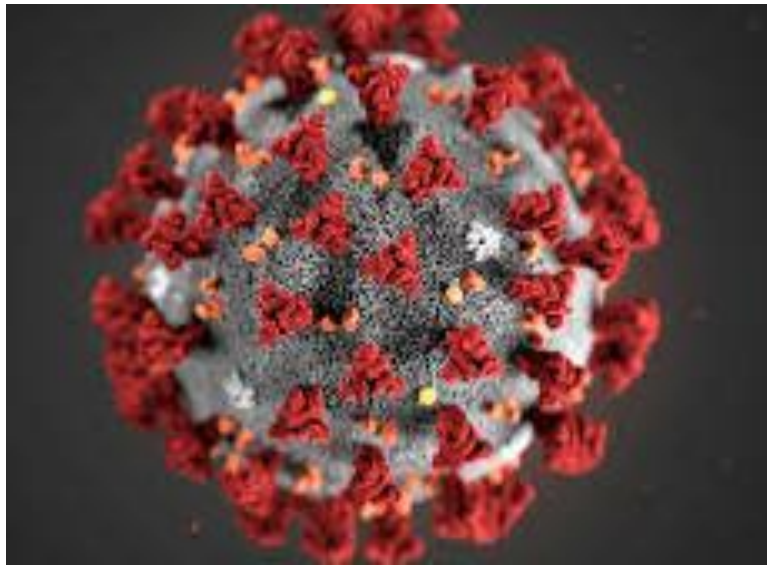


(1) Fonte: www.agendadigitale.eu

(2) Fonte: www.corrierecomunicazioni.it

PANDEMIA COVID 19 = TAGLI

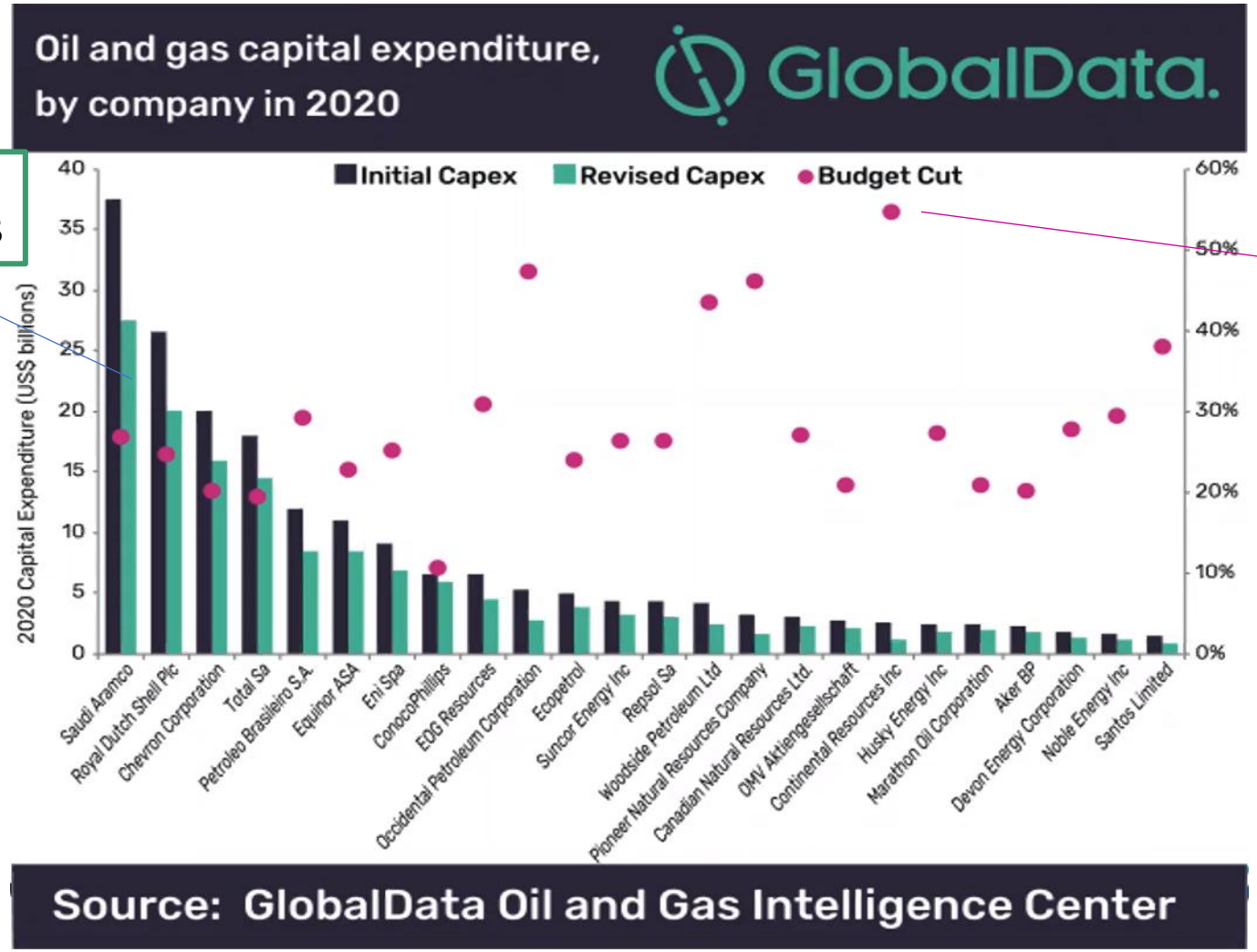
- I budget CAPEX delle maggiori aziende di processo sono stati tagliati
- I budget statali e regionali (in attesa del recovery fund e plan n.d.r.) soffrono per la riduzione delle imposte in entrata impattando sugli investimenti delle utilities
- La forza lavoro nel manifatturiero e nei trasporti si sta riducendo



ARC Advisory Group

UN ESEMPIO: BUGDET 2020 NEL SETTORE OIL & GAS

La spesa Iniziale
e Rivista in miliardi di US$



I Tagli in percentuale

ARC Advisory Group

COSA PEGGIORA LA SITUAZIONE?

ARC Advisory Group

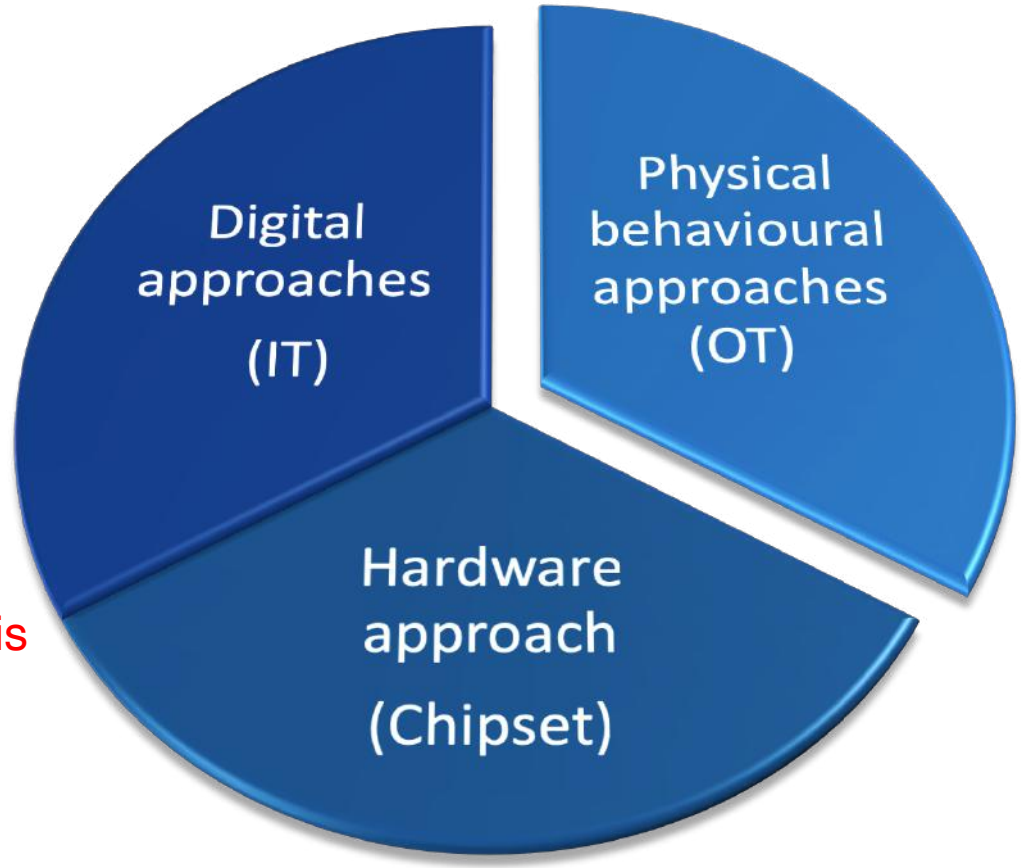
- In generale lavorare da casa crea problemi di security di livello elevato dovendo utilizzare connessioni remote non sempre protette
- Spostare la gestione e il controllo dei sistemi OT e IT a livello remoto richiede l'accesso a dati e dispositivi sensibili dall'esterno con una evidente maggiore esposizione a possibili incidenti.
- Si stanno sviluppando attacchi Cyber opportunistici legati alla pandemia

E DOPO LA PANDEMIA?

- Al temine della pandemia la gente ritornerà in ufficio e negli spazi di lavoro aziendali ma un gran numero di persone rimarrà in smart working
- La gestione e il controllo remoto degli asset OT continueranno ad aumentare
- Un sempre più piccolo numero di persone avrà bisogno di accedere a un sempre più ampio numero di asset e sistemi: meno persone vuole dire maggiore responsabilità
- Gli attacchi specificatamente mirati agli asset OT aumenteranno, in particolare dalle minacce avanzate e persistenti (APT)
- Le utilities implementeranno sempre maggiori soluzioni Smart (es. Grid) fortemente integrate
- Il volume dei dati si incrementerà esponenzialmente, includendo Cloud Computing, Edge Computing, Containers e molto altro.

SU COSA PUNTARE?

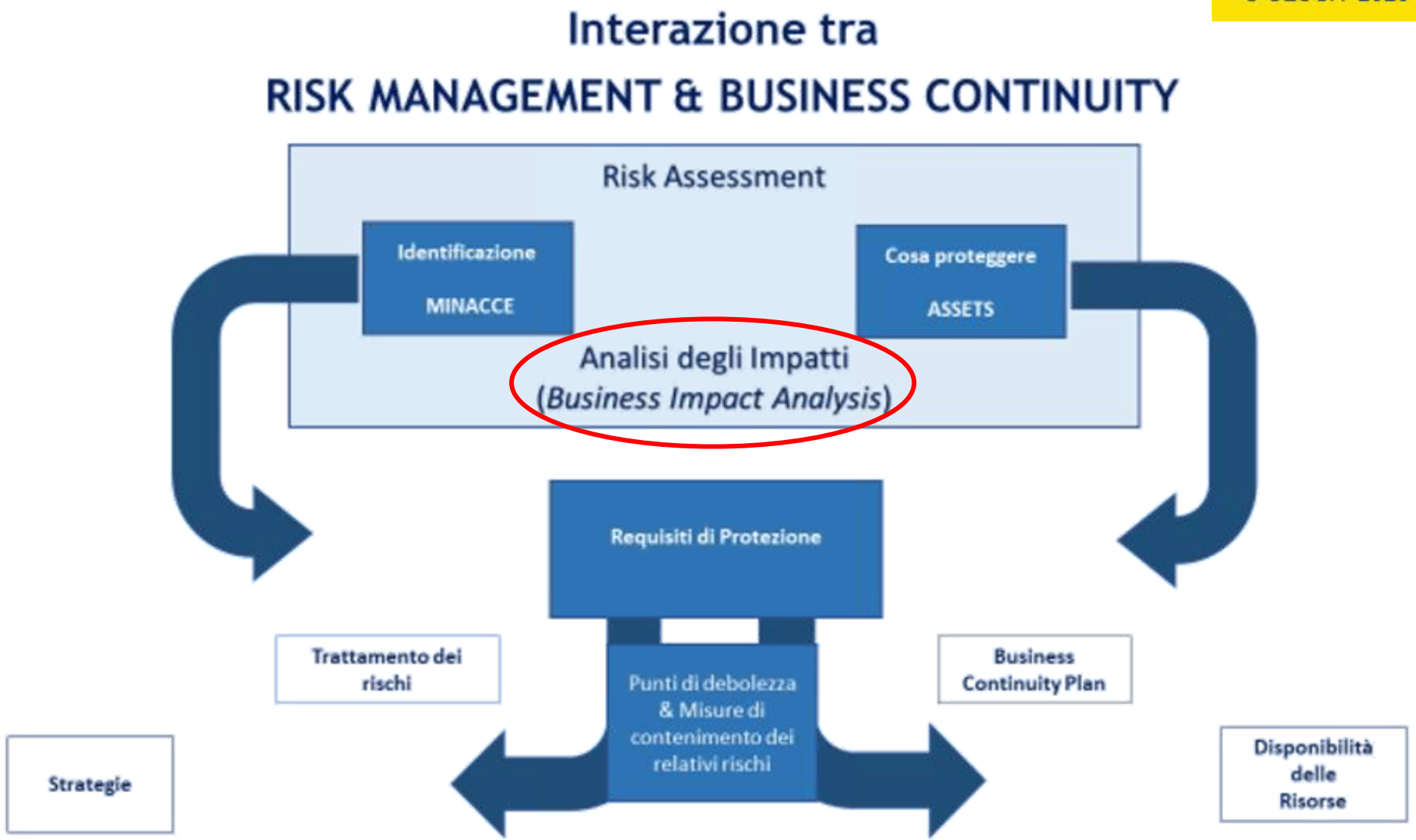
Data Protocol
Secure communication
Crypto
IDS
Antivirus
Industrial Firewall
Traffic Learning
SCADA protocol analysis
FIELDBUS protocol analysis



Process Model-based
Correlations between
• Physical laws
• Control laws
and control signals

Secure Life Cycle of System-On-Chip
Secure Embedded System Debug
Secure Processor Design
Design and Test of Secure IC

SENZA DIMENTICARE CHE...



La Formazione

ROMA TRE
UNIVERSITÀ DEGLI STUDI

iNGEGNERIA
DIPARTIMENTO DI ECCELLENZA

accenture

La cybersecurity per la protezione dei sistemi di controllo nell'industria 4.0 e nelle infrastrutture critiche

Master di II livello 2021

industrialsecurity.it

SIEMENS
Ingegno per la vita

Life Is On Schneider Electric

BECKHOFF

Rockwell Automation

GE Digital

ServiTecno

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

ANIE AUTOMAZIONE

ANIE FEDERAZIONE CONFINDUSTRIA

ANIPLA
A.N.I.P.L.A.
ASSOCIAZIONE NAZIONALE ITALIANA PER L'AUTOMAZIONE

Ordine degli Ingegneri della Provincia di Roma

UNINDUSTRIA
UNIONE DEGLI INDUSTRIALI E DELLE IMPRESE
ROMA • FROSINONE • LATINA • RIETI • VITERBO

sps ITALIA
smart production solutions

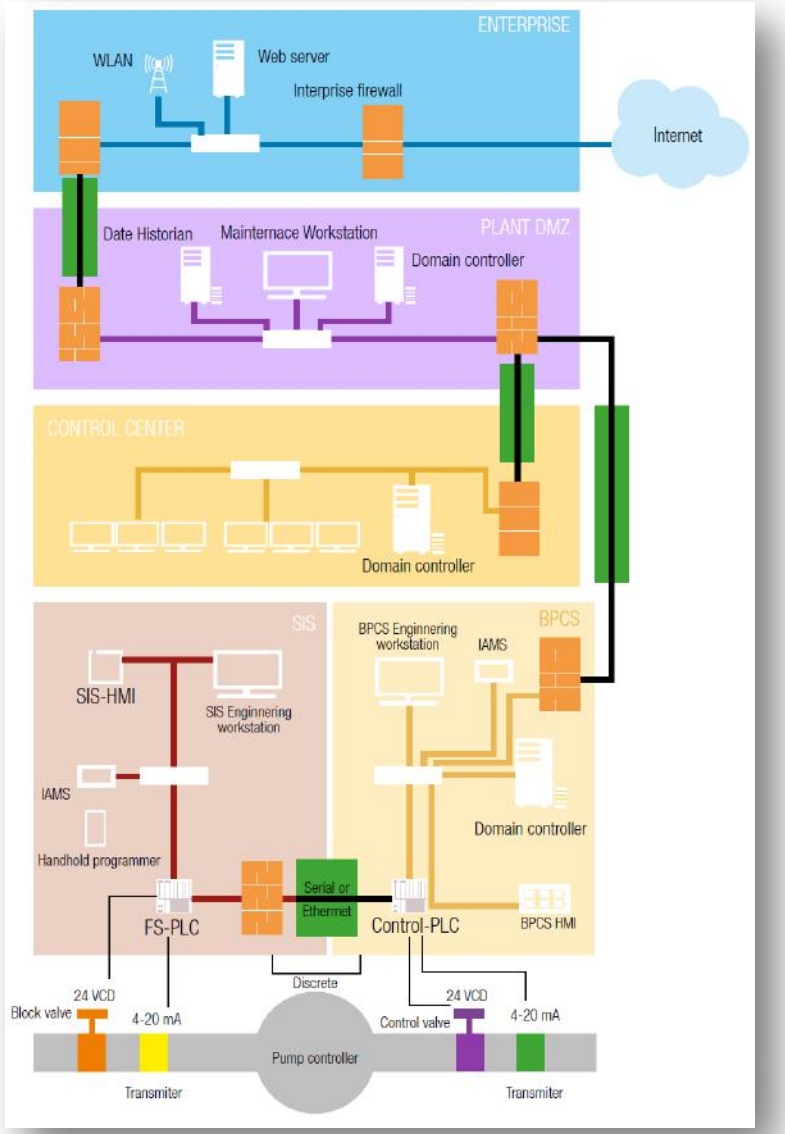
AIIC

Struttura

Modulo 1	• Industrial Control Systems (7 CFU, 49 ore)
Modulo 2	• Normative di Riferimento (10 CFU, 70 ore)
Modulo 3	• Technology Providers (15 CFU, 105 ore)
Modulo 4	• Risk Assessment for Industrial Control Systems and Critical Infrastructures (6 CFU, 42 ore)
Modulo 5	• Analisi del traffico e vulnerabilità (10 CFU, 70 ore)
Modulo 6	• Contromisure (12 CFU, 84 ore)

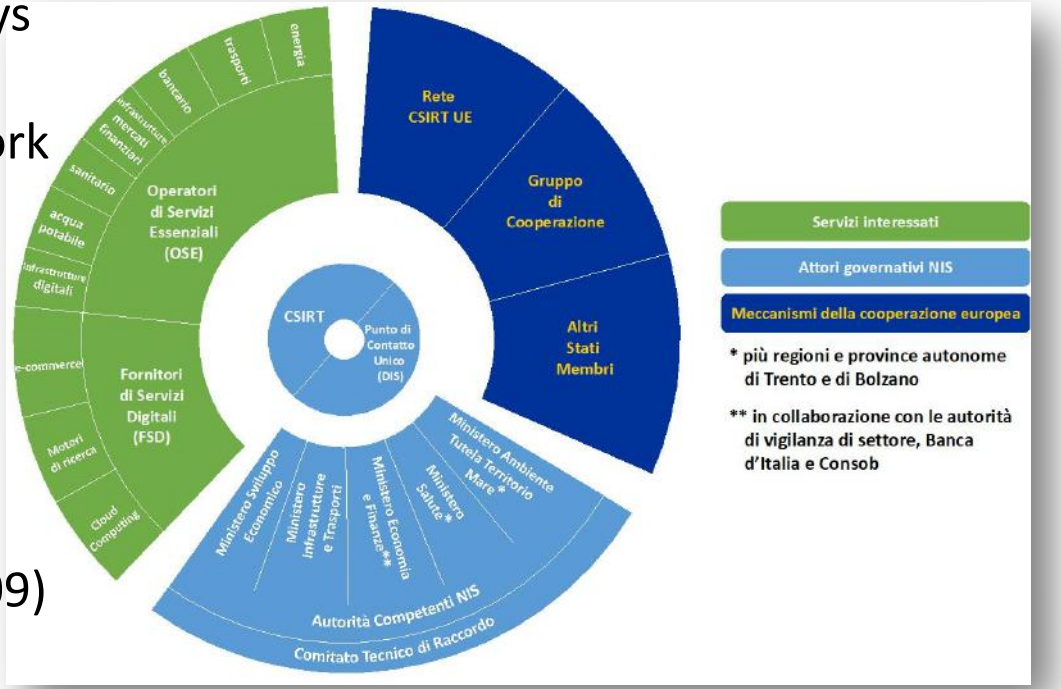
Modulo 1 - Industrial Control Systems

- Introduzione all'Automazione Industriale. Modelli di riferimento per le reti per l'automazione. Piramide CIM e ISA 95.
- PLC, architetture hardware. e software. Standard IEC 61131. Istruction List. Structured Text. LD (Ladder Diagram). FBD (Functional Block Diagram). SFC (Sequential Function Chart).
- Sensori e Attuatori Industriali. Motion Control
- Sistema SCADA: definizione, caratteristiche ed esempi. Base dati del processo, interfaccia operatore, Driver, Gestione allarmi, trend e rapporti, supporto alla manutenzione, sistema esperto, controllo statistico.
- Safety & Security, SIL, Piping and Instrument Diagram.
- Fieldbus e HART, Foundation Fieldbus, Profibus e sue versioni. Modbus e sue versioni, CANbus, Controlnet. DNP3 vs. IEC 60870, IEC 61850 per RTU. Ethernet Industriale, EtherCAT.
- Wireless Sensor Network Industriale. Industrial IoT. OPC UA, Time Sensitive Network. 5G per l'industria



Modulo 2 – Normative di Riferimento

- Introduzione alla Cybersecurity nel mondo SCADA/ICS; Settori interessati;
- Casi di studio: incidenti pubblici; Hacker's Profiling ed Agenti di Minaccia;
- Introduzione a scenari correlati; Dark Web e black forums; 0days e black markets; Cyber Threat Intelligence;
- NIST (National Institute of Standards and Technology) Framework for Improving Critical Infrastructure Cybersecurity»
- **Direttiva NIS** e gli adempimenti per le infrastrutture critiche
- STARTEGIA ITALIANA DI CYBER SECURITY, **Perimetro Digitale**
- I CERT e gli CSIRT nel contesto nazionale
- **Dlg 231** e reati informatici
- ISO/IEC 27001- ISO/IEC 27002 Annex Control
- NERC (North America Electric Reliability Council CIP-002/CIP-009)
- Evoluzione normativa in materia di protezione dei dati
- Anonimizzazione e pseudoanonimizzazione
- Linee guida per IoT - approcci **ENISA** e **NIST**



SIEMENS

Ingegno per la vita

BECKHOFF

Rockwell Automation

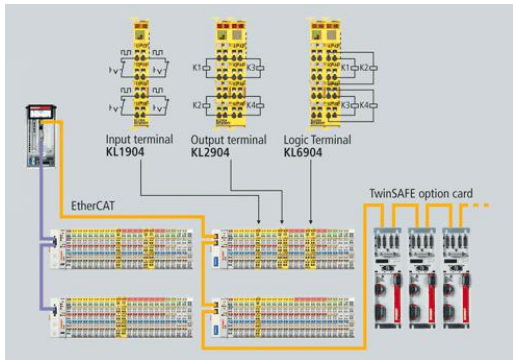
Life Is On | Schneider Electric

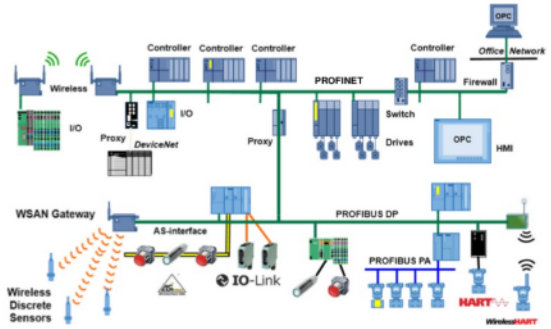
GE Digital

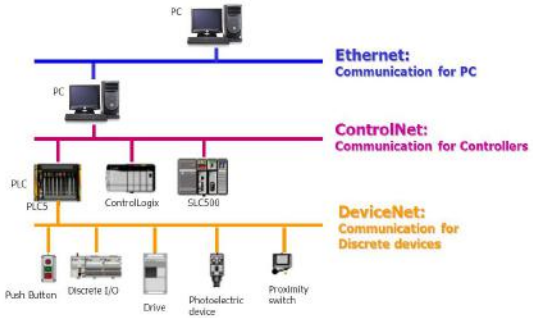
ServiTecno

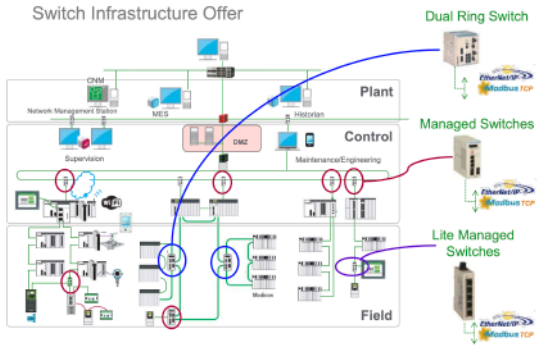
NOZOMI NETWORKS

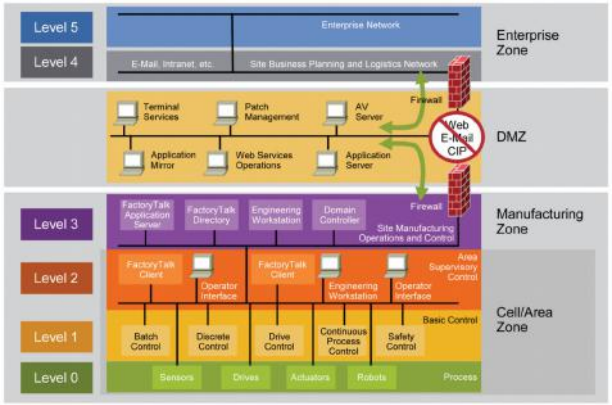
accenture

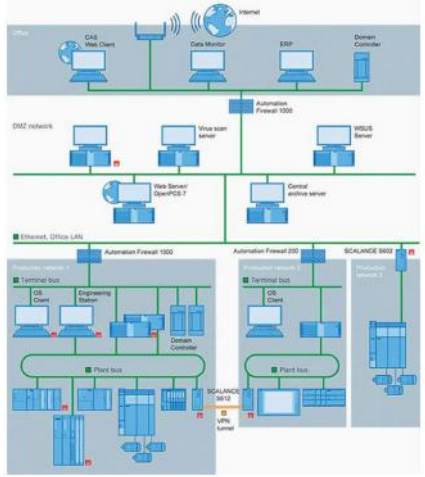






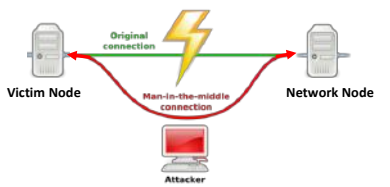




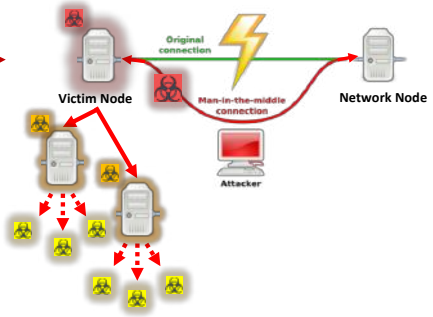


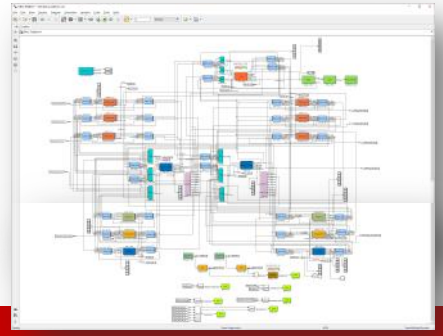
- Metodologie per l'analisi del rischio
- I modelli di enterprise risk management secondo gli standard ISO/IEC 27005:2011 e ISO 31000:2018
- Data Protection Impact Assessment (DPIA)
- Modellistica Interdipendenze
- Best Practices, OSSTMM (Open Source Security Testing Methodology Manual).
- ISECOM Proactive Security Square
- OWASP; Secure Coding; SLD; S-SLDC
- GAMP (ISPE) Pharma

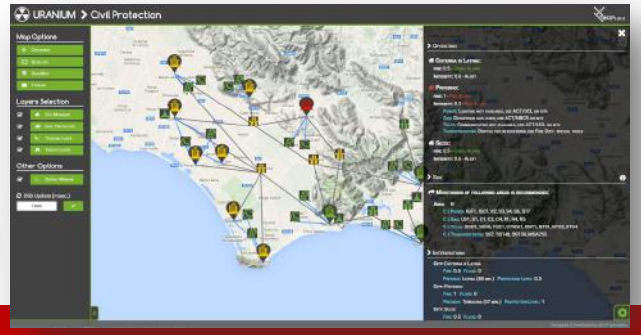
MITM – MAN IN THE MIDDLE

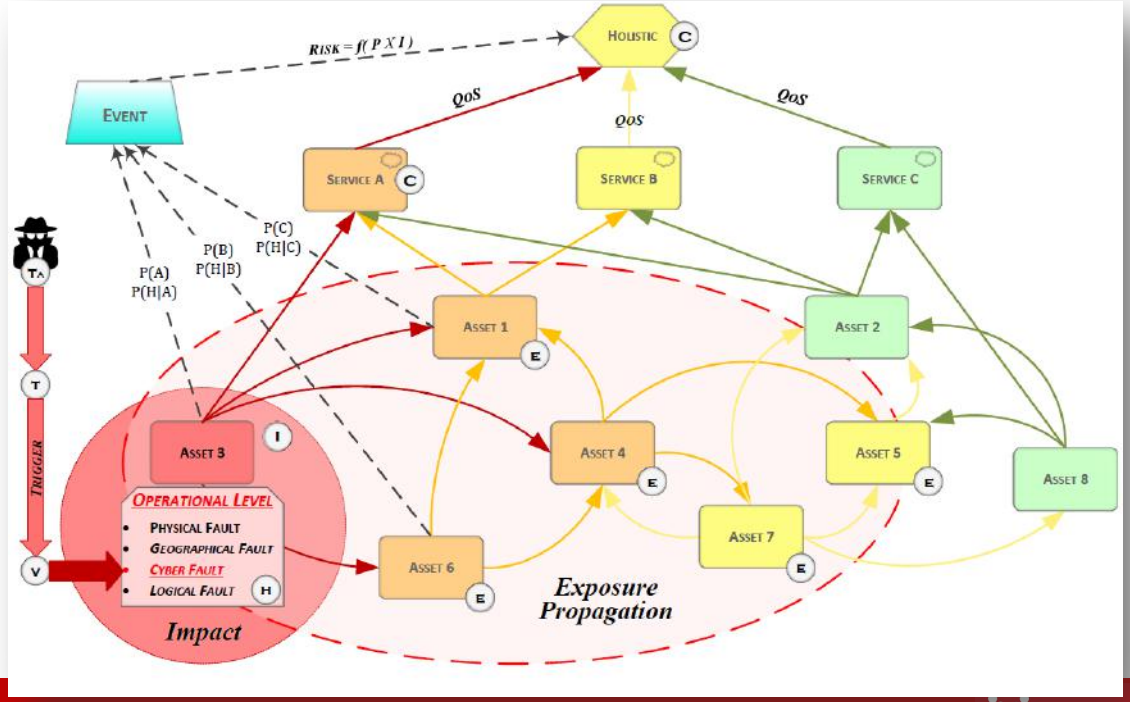


INFECTION ATTACK



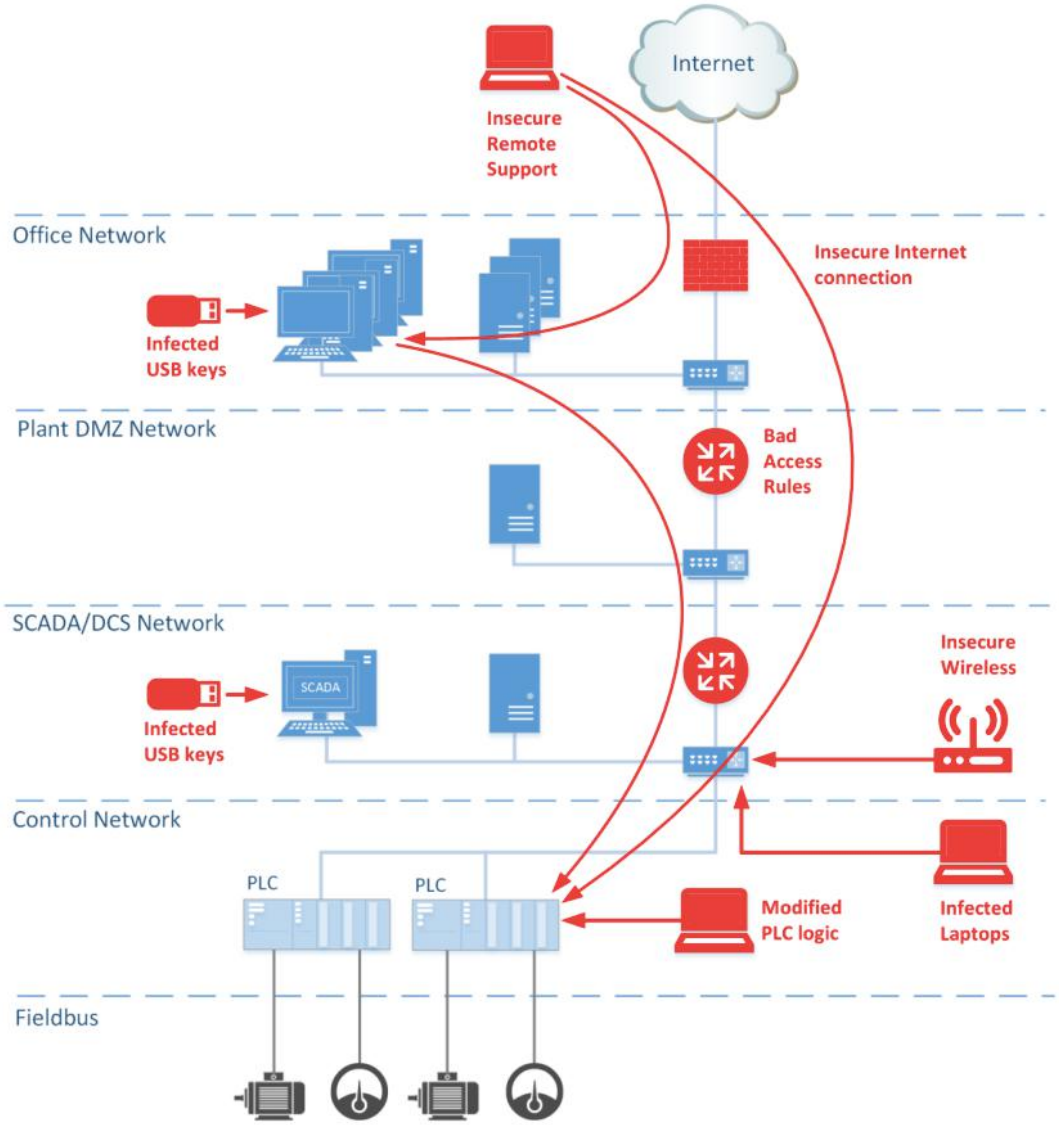






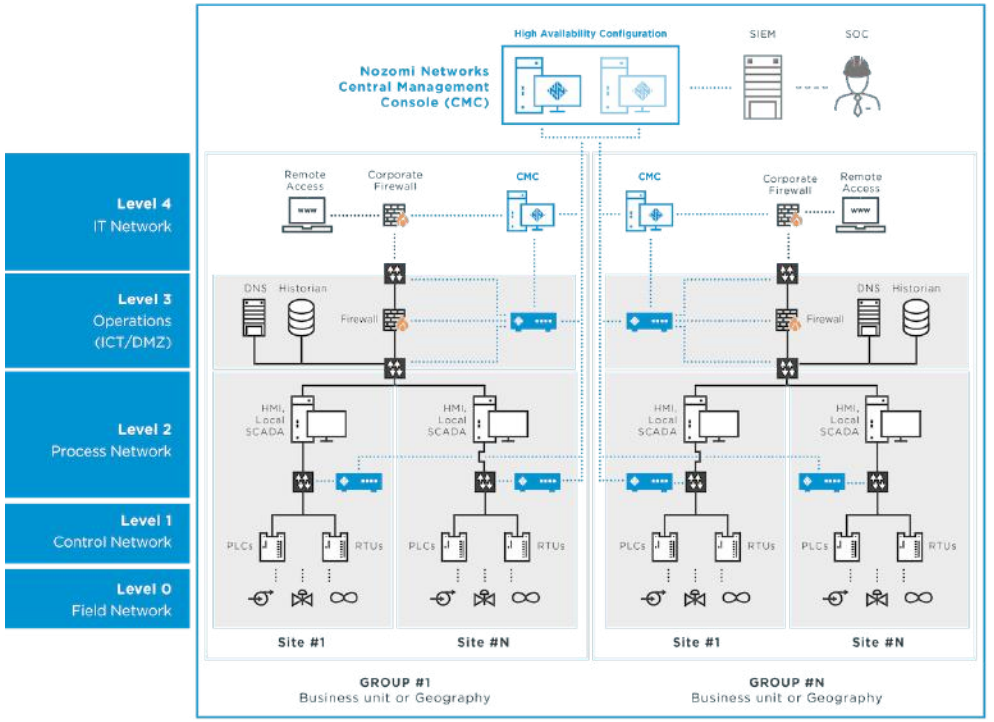
Modulo 5 – Traffic analysis and Vulnerabilities

- Attacchi e vulnerabilità informatiche e alcuni incidenti pubblici
- Analisi traffico, IDS, network scanner, Rilevamento e gestione incidenti
- Industrial IoT, 5G Security, Wireless hijacking and jamming
- Attacchi livello 1 e 2, Vulnerabilità reti per il controllo
- Attacchi livello 0 e 1, Vulnerabilità bus di campo
- Active and passive filtering
- SCADA Forensic
- Reverse Engineering, Sandboxing, Hardware Attacks
- Attack and fault recognition by anomaly detection
- Commercial appliances for SCADA security



Modulo 6 – Countermeasures

- **Crittografia** nei sistemi SCADA (E2EE, OPC UA, USB control, covert channels)
- **IEC 62443-4-2**
- Packet filtering and **deep packet inspection** and Artificial Intelligence
- **LAB** (practical experience on simulated scenarios): ICS Single Asset; ICS Base replication; ICS Complex replication; Energy power scenario; Highway scenario; Transportation scenario; Smart City scenario; Hands-on exercises; CTF challenge
- **SCADA Red Teaming** (Attack classes, Security Assessment, Penentration testing, Vulnerability Exploiting, Shellcodes, 0days
- **SCADA Blue Teaming** (Defense classes, Cyber Threat Intelligence, Forensics, Cyber Investigations)
- La sicurezza nelle **Utilities**
- Progettazione di soluzioni per la raccolta e monitoraggio degli eventi tramite connettori (raccolta log, d.lgs. n. 231/2001, ecc.) creazione use case per obiettivi di monitoraggio eventi di sicurezza
- Siemens security approach



MCIPLab.it

ROMA TRE
UNIVERSITÀ DEGLI STUDI

THANK YOU

stefano.panzieri@uniroma3.it