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

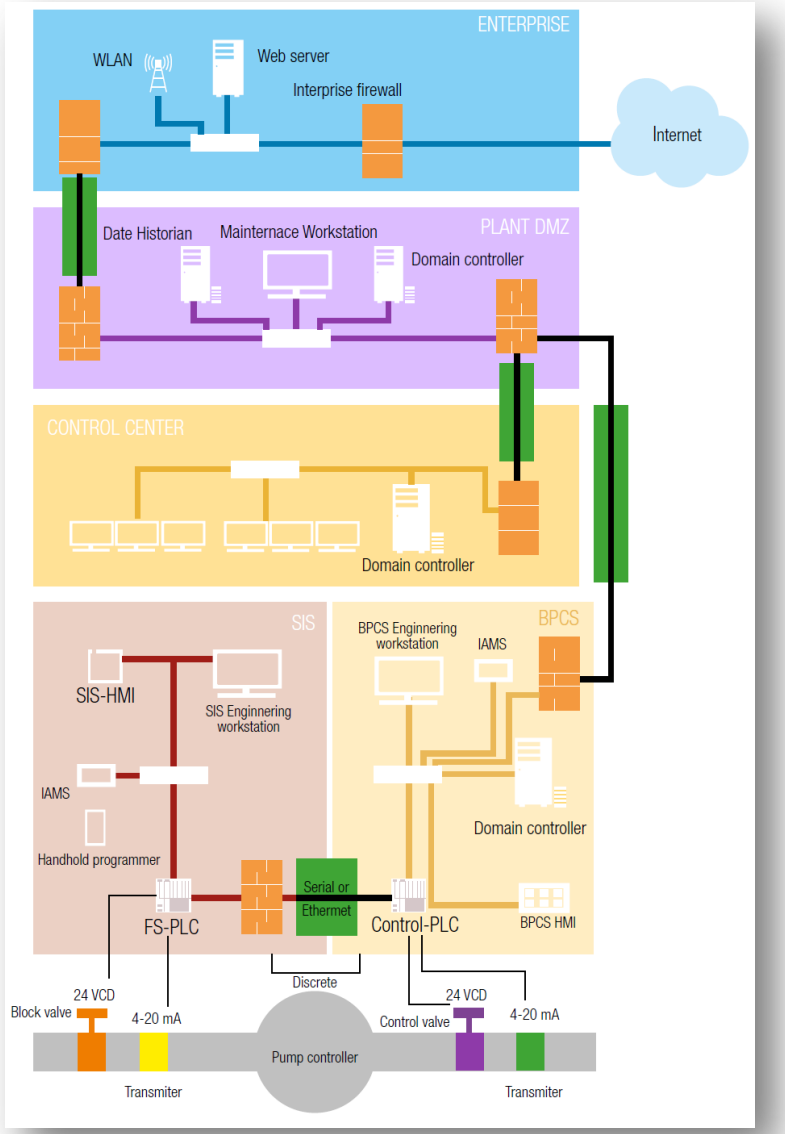
AIIC

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)

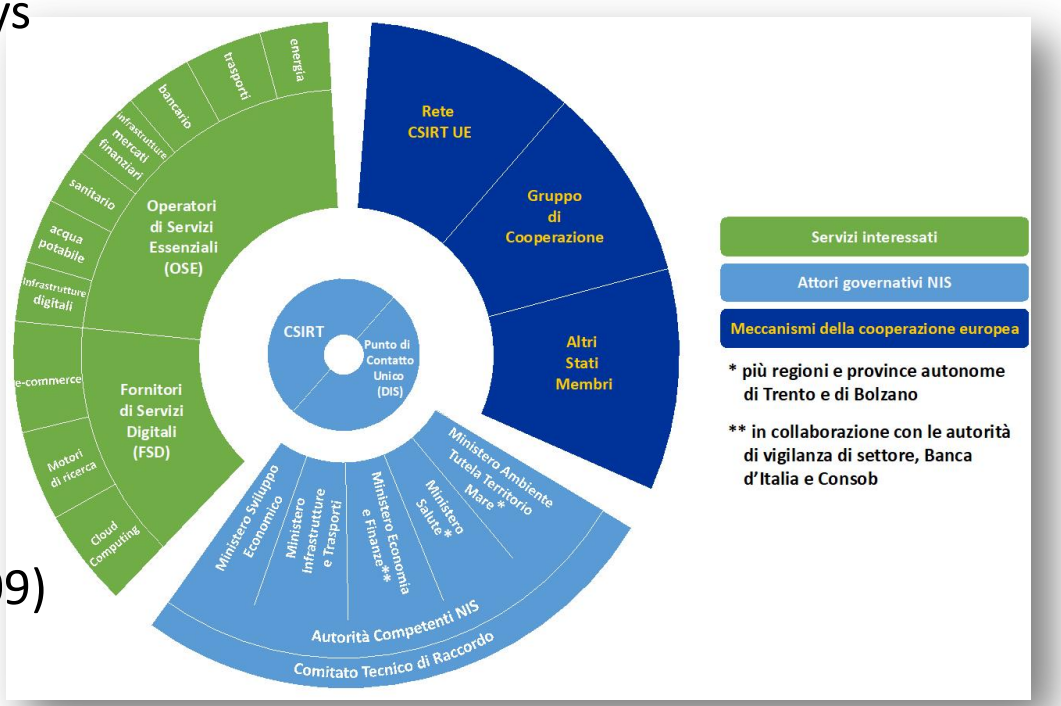
Modulo 1 - Industrial Control Systems

- 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
- Big data analytics



SIEMENS
Ingegno per la vita

BECKHOFF

Rockwell Automation

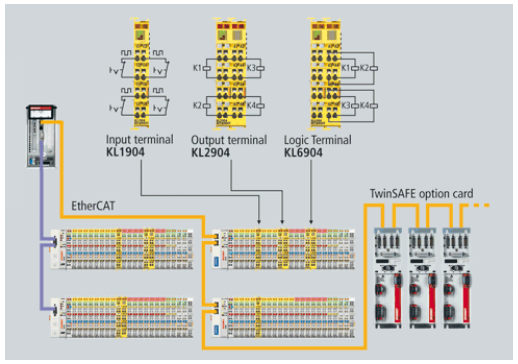
Life Is On | Schneider Electric

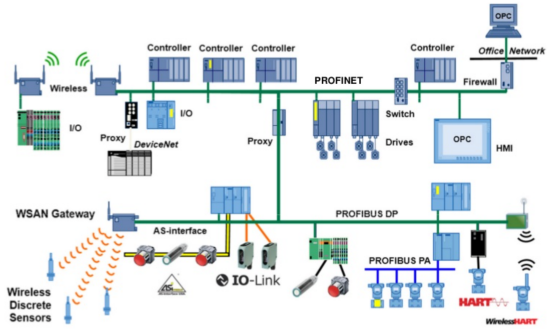
GE Digital

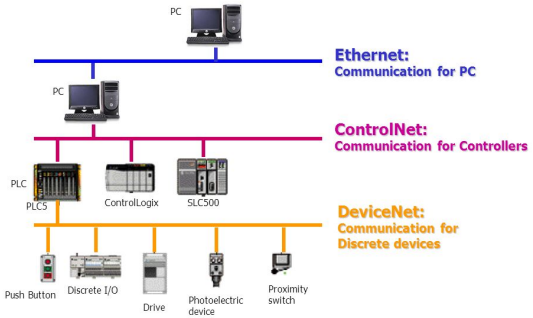
ServiTecno

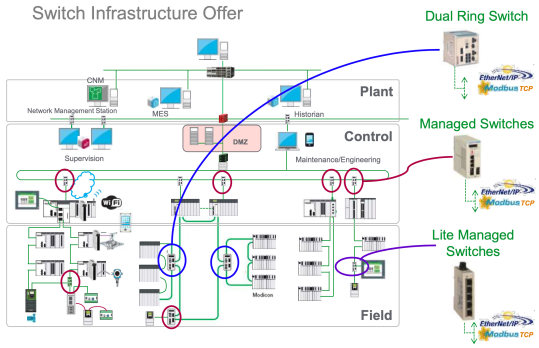
NOZOMI NETWORKS

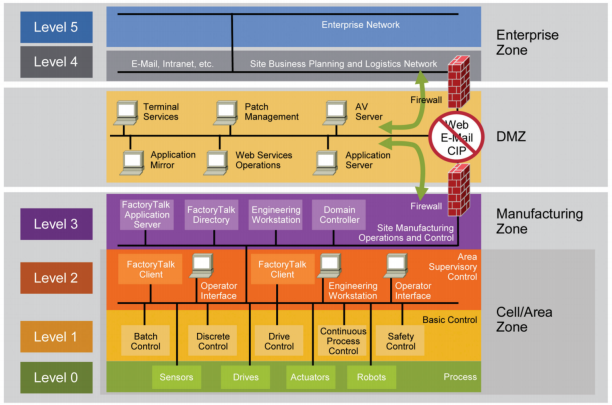
accenture

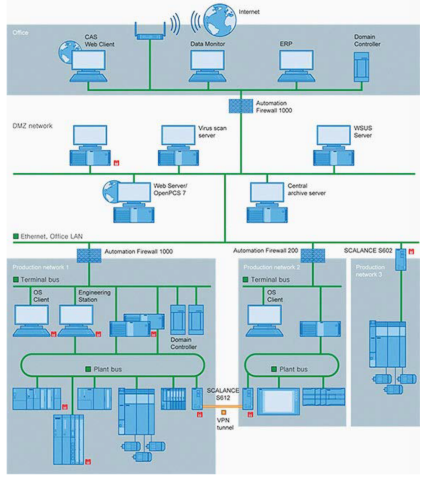






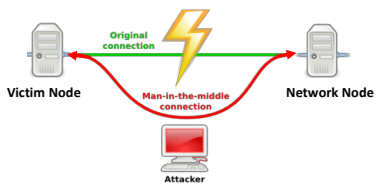




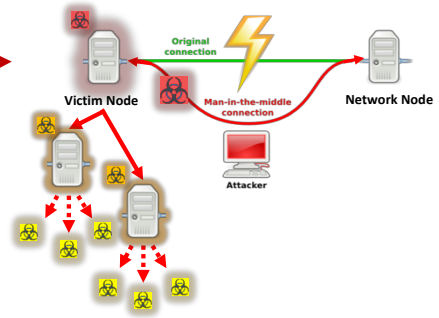


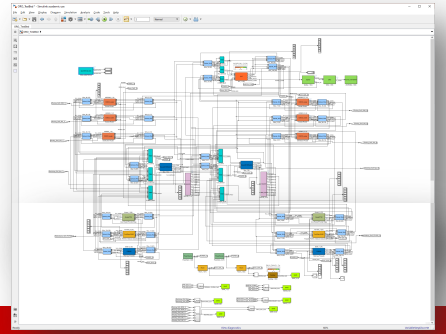
- Metodologie per l'analisi del rischio
- I modelli di enterprise risk management secondo gli standard ISO/IEC 27005:2011 e ISO 31000:2018
- Data Protection Impact Assessment (DPIA)
- Modellistica Interdipendenze
- Best Practices, OSSTMM (Open Source Security Testing Methodology Manual). ISECOM Proactive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

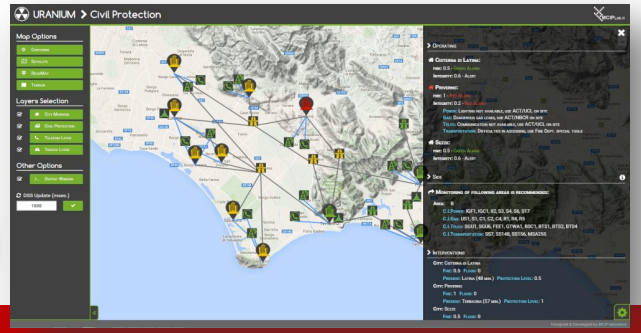
MITM – MAN IN THE MIDDLE

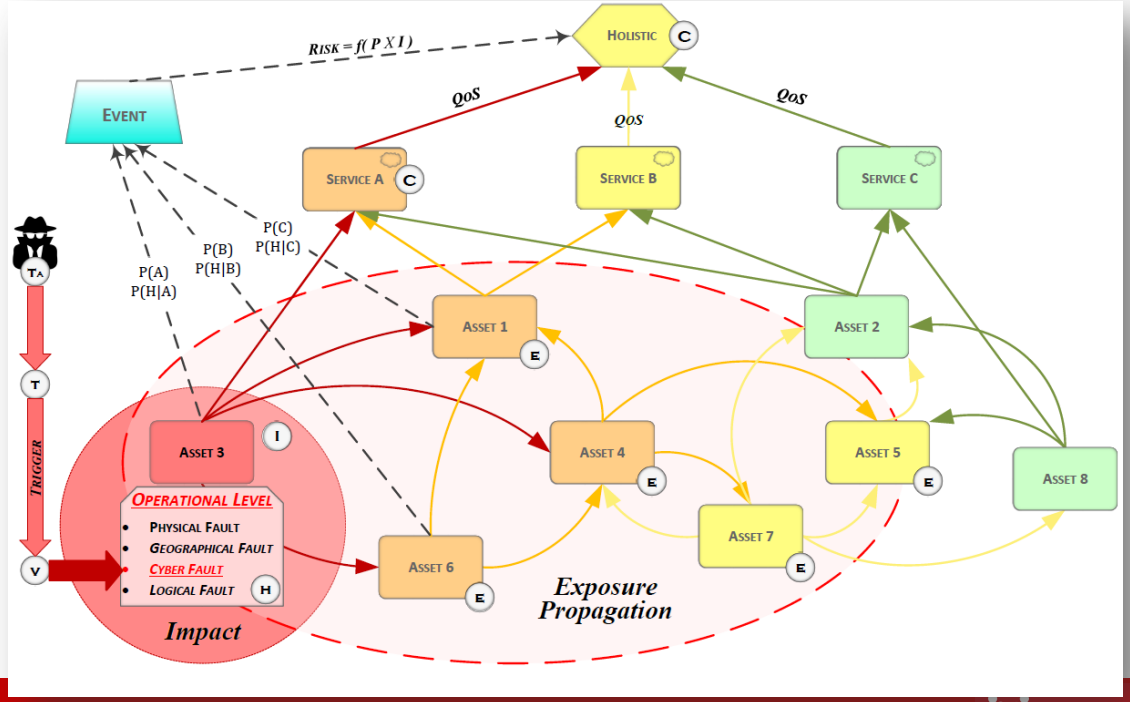


INFECTION ATTACK



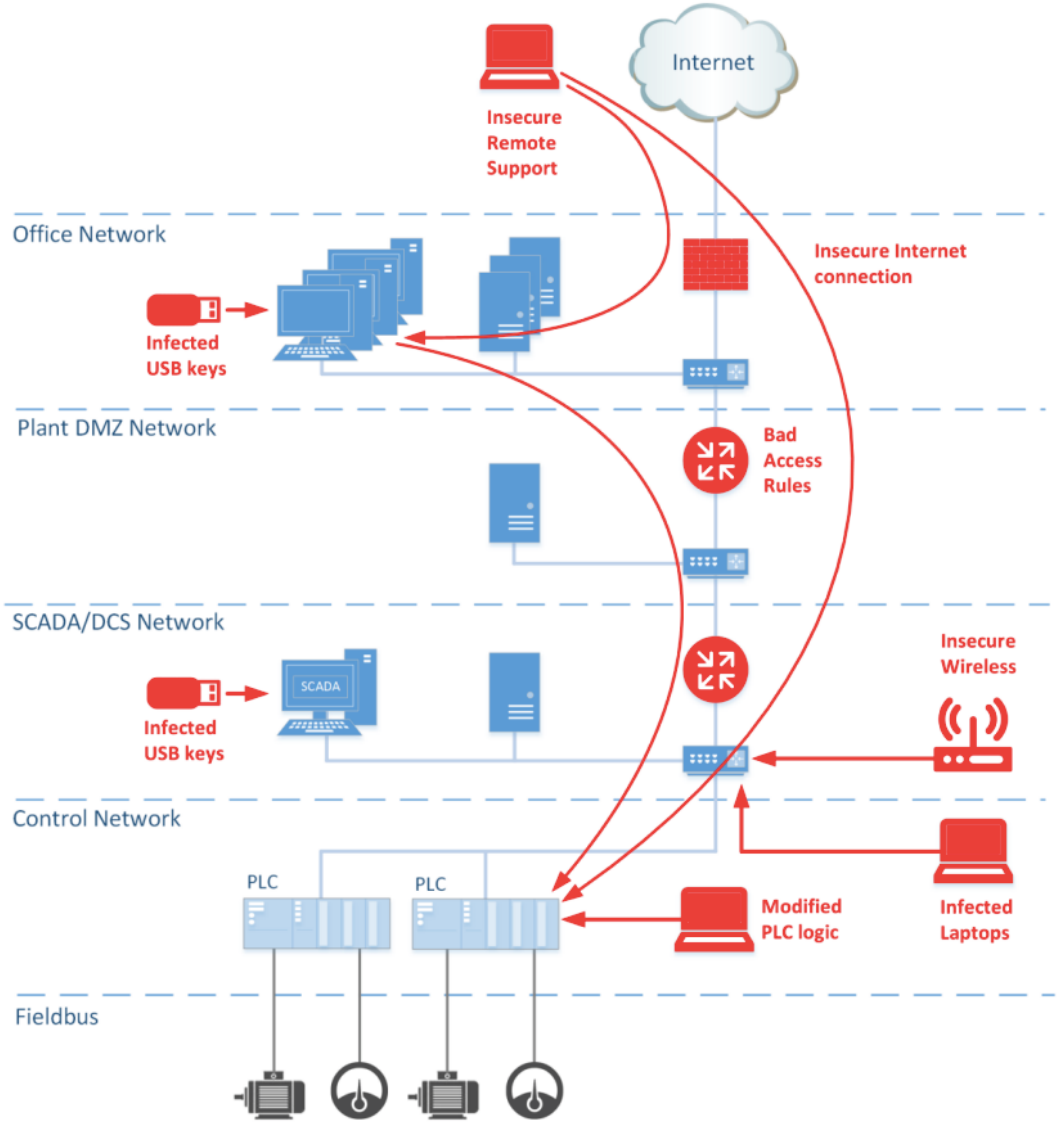






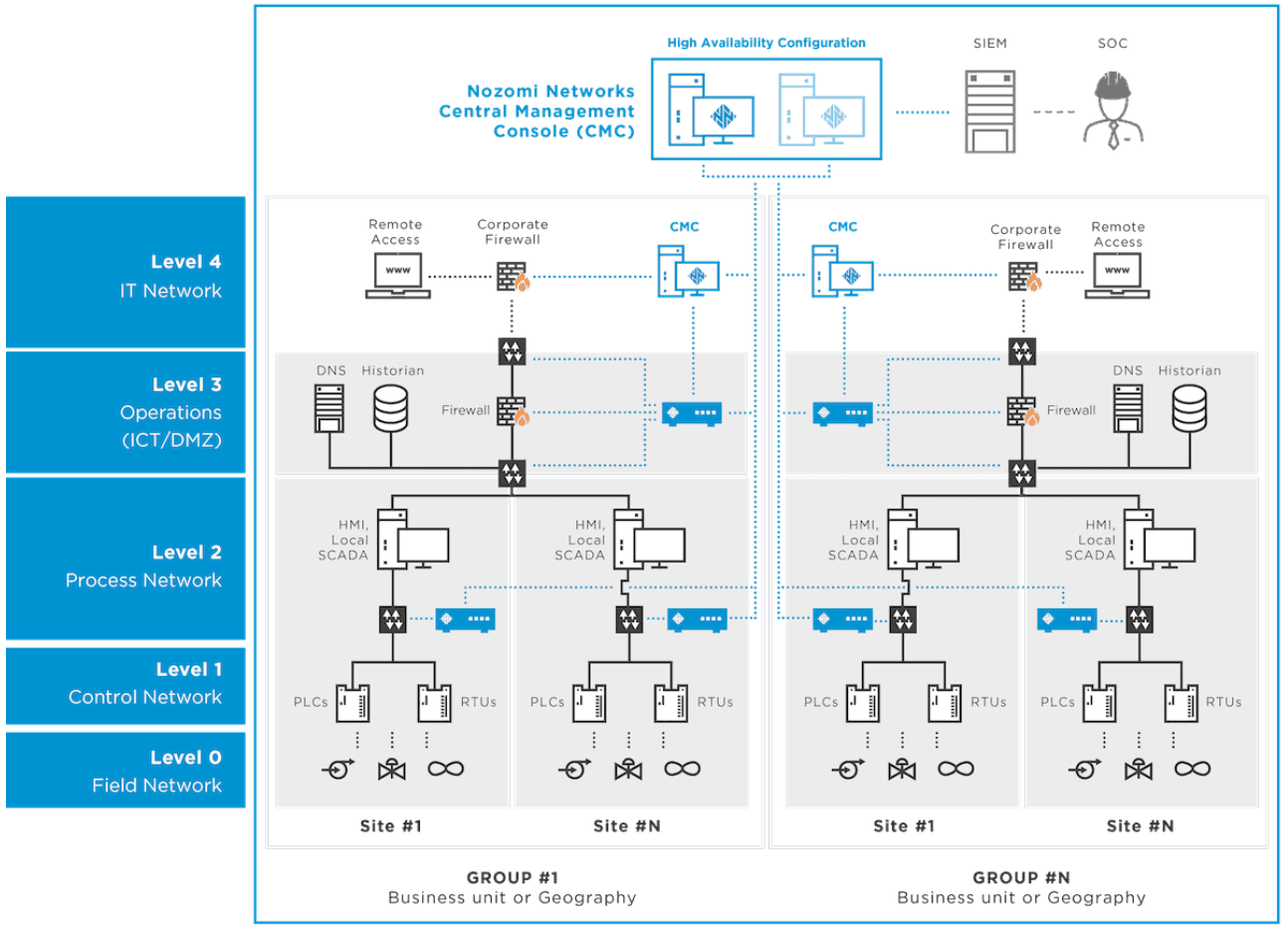
Modulo 5 – Traffic analysis and Vulnerabilities

- 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 Modbus, AMS/ADS, Profinet
- Attacchi livello 0 e 1, Vulnerabilità CANbus
- 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
- Scada Filtering 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