UNIVERSITÀ POLITECNICA DELLE MARCHE

DII
Dipartimento di Ingegneria dell'Informazione

unimc

Operational Technology e Cyber Security

Diego Chiozzi – dchiozzi@gmail.com

Martedì 19 Luglio 2022

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

Introduzione e stato dell’arte

Industria 4.0

Tecnologie principali ICS: SCADA, PLC, DCS, RTU → Operational technology

Problemi OT rispetto a IT

- IT aggiornamento è più frequente e più agevole da distribuire
  - OT difficoltà nell'aggiornamento
- OT sistemi operativi sono proprietari e non standard
  - IT nella maggior parte dei casi sono Microsoft Windows e/o Linux
- OT protocolli TLC proprietari e chiusi
  - IT sono standardizzati
- IT attacchi legati alle vulnerabilità e vantaggio economico
  - OT basati sul settore industriale e distruttici

Principali conseguenze di attacchi OT[1]

- Danneggiamento qualità prodotti e servizi
- Perdita della fiducia del cliente
- Danni ambientali
- Perdita di opportunità e contratti
- Danneggiamento degli equipaggiamenti/macchine.

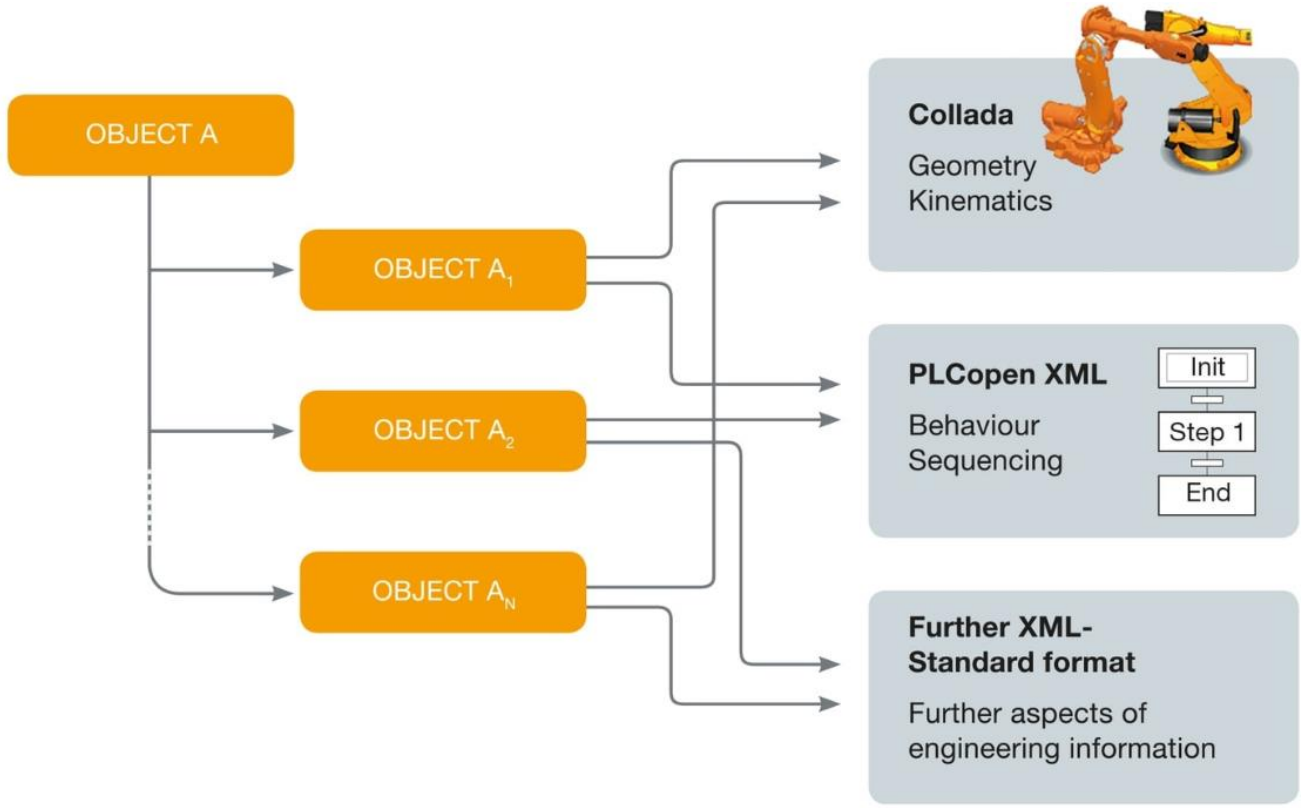
1) W. Schwab e M. Poujol, “The State of Industrial Cybersecurity 2018”, Kaspersky Lab AO, Moscow, Russia, Tech. Rep. PAC A CXP Group Company 2018, Jun. 2018.

Convergenza OT/IT cyber security e strumenti

Capire l’ambiente OT

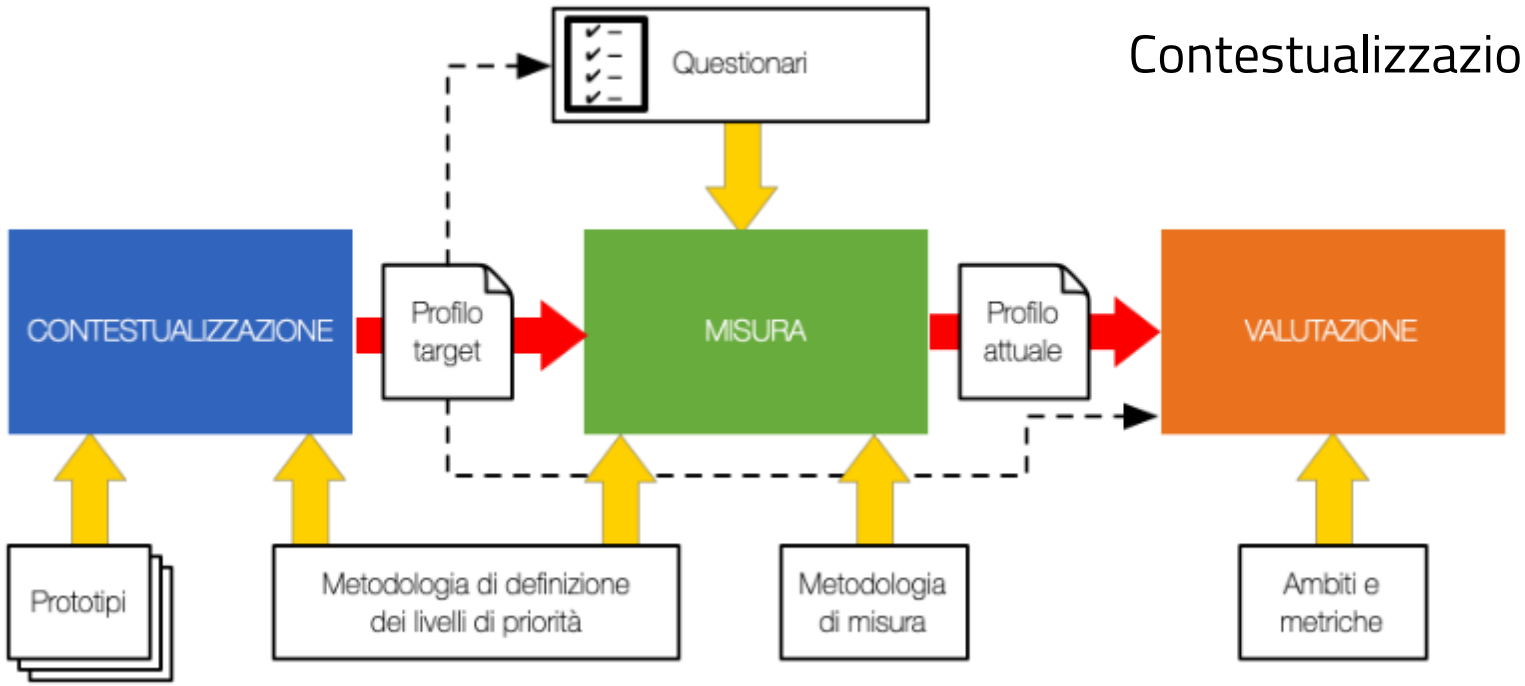
- Golden Rules OT
  - “La sicurezza prima di tutto”
  - “Quello che funziona non si tocca”
- I Gap
  - Mancanza di forza lavoro che comprenda l’ambito IT e l’ambito OT
  - Mancanza di comunicazione tra staff IT e staff OT
  - Riduzione del rischio è connesso all’ambiente

Automation Markup Language (AML)[2]



2) R. Reussner, A. Koziolek, R. Heinrich, “Aligning with cybersecurity framework by modeling OT security”, Lecture Notes in Informatics in INFORMATIK 2020, Bonn, Germany, Sep.-Oct. 2021, pp. 311-319.

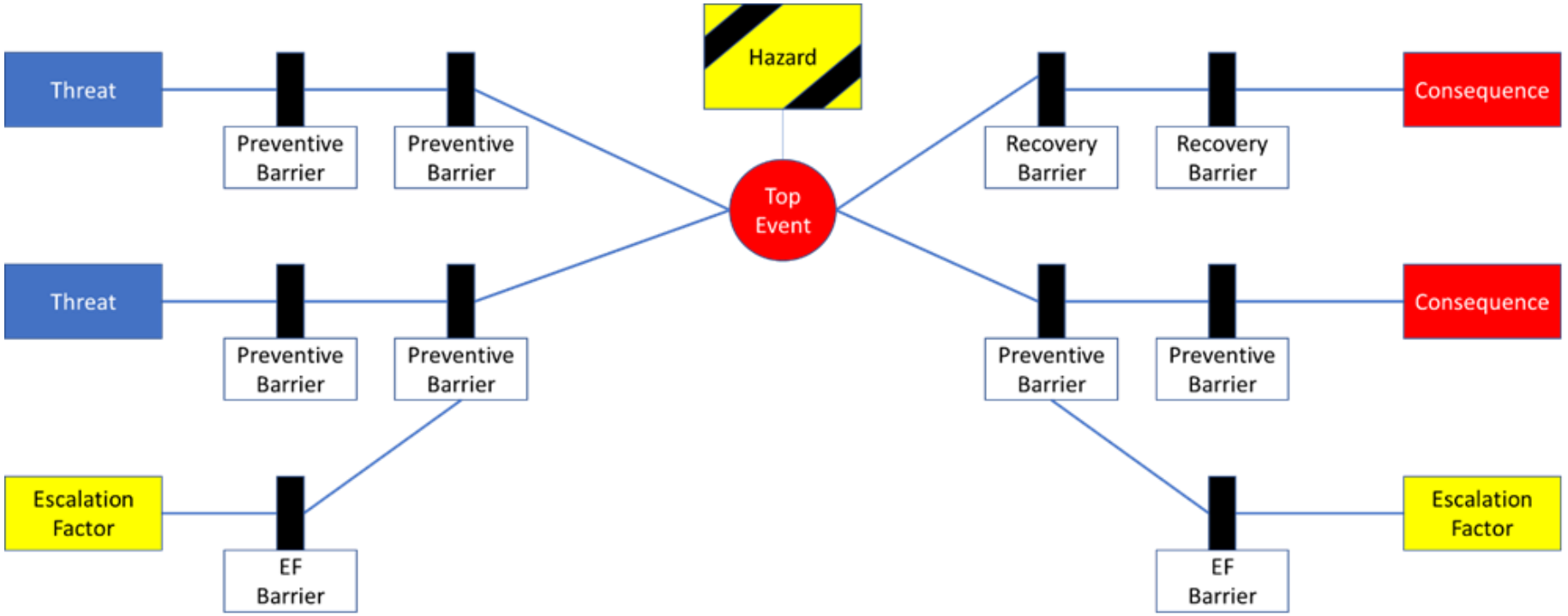
Framework per la cyber sicurezza nazionale[3]



Contestualizzazione in ambito OT

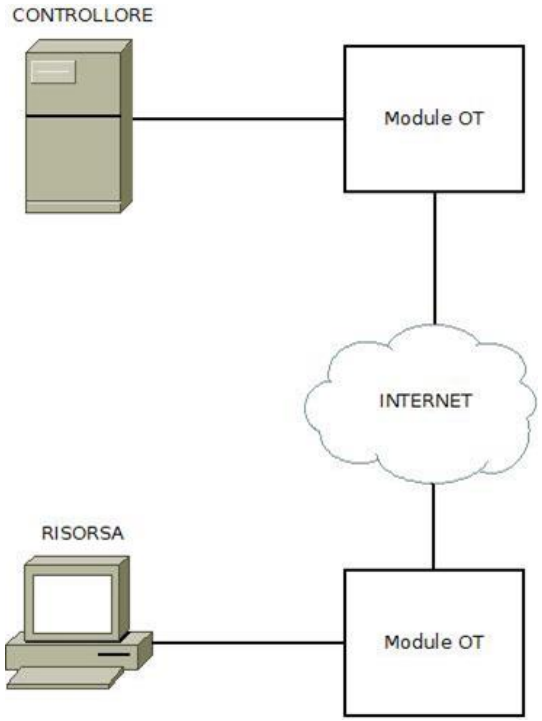
3) G. Murino, M. Ribaudo, S.P. Romano e A. Tacchella, "OT Cyber Security Frameworks Comparison Tool", in Proceedings of the Italian Conference on Cybersecurity, Online, Italy, Apr. 2021, pp. 1-14.

BOWTIE[4]



4) M. Hoeve, C. Monte Portela e G. Brouns, “Managing OT cyber-security risks using BOWTIES and Risk & Opportunity based asset management at Dutch DSO ENEXIS”, Proceedings of the 25th International Conference on Electricity Distribution, Madrid, Spain, Jun. 2019, pp. 141/1-5.

ModuleOT[5]



Caratteristiche ModuleOT

Caratteristica	IT
1	End-to-End Encryption
2	Hardware Crypthographic Acceleration
3	IP White-listing
4	key Management
5	Serial Device Support
6	Role-Based Access Control

5) W. Hupp, A. Hasandka, R. Siqueria de Carvalho e D. Saleem, “ModuleOT: A Hardware Security module for operational Technology”, Proceedings of the IEEE Texas Power and Energy Conference (TPEC) 2020, College Station, USA, Feb. 2020, pp. 1-6.

Casi di studio e Conclusioni

Settori diversi, priorità diverse, ma stessi problemi

- Approvvigionamento idrico
  - Impianti governabili manualmente in caso di attacco
  - Sversamenti di prodotti mai possibili da remoto
- Costruzioni
  - Ambienti mutevoli e molti appaltatori
  - Sicurezza cantieri
- Approvvigionamento elettrico
  - Perdita prestazioni graduale in caso di attacco
  - Gestire incidenti e resilienza

Una fotografia della situazione delle PMI Italiane

- Dati raccolti intervistando i consulenti Ingfor Srl

- 5 Consulenti
  - 111 Aziende che hanno fatto investimenti Industria 4.0
  - Anno 2021
  - Aziende di Lombardia, Emilia-Romagna, Veneto, Piemonte, Liguria, Toscana e Marche
  - 5 Domande

IngFor ENGINEERING

Risultati

- D1: Quante aziende hanno implementato un monitoraggio continuo della rete al fine di verificare modifiche degli Asset?
  - SI → 23% - NO → 60% - ND → 17%

- D2: Quante aziende hanno attuato meccanismi di segmentazione della rete attraverso DMZ o regole di routing che mantengano separate le componenti OT dalle componenti IT?
  - SI → 34% - NO → 62% - ND → 4%

Risultati

- D3: Quante aziende utilizzano sistemi dedicati per la teleassistenza e l'accesso remoto come router su attivazione o sistemi di replicazione schermo tramite VPN?
  - SI → 49% - NO → 45% - ND → 6%

- D4: Quante aziende hanno dotato le componenti OT di antivirus o le hanno protette tramite firewall?
  - SI → 31% - NO → 37% - ND → 32%

Risultati

- D5: Quante aziende hanno avviato contratti di manutenzione delle componenti OT?
  - SI → 35% - NO → 36% - ND → 29%

- COMMENTO
  - Prima di interventi tecnici, è necessaria la sensibilizzazione delle PMI italiane sul tema della cyber security in ambito OT.

Conclusioni

- La cyber security in ambito OT è un problema sentito ma sottovalutato

- Possibili soluzioni
  - Formazione sulle tematiche legate alla cyber security a personale coinvolto nella gestione delle apparecchiature OT
  - Valutazione della cyber security focalizzata alle apparecchiature OT, con stima dei costi legati ad un incidente

Domande