Facoltà di Ingegneria Civile ed Industriale

"Sustainability" 2021

24 novembre 2021

ITALY SECT ION CHAPTER
R8 AREA CHAPTER

PROBLEMATICHE DI CYBERSICUREZZA NELL'INDUSTRIA 4.0 SOSTENIBILE

Domenico Barone

Sala del Chiostro - S. Pietro in Vincoli
Via Eudossiana 18, 00184 Roma

Sezione di Roma

PROBLEMATICHE DI CYBERSICUREZZA NELL'INDUSTRIA 4.0 SOSTENIBILE

Seminario ASTRI

"Sustainability" 2021 Implicazione delle Innovazioni Tecnologiche"

Roma, 24 Novembre 2021

Ing. Domenico Barone *- Coordinatore della Commissione Tecnica 266 – Sicurezza degli impianti a rischio di incidente rilevante del Comitato Termotecnico Italiano (CTI-UNI)*

Tecnologie Sicurezza Industriale S.r.l., via P. Lomazzo 51, 20154 Milano, do.barone.tsi@gmail.com

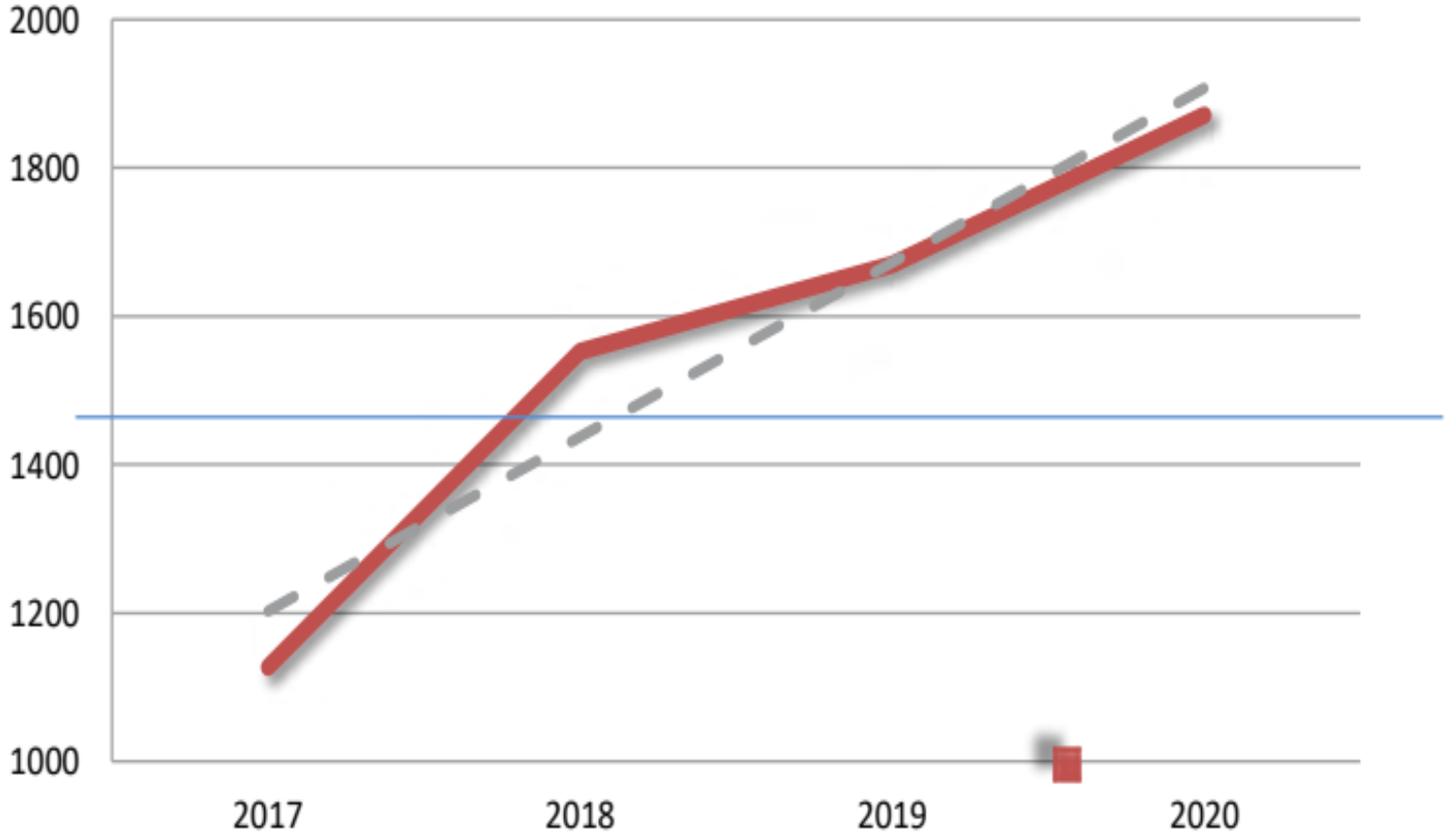
Indice

1. Situazione attuale
2. Principali problematiche
3. Possibili soluzioni

1. Situazione attuale

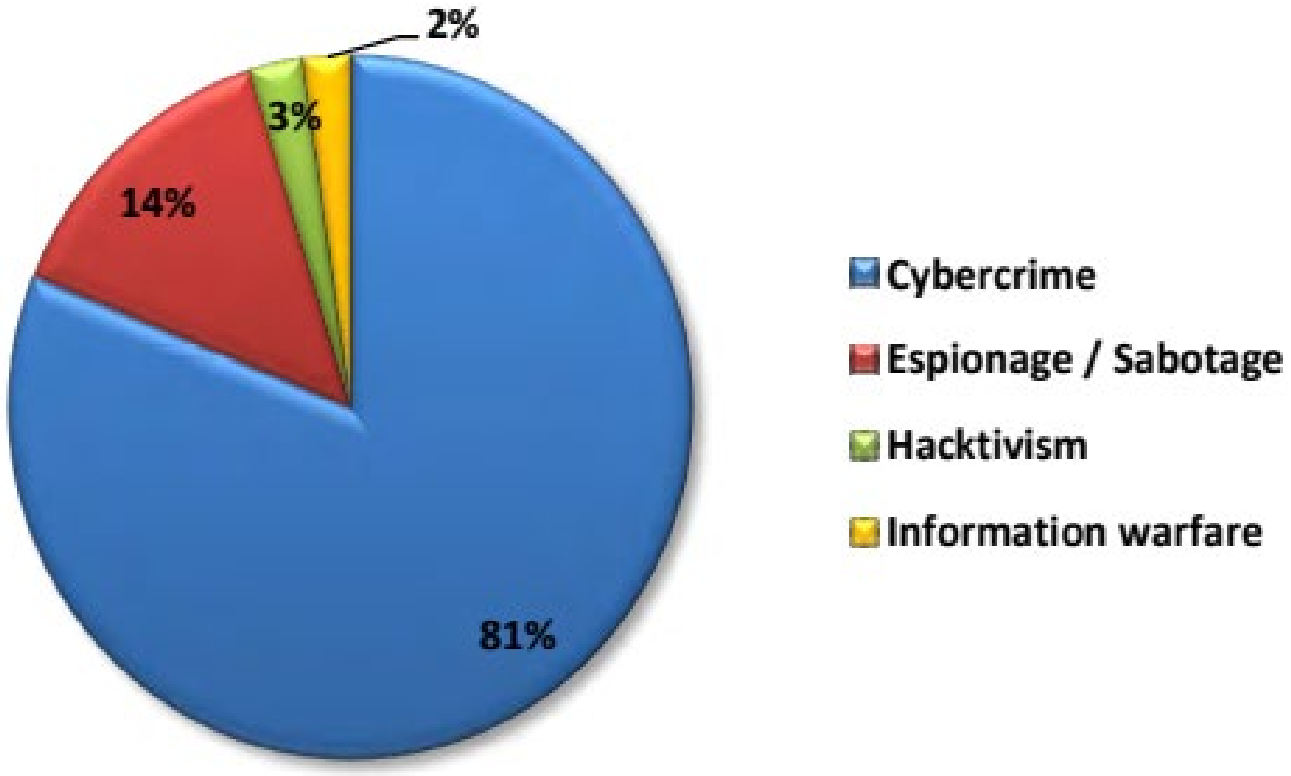
- Impegno delle aziende nella cybersicurezza descritto nei Rapporti di Sostenibilità
- I grandi attacchi sono dovuti a ransomware e comportano esborsi di notevoli somme
- Il Rapporto CLUSIT 2021 mostra che il numero degli attacchi è in continuo aumento (vedi figure)

Numero di attacchi per anno (2017 - 2020)



© Clusit - Rapporto 2021 sulla Sicurezza ICT in Italia

Tipologia e distribuzione degli attaccanti (2020)

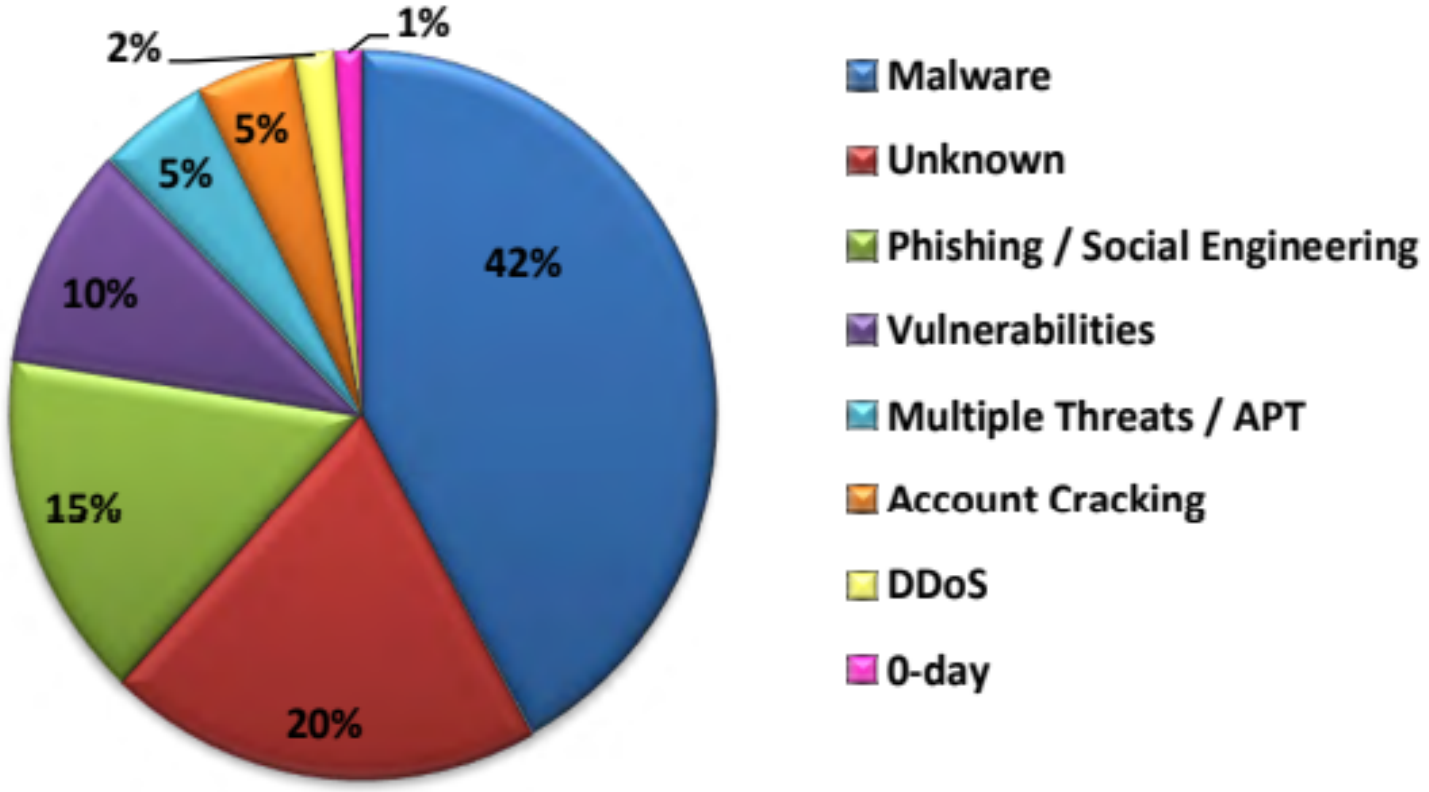


© Clusit - Rapporto 2021 sulla Sicurezza ICT in Italia

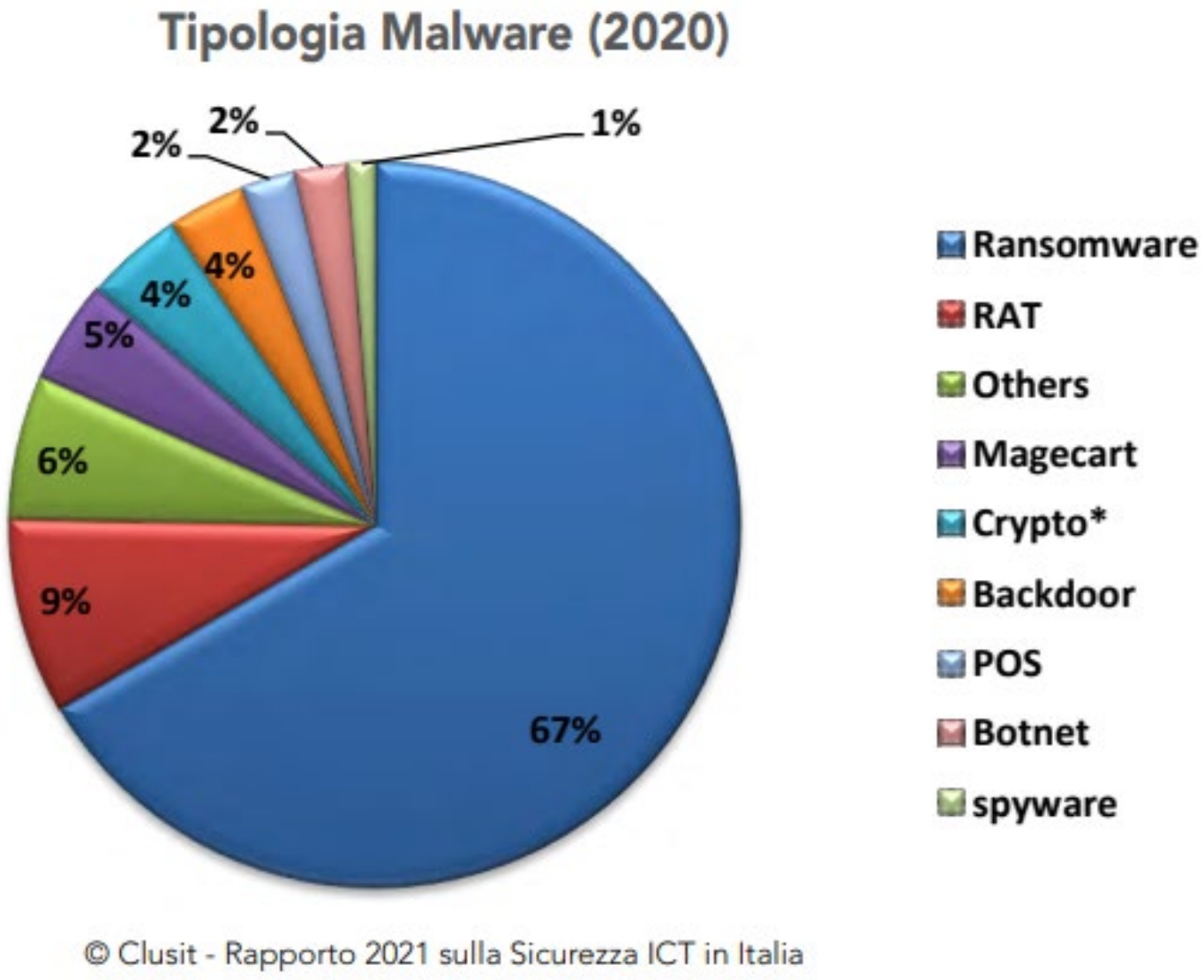
- Gli attacchi noti che hanno comportato i maggiori danni economici sono stati quelli di ransomware (crittografia, espianto dati, vendita di prodotti/dati)

- Il phishing e/o l'ingegneria sociale sono generalmente i canali che permettono l'ingresso indesiderato nei sistemi informatici aziendali

Tipologia e distribuzione delle tecniche di attacco (2020)



© Clusit - Rapporto 2021 sulla Sicurezza ICT in Italia


Tipologia Malware (2020)
67%
9%
6%
5%
4%
4%
2%
2%
1%
Ransomware
RAT
Others
Magecart
Crypto*
Backdoor
POS
Botnet
spyware
© Clusit - Rapporto 2021 sulla Sicurezza ICT in Italia

- L’autenticazione a più fattori, cioè con password e altro sistema di riconoscimento (ad es. SMS) consente di controllare in modo efficace l’accesso da parte di terzi

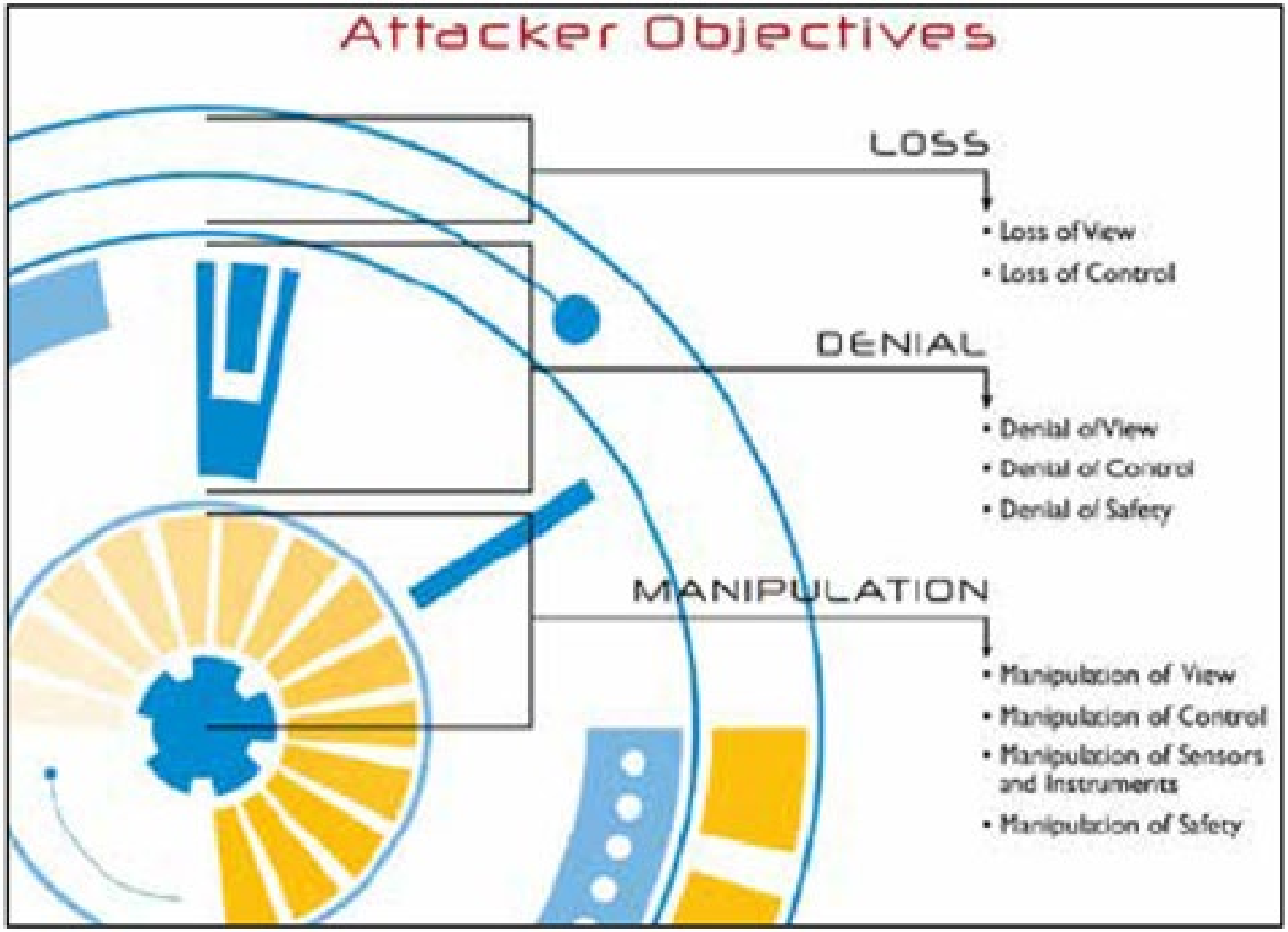
- Il controllo del traffico dei dati costituisce una buona pratica per evidenziare eventuali situazioni anomale nel sistema

- Attualmente risulta che il sistema IT (Information Technology) è più soggetto ad attacchi rispetto al sistema OT (Operational Technology), che generalmente interessa l’industria 4.0

2. Principali problematiche

- Inserimento di malware nei sistemi digitali (DCS/PLC) utilizzati nelle sale controllo di impianti industriali (vedi figura)

- I possibili obiettivi di un cyber attacco ad un sistema ICS e/o ESD sono (vedi figura)
  - perdita dati (visione, controllo)
  - blocco (visione,controllo,sicurezza)
  - manipolazione (visione,controllo,sensori,sicurezza)

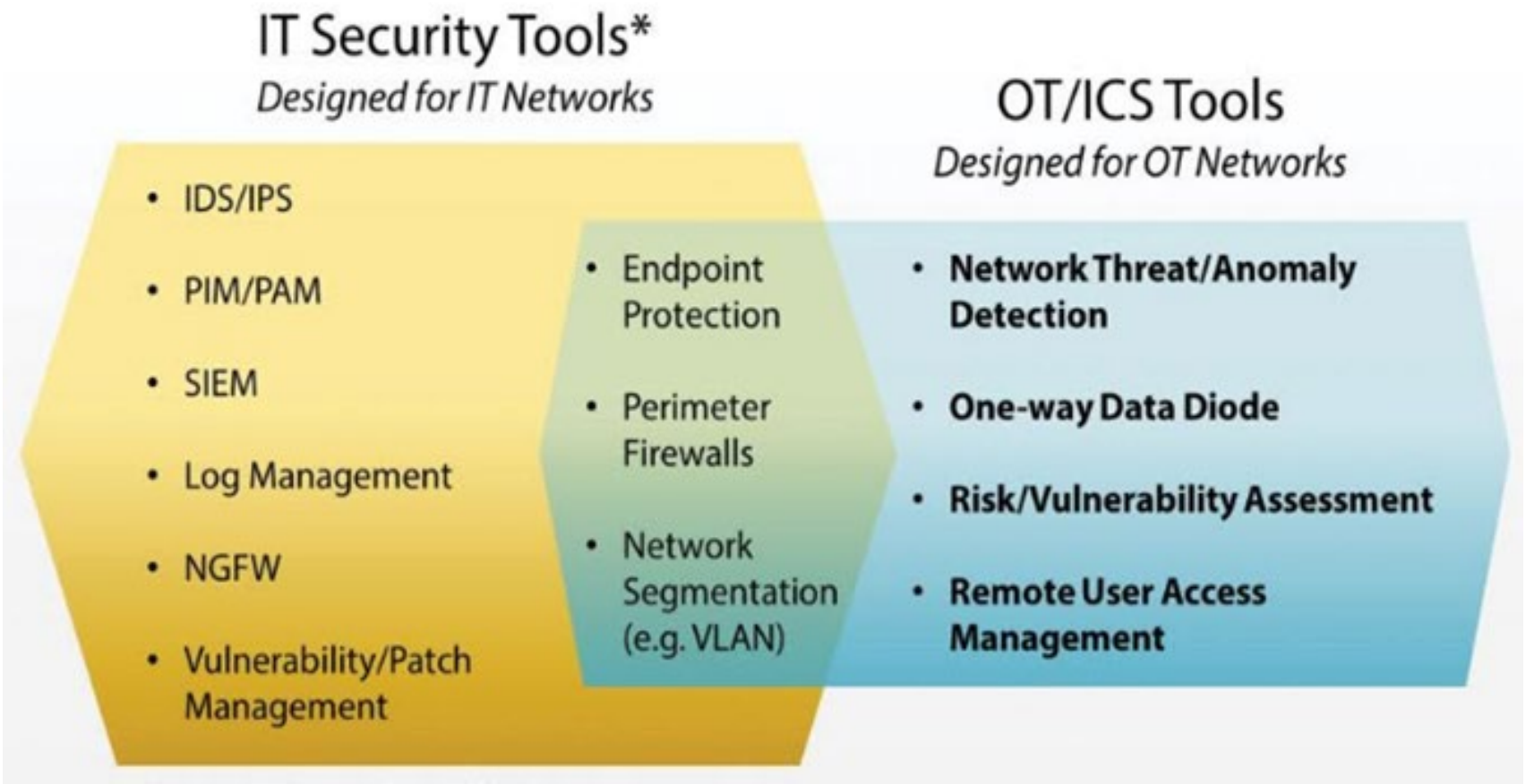

Attacker Objectives
LOSS
• Loss of View
• Loss of Control
DENIAL
• Denial of View
• Denial of Control
• Denial of Safety
MANIPULATION
• Manipulation of View
• Manipulation of Control
• Manipulation of Sensors and Instruments
• Manipulation of Safety

- Il punto debole dei sistemi digitalizzati è l'impiego di sistemi operativi (es Windows,SAP) accessibili ad hacker.
- Non è praticamente possibile quantificare in termini numerici (tasso di guasto) l'affidabilità del software come nel caso dell'hardware.
- Errori di programmazione possono rimanere allo stato latente per lunghi tempi
- La stima dell'affidabilità del software tramite SIL (Safety Integrity Level) è possibile sulla base del giudizio di esperti

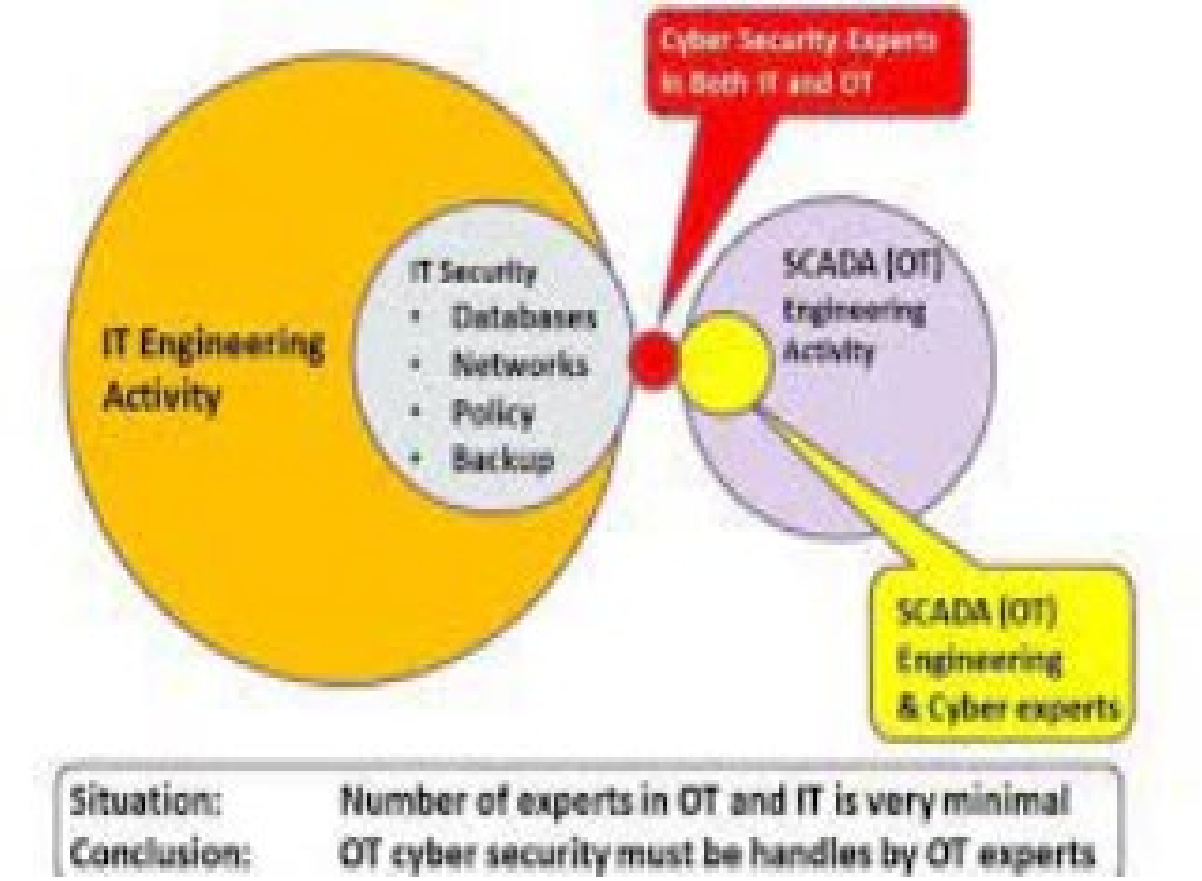
- Per motivi di riservatezza si riscontra una mancanza di informazioni specifiche di dettaglio sugli attacchi avvenuti (modalità, conseguenze, ripristino)

- Solamente gli addetti alla IT (Information Technology) ed alla OT (Operational Technology) sono al corrente degli attacchi e delle misure adottate

- Esempi di interferenze tra IT (Information Technology) ed OT (Operational Technology) sono rappresentati nelle due figure


IT Security Tools*
Designed for IT Networks
IDS/IPS
PIM/PAM
SIEM
Log Management
NGFW
Vulnerability/Patch Management
Endpoint Protection
Perimeter Firewalls
Network Segmentation (e.g. VLAN)
OT/ICS Tools
Designed for OT Networks
Network Threat/Anomaly Detection
One-way Data Diode
Risk/Vulnerability Assessment
Remote User Access Management

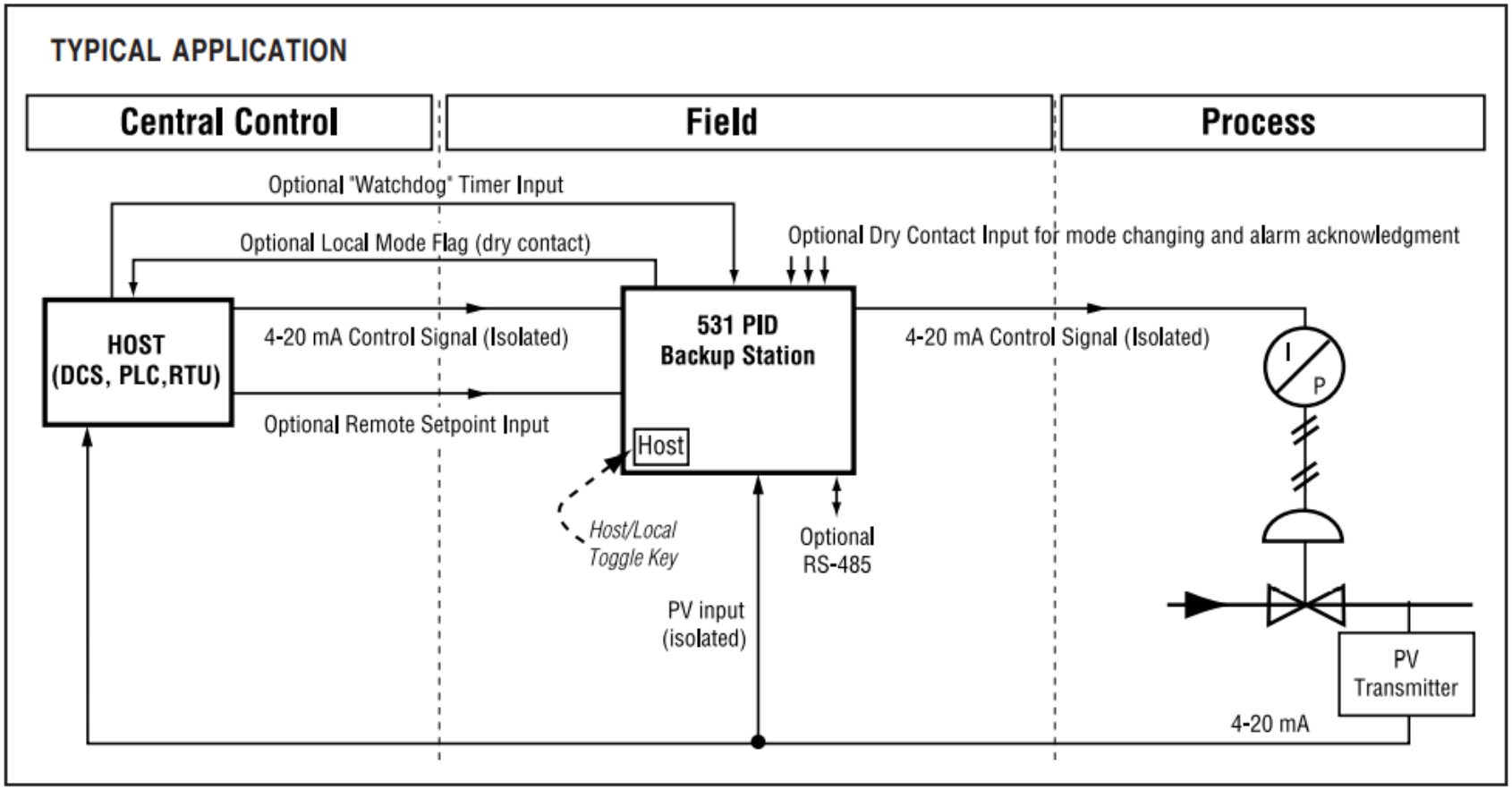
- Nella figura è possibile individuare i sistemi di protezione comuni e specifici per IT ed OT



3. Possibili soluzioni

In aggiunta a quanto previsto dalle normative e/o a standard per la cybersicurezza (IEC, API,…) è possibile:

- Impiegare sistemi di controllo e/o di blocco automatico senza sistemi operativi (tipo analogico moderno con elettronica distribuita digitale - tipo elettronico con matrici di porte programmabili in campo (vedi figura –stazione di back up analogica)


TYPICAL APPLICATION
Central Control
Field
Process
Optional "Watchdog" Timer Input
Optional Local Mode Flag (dry contact)
Optional Dry Contact Input for mode changing and alarm acknowledgment
HOST
(DCS, PLC,RTU)
4-20 mA Control Signal (Isolated)
Optional Remote Setpoint Input
531 PID
Backup Station
Host
Host/Local
Toggle Key
Optional
RS-485
PV input
(isolated)
4-20 mA Control Signal (Isolated)
I
P
PV
Transmitter
4-20 mA

- Effettuare Audit indipendenti da parte di terzi sui sistemi OT per verificare il livello di conformità a standard di riferimento
- Organizzare seminari allo scopo di favorire la diffusione e la condivisione delle esperienze in materia di attacchi ai sistemi OT

GRAZIE PER L'ATTENZIONE !