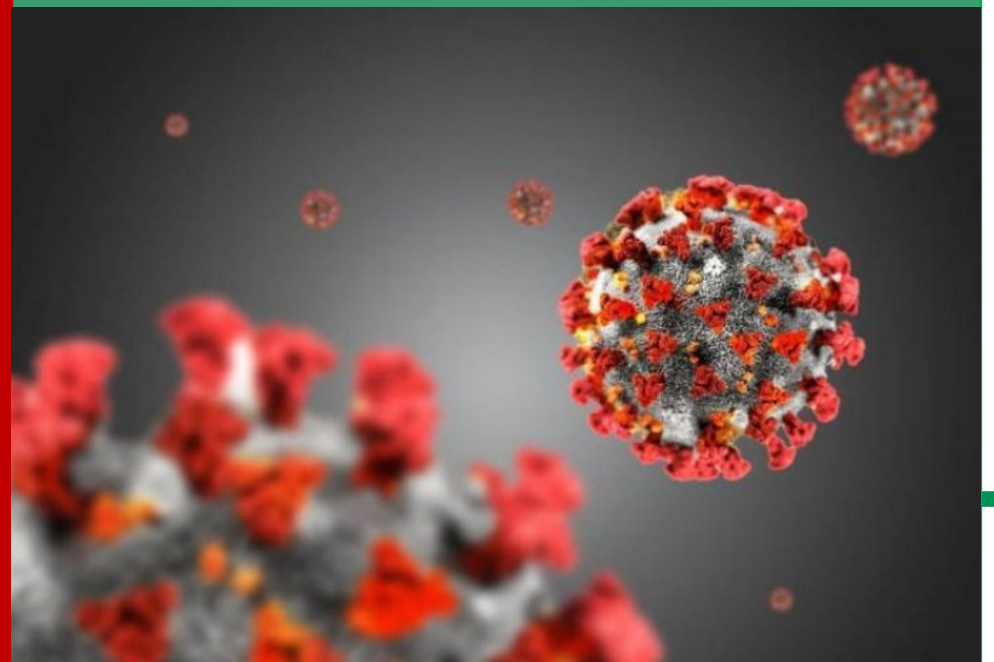
ServiTecno
Technology 4.0 da 40 anni

OT/ICS Cyber Security e Pandemia

www.servitecno.it



GE Digital
Alliance Partner

Agenda

10.30 Saluto ai partecipanti (Enzo M Tieghi), apertura webinar e Introduzione al tema OT Cyber Security (Stefano Panzieri, Roma Tre)

10.45 Gli effetti della epidemia COVID-19 sul mercato del software industriale e dell'automazione (vedi dati e materiale ANIE e ARC Advisory).

11.00 I cambi di paradigma sulle Operations e sul Monitoraggio Remoto causati dal COVID -19 e i risvolti legati alla Cyber Security.

11.20 Migliorare la Cyber Resilienza di SCADA e sistemi di automazione esistenti, come opportunità per tornare a parlare con i Clienti di nuovi progetti in epoca di lockdown.

11.40 Le soluzioni Cyber Security ICS/OT per reti di fabbrica e l'integrazione con il Cloud

12.00 Q&A

12.15 Conclusione

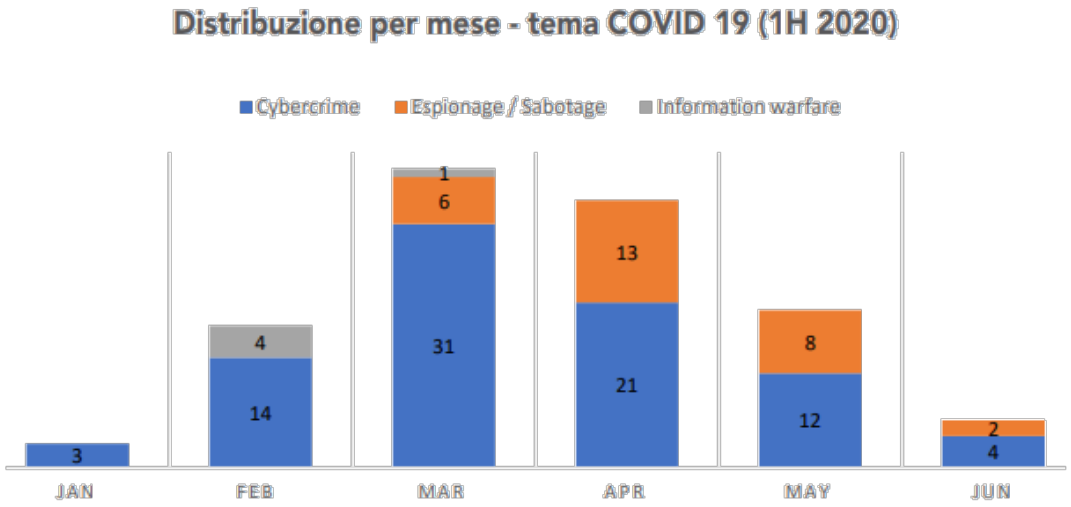
1979-2019 TECHNOLOGY 4.0 DA 40 ANNI
Via Francesco Koristka, 10 – 20154 Milano
Tel. +39 02 48 61 41 - Fax +39 02 48 61 44 41
info@servitecno.it - www.servitecno.it

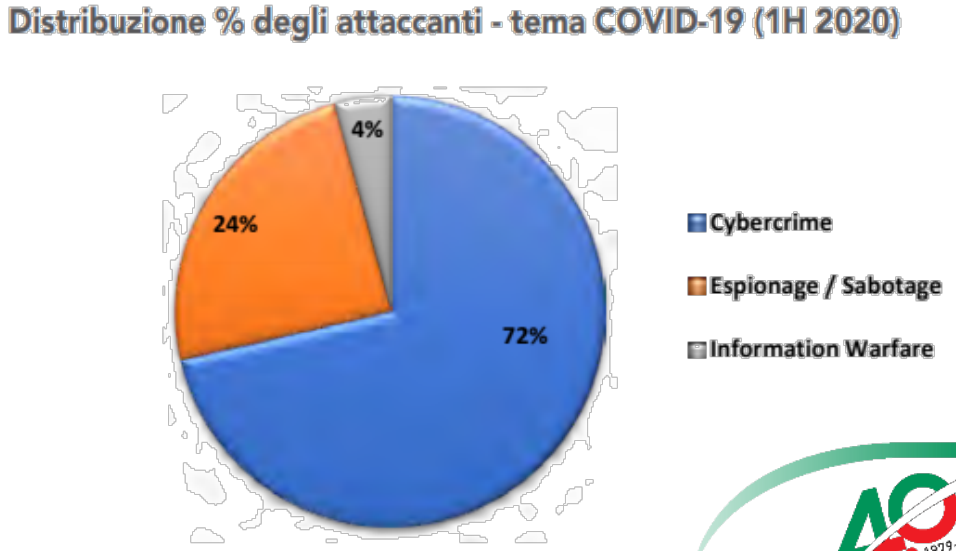
I cambi di paradigma su Operations e su Monitoraggio da Remoto causati dal COVID -19 e i risvolti legati alla OT/ICS Cyber Security.

(dai dati e analisi di CLUSIT, ARC Advisory Group ed ENISA)

1979-2019 TECHNOLOGY 4.0 DA 40 ANNI
Via Francesco Koristka, 10 – 20154 Milano
Tel. +39 02 48 61 41 - Fax +39 02 48 61 44 41
info@servitecno.it - www.servitecno.it

Report Clusit - Speciale Pandemia, Ottobre 2020





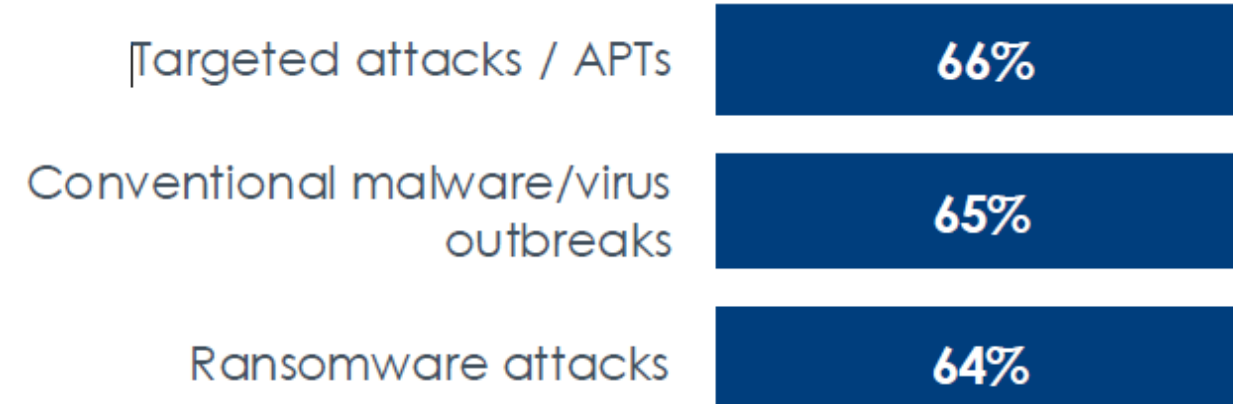
Via Francesco Koristka, 10 – 20154 Milano
Tel. +39 02 48 61 41 - Fax +39 02 48 61 44 41
info@servitecno.it - www.servitecno.it

Già in epoca non sospetta…ENISA

Controlli: Segmentazione e Segregazione

2/3 degli "incidenti" OT/ICS sono APT, Malware, Ransomware:

- arrivati dalla rete interna, non segmentata?
- È un "danno collaterale"?

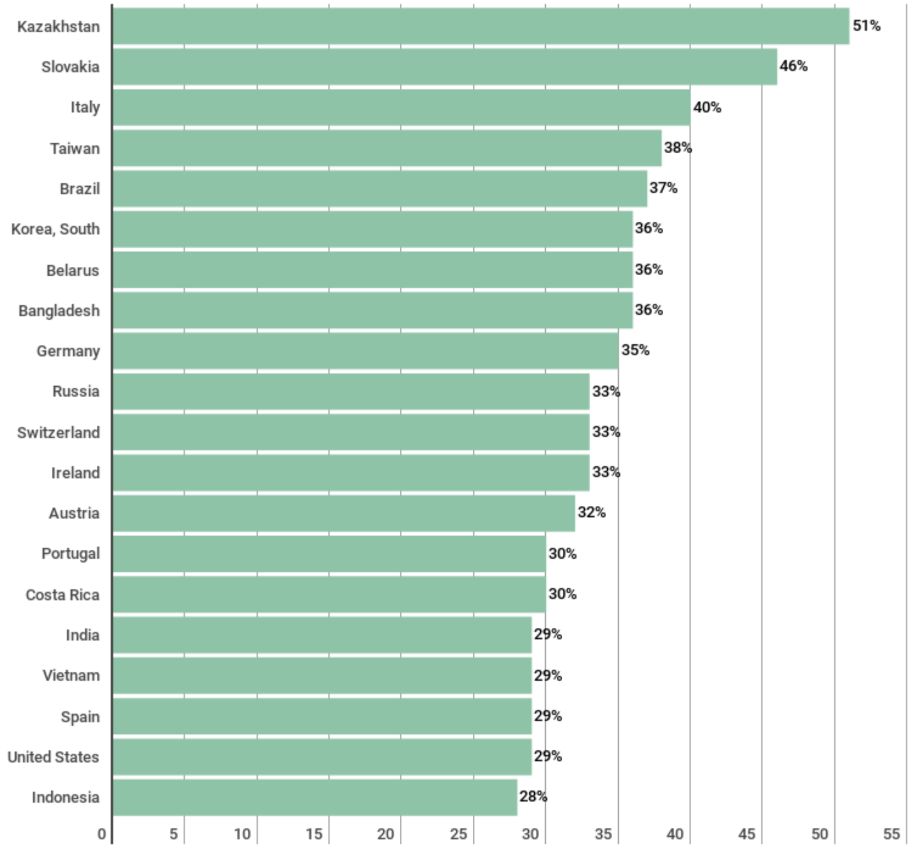


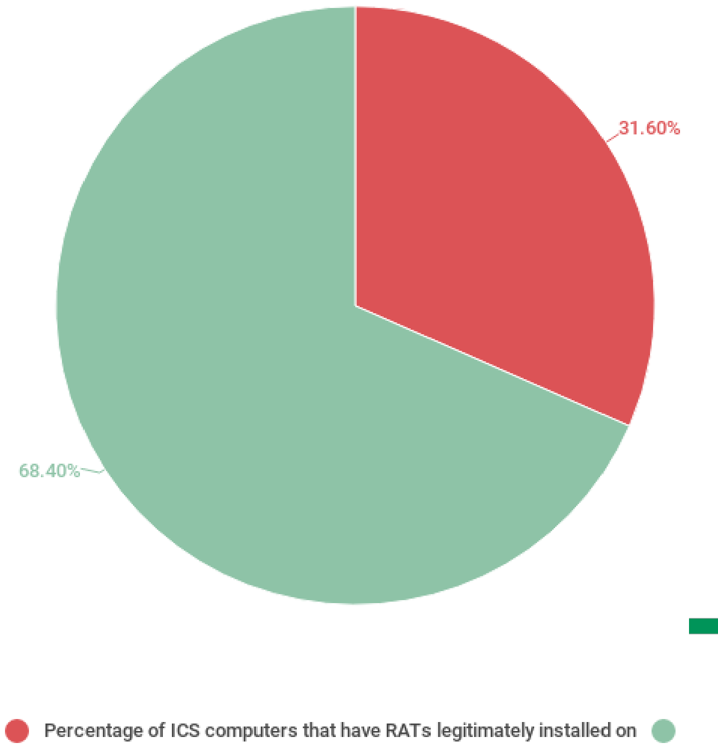
Via Francesco Koristka, 10 – 20154 Milano
Tel. +39 02 48 61 41 - Fax +39 02 48 61 44 41
info@servitecno.it - www.servitecno.it

Già in epoca non sospetta…ENISA

Remote Access/Administration Tools installati

Operational Technology (OT) networks of industrial enterprises is a field of glory for espionage threat actors. These actors use remote administrator tools (RATs) which are already installed in the industrial control systems (ICS). (RATs installati su 40% reti OT in Italia, solo 1 su 3 è legittimo e saputo)

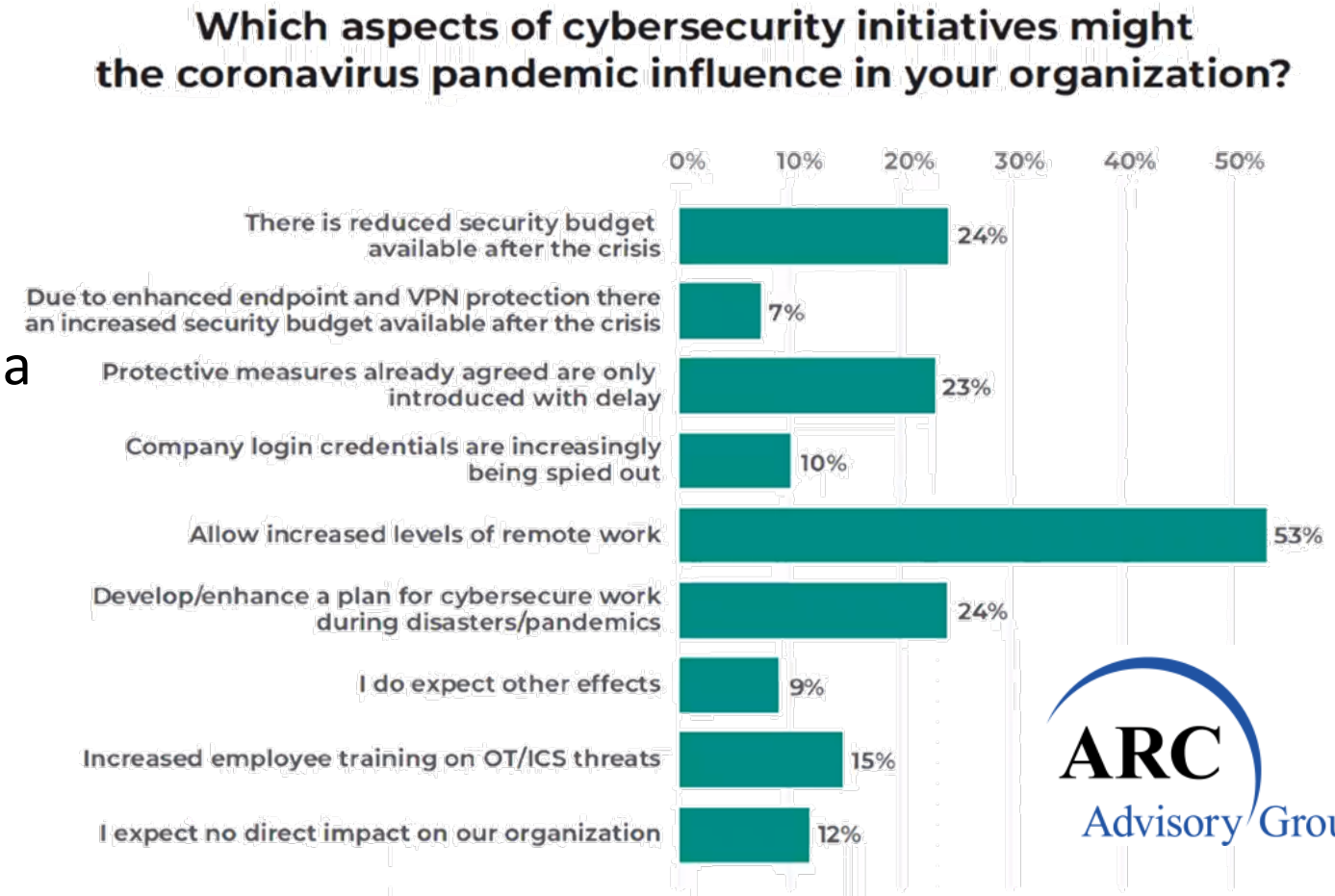




ServiTecno
Technology 4.0 da 40 anni

L'impatto del COVID-19 sulle iniziative di Cyber Security e in genere sui nuovi Progetti

- Spesa Cyber Security è aumentata durante fase 1 di COVID-19: è ancora sostenibile?
- Per il 24% la riduzione CAPEX porta a minore spesa per Cyber Security
- Nuovi progetti difficili a causa restrizioni attività on-site di tecnici e installatori
- Salvaguardiamo la spesa per proteggere accessi da remoto

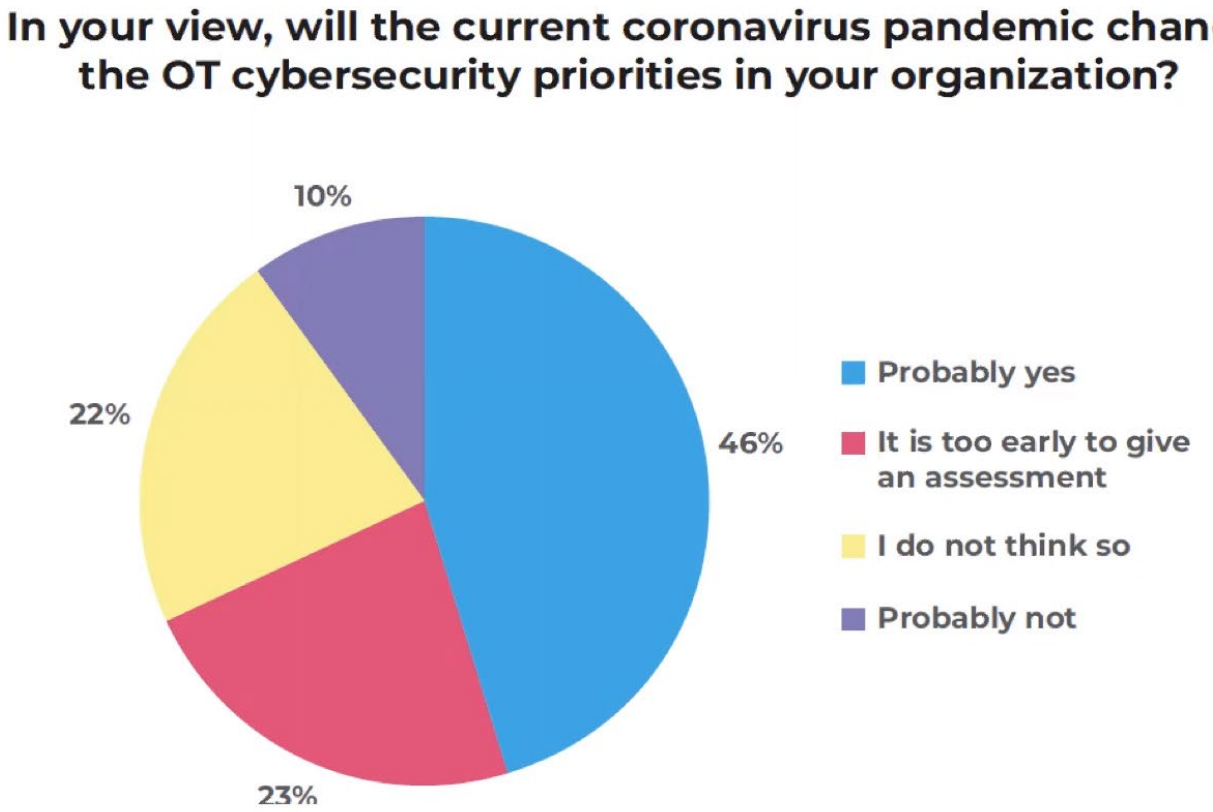


Q10 – Global pandemic influences. 606 answers from 337 participants. "Prefer not to answer" (PNA) excluded.

BAYSHORE NETWORKS
INDUSTRIAL AND IT NETWORK SECURITY

Via Francesco Koristka, 10 – 20154 Milano
Tel. +39 02 48 61 41 - Fax +39 02 48 61 44 41
info@servitecno.it - www.servitecno.it

Impatto del COVID-19 sulle priorità Cyber Security



Q9 – Global coronavirus impact on OT cybersecurity. 336 answers from 337 participants[3].

La pandemia cambierà le priorità OT Cyber Security per quasi il 50% degli intervistati

BAYSHORE NETWORKS
INDUSTRIAL AND IT NETWORK SECURITY

ARC Advisory Group

Via Francesco Koristka, 10 – 20154 Milano
Tel. +39 02 48 61 41 - Fax +39 02 48 61 44 41
info@servitecno.it - www.servitecno.it

Impatto del COVID-19 sulle sfide della Cyber Security

Q8 – Global cybersecurity related challenges. 758 answers from 337 participants. PNA excluded.

Preoccupazioni/Sfide:

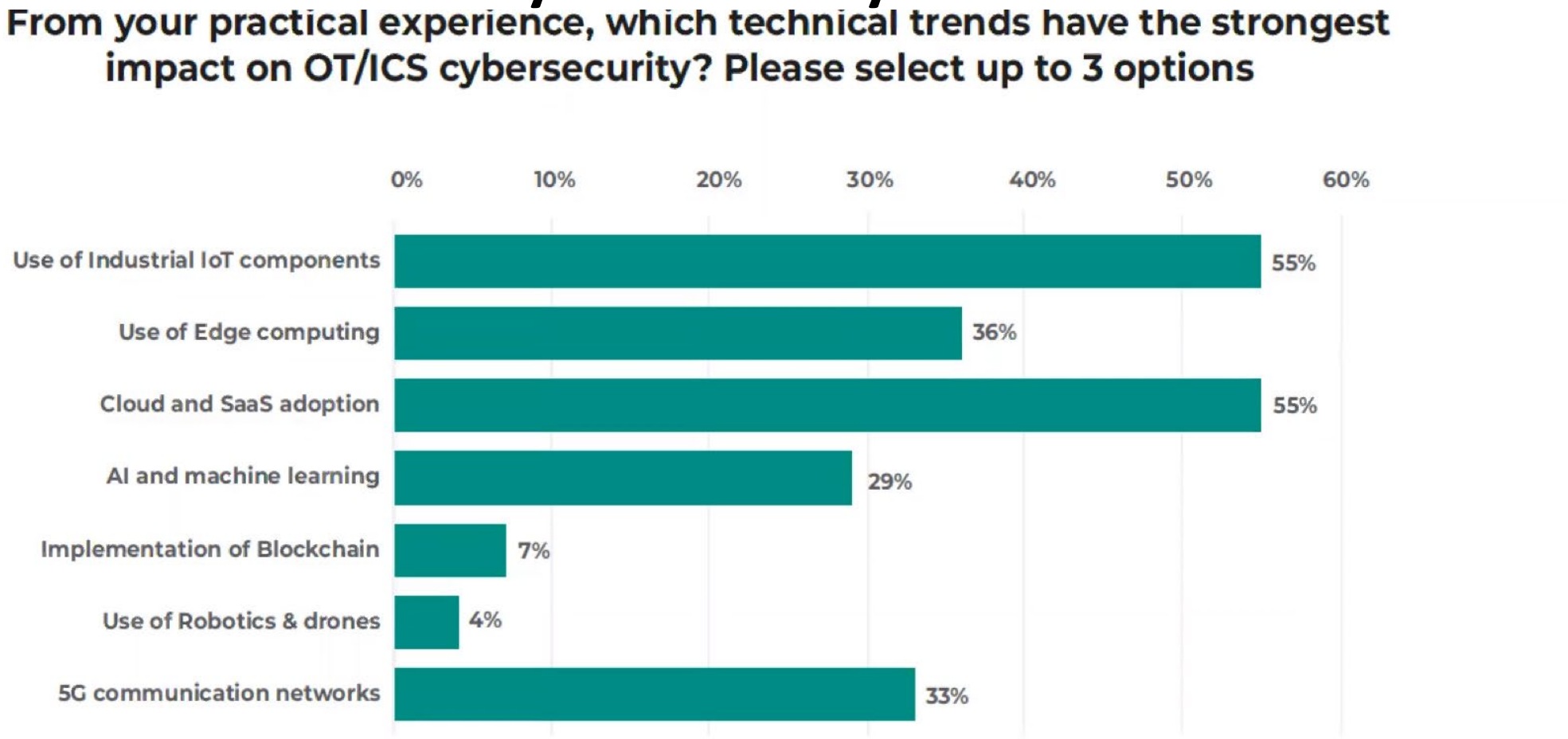
- Safety/Incolumità persone
- Danni a prodotto/servizio
- Perdita I.P.
- Costi/impatto ripartenza
- Danno reputazione

BAYSHORE NETWORKS
INDUSTRIAL AND IT NETWORK SECURITY

ARC Advisory Group

Via Francesco Koristka, 10 – 20154 Milano
Tel. +39 02 48 61 41 - Fax +39 02 48 61 44 41
info@servitecno.it - www.servitecno.it

Impatto del COVID-19 sui trend legati alla Cyber Security



Q26 – Global digital trends impact OT cybersecurity. 756 answers from 337 participants. PNA excluded.

BAYSHORE NETWORKS
INDUSTRIAL AND IT NETWORK SECURITY

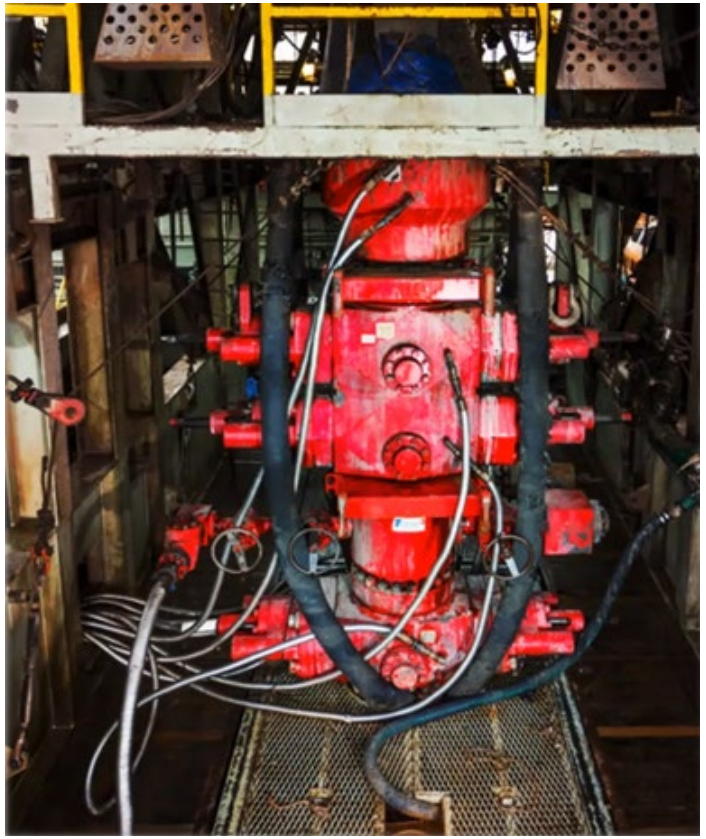
ARC Advisory Group

Via Francesco Koristka, 10 – 20154 Milano
Tel. +39 02 48 61 41 - Fax +39 02 48 61 44 41
info@servitecno.it - www.servitecno.it

ServiTecno
Technology 4.0 da 40 anni

COVID-19 Business & Cybersecurity situazione: esempio Oil & Gas

- **Asset datati** «non-smart» vengono **connessi al Cloud (IIoT)**
- **Sistemi «oscuri»**, "proprietari" o non documentati e **non protetti**
- Ridotto **Skill del personale OT** e la **complessità di cyber security** sono preoccupazioni
- Convergenza di **Cyber Security e Safety**/Sicurezza Fisica
- **Operations** autonome e **controllate da remoto**



BAYSHORE NETWORKS
INDUSTRIAL AND IT NETWORK SECURITY

ARC Advisory Group

1979-2019 TECHNOLOGY 4.0 DA 40 ANNI
Via Francesco Koristka, 10 – 20154 Milano
Tel. +39 02 48 61 41 - Fax +39 02 48 61 44 41
info@servitecno.it - www.servitecno.it

COVID-19 Business & Cybersecurity situazione: es. Farmaceutico & Life Sciences

- **Aziende Farmaceutiche** preoccupate per **integrità e perdita di dati** critici
- **APT** (Advanced Persistent Threats) mirano a **dati della ricerca sul vaccino**
- **Healthcare** è un settore nel mirino di attacchi **ransomware**
- **Dispositivi medici** (Medical Devices) che non forniscono **adeguate garanzie di sicurezza**

Russia trying to steal COVID-19 vaccine data, say UK, U.S. and Canada

By William James, Steve Scherer

3 MIN READ

LONDON/OTTAWA (Reuters) - Hackers backed by the Russian state are trying to steal COVID-19 vaccine and treatment research from academic and pharmaceutical institutions around the world, Britain's National Cyber Security Centre (NCSC) said on Thursday.

DOJ Accuses China of Targeted Hacking on COVID-19 Research Data

Two hackers are accused by DOJ of working with the Chinese government to target and hack hundreds of US entities, stealing more than a terabyte of data, including COVID-19 research.[14]

DoJ = US Department of Justice

ARC Advisory Group

BAYSHORE NETWORKS
INDUSTRIAL AND IT NETWORK SECURITY

Via Francesco Koristka, 10 – 20154 Milano
Tel. +39 02 48 61 41 - Fax +39 02 48 61 44 41
info@servitecno.it - www.servitecno.it

Migliorare la Cyber Resilienza di SCADA e sistemi di automazione esistenti, come opportunità per tornare a parlare con i Clienti di nuovi progetti in epoca di lockdown.

1979-2019 TECHNOLOGY 4.0 DA 40 ANNI
Via Francesco Koristka, 10 – 20154 Milano
Tel. +39 02 48 61 41 - Fax +39 02 48 61 44 41
info@servitecno.it - www.servitecno.it

La strategia di Protezione nell'Architettura di Rete

Internet

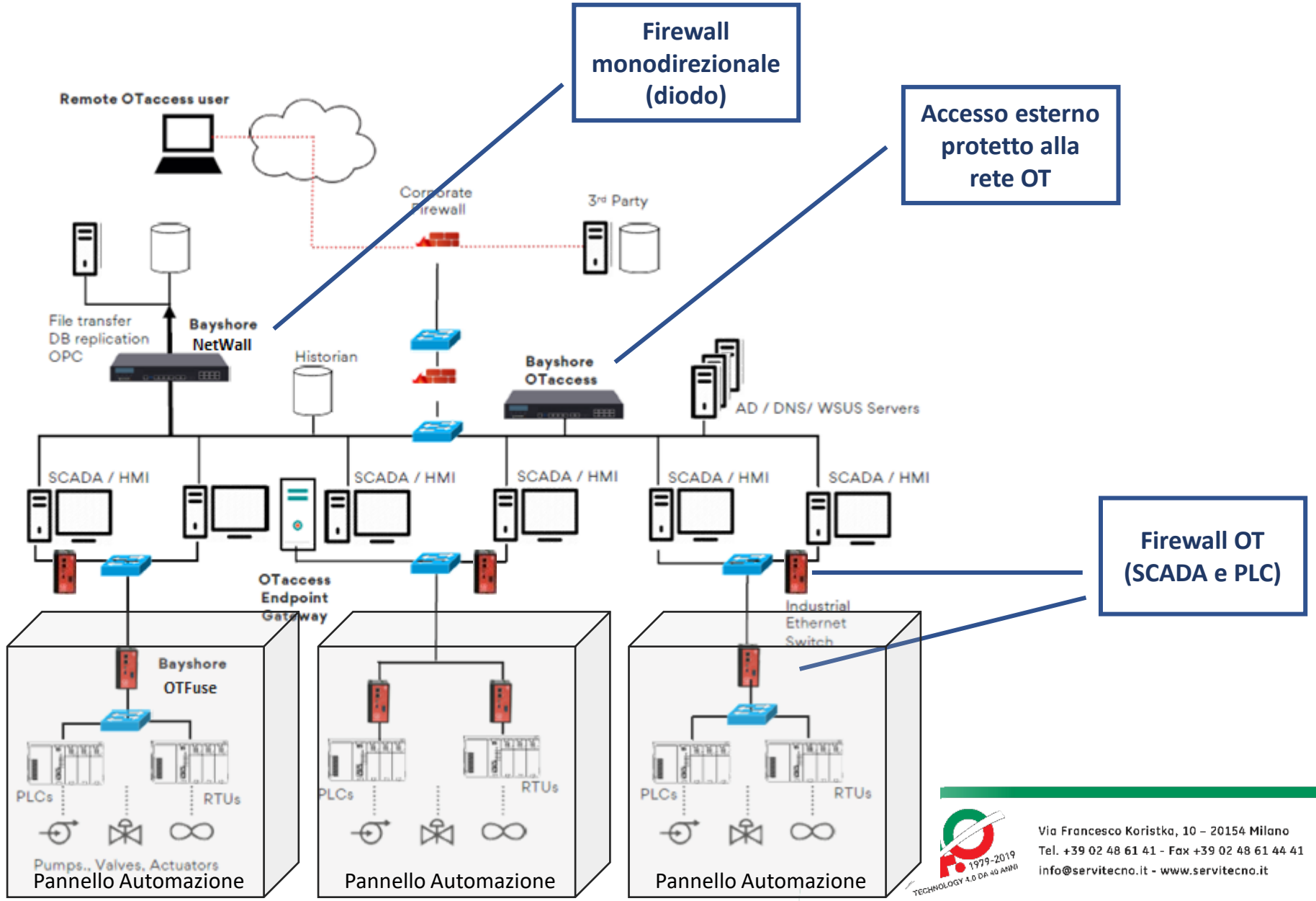
Level 4
IT Network

Level 3
Operations

Level 2
Process Network

Level 1
Control Network

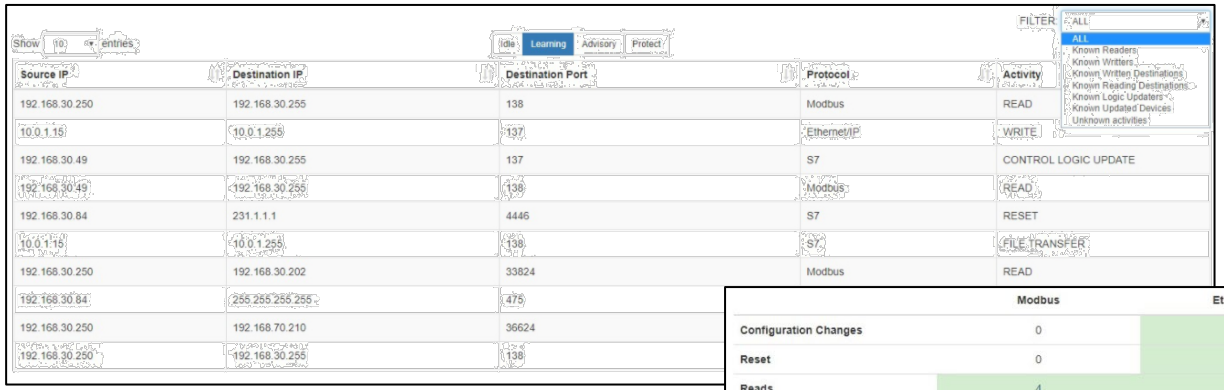
Level 0
Field Network



Via Francesco Koristka, 10 – 20154 Milano
Tel. +39 02 48 61 41 - Fax +39 02 48 61 44 41
info@servitecno.it - www.servitecno.it

Bayshore OTFuse

- OTfuse offre una protezione completa per I PLCs e tutti gli SCADA/DCS
- Ha supporto nativo per Modbus, Ethernet/IP, S7, DNP3, BACnet, SLMP, FINS, EGD
- Reports via Modbus per l'HMIs
- Syslog e email alerting
- Autenticazione Hardware per setup/admin (doppia chiave hardware)
- Contenitore Standard DIN rail, alimentazione 24VDC
- Si installa in meno di 1 ore



Reject unauthorized...	Protect PLCs and SCADA/DCS devices from...	Modbus	Ethernet/IP	Siemens S7	SLMP	FINS	DNP3	Bacnet
Config Changes	Attempted config changes from unknown sources	✓	✓	✓	✓	✓	✓	✓
Device Resets	Attempted writes/resets from unknown sources	✓	✓	✓	✓	✓	✓	✓
Device Reads	Attempted interrogations from unknown sources	✓	✓	✓	✓	✓	✓	✓
Logic Updates	Programming changes		✓	✓	✓	✓	✓	✓
		✓	✓	✓	✓	✓	✓	✓

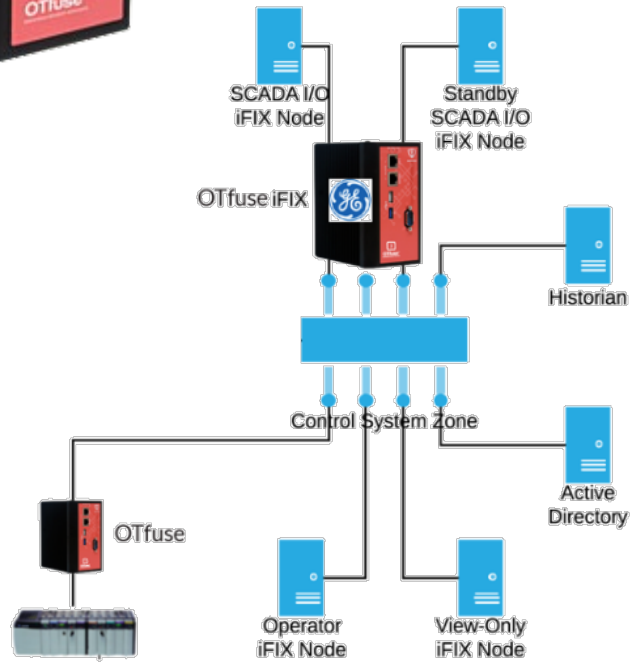
	Modbus	Ethernet/IP	S7	DNP3
Configuration Changes	0	3	0	0
Reset	0	2	0	1
Reads	4	2	4	0
Logic Updates	N/A	0	0	1
File Transfers	N/A	0	0	0

BAYSHORE NETWORKS
INDUSTRIAL AND IT NETWORK SECURITY

Via Francesco Koristka, 10 – 20154 Milano
Tel. +39 02 48 61 41 - Fax +39 02 48 61 44 41
info@servitecno.it - www.servitecno.it

Bayshore OTFuse iFIX

- OTfuse offre una protezione completa per **tutti gli SCADA e GE Digital IFIX** specialmente
- Ha supporto nativo per i protocolli di rete iFIX (vedi scheda)
- Reports via Modbus per l'HMIs
- Syslog e email alerting
- Autenticazione Hardware per setup/admin (doppia chiave hardware)
- Contenitore Standard DIN rail, alimentazione 24VDC
- Si installa in meno di 1 ora



PROTOCOL SUPPORT

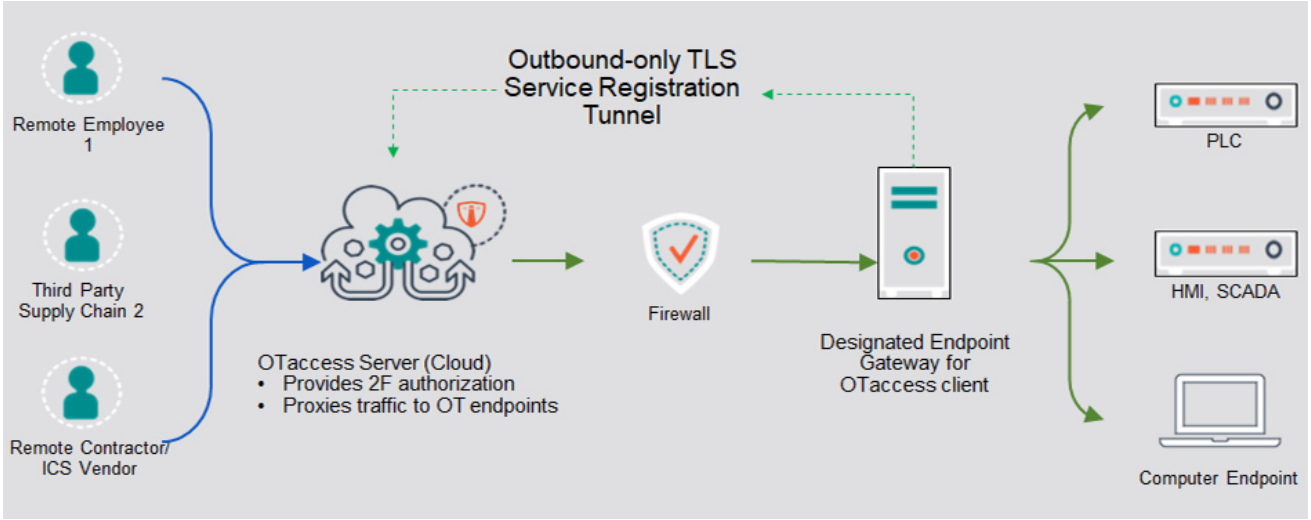
Protocol	Variable Access	Alarm Handling	Session Alarming	Connection Management	Data Transfer	MDBA Handshake
Read Functions	✓	✓	✓	✓	✓	✓
Write Functions	✓	✓	✓	✓	✓	✓

BAYSHORE NETWORKS
INDUSTRIAL AND IT NETWORK SECURITY

Via Francesco Koristka, 10 – 20154 Milano
Tel. +39 02 48 61 41 - Fax +39 02 48 61 44 41
info@servitecno.it - www.servitecno.it

Bayshore OTAccess

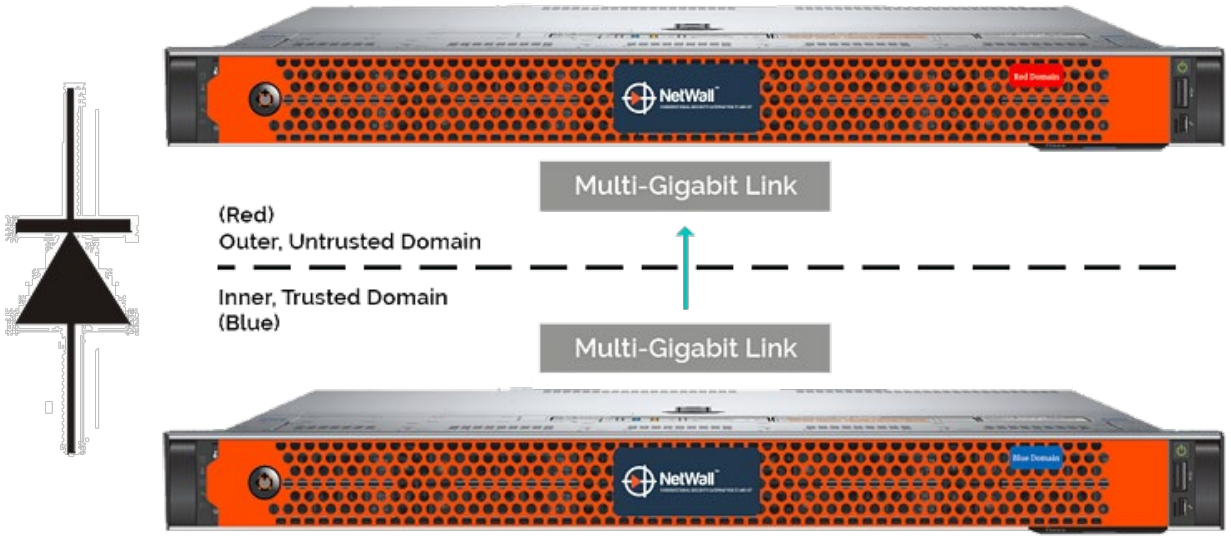
- Supporto nativo dei protocolli OT per **l'ispezione e la prevenzione delle intrusioni**
- **Deep Content Inspection** delle attività dell'utente
- Opzioni per modelli di distribuzione in hosting e on site
- Non sono necessarie apparecchiature di rete aggiuntive
- Applicazione delle **policy basata sul comportamento**
- Protezione attraverso ispezioni continue durante le sessioni utente
- Modelli di configurazione gerarchici per l'utilizzo da parte degli utenti interni e fornitori di terze parti



BAYSHORE NETWORKS
INDUSTRIAL AND IT NETWORK SECURITY

Via Francesco Koristka, 10 – 20154 Milano
Tel. +39 02 48 61 41 - Fax +39 02 48 61 44 41
info@servitecno.it - www.servitecno.it

Bayshore NetWall



- **Trasferisce i dati** dalla **rete affidabile** (impianto) senza esporre le macchine a una **rete non affidabile** (IT aziendale, destinazioni aziendali)
- Funzionalità di **diodo dati unidirezionale** che fornisce un ponte di air-gap industriale per limitare e abilitare le comunicazioni da risorse sensibili e riservate
- **Consegna garantita** da origine a destinazione con verifica dimostrabile (a differenza della maggior parte dei gateway unidirezionali che utilizzano metodi di ritrasmissione)
- **Ridotti costi e complessità** dell'accesso solo fisico o dei diodi dati con una soluzione di connettività più **efficace ed efficiente**

BAYSHORE NETWORKS
INDUSTRIAL AND IT NETWORK SECURITY

Via Francesco Koristka, 10 – 20154 Milano
Tel. +39 02 48 61 41 - Fax +39 02 48 61 44 41
info@servitecno.it - www.servitecno.it

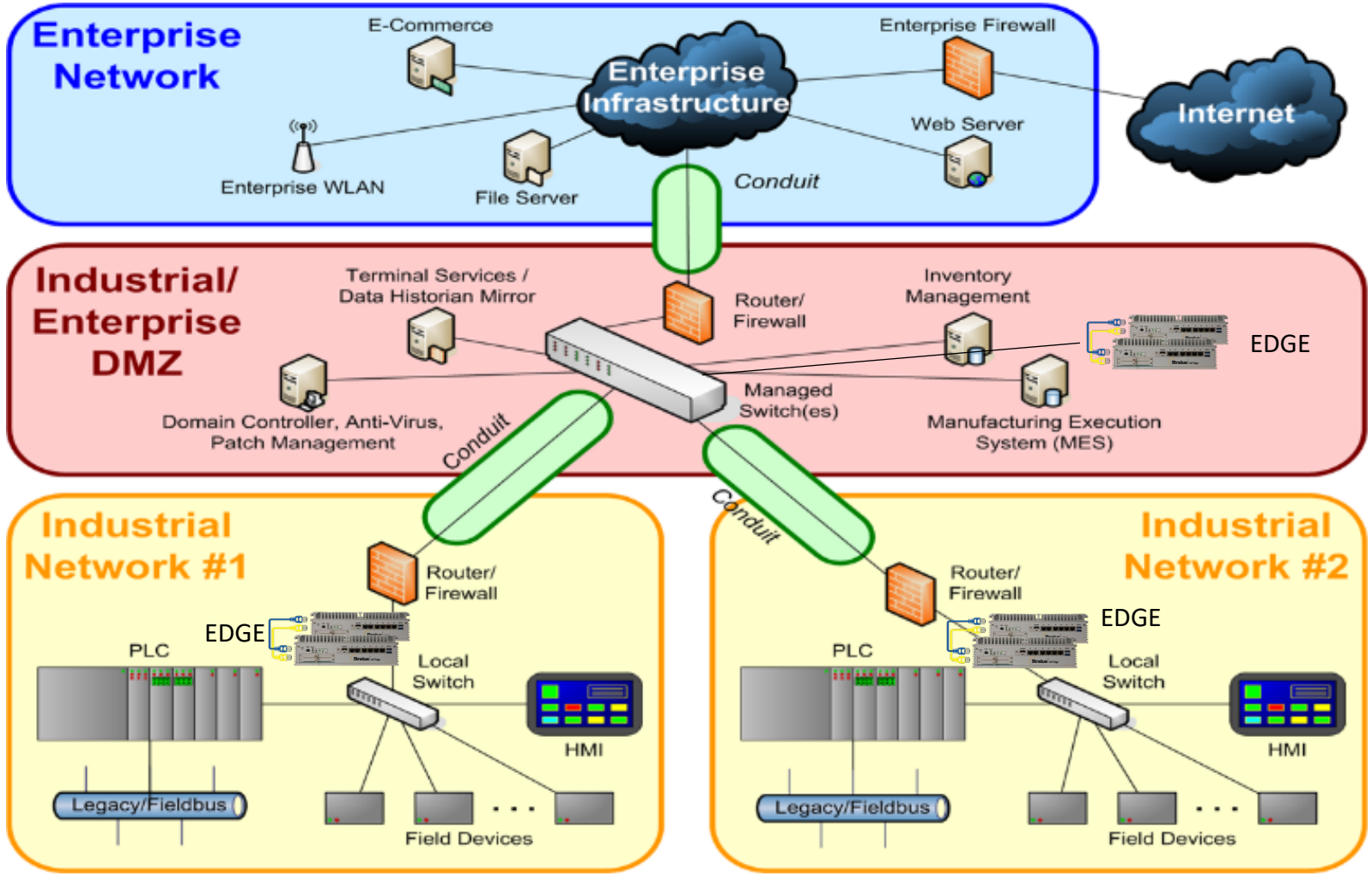
ServiTecno
Technology 4.0 da 40 anni

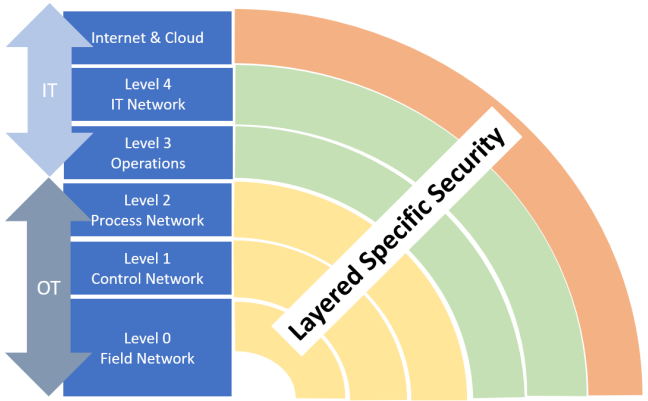
Le soluzioni Cyber Security ICS/OT per reti di fabbrica e l'integrazione con il Cloud

BAYSHORE NETWORKS
INDUSTRIAL AND IT NETWORK SECURITY

Via Francesco Koristka, 10 – 20154 Milano
Tel. +39 02 48 61 41 - Fax +39 02 48 61 44 41
info@servitecno.it - www.servitecno.it

IEC 62443 Architettura di sicurezza logica (Zones & Conduits…and Edge)



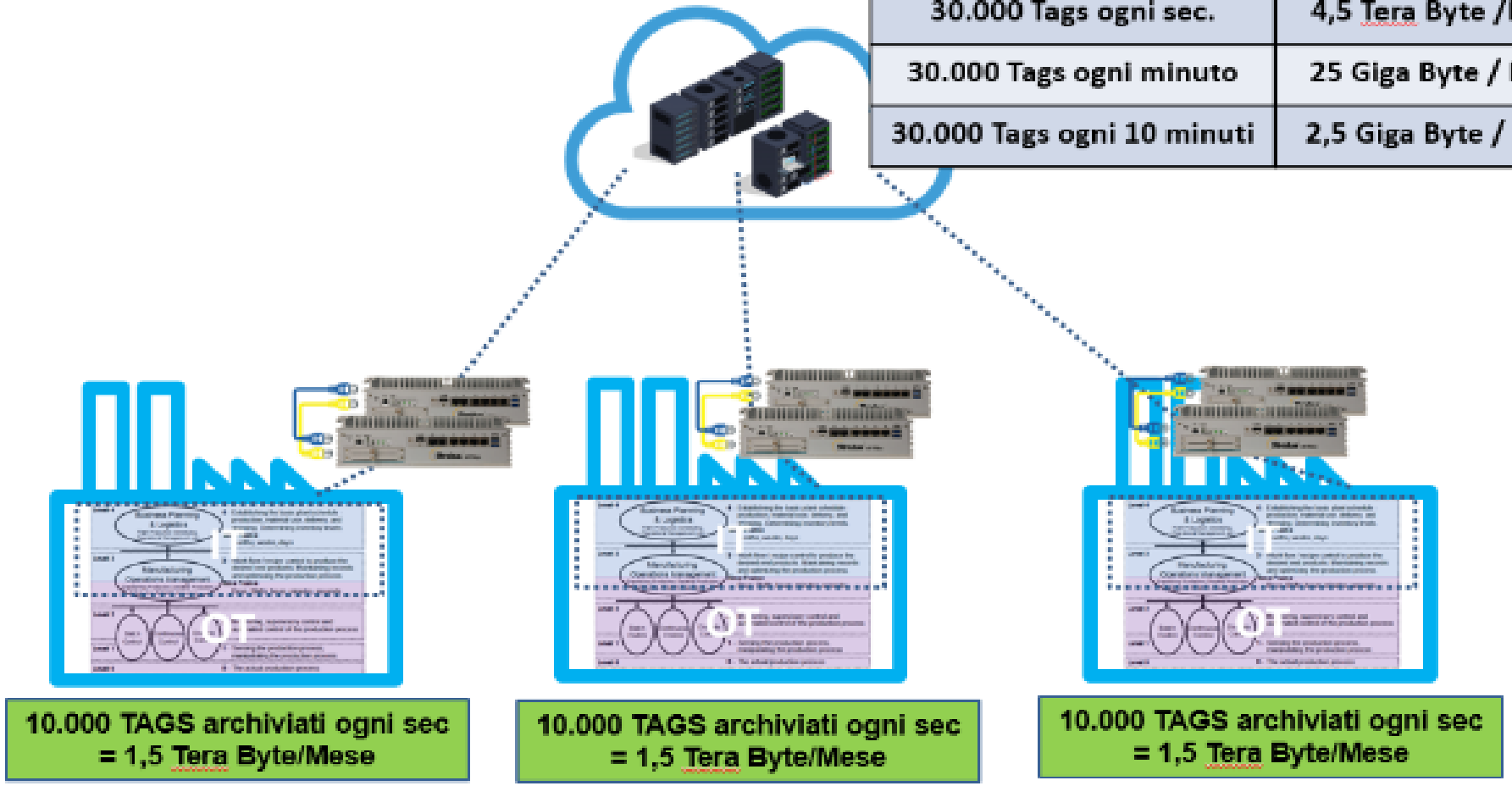


BAYSHORE NETWORKS
INDUSTRIAL AND IT NETWORK SECURITY

Via Francesco Koristka, 10 – 20154 Milano
Tel. +39 02 48 61 41 - Fax +39 02 48 61 44 41
info@servitecno.it - www.servitecno.it

Abbattimento della quantità di dati trasferiti attraverso l'EDGE

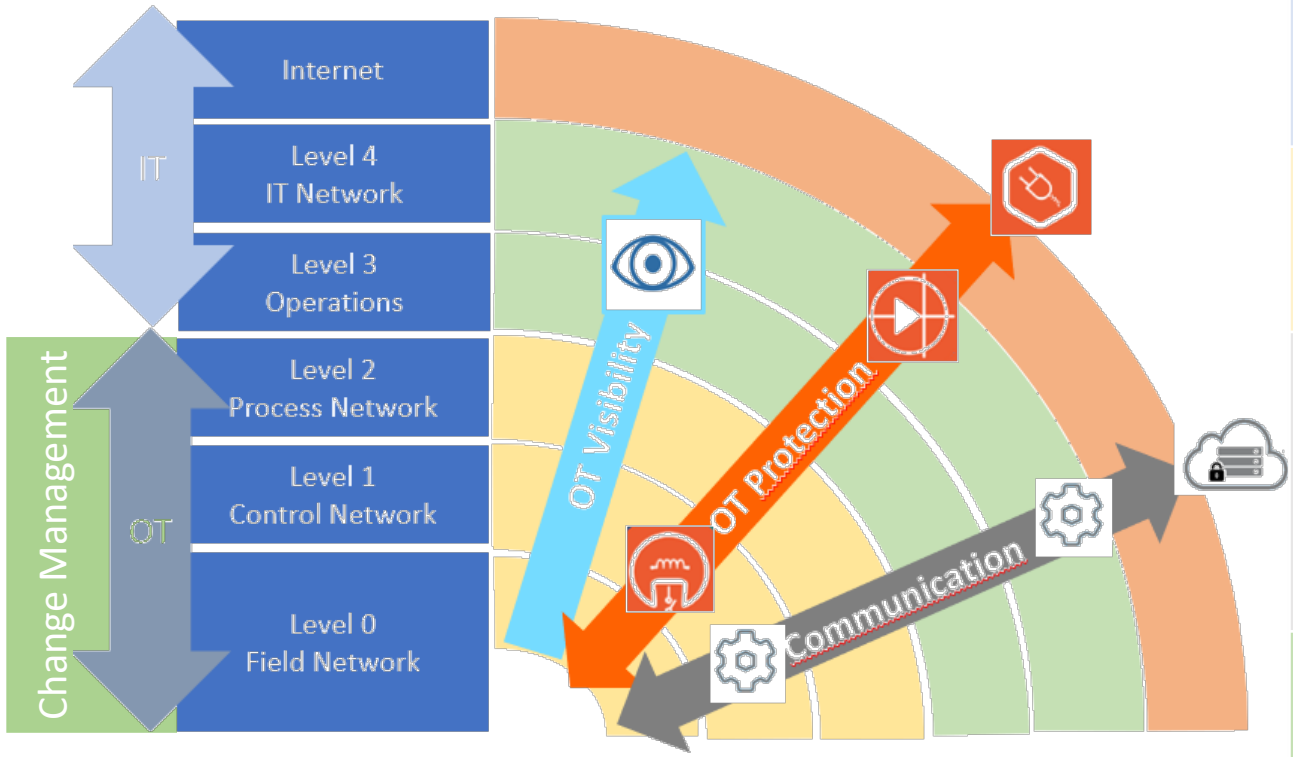
30.000 Tags ogni sec.	4,5 Tera Byte /Mese
30.000 Tags ogni minuto	25 Giga Byte / Mese
30.000 Tags ogni 10 minuti	2,5 Giga Byte / Mese



Via Francesco Koristka, 10 – 20154 Milano
Tel. +39 02 48 61 41 - Fax +39 02 48 61 44 41
info@servitecno.it - www.servitecno.it

ServiTecno
Technology 4.0 da 40 anni

Strategie di Protezione OT/ICS: Layered Security (NIST)



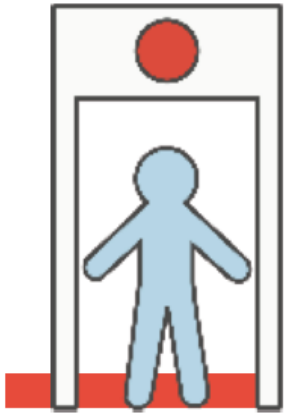
Assessment & Visibility	Identify (Asset Inventory & Intelligence)
	Assess (Vulnerability & Remediation)
	Detect (Anomaly & Threats)
	Act (Dashboard Alerts, Highlights & Notification)
Protection	Access On Site (VPN, High granular access policies)
	OT Segmentation (self configuration, DPI)
	AirGap bridge
Secure Streaming of Data	Data Tunneling (OPC DA/UA, Modbus)
	Data Bridge (OPC DA<->UA, OPC DA/UA<->Modbus)
	Data Gateway (OPC DA/UA, ModBus, MQTT)
	Data Logging (OPC DA/UA, Modbus to SQL)
	Cloud Secure Streaming (VPN)
Change Management & Control	PLC, ICS, SCADA versioned back-up
	SW & configuration scheduled consistency control
	Disaster Recovery

BAYSHORE NETWORKS
INDUSTRIAL AND IT NETWORK SECURITY

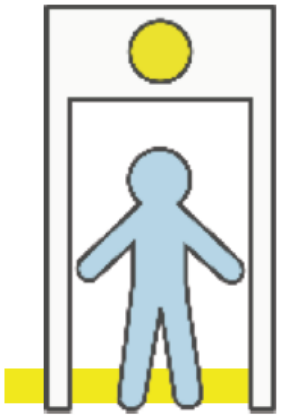
Via Francesco Koristka, 10 – 20154 Milano
Tel. +39 02 48 61 41 - Fax +39 02 48 61 44 41
info@servitecno.it - www.servitecno.it

Strategie di Protezione OT: Layered Security (Esempio)

Last line of defense



STEP
03
Reinforced, locked cockpit door
Last line of defense / Endpoint protection



STEP
02
Only ticketed Passengers allowed on board
Segmentation (Authentication / Authorization enforcement)

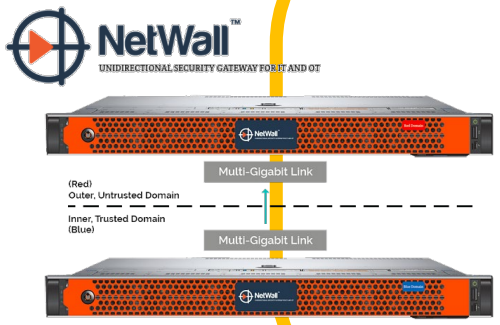
ID check / Physical inspection
Perimeter protection
STEP
01

BAYSHORE NETWORKS
INDUSTRIAL AND IT NETWORK SECURITY

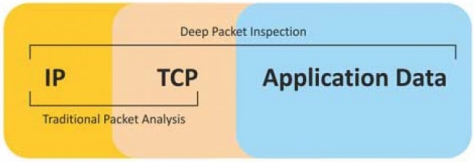
Via Francesco Koristka, 10 – 20154 Milano
Tel. +39 02 48 61 41 - Fax +39 02 48 61 44 41
info@servitecno.it - www.servitecno.it

Open & Closed Loop in the Cloud

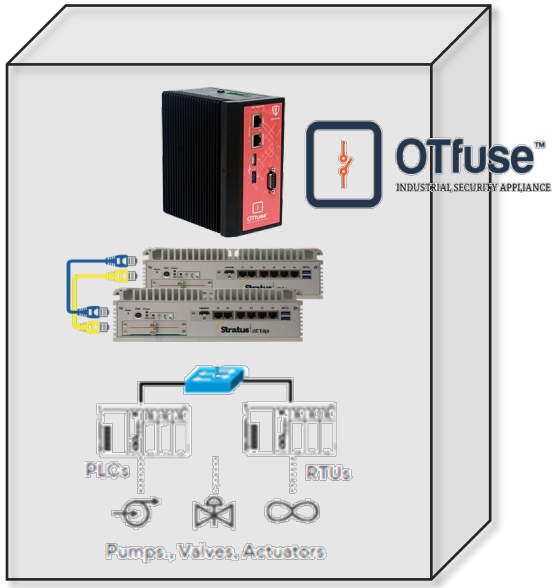
Cloud



DPI & DCI
Deep Content and Packet Inspection



Edge



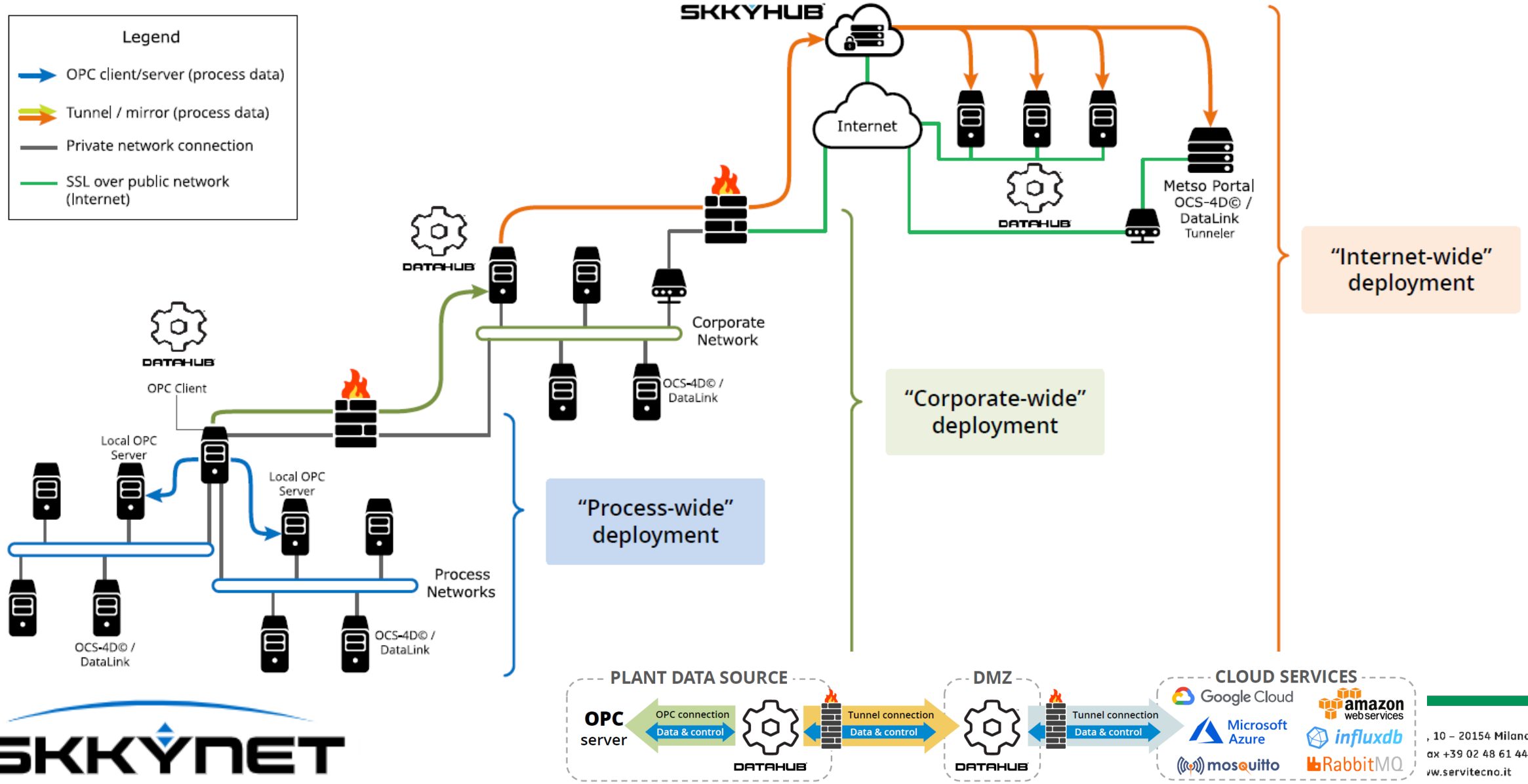
Automation

BAYSHORE NETWORKS
INDUSTRIAL AND IT NETWORK SECURITY

Via Francesco Koristka, 10 – 20154 Milano
Tel. +39 02 48 61 41 - Fax +39 02 48 61 44 41
info@servitecno.it - www.servitecno.it

ServiTecno
Technology 4.0 da 40 anni

La strategia di Trasferimento Dati nell'Architettura Corporate



SKKYNET

, 10 – 20154 Milano
ax +39 02 48 61 44 41
ww.servitecno.it

ServiTecno
Technology 4.0 da 40 anni

Dubbi? Domande?

Riferimenti:

Enzo M Tieghi
etieghi@clusit.it

Mario Testino
mtestino@servitecno.it

GE Digital
Alliance Partner

OT/ICS Cyber Security e Pandemia

www.servitecno.it