SAVE
web edition
27 - 28 ottobre 2020

Tre punti da considerare per *la* ***cyber security***:
ultima linea di difesa, ***anomaly detection*** e ***piano B***

ServiTecno

1900

Velocità massima 100 Km/h
Quando la massima in carrozza era 20-30 km/h

Ma con una mortalità dell’85%

2020

Industry 4.0 permette un miglioramento sino all’80% della produzione

Ma con vulnerabilità sui sistemi:
Informazioni riservate e brevetti
Sicurezza fisica delle persone

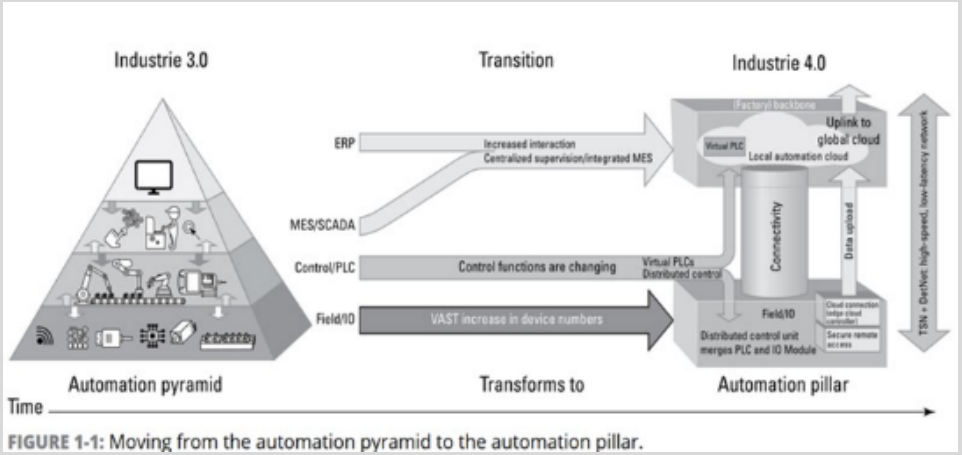
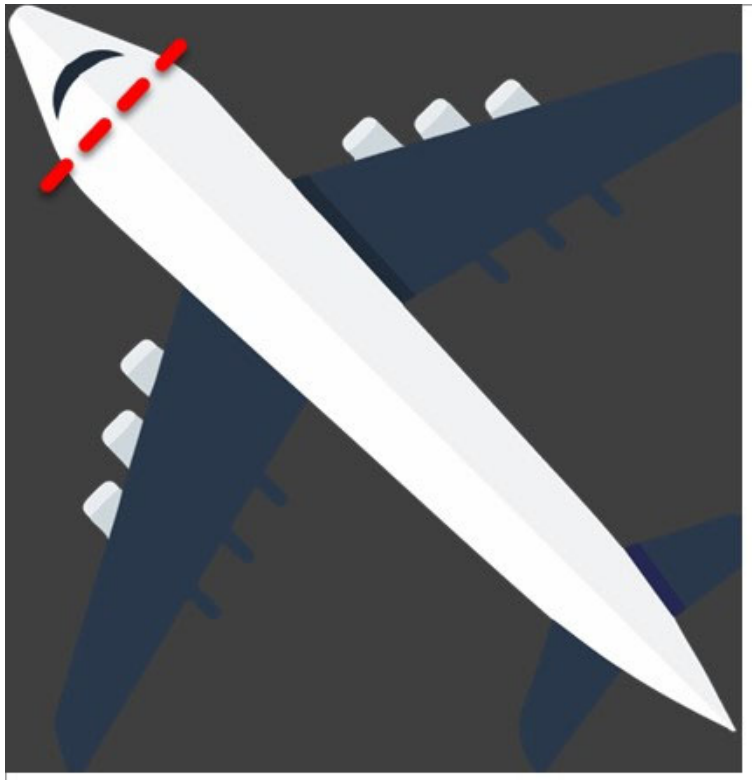


FIGURE 1-1: Moving from the automation pyramid to the automation pillar.

SAVE web edition



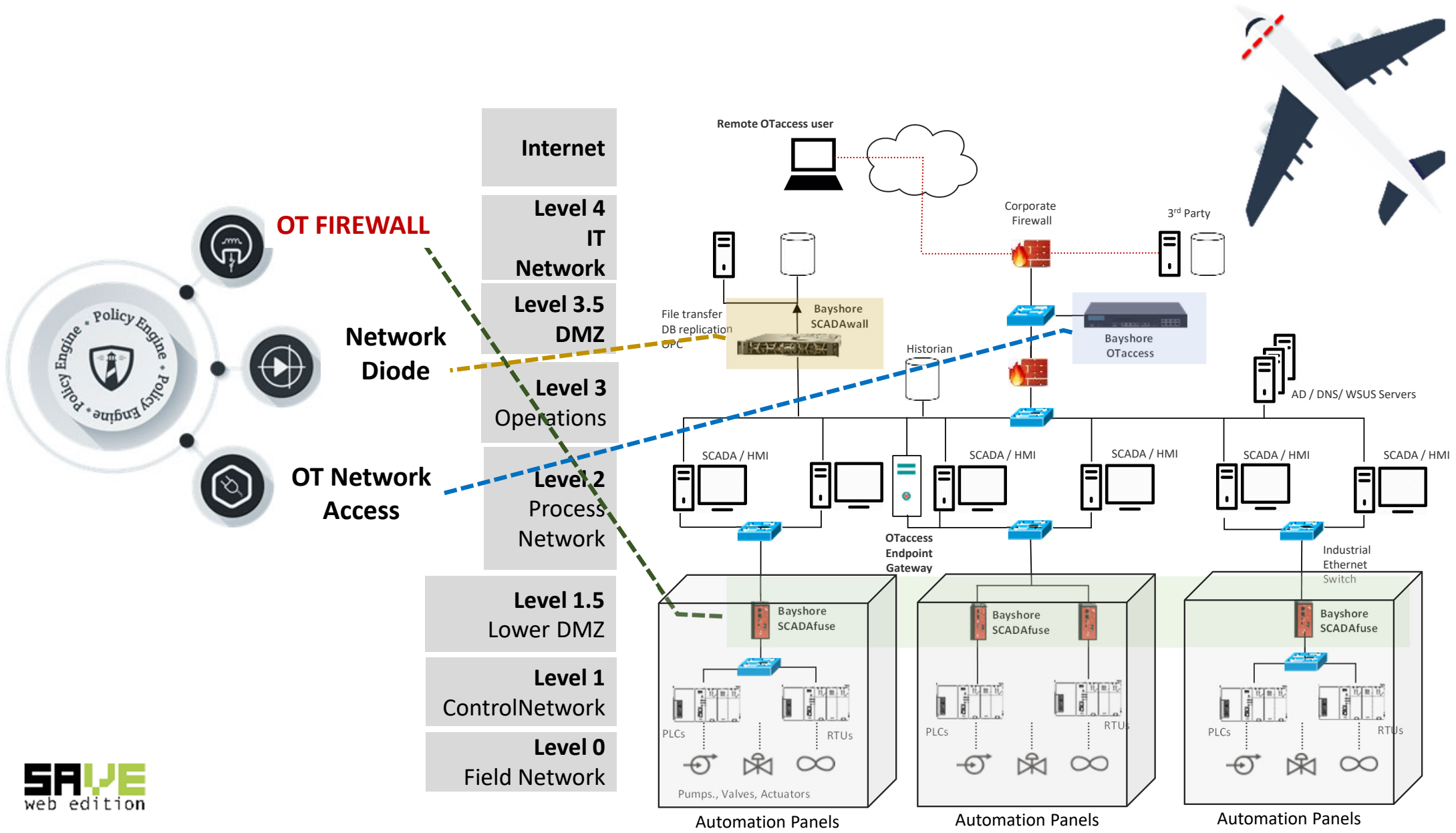
ULTIMA LINEA
DI DIFESA

ANOMALY
DETECTION

IL PIANO
«B»

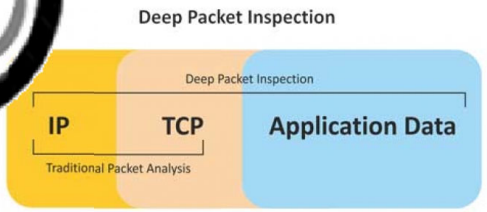
Come gestire il budget per la Cyber Security 2021?

SAPE
web edition



SAVE web edition

Perché utilizzare dispositivi di sicurezza industriali?



Modbus

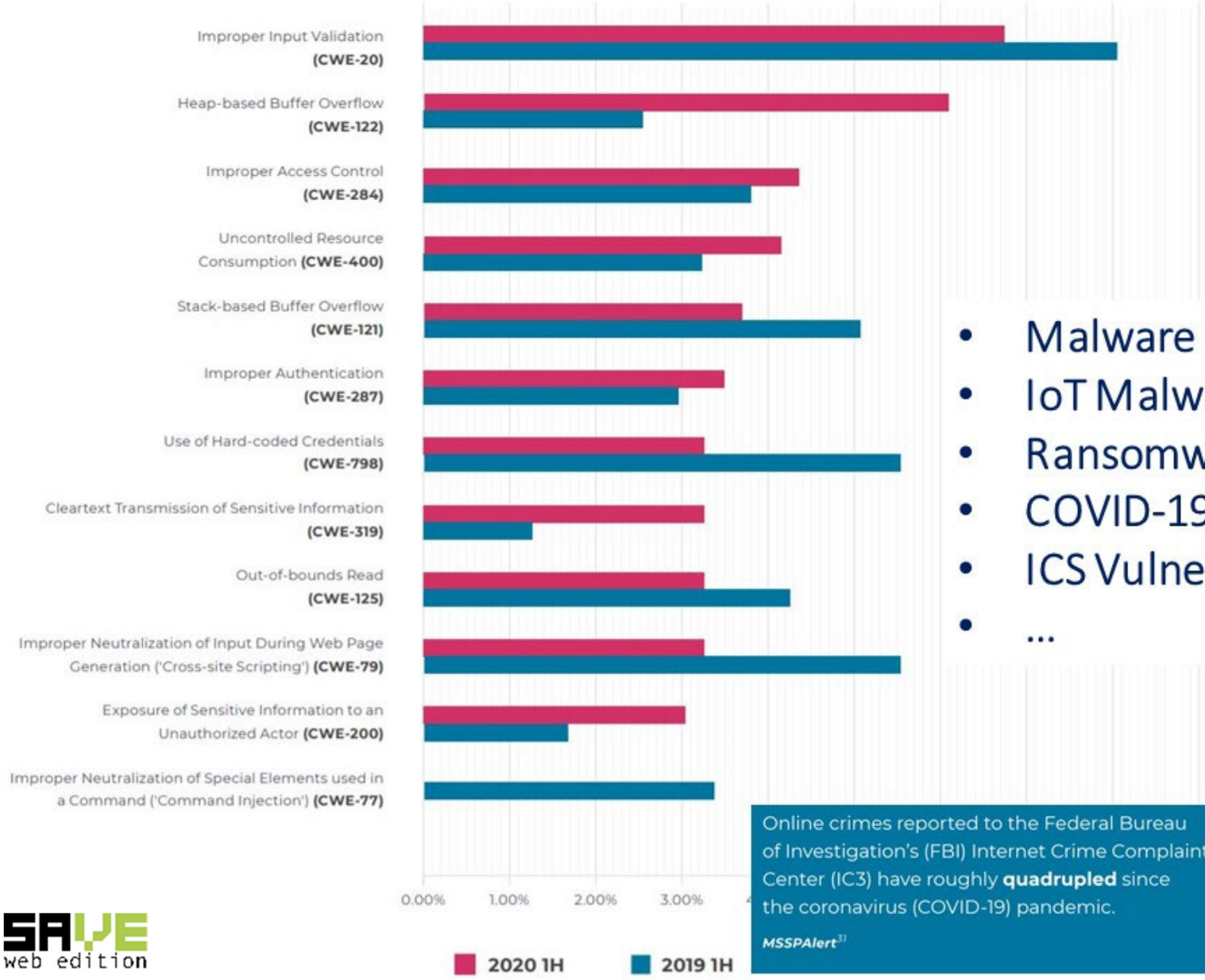
EtherNet/IP

PROFINET INDUSTRIAL ETHERNET

SAVE web edition

Perché Firewall OT?

- Perché l'hardware ha caratteristiche industriali tali da poter essere installati a livello di production floor nei quadri elettrici di automazione
- Perché sono stati progettati per avere un manutenibilità ridotta e semplificata
- Perché non è necessario essere specialisti di rete per poterli configurare
- Perché riescono ad analizzare in profondità di protocolli di rete industriali, conoscendone le caratteristiche e le funzionalità



- Malware
- IoT Malware (Tactics & Techniques)
- Ransomware (Tactics & Techniques)
- COVID-19 Themed Malware
- ICS Vulnerabilities
- ...

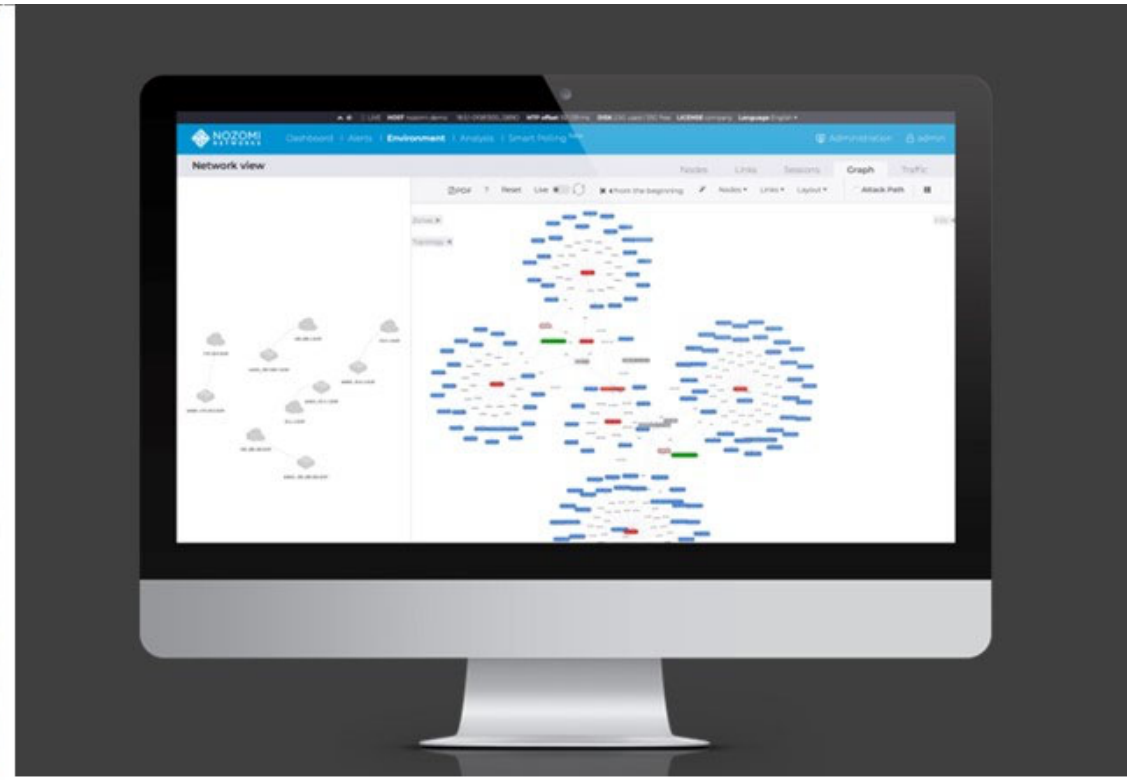
Online crimes reported to the Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center (IC3) have roughly **quadrupled** since the coronavirus (COVID-19) pandemic.

MSSPAlert[37]

before the pandemic 1,000/day

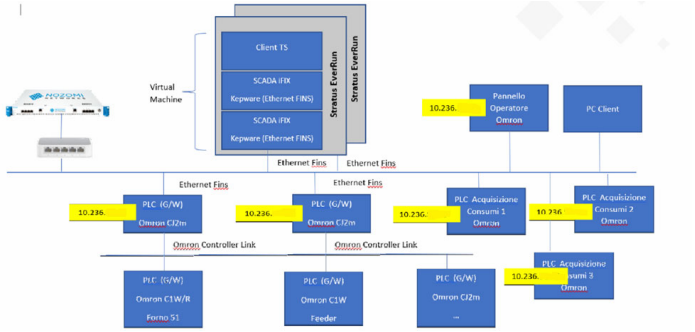
since the pandemic 4,000/day

SAVE web edition



MEGLIO UNA FOTO O UN VIDEO?

Quali Sono i principali Findings di un POC?

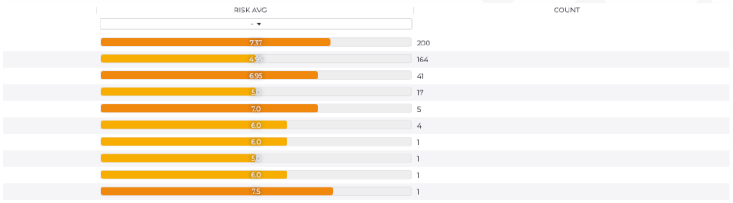


Win XP host

Port scan on the network

Internet Connections to public IPs

Main alerts and types



icked up by Guardian during the PoC.
n the most relevant in terms of risk.

www.nozominetworks.com/ CONFIDENTIAL 15

alerts for attempted over a variety of

ict in control od of threat increases ence makes a

ess to/from the tworks that require ol networks.

/ CONFIDENTIAL 19

301) on

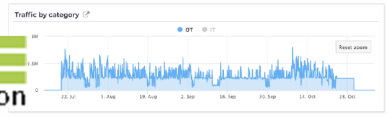
eck if

NTIAL 22

epth.

IAL

Throughput



Findings

This graph shows the throughput all over the network. As we see, everything is green indicating that there are no peaks in terms of high load links. The graph below indicates an average rate for OT protocols of approx. 2Mbps.

Level of Risk

NA

Suggested Action

None

www.nozominetworks.com/ CONFIDENTIAL 9

SAVE web edition

Nei POC cosa abbiamo trovato

Abbiamo trovato:

- Pochissima segmentazione di rete (reti largamente piatte)
- Una quantità enorme di apparati obsoleti (PC, PLC, SO, Schede, Interfacce)
- Un grande numero di vulnerabilità standard non rilevate CVE
- Un grande numero di dispositivi IP in rete non inventariati
- Moltissime connessioni sconosciute a IP pubblici da IP di impianto
- Pochi controlli sugli accessi dall'esterno
- Identificati e tracciati Port Scan sulla rete

Piano B

RECOVERY POINT/TIME OBJECTIVE

Ripartire in fretta, 50 sfumature di versioning

SAVE web edition

Perché OT Versioning?

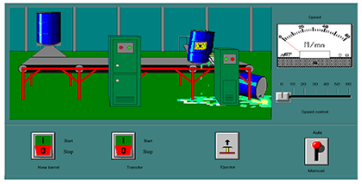
Conveyor from current

Application Logic from Current
(Revision: 68)

```
174  ENDIF;
175
176  IF Cycle == 1 THEN
177    VerticalMove = VerticalMove + Speed;
178    IF VerticalMove >= 41 THEN
179      VerticalMove = 45;
180      IF Auto THEN
181        Cycle = 2;
182      ENDIF;
183    ENDIF;
184  ENDIF;

255  IF Cycle == 7 THEN
256    Ejector = 1;
257    IF HorizontalMove < 272 THEN
258      HorizontalMove = HorizontalMove + Speed;
259    ELSE
260      HorizontalMove = 274;
261      Cycle = 5;
262    ENDIF;
263  ENDIF;
264
265  ENDIF;
```

Conveyor from ver000-00001 (Revision: Current)



Application Logic from Current
(Revision: 67)

```
174  ENDIF;
175
176  IF Cycle == 1 THEN
177    VerticalMove = VerticalMove + Speed;
178    IF VerticalMove >= 41 THEN
179      VerticalMove = 41;
180      IF Auto THEN
181        Cycle = 2;
182      ENDIF;
183    ENDIF;
184  ENDIF;

255  IF Cycle == 7 THEN
256    Ejector = 1;
257    IF HorizontalMove < 272 THEN
258      HorizontalMove = HorizontalMove + Speed;
259    ELSE
260      HorizontalMove = 272;
261      Cycle = 5;
262    ENDIF;
263  ENDIF;
264
265  ENDIF;
```

SAVE web edition

Adobe
- Adobe pdf

AUTODESK AUTOCAD
- AutoCAD DWG

AVEVA
- InTouch
- System Platform
- CitectSCADA

FIND US ON THE AVEVA DIGITAL EXCHANGE exchange.aveva.com
- AutoSave for System Platform

Atlas Copco
- PowerFocus
- PowerMACS
- SpotPoint

AUTOMATIONDIRECT
- DirectSOFT

rexroth A Bosch Company
- Indraworks MTX CNC
- WinMTC CNC
- MTX CNC
- MTA CNC*
- WinSPS*

B&R
- Automation Studio

CODESYS
- CODESYS v2.3

COGNEX
- Insight

COMAU
- Robots

DENSO
- DENSO Robots

EMERSON
- Emerson Machine Edition

FANUC
- FANUC Robots
- FANUC CNC Controls
- FANUC PMC Controls

GE
- LogicMaster 90*
- Proficy Machine Edition
- IFIX

G & L Motion Control
- PicPro*

inductive automation
- Ignition SCADA

Kawasaki
- Kawasaki Robots

KUKA
- KUKA Robots

MDT SOFTWARE Automation Change Management
- Universal
- FTP
- ARMS
- Scripting Module
- Windows File (by extension)

MDT Universal Suite

Microsoft
- Microsoft Word
- Microsoft Excel
- Microsoft PowerPoint

MITSUBISHI ELECTRIC
- GX Developer
- GX IEC Developer
- GX Works2
- GX Works3
- GT Designer 3
- Mitsubishi C64 CNC
- Mitsubishi C70 CNC
- Mitsubishi Robots

MOTOMAN A YASKAWA COMPANY
- Motoman Robots

OMRON
- CX Programmer & Backup
- Sysmac Studio

Pro-face
- GP-Pro EX

PROMESS
- UltraPRO

Rockwell Automation
- RSLogix 5
- RSLogix 500
- RSLogix 5000
- Stratix Switches
- Logix Designer
- FactoryTalk View ME
- FactoryTalk View SE
- RSView ME
- PanelBuilder32*

Schneider Electric
- Control Expert
- Unity Pro
- Concept
- ClearSCADA
- PL7 Pro
- ProWORX32
- ProWORX NxT*
- ProWORX Plus*

Master Techology Partner

Available on exchange.se.com

SIEMENS
- 840D CNC: Solution Line
- 840D CNC: Power Line
- STEP 7
- STEP 7 Professional
- STEP 7 TIA Portal
- STEP 7 Multiproject
- STEP 5*
- WinCC TIA Portal
- WinCC
- WinCC Flexible*

Siemens Solution Partner

STÄUBLI
- Robots

Elementi per il «B-Plan»

I sistemi di elaborazione presenti in impianto sono tutti critici ed hanno caratteristiche molto diverse fra loro. Di tutti è necessario gestire la versione, controllare le variazioni ed archiviare correttamente i back-up. Per fare ciò è necessario un sistema che permetta di comprendere ed interfacciare tutte le tecnologie presenti ed essere in grado di intercettare le più piccole variazioni nei codici applicativi e nelle configurazioni generando in tempo reale report dettagliati per il personale respondabile di manutenzione e di impianto.

ServiTecno www.servitecno.it - info@servitecno.it

Mario Testino
mtestino@servitecno.it

Francesco Tieghi
ftieghi@servitecno.it

SAVE web edition