



Cybersecurity focused on Safety

Octubre 2022

Agustin Valencia Gil-Ortega

Operational Technology IBERIA





IRSC 2022

INTERNATIONAL RAILWAY
SAFETY COUNCIL

SEVILLA, OCTOBER 16-21, 2022



FORTINET®



Who am I? Agustin Valencia Gil-Ortega

Experience

OT Security Business Manager Fortinet (2021-)
Associated Professor MsC Cybersecurity Univ.Pontificia Comillas ICAI (2019-)
Head of Global OT Cybersecurity Iberdrola (2017-2021)
Head of I&C Engineering &+ Cybersecurity Director CN Cofrentes Iberdrola (2010-17)
O&M Manager CC Santurce Iberdrola (2006-2010)

Education

Industrial Engineer (Univ.Pontificia Comillas ICAI)
Msc Maintenance Management (US)
BWR Nuclear Technology Specialist (Tecnatom)
MsC Information Security (UPC-ViU), Director of Security (UDIMA)
CISM

Others:

Professor & collaborator Industrial Cybersecurity Centre (CCI)
Collaborator ISA 99 Committees & Co-chair ISA-Spain Cybersecurity WG
Collaborator Top 20 Secure PLC Coding Practices
Collaborator book “Ciberseguridad Industrial e Infraestructuras Críticas” Ed. Ra-Ma
Collaborator “Cyber Resilience in Electricity” Workgroup – World Economic Forum



Centro de
Ciberseguridad Industrial



IRSC 2022
INTERNATIONAL RAILWAY SAFETY COUNCIL
SEVILLA, OCTOBER 16-21, 2022



Who am I?

Agustín Valencia Gil-Ortega

Experiencia

Responsable Desarrollo Negocio OT Fortinet (2021-)

Profesor Máster Ciberseguridad Univ.Pontificia Comillas ICAI (2019-)

Responsable Ciberseguridad Global OT Iberdrola (2017-2021)

Jefe de Ingeniería I&C+Responsable Ciberseguridad CN Cofrentes (2010-17)

Jefe de O&M CC Santurce (2006-2010)

Formación

Ingeniero Industrial por Univ.Pontificia Comillas ICAI

Máster en Gestión de Mantenimiento (US)

Especialista Tecnología Nuclear BWR (Tecnatom)

Master de Seguridad Informática (UPC-ViU), Director de Seguridad (UDIMA)

CISM

Otros:

Profesor y colaborador Centro de Ciberseguridad Industrial

Colaborador Comités ISA 99 y Co-Líder Grupo Ciberseguridad ISA-España

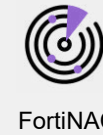
Colaborador Top 20 Secure PLC Coding Practices

Colaborador del libro “Ciberseguridad Industrial e Infraestructuras Críticas” Ed. Ra-Ma

Colaborador “Cyber Resilience in Electricity” Workgroup – World Economic Forum



Railway Ecosystem



Operations Control Centers

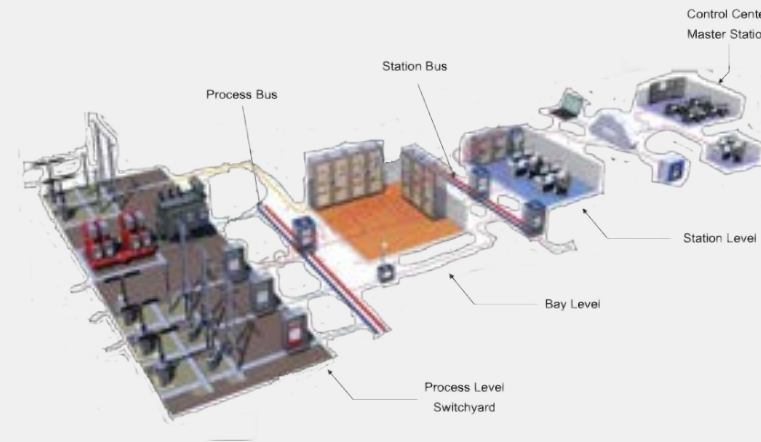
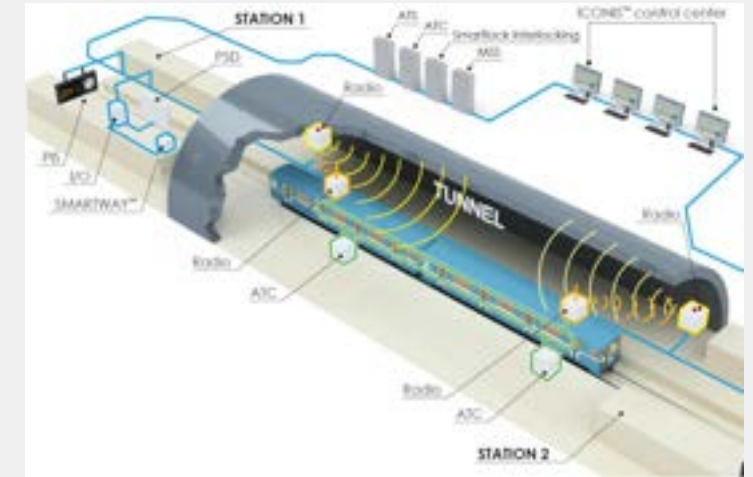
Substations

Railway Stations

Signalling

Communications

Rolling Stock



Attacks against Safety

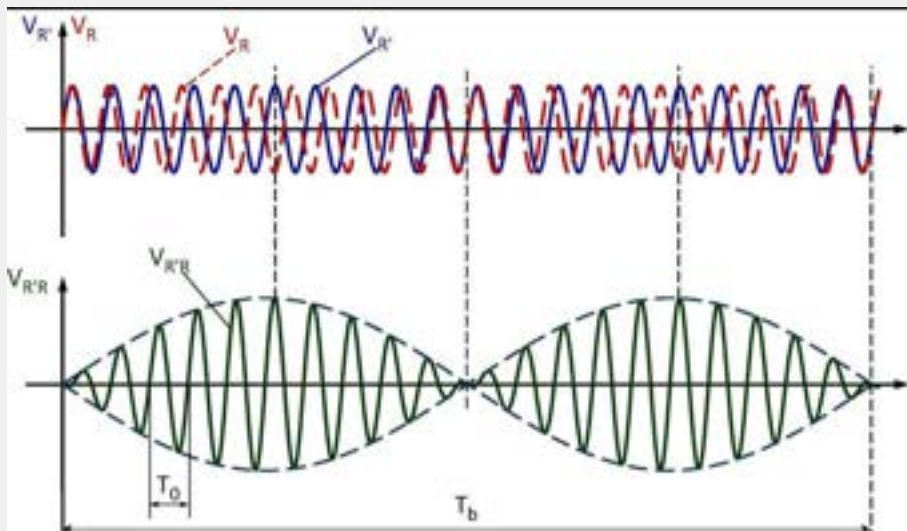
Aurora Project (2007)

Origin: Idaho National Laboratory

Objective: Demonstrate Emergency Diesel Generators vulnerabilities

Syncho coupling logic modified

Catastrophic coupling by changing conditions



Attacks against Safety

Crash Override (2016) - Ukraine

CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack

- 2015 Vulnerability Exploitation leaving IED protections in “Test” mode
- Potentially destructive attack (discovered in 2018)
- Mitigated by personnel acting manually



CISA
CYBER-INFRASTRUCTURE

About Us Alerts and Tips Resources Industrial Control Systems

ICS-CERT Landing > ICS-CERT Advisories > Siemens SIPROTEC Denial-of-Service Vulnerability

ICS Advisory (ICSA-15-202-01)

Siemens SIPROTEC Denial-of-Service Vulnerability

Original release date: July 21, 2015 | Last revised: August 27, 2018



Figure 5: CRASHOVERRIDE Attack Intentions

Attacks against Safety

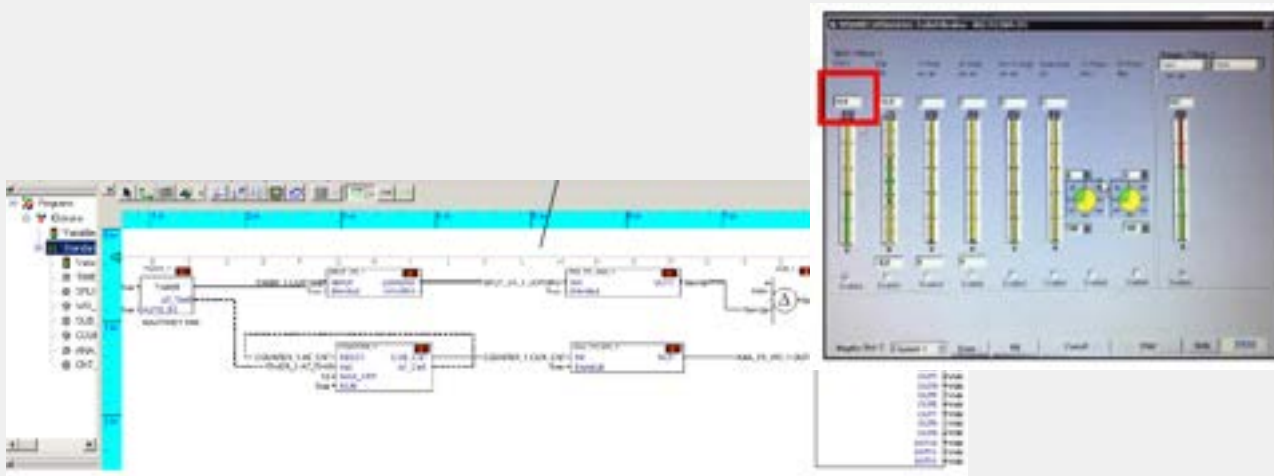
- **Triton (2017) - Arabia:** 1st Attack specifically focused on Safety Instrumented System –SIS- (Schneider Triconex) in Petrochemical plant
- Strong protections against program changes...por change management
- Malware became persistent in SCADA and Engineering Stations
 - Libraries modification in SCADA
 - Libraries modification in SIS
 - Became able to make changes bypassing change control protections
- Attackers also hire Safety experts
 - *(and they might work blind without knowing that is for an attack)*



Attacks against Safety

- Real failures in pitch angle control
- Alter Wind speed measure conversion
- Alter Protection Setpoints for high wind speed
 - Pitch
 - Brake

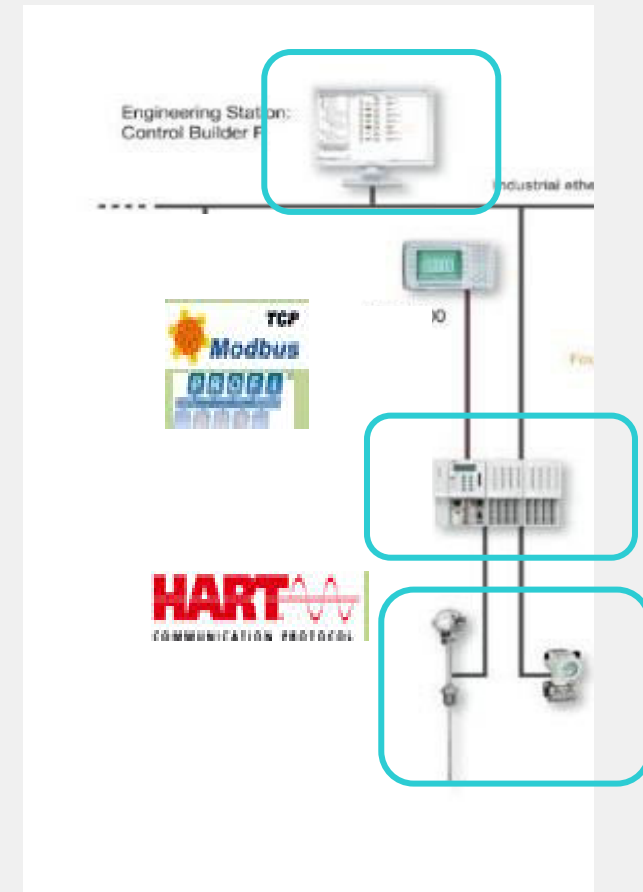
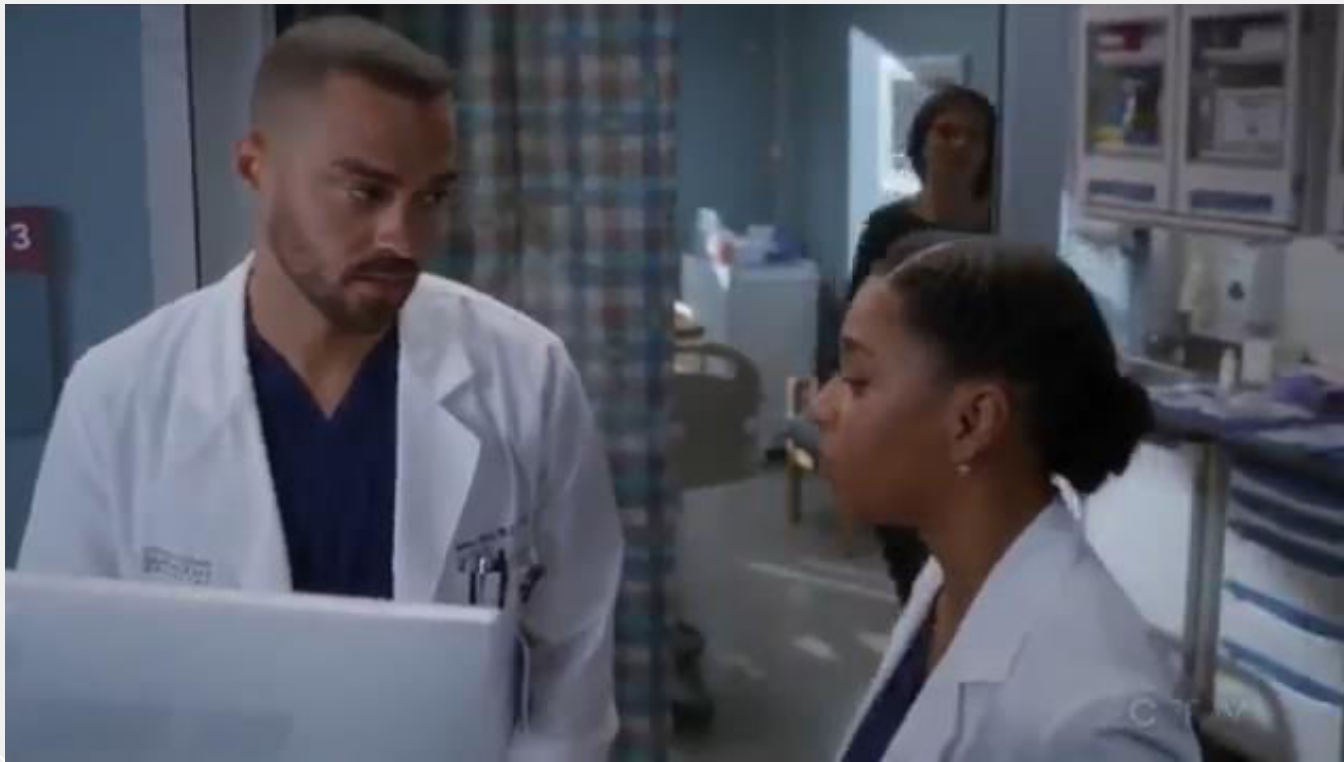
Stuxnet (2010)



Attacks against Safety

- Change in Measurements?
- Change in Screen Values? Stuxnet (2010)
- Change in Conversion Constants?
- Change in Sensor type?

Operations driven to failure!!

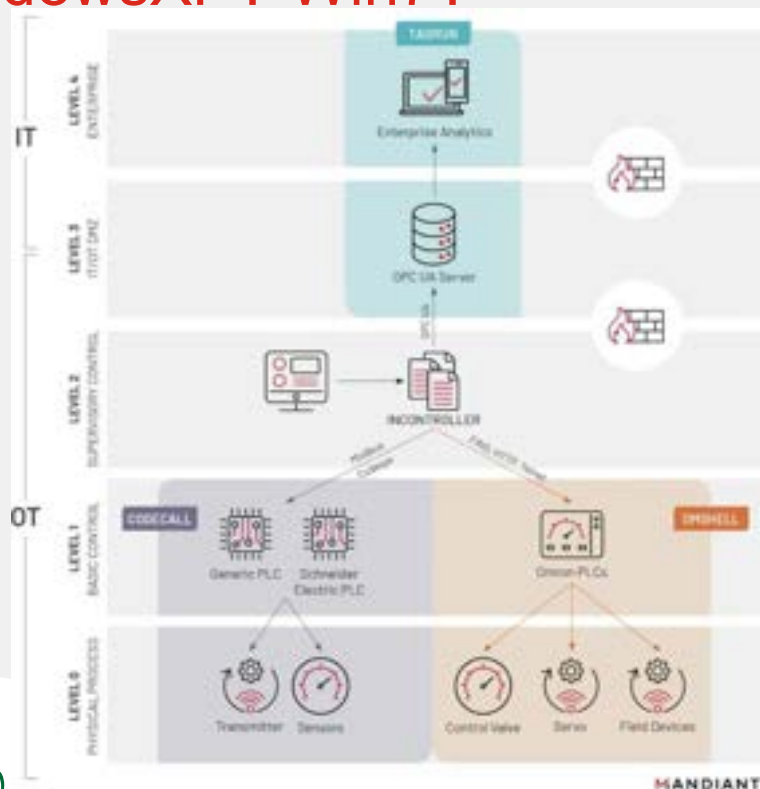


New generation of attacks against ICS

Public exploits significantly lower the skill and effort needed to exploit a vulnerability.

Many ICS/OT systems are deployed on top of Windows, and exploits like ETERNALBLUE 15 (MS17-010) have been used to infiltrate ICS/OT networks on a number of occasions →

WindowsXP? Win7?



Dragos 2022

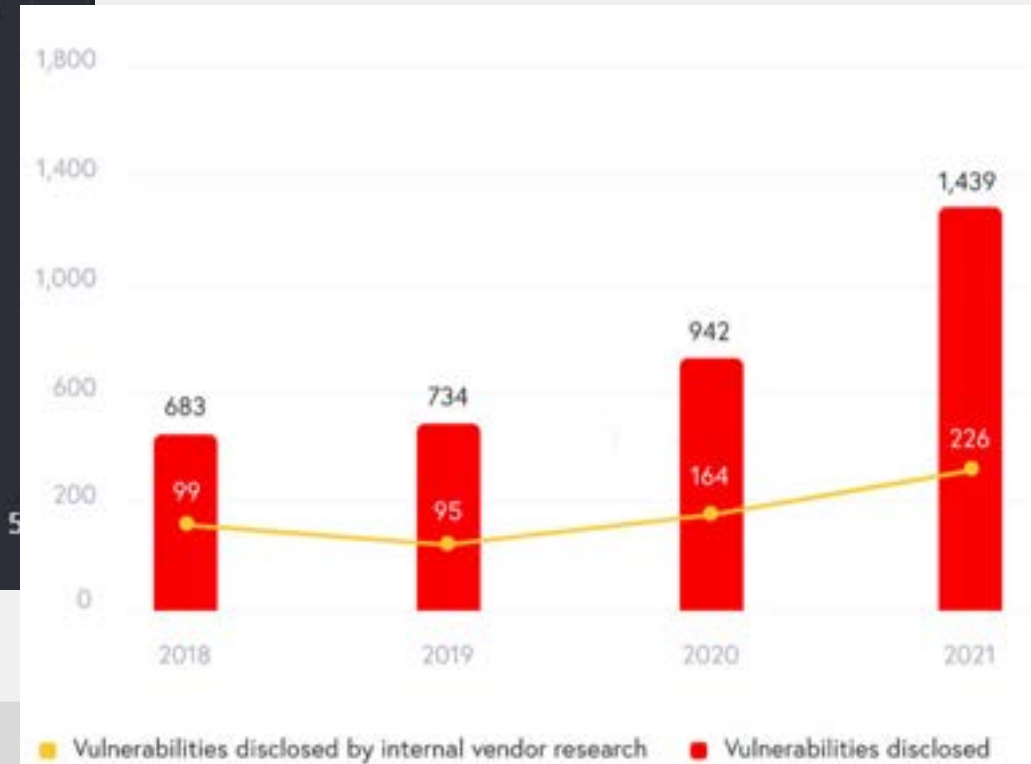
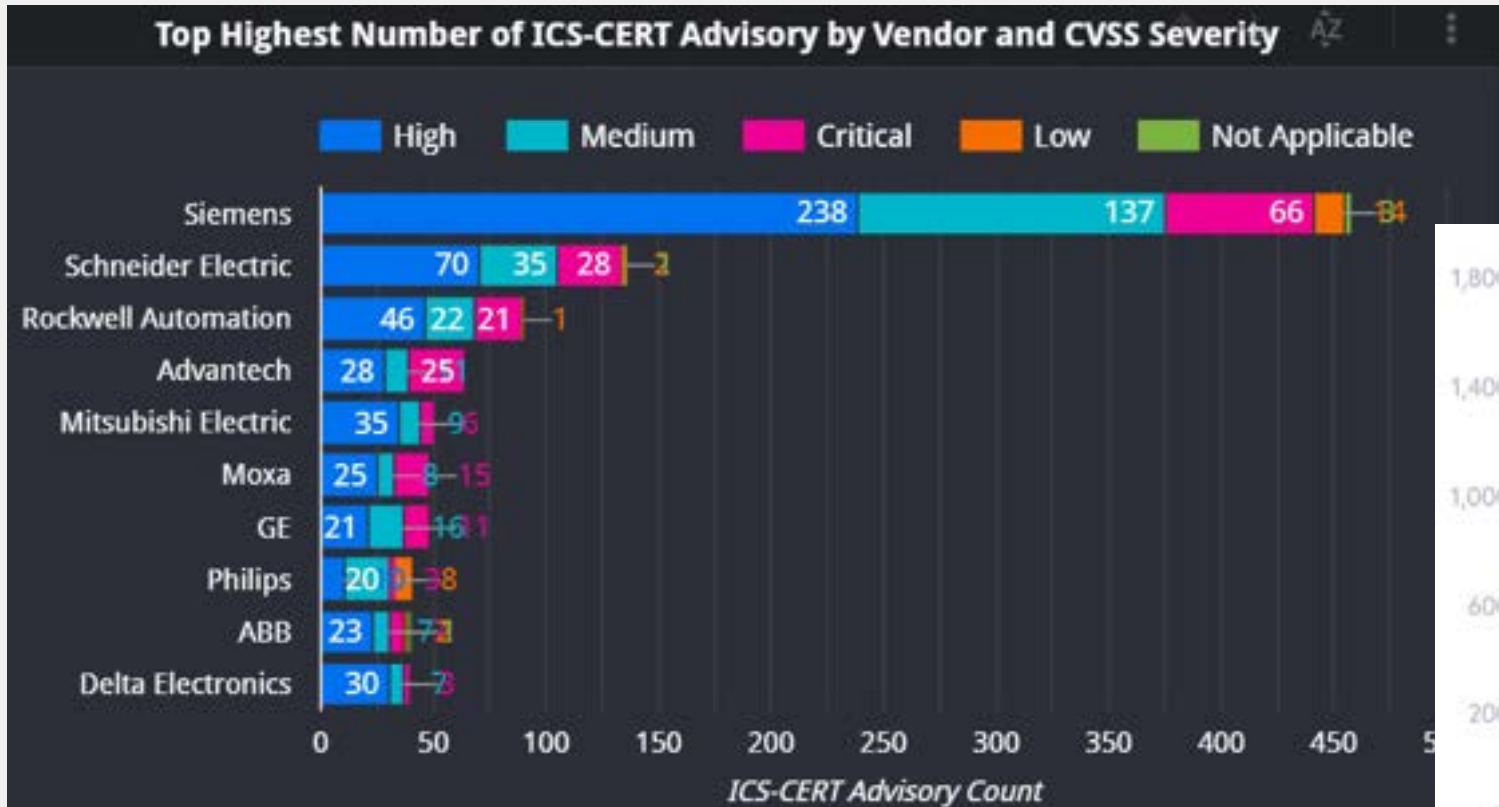
INCONTROLLER // PIPEDREAM → Stuxnet+Triton+Industroyer

New malware targeting generic PLCs → *Russia?*

Mandiant / Dragos 2022

ICS - vulnerabilities and obsolescence

ICS-CERT



Understand Industrial Protocols

Protocols to be deeply understood

Commands!

- Cannot forbid our whole protocol
- **Context** for security monitoring
- Granularity - actions allowed only to:
 - Operations, Engineering, Historian...
 - Achieved from SCADA, **needed from Network**
 - Proper Virtual Patching!

Applications!

- Only Authorized applications reduce exposure
- Patching also over actions on apps

(Much more than Port & IP address)

Name	Severity
Siemens.Simatic.WinCC.Default.Password	★★★★
Siemens.SIMATIC.WinCC.Flexible.HmiLoad.Multiple.Vulnerabilities	★★★★★
Siemens.SIMATIC.WinCC.Flexible.miniweb.DoS	★★★★

The screenshot shows the FortiGuard Labs search results page. The page title is "Search Results". On the left, there is a "Refine Search" sidebar with options for "All Results (304)", "Search time: 23ms", "Search Engine" (Normal selected, Exact Match, CVE Lookup, ID Lookup, Zero-Day Lookup, PSIRT Lookup, Antispam Lookup, Outbreak Alert Lookup), and "Filter by Industrial Security" (Industrial Security - IPS (533) selected, Industrial Security - APP Control (1890)). The main content area lists several search results:

- CIP_File.Upload.Transfer**: This indicates detection of CIP File Upload Transfer command. Common Industrial Protocol is a protocol that runs on top of...
- Rockwell.Automation.FactoryTalk.RSLinxNG.DoS**: This indicates an attack attempt to exploit a Denial of Service Vulnerability in FactoryTalk Lincx. The vulnerability is cau...
- Moxa.AWK-3131A.iw_console.Privilege.Escalation**: This indicates an attack attempt to exploit a Privilege Escalation Vulnerability in Moxa AWK-3131A. This vulnerability is d...
- Application Modbus_Unity.Write.Variables**: This indicates detection of the Modbus Unity Write Variables command. MODBUS is an application-layer messaging protocol, positioned at level 7 of the OSI model. It provides client/server communicatL...
- IPS Modbus.TCP.Unauthorized.Read.Request.PLC**: This indicates that an unauthorized Modbus client attempted to read information from a PLC or other device. Modbus TCP is a protocol often found in SCADA networks where it is used for process contro...

Protocols & Rules available in <https://www.fortiguard.com/services/is>

2022 State of Operational Technology and Cybersecurity Report



People



33% of organizations entrust OT security to the VP/director of network engineering/operations



67% of OT security leaders come from an OT engineering background



43% of respondents have security-incident response time as a top-three success measurement

Security Posture



56% of organizations report being at level 3 or level 4 of OT security maturity



50% say the OT security posture is a significant factor in the overall risk score



13% of organizations have centralized visibility of all OT activities

Security Practices



48% report security compromises to executive management



32% have deployed role-based network access control



52% say all OT activities are monitored and tracked by the SOC

Security Outcomes



93% of organizations had 1+ intrusions in the past year; **78%** had 3+



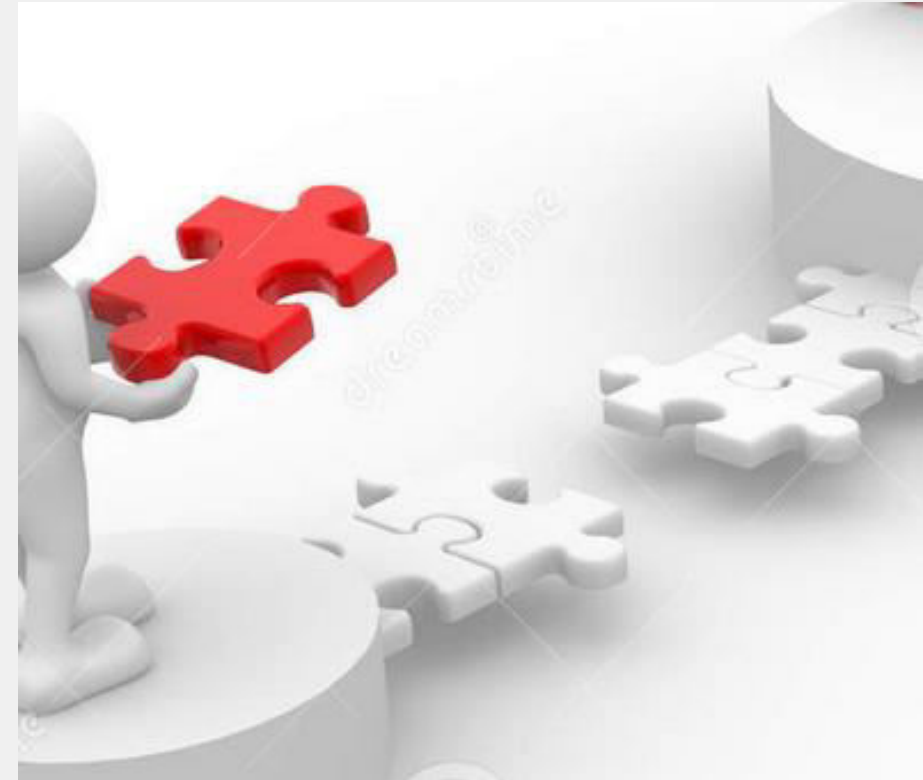
61% of intrusions impacted OT systems



90% of intrusions required hours or longer to restore service

Lessons to Learn

- UX at station or Rolling stock is a cybersecurity challenge
- Attacks to Safety on the rise
- Attacks to Safety may have catastrophic consequences
- Most attack leverage vulnerabilities
- Patching is a must (think of virtual patching!)
- Safety & Cybersecurity need to coordinate and complement each other.
 - Data integrity is a must for Safety systems
 - Integrate monitoring and protection focused on industrial protocols
 - Cross change control and process analysis
 - Change control validation coordinating cyber+engineering





www.irsc2022.com

