

**XIII
JORNADAS
STIC
CCN-CERT**



**Caracterización
Casos de Uso en
Incidentes de
Ciberseguridad
Industrial**

**COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD**

#XIIIJORNADASCCNCERT



Agustín Valencia Gil-Ortega
Francisco Rivero Pérez



<https://www.linkedin.com/in/agustin-v-6035849/>

<https://www.linkedin.com/in/francisco-rivero-perez-2a016642/>

Índice

1. Un poco de Historia
2. Enfoque Hacia Industrialización
3. Ataques Hacia el Control
4. Ataques Hacia la Información
5. Ataques Hacia las Protecciones
6. Reflexiones sobre la Monitorización
7. Caracterización de Casos de Uso - Beneficios

UN POCO DE HISTORIA

2010 Stuxnet

USB's

PLC Attack

SCADA/HMI Attack

2015 Blackenergy

Serial/TCP Gateway

Office Macro

Firmware Attack

2016 Crashoverride

Industrial Protocols

Destructive Purpose

2017 Triton

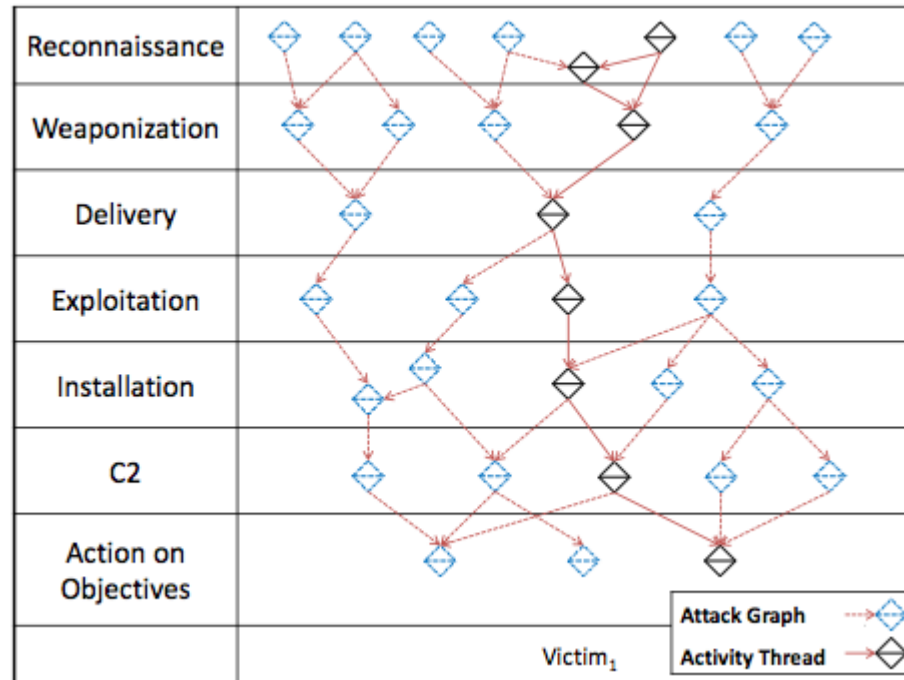
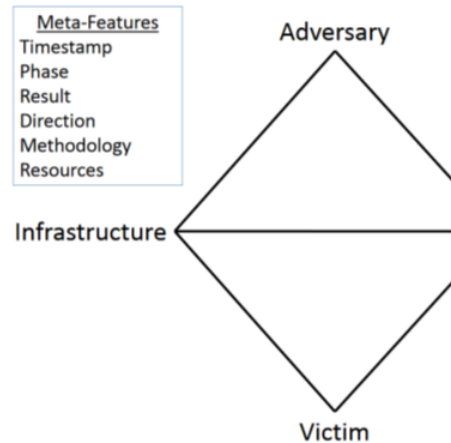
SIS Attack

Firmware/Scripting Deep Level
Attack

Destructive Purposes

ENFOQUE HACIA INDUSTRIALIZACIÓN

METODOLOGÍAS



IMPACT

TIME TO
REACT**STAGE 2 – ICS Attack**

Develop

Test

Deliver

Install / Modify

Execute ICS Attack

ENFOQUE HACIA INDUSTRIALIZACIÓN

ENFOQUE IT vs INDUSTRIAL

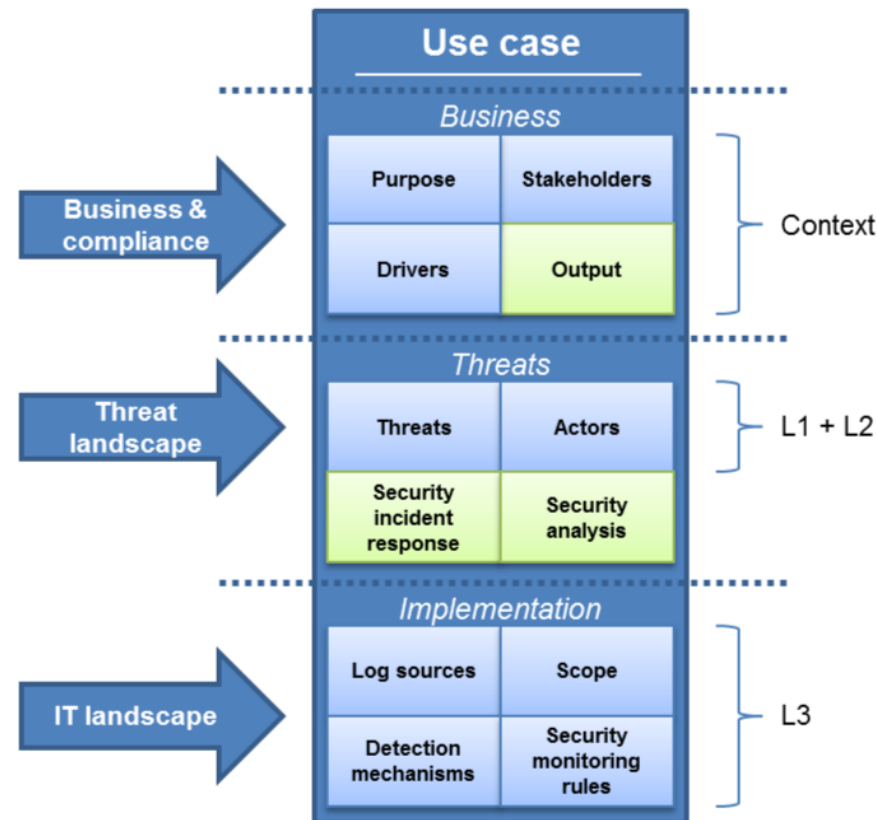
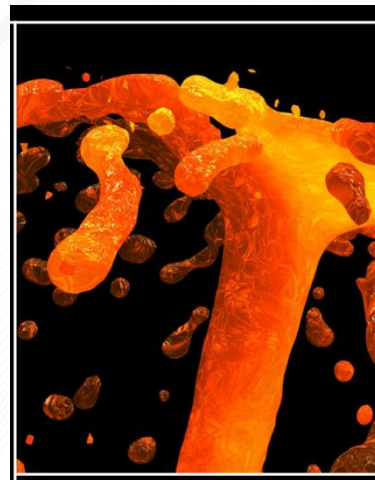


Figure 3: MaGMA UCF use case model

- Use Cases Framework
- L1: 12 cases (incl. 7 steps CyberkillChain)
- L2: Tactical Use Cases 62
 - (Industrial Approach → <15)

POS	Port Scanning
BRU	Brute force
WRM	Worm propagation
EXF	Data exfiltration
LAT	Lateral movement
BRU	Internal Brute force
PRI	Privilege escalation
FIL	File corruption, encryption and unauthorized access
AO-DBC	Database compromise attempt
AO-RAT	Usage of remote access tool
AO-ALL	Multiple AO categories

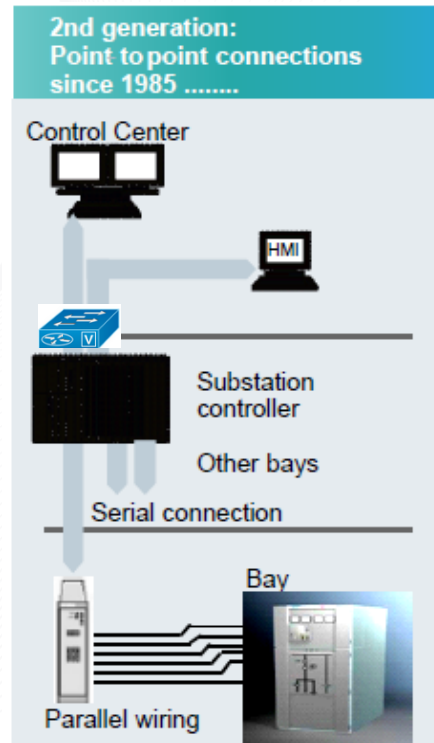
- L3: Mitre ATT&CK Enterprise
 - (Industrial Approach to Mitre ICS?)

ATAQUES HACIA EL CONTROL

- STUXNET
- BLACKENERY

was used on other computers in the same facility to open dozens of circuit breakers, cutting power to more than a hundred thousand Ukrainians.

ATAQUES HACIA EL CONTROL


[About Us](#)
[Alerts and Tips](#)
[Resources](#)
[Indu](#)
[ICS-CERT Landing](#) > [ICS-CERT Alerts](#) > [Cyber-Attack A](#)

ICS Alert (IR-ALERT-H-16-05)

Cyber-Attack Against Ukrainian Cr

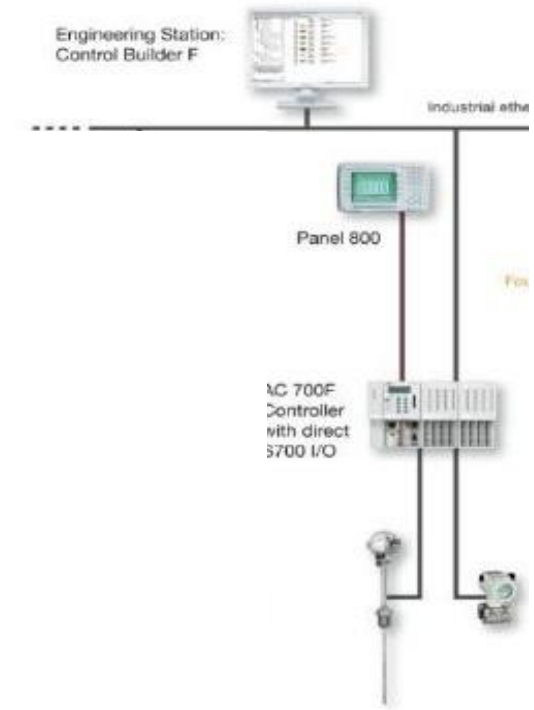
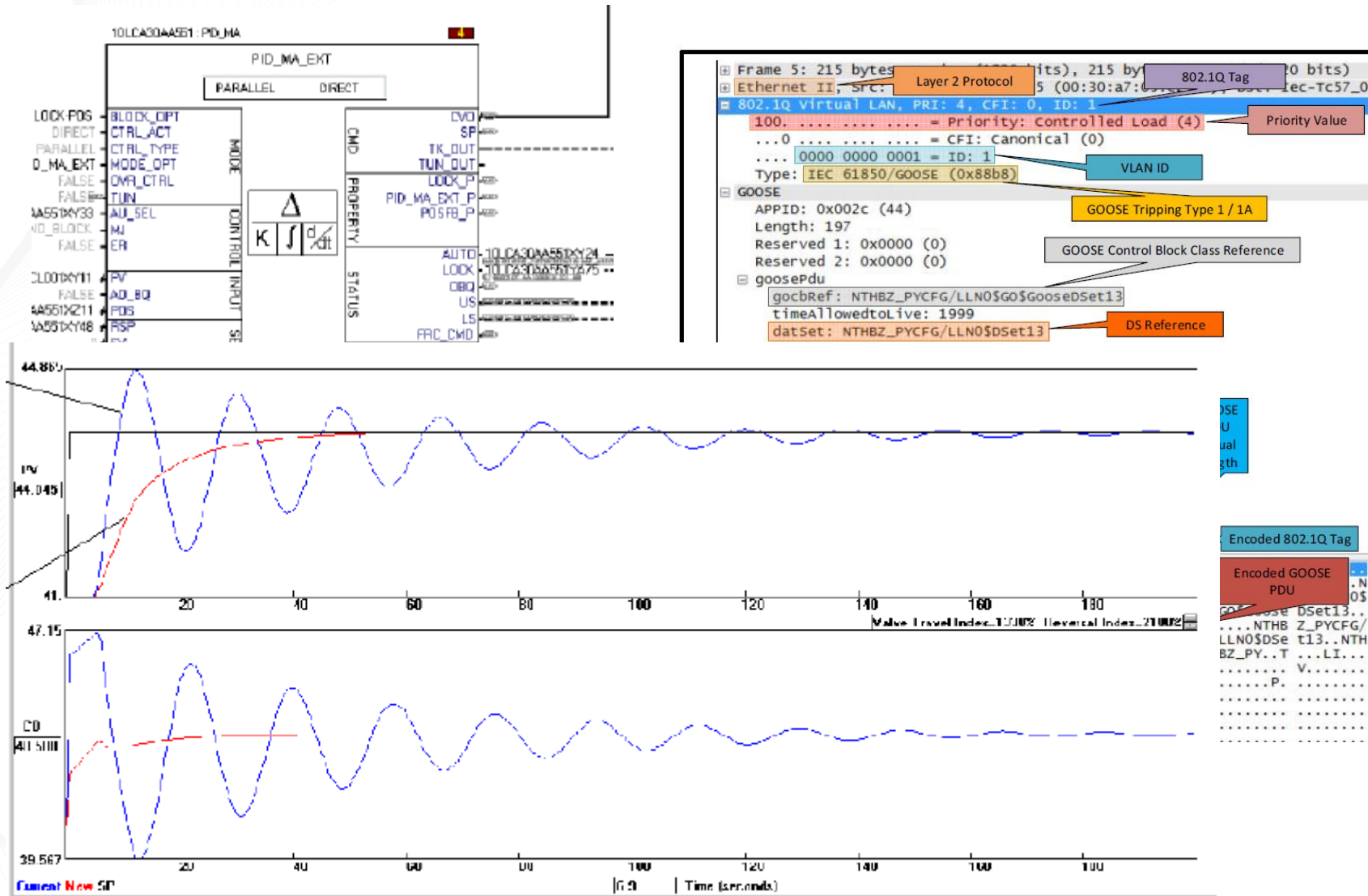
Original release date: February 25, 2016 | Last revised: August 23



Device	A	B	C	D	E
Backdoors / Auth Bypass	✗	!	✗	✗	✗
Fuzzing	!	✓	✗	✗	!
Bruteforce	✗	✗	✗	✗	✗
MITM	✗	!	✗	✗	✗

https://www.slideshare.net/codeblue_jp/industroyer-biggest-threat-to-industrial-control-systems-since-stuxnet-by-anton-cherepanon-rbert-lipovsk

ATAQUES HACIA EL CONTROL



ATAQUES HACIA EL CONTROL

¿Cómo se materializa?

- Cambio en controladores (difícil de ver)
- Observación de comportamiento anómalo (historizadores)
- Aviso Plataformas OT – cambio archivos de configuración



Event Details

RESULTS (26/21)

ID	DESCRIPTION	TYPE
26247	3500 Rack Configuration: Get rack status	BaselineDeviation
26248	3500 Rack Configuration: Get configuration of slot 2	BaselineDeviation
26249	3500 Rack Configuration: Get configuration of slot 8	BaselineDeviation
26250	3500 Rack Configuration: Get configuration of slot 4	BaselineDeviation
26251	3500 Rack Configuration: Get configuration of slot 12	BaselineDeviation
26252	3500 Rack Configuration: Get configuration of slot 13	BaselineDeviation
26253	3500 Rack Configuration: Get configuration of slot 14	BaselineDeviation
26254	3500 Rack Configuration: Get configuration of slot 15	BaselineDeviation
26255	3500 Rack Configuration: Clear slots configuration sequence	BaselineDeviation
26256	Get Setpoints for slot 2 channel W1	ProtocolSpecific
26257	Get Setpoints for slot 2 channel W2	ProtocolSpecific

Configuration Upload

A configuration has been uploaded from control...

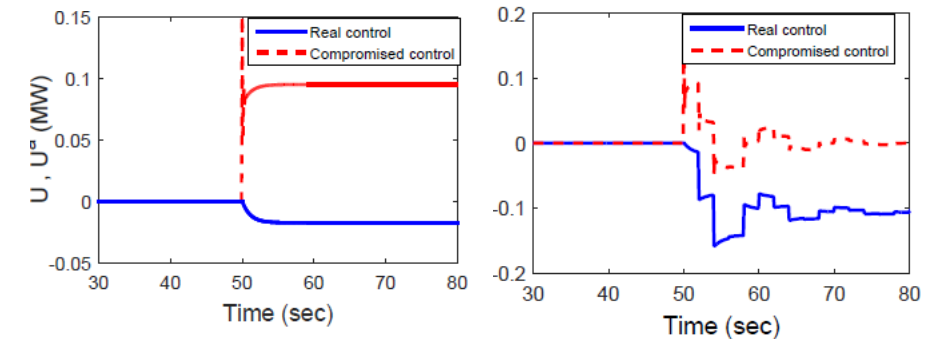
What does this mean?
An attacker may want to interfere with normal critical infrastructure activity by changing a PLC code if the PLC is running and as a result stops functioning. It may cause a significant production loss.

ALERT DETAILS - ID 21085

IP: 192.168.1.15
Network: default
Risk Level: High
Site: CENSA
Asset Type: Engineering Station

Criticality: Medium
Vulnerability: Virtual Control Engineering Station 3500-ENV

IP: 192.168.1.15
Network: default
Risk Level: Moderate
Asset Type: PLC



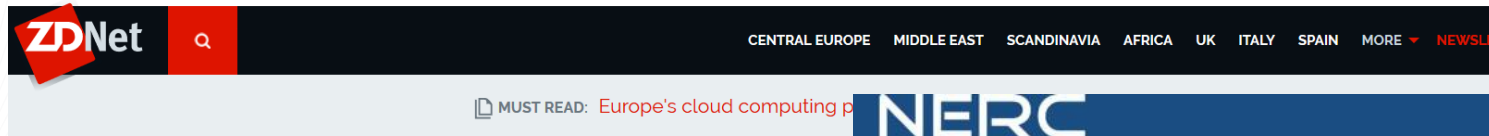
BASELINE TABLE FOR ALERT

RESULTS (22)

1 baseline selected (Select all 22 baseline(s) / Clear)

Baseline Name	Transmission	Frequency	Source Address	Destination Address	First Seen	Last Seen	Communication Type	Access Type
3500 Rack Configuration: Acquire configuration token	TCP / 3500	Minutes			12-11-2018, 13:23:08	12-11-2018, 13:44:56	Protocol	None

ATAQUES HACIA LA INFORMACIÓN



Cyber-attack hits Utah energy provider

of-its kind attack to hit a renewable energy provider. tor from its power generation station.

by Catalin Cimpanu for Zero Day | October 31, 2019 -- 23:40 GMT (23:40 GMT) | T



Lesson Learned

Risks Posed by Firewall Firmware Vulnerabilities

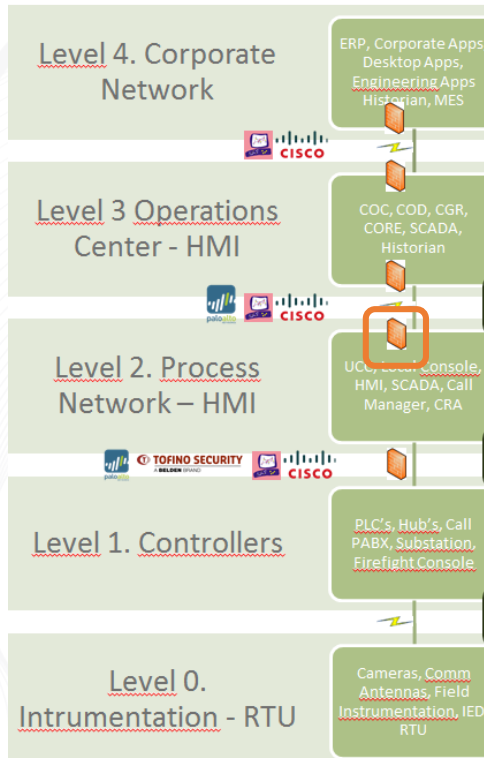
Problem Statement

A vulnerability in the web interface of a vendor's firewall was exploited, allowing an unauthenticated attacker to cause unexpected reboots of the devices. This resulted in a denial of service (DoS)¹ condition at a low-impact control center and multiple remote low-impact generation sites. These unexpected reboots resulted in brief communications outages (i.e., less than five minutes) between field devices at sites and between the sites and the control center.

Details

A registered entity with a low-impact control center experienced brief (i.e., less than five minutes) outages of internet-facing firewalls that controlled communications between the control center and multiple remote generation sites and between equipment on these sites. The affected firewalls were all perimeter devices that served as the outer security layer. These outages had no impact to generation. Seeing several of these outages at different sites raised suspicion and led to a more in-depth investigation. This investigation revealed that the communications outages were due to reboots of the firewalls at each of the sites. The entity's system monitoring tools also provided notification of the firewall reboots. These records show the firewall reboots occurred over a 10-hour time period with each firewall showing offline status for

less than five minutes

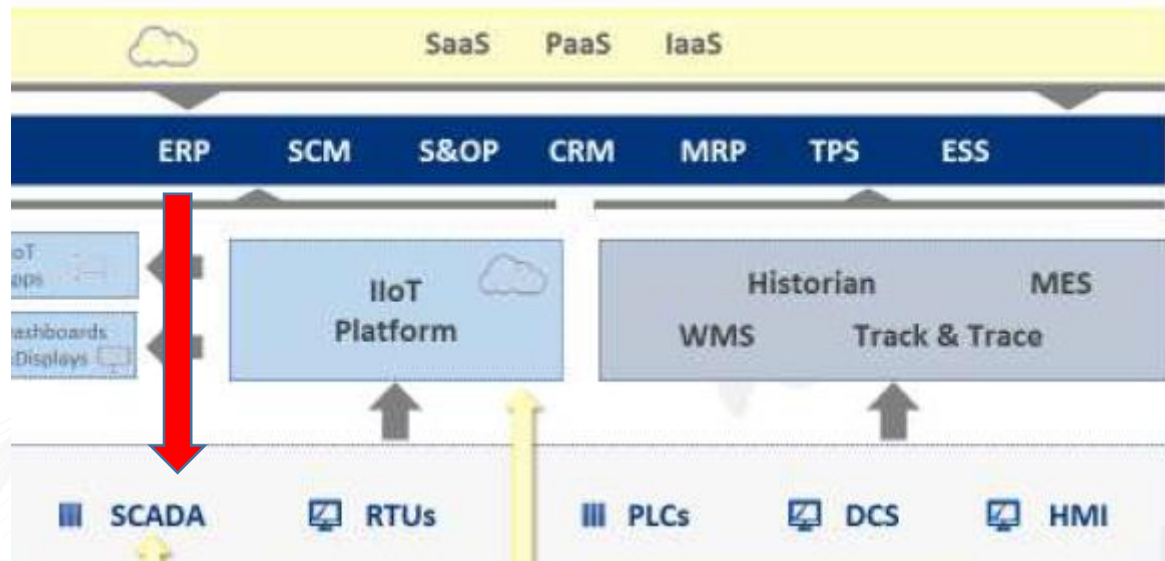


DD

PRO

Exploitation of Vulnerability / Shutdown Device

ATAQUES HACIA LA INFORMACIÓN



Home > Cyberwarefare



Several U.S. Gas Pipeline Firms Affected by Cyberattack

By [Eduard Kovacs](#) on April 04, 2018



Tweet



Recomendar 49



RSS

Several natural gas pipeline operators in the United States have been affected by a cyberattack that hit a third-party communications system, but the incident does not appear to have impacted operational technology.

Energy Transfer Partners was the first pipeline company to report problems with its Electronic Data Interchange (EDI) system due to a cyberattack that targeted Energy Services Group, specifically the company's Latitude Technologies unit.

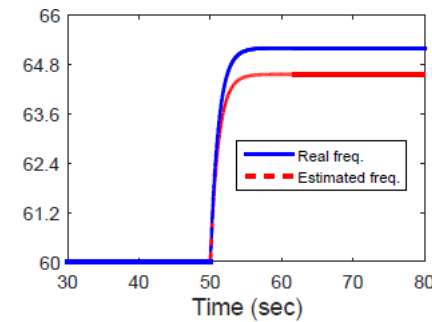
ALTERAR COMPORTAMIENTO DEL OPERADOR

- El fallo de un componente, con otras informaciones, puede identificarse fácilmente
- Múltiples fallos pueden llevar a la confusión
 - Efectos cascada “naturales”
 - Ataques masivos?
- Fallos de sistemas en remoto, son más difíciles
- Diferente protección información vs control
- No falla el control pero se corta el suministro igualmente

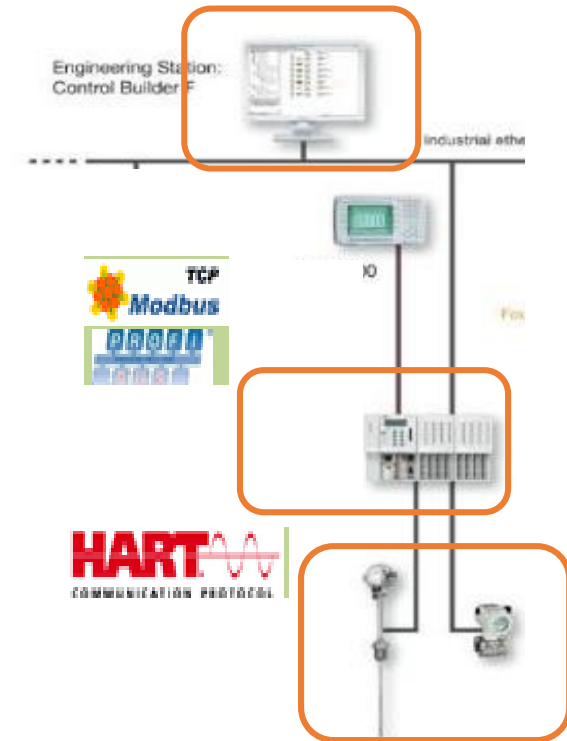
ATAQUES HACIA LA INFORMACIÓN

ALTERAR COMPORTAMIENTO DEL OPERADOR

- Cambio en Lecturas
- Cambio en valores de pantalla
- Cambio en Coeficientes de Conversión
- Cambio en Tipo de Instrumento

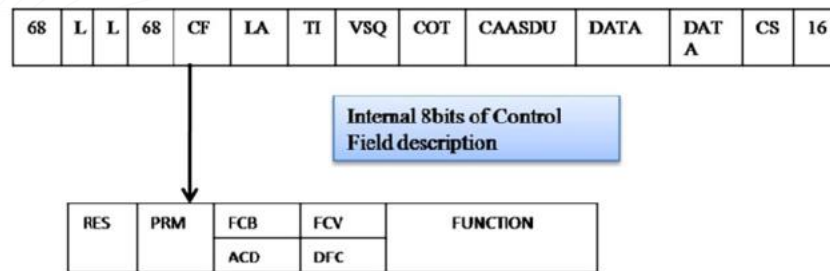


AO	DBC	Modify Parameter
AO	ALL	Modify Parameter
AO	RAT	Modify System Settings



ATAQUES HACIA LAS PROTECCIONES

- Simple cambio en el valor de tolerancia para permitir acoplamiento
- Los efectos no se ven inmediatamente
- El tráfico no puede ser malware como tal



- Enfoque “activo” para revisar cambios en configuración
- Coordinación con Ingeniería



ATAQUES HACIA LA PROTECCIÓN

CRASHOVERRIDE

Main backdoor – List of commands

- Execute process
- Execute process using specified user account
- Download file from C&C server
- Copy & upload file
- Execute shell command
- Execute shell command using specified user account
- Quit
- Stop service
- Stop service using specified user account
- Start service using specified user account
- Replace "Image path" registry value for service



DRAGOS

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

By Joe Slowik, Dragos Inc

https://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-732541.pdf
<https://dragos.com/blog/crashoverride/>

ATAQUES HACIA LA PROTECCIÓN

CRASHOVERRIDE



[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

DD	PRO	Alternate Modes of Operation
----	-----	------------------------------

The DoS condition places the victim SIPROTEC device in “firmware update” mode. The effect triggered is practical and useful in legitimate firmware update instances given the limited resources available to legacy SIPROTEC devices (especially for memory). However, when activated, the impacted SIPROTEC no longer performs designed protective functions – including overcurrent protection³³ – on the relevant transmission lines even if still present, powered on, and network accessible. Essentially the receiving device is placed in an inoperative holding pattern for future instructions. When triggered outside of normal or intended operations, this is a mission kill impact from the perspective of the targeted SIPROTEC relay. The SIPROTEC is still present on the network but no longer performing intended functions due to the exploit. The result is an unprotected link in electric transmission, with normal safeguards disabled.

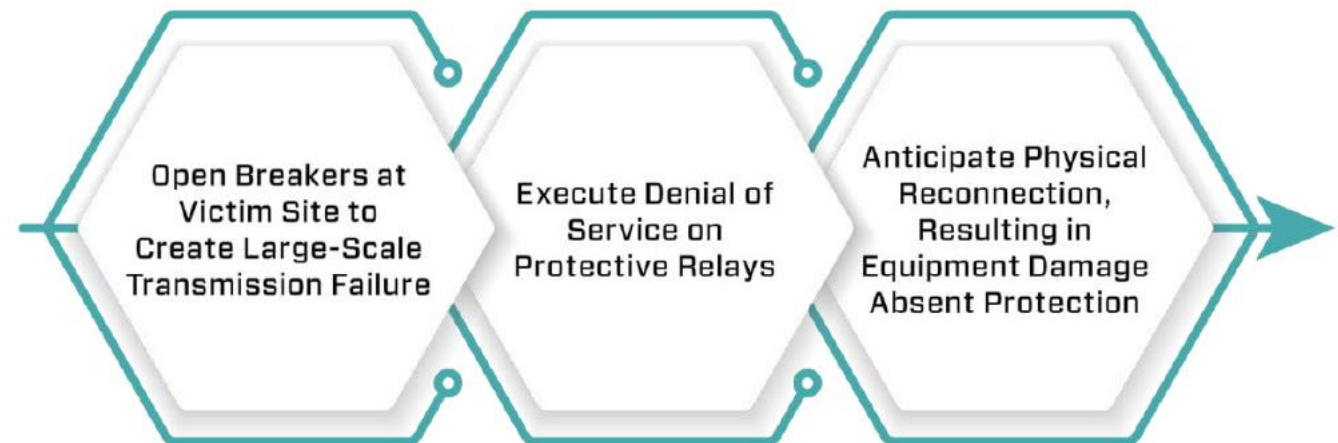


Figure 5: CRASHOVERRIDE Attack Intentions

ATAQUES HACIA LAS PROTECCIONES

- Fallos reales en pitch control y en reductora
- Causas ciber que podrían haber llegado al mismo desenlace?
- Variación conversión lectura de velocidad
- Alteración Protecciones por alta velocidad
 - Pitch
 - Actuación Freno



ATAQUES HACIA LAS PROTECCIONES

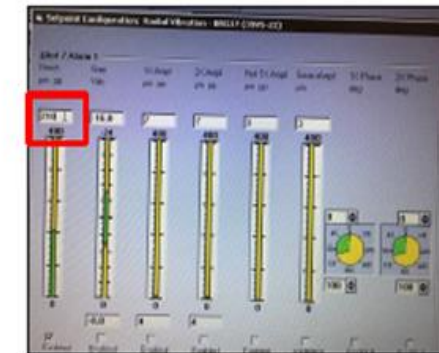
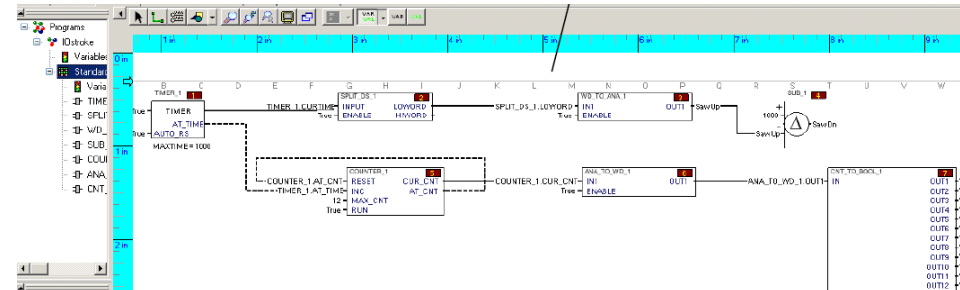
Involved nodes (at the current time)



A configuration has been downloaded to controller
Downloaded by 1.191 by
145
Today, 14:00



Event Details		
RESULTS (7/7)		
ID	DESCRIPTION	TYPE
24137	Enables software switch 'Configuration Mode' of slot 2	ProtocolSpecific
24138	Set configuration of slot 2	ProtocolSpecific
24139	Set setpoints for slot 2 channel #1	ProtocolSpecific
24140	Set setpoints for slot 2 channel #2	ProtocolSpecific
24141	Set setpoints for slot 2 channel #3	ProtocolSpecific
24142	Set setpoints for slot 2 channel #4	ProtocolSpecific
24143	Disables software switch 'Configuration Mode' of slot 2	ProtocolSpecific



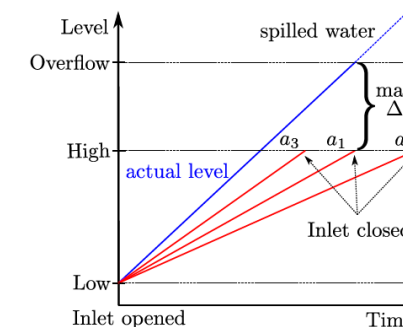
DISTRIBUTION CENTER



SUBSTATION



RTU / IED



ATAQUES HACIA LAS PROTECCIONES

TRITON

- TRITON



Initial Movement	Execution	Command and Control	Disruption	Destruction
Default Credentials	Command-Line Interface	Commonly Used Port	Alternate Modes of Operation	Block Command Message
Exploitation of Vulnerability	Exploitation of Vulnerability	Connection Proxy	Block Command Message	Block Reporting Message
External Remote Services	Graphical User Interface		Block Reporting Message	Device Shutdown
Modify Control Logic	Man in the Middle		Block Serial Comm Port	Exploitation of Vulnerability
Valid Accounts	Modify System Settings		Device Shutdown	Modify Command Message
	Scripting		Exploitation of Vulnerability	Modify Control Logic
	Alternate Modes of Operation		Masquerading	Modify I/O Image
			Modify Command Message	Modify Parameter
			Modify Control Logic	Modify Reporting Message
			Modify I/O Image	Modify Reporting Settings
			Modify Parameter	Modify Tag
			Modify Reporting Message	Module Firmware
			Modify System Settings	Spoof Command Message
			Modify System Settings	Spoof Reporting Message
			Modify Tag	System Firmware
			Module Firmware	
			Spoof Command Message	
			Spoof Reporting Message	
			System Firmware	

SOURCE:MITRE

RSAConference2019

/sessionsFiles/14184/SBX4-

REFLEXIÓN SOBRE LA MONITORIZACIÓN



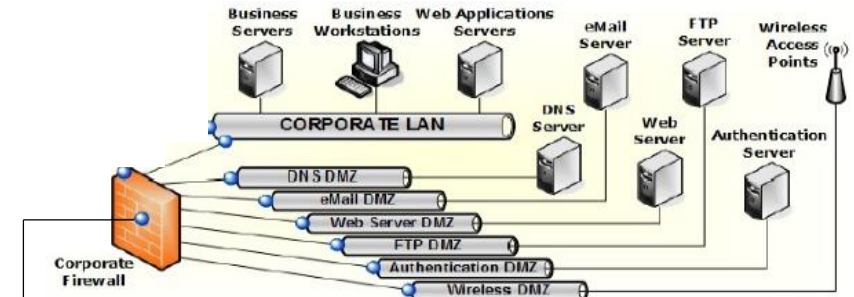
Centro de
Ciberseguridad Industrial

HIDS

SIEM

NIDS

EDR/EPP



OBJETO		Detectar la conexión
MODO DE DETECCIÓN		El HIDS detecta los identificadores del hardware
ORIGEN DE DATOS		SIEM NEG ☒ HIDS ☐ NIDS ☐
PROCEDIMIENTO DE ACTUACIÓN	TIER 1	Deberá contactar tele
	TIER 2	Confirmar validez de a
DEFINICIÓN MAGMA	LEVEL 3	AO-LAT-006
	LEVEL 1	AO
	LEVEL 2	AO-LAT
DEFINICIÓN MITRE ATT&CK	TACTIC	Lateral Movement, In
	TECHNIQUE	T1091

SECTORES

ESCENARIO
DE
INCIDENTE
CRÍTICO

SECTOR

PROCESOS

NATURALEZA

ELÉCTRICO

Generación Térmica

Generación Renovable

Distribución

Transporte

Distribución

Smartgrid

Contenido dañino

Obtención de información

Intento de intrusión

Disponibilidad

OIL & GAS

Extracción

Refinería

Distribución GAS

Almacenamiento GAS

Compromiso de operación

Compromiso información

Fraude

Vulnerable

AGUA

EDAR

ETAP

ORIGEN

SALUD

Equipos Diagnóstico

Monitorización

Equipo Quirúrgico

Dosificación

INTERNO

TRANSPORTE

Ferroviario

EXTERNO

ALIMENTACIÓN

TIPO

FABRICACIÓN

NO INTENCIONADO

Otros

INTENCIONADO

Descripción de debilidad(es) explotada(s)

Amenaza(s)

Impacto de negocio

Impacto técnico

REFLEXION SOBRE LA MONITORIZACION

- ENFOQUE ESPECÍFICO HACIA EL MUNDO INDUSTRIAL
- HERRAMIENTAS QUE DEN INFORMACIÓN SOBRE EL PROCESO AFECTADO
- ESTUDIAR INTEGRACIÓN DE HERRAMIENTAS ESPECÍFICAS EN SIEM GENERALES
- CRITICIDAD EVENTOS Y ACTIVOS → CONSECUENCIAS → CLASIFICACIÓN POR OT
- ENFOQUE CRUZADO SOBRE EL IMPACTO DE SISTEMAS IT EN PROCESOS INDUSTRIALES
 - Ataques no dirigidos (NotPetya, sPower, NorskHydro, PEMEX)
- DISTINTAS CRITICIDADES DE EMPLAZAMIENTOS IGUALES
- ROLES Y RESPONSABILIDADES ENTRE IT y OT
 - CONTENCIÓN SEGÚN NIVELES
 - REPORTE
 - NOTIFICACIÓN (ENS, PIC, NIS)

CARACTERIZACIÓN DE CASOS DE USO

BENEFICIOS

- Afinamiento de Plataformas en fase de despliegue
- Facilidad en comunicación de eventos
- Reducción de errores de comunicación e interpretación
- Rapidez de reacción y coordinación ante casos identificados como
- Posibilidad de Automatismos entre organizaciones
- Reducción Falsos Positivos



COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD

#XIIIJORNADASCCNCERT

OC.CCN.CNI.ES

WWW.CCN.CNI.ES

WWW.CCN-CERT.CNI.ES

XIII JORNADAS STIC CCN-CERT

ccn-cert
centro criptológico nacional