

# Schrödinger's Hack: Are Hacktivist Operations Placing Operational Technology at Risk?

Daniel Kapellmann Zafra

Technical Analysis Manager

Kapellmann@google.com

@Kapellmann

[www.kapell.tech](http://www.kapell.tech)



**Photo:** [Anonymous V for Vendetta Guy Fawkes Costume Halloween Mask](#) by [Marco Verch](#) under [Creative Commons 2.0](#)





Photo by [Daniele Franchi](#) on [Unsplash](#)

# Is there a hack in the box?

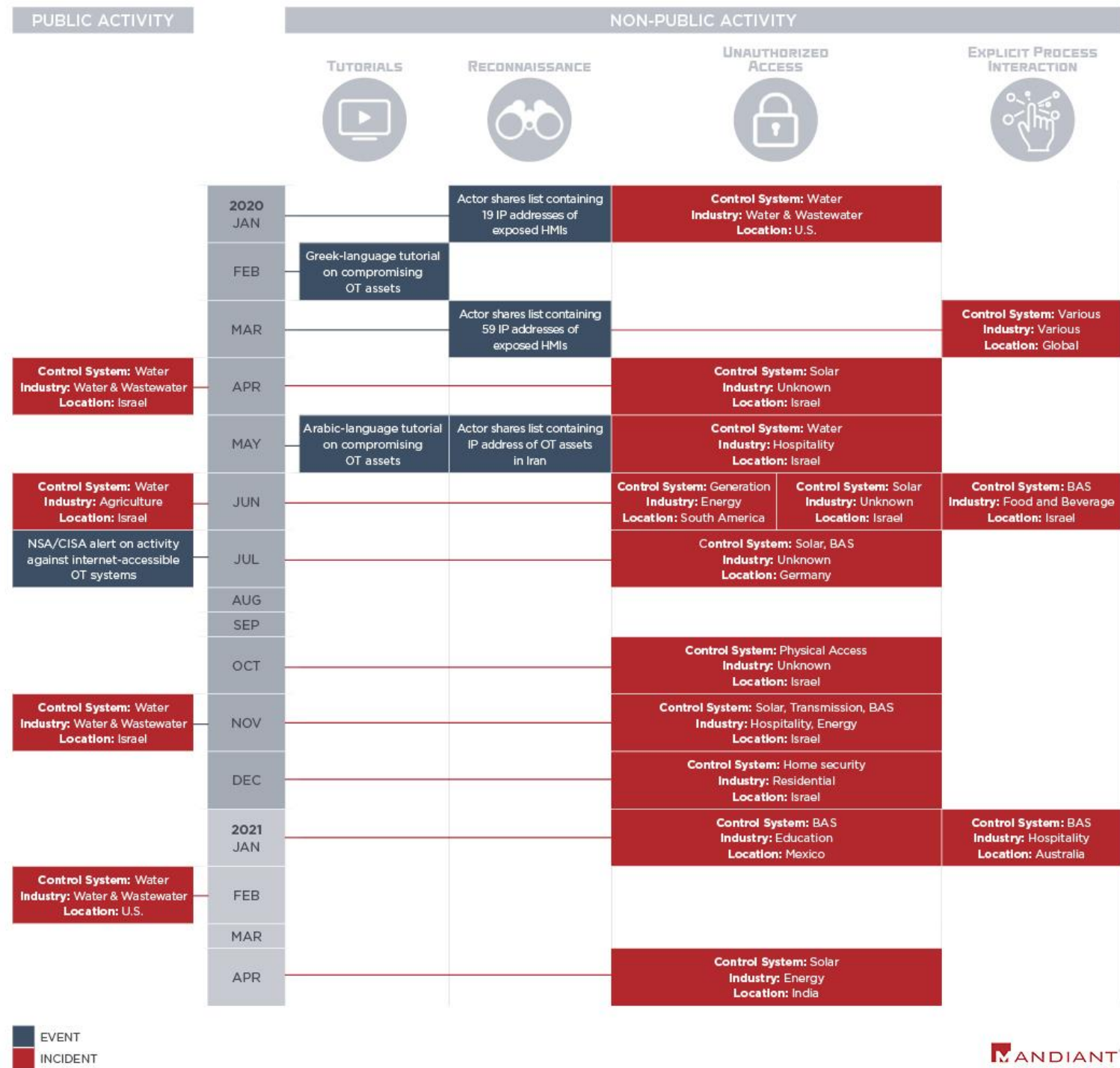


# Hacktivists Increasingly Claim to Target OT



# Timeline 2020

- Low sophistication attacks
- Attacks vs. unsecure OT assets
- Actors interacted with OT processes
- Some hacktivist tutorials



■ EVENT  
■ INCIDENT





# Note: Hacktivist Claims?

The attack was carefully planned and executed when the plant was first turn-on in the morning. 😊 The Orcs fought back, but they failed in the end as we destroyed the backup database and corrupted the primary. 30 hours later it is still gone. 🖐️ 🇺🇦  
[#StandWithUkraine](#) [#TeamOneFist](#)

The last moments of life for the Paper Mill.. SCADA system still gone, operation complete. We will not tweet for some time, until a new group of attacks is complete. Please enjoy the final moments for the Orcs, [#Ukraine](#) 🖐️ 🇺🇦

**OpenSCADA, Системний конфігурацій (WEB)**

OpenSCADA станція: "Line OneFist"

**We locked everyone else out and made it impossible to recover the password without a full re-install. We re-branded the server so the Orcs would see our logo and name on the control screen to troll them while launching the mill programs automatically.**

**Ми заблокували всіх інших і зробили неможливим відновлення паролів без повної переінсталяції. Ми змінили бренд сервера, щоб орки бачили наш логотип і назву на екрані керування, щоб тролити їх під час автоматичного запуску програм млина.**

The level of control once inside a SCADA system as Root (master) user is total. It is how Student was able to destroy Iranian centrifuges, and how we are able to set so many actual fires by burning out motors, pumps and electrical equipment. Without an extremely robust and expensive backup solution, which IUPROB

Ми запрограмували ПЛК, як намагаються вивести паперовий машини, запустити фабрику за допомогою діючих промислових новоств, виконати повільно, високою частотою дивує мікроарти, встановити та виконати всі програми

Рівень контролю після входу в систему SCADA в якості екранного (оперуючого) користувача є повним. Як студент зміг знищити іранські центрифуги, і як ми можемо виконати реальні операції пожежі, аварійні дії, насоси та електричне обладнання. Без надзвичайно надійного та дорогого рішення для резервного копіювання, якого не було у IUPROB, отримати виробничий час для

Скорість (м/мин)	Давлення воздуха (бар.)	НВД на стрелка (бар)	Температура пара	Температура УННОГ	Масса	Вакуум (бар.)
115.9	7.1	21.0	174.0	0.0	0.0	-0.18
Подана АКД (р/ч)	Расход возд. (л/мин)	XXX	Давление пара (бар.)	Темп-ра суш. цилиндра	Влажность	Ток Вдуум. Насоса (А)
0	3080	0	4.20	125.2	5.9	95.3

Вент. лицо	Задание температуры	Скорости вентиляторов		
Вент. привод		100 %	84 %	79 %
XXX	190	Верхний ряз 90%-100%	Средний ряз 80%-100%	Нижний ряз 70%-100%
Сброс Аварий		100%	84%	79%
		Работа		

Давление воздуха для группы 5-8 в норме				Давление воздуха для группы 1-4 в норме			
Камера №8	Камера №7	Камера №6	Камера №5	Камера №4	Камера №3	Камера №2	Камера №1
Температура в камере	Температура в камере	Температура в камере	Температура в камере	Температура в камере	Температура в камере	Температура в камере	Температура в камере
172.2 °C	124.7 °C	185.6 °C	190.2 °C	164.1 °C	179.0 °C	218.3 °C	229.6 °C
Задание: 190°C	Задание: 190°C	Задание: 190°C	Задание: 190°C	Задание: 190°C	Задание: 190°C	Задание: 190°C	Задание: 190°C
Вкл/выкл	Вкл/выкл	Вкл/выкл	Вкл/выкл	Вкл/выкл	Вкл/выкл	Вкл/выкл	Вкл/выкл
Больше	Меньше	Больше	Меньше	Больше	Меньше	Больше	Меньше
Пуск	Стоп	Пуск	Стоп	Пуск	Стоп	Пуск	Стоп
Работа	Выключена	Выключена	Работа	Работа	Выключена	Работа	Работа
Пуск	Стоп	Пуск	Стоп	Пуск	Стоп	Пуск	Стоп

0:04 812 views



## Alert: This is most likely false/ inaccurate



*“Buratiya was hit in this attack causing 96,000 Siberians to lose power during cold weather. We, Ghostsec declare that we were infact responsible for the (highlighted as) “mysterious” emergency shutdown.*

*Although some of us have remorse for the civilians affected, we are pleased to state that the ICS attack was successfully executed with 0 casualties in the actual explosion due to our proper timing while performing our attacks.”*

During #OPRUSSIA, #GhostSec had participated and executed in outstanding hacks such as the train hacks resulting in completely stopping trains owned and run by Metrospetstekhnika and printer attacks.

However We preformed a ICS hack on Russian modbus,IEC, and moxa devices which is also known to control some electrical systems.

Our main objective was to try and cause a small/large scale blackout. However this news article caught our eye <https://www.mirror.co.uk/news/world-news/breaking-giant-explosion-russian-power-27308819> (The press service at Gusinoozerskaya said “spontaneous damage to the transformer” occurred, which caused the shutdown of all power units of the station that were in operation.)

Buratiya was hit in this attack causing 96,000 Siberians to lose power during the cold weather. We, GhostSec declare that we were infact responsible for the (highlighted as) “mysterious” emergency shutdown.

Although some of us have remorse for the civilians affected, we are pleased to state that the ICS attack was successfully executed with 0 casualties in the actual explosion due to our proper timing while preforming our attacks.

The timing does in fact fit correctly with the timings of our ICS hack and is clearly mentioned in the article the attack was due to the transformer taking damage and “It is unclear if there is a connection but there has been speculation on a sabotage.”

mirror

Giant explosion at Russian power station causes blackout near uranium mine

It comes after a huge explosion rocked an oil refinery in Russia’s Rostov region, which borders Ukraine, some four miles inside Ru...



# Opening the Box: Are These Attacks Real?

# Hacktivist Techniques in MITRE ATT&CK for ICS

Tactic	Technique
Initial Access	T0883: Internet Accessible Device
Initial Access	T0819: Exploit Public-Facing Application
Execution	T0807: Command-Line Interface
Execution	T0823: Graphical User Interface
Persistence	T0859: Valid Accounts
Evasion	T0872: Indicator Removal on Host
Lateral Movement	T0859: Valid Accounts
Collection	T0852: Screen Capture

Tactic	Technique
Collection	T0811: Data from Information Repositories
Command and Control	T0885: Commonly Used Port
Command and Control	T0869: Standard Application Layer Protocol
Inhibit Response Function	T0816: Device Restart/Shutdown
Inhibit Response Function	T0809: Data Destruction
Impair Process Control	T0855: Unauthorized Command Message
Impact	T0831: Manipulation of Control
Impact	T0882: Theft of Operational Information
Impact	T0826: Loss of Availability





**Archived Content**

In an effort to keep CISA.gov current, the archive contains outdated information that may not reflect current policy or programs.

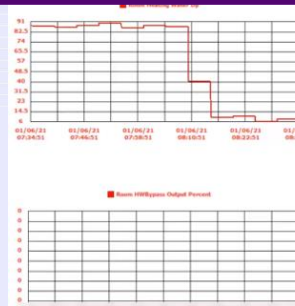
ALERT

# Mitigating Attacks Against Uninterruptable Power Supply Devices

Last Revised: April 29, 2022

# Graphical User Interfaces

Water treatment control panel. The top section features a schematic diagram of a water treatment system with components labeled A1, B1, C, A2, and B2. A central tank is labeled "EC 2.0=2.0" and "pH 5.5=5.5". Below the diagram are buttons for "정지해제", "관수종료", and "구역넘김". The bottom section shows a large cylindrical tank with a digital display showing "102" and "4,6". Labels include "PRESSURIZAÇÃO" and "SAÍDA LÍQUIDA".



Dashboard for Heating and Chilled water valve positions. It lists various AHU (Air Handling Unit) statuses for different locations like Kitchen, Fremantle, Light Meals, Bar & Conference, Reception, Brasserie, and Hotel North/South. It also displays "Master Heating Call" and "Master Cooling Call" indicators, along with ambient heating and cooling signals and O/A temperatures.

Dampers System control interface. It shows a table of damper statuses for zones Z1 through Z9. The table includes columns for damper status, temperature (TS), and Inlet Return Temperature (IRT). A "Dampers System" control bar with "Start" and "Stop" buttons is visible at the top.

Zone	Status	TS (°C)	IRT (°C)
Z1	24.89 °C	327.67 °C	54.6 °C
Z5	35.88 °C	75.3 °C	75.3 °C
Z6	35.88 °C	-	-
Z9	29.12 °C	-	81.6 °C

Lindner Sommerauer Hackgut SL 150 control panel. It features a central image of the machine and a list of operating modes: Energieanforderung, Dauerbetrieb, Uhrzeitbetrieb, Boilerbetrieb, Uhr+Boilerbetrieb, and Handbetrieb. A status panel on the right shows "Anlagenstatus" with indicators for Uhr, Boiler, Heizkreis, Parameter, and Kessel. Buttons for "Ein" and "Aus" are at the bottom.

Water flow visualization showing flow rates and valve positions. It features a 3D-style rendering of pipes and valves. Flow rates are indicated as 0.00 l/s, 9.43 l/s, and 1.86 l/s. A valve is labeled "IN CHIUSURA".

GFORNOVOGAS control panel. It displays a schematic diagram of a gas flow system with two pressure gauges labeled PT105 (240.1 bar) and PT107 (209.6 bar). The interface includes a navigation menu on the left and a status bar at the top with the date "17/03/2020 02:33:27".

WAGO Web-based Management interface. It displays "PLC Runtime Information" for a WAGO 750-8202 PFC200 2ETH RS. The interface includes a navigation menu, a "Status" panel with LEDs, and a "Task 0: MAIN: Id: 2" section showing cycle counts and times.

WesTech ALTAPAC water filtration control panel. It shows a detailed schematic of a water filtration system with various tanks, pumps, and filters. Key parameters include "Flow Totals" (Totalizer: 16994.60, 3753.10 Kgal), "UF Inlet" (0.4 psi), "UF Outlet" (0.35 psi), and "PDT Pressure Loss" (0.00 psi/min). Buttons for "DIRECTORY", "BACK", "CONTROLS", "ALARM HISTORY", and "ALARM RESET" are visible.

# Exploit Public-Facing Applications

```
[*] 44818 - CIP - Running CRASHETHER attack.
[*] 44818 - CIP - Got session id: 0xdb5f9d5c
[*] 44818 - CIP - CRASHETHER attack complete.
[*] Running module against
[*] 44818 - CIP - Running CRASHETHER attack.
[*] 44818 - CIP - Got session id: 0xa006900
[*] 44818 - CIP - CRASHETHER attack complete.
[*] Running module against
[*] 44818 - CIP - Running CRASHETHER attack.
[*] 44818 - CIP - Got session id: 0x1001b00
[*] 44818 - CIP - CRASHETHER attack complete.
[*] Running module against
[*] 44818 - CIP - Running CRASHETHER attack.
[*] 44818 - CIP - Got session id: 0x68004800
[*] 44818 - CIP - CRASHETHER attack complete.
[*] Running module against
[*] 44818 - CIP - Running CRASHETHER attack.
[*] 44818 - CIP - Got session id: 0x3001800
[*] 44818 - CIP - CRASHETHER attack complete.
[*] Running module against
[*] 44818 - CIP - Running CRASHETHER attack.
[*] 44818 - CIP - Got session id: 0xc29d36d8
[*] 44818 - CIP - CRASHETHER attack complete.
[*] Running module against
[*] 44818 - CIP - Running CRASHETHER attack.
[*] 44818 - CIP - Got session id: 0xd9b75c51
[*] 44818 - CIP - CRASHETHER attack complete.
[*] Running module against
[*] 44818 - CIP - Running CRASHETHER attack.
[*] 44818 - CIP - Got session id: 0x2e023b00
[*] 44818 - CIP - CRASHETHER attack complete.
[*] Running module against
```

- Metasploit
  - IEC-104
  - EtherNet-IP CIP
- Killbus
  - Modbus



What's the Impact?!



# Debunking Some OT Hacking Claims

# Case 1: GhostSec Claimed to Deploy Ransomware on Belarusian RTU





root@178.163.133 password:

BusyBox v1.23.2 (2021-03-29 10:37:34 MSK) built-in shell (ash)

```
#####          #          #####          #          #####
# # # # # # # # # # # # # # # # # # # # # # #
# # # # # # # # # # # # # # # # # # # # # # #
# ##### # ##### # ##### # #####
# # # # # # # # # # # # # # # # # # # # # # #
# # # # # # # # # # # # # # # # # # # # # # #
# ##### ##### ##### ##### # ## #####
```

Build for RTU968V2 v.2.6.9S  
OpenWrt Chaos Calmer

root@TELEOFIS-RTU968V2:~# ls /bin ; uname -a

ash	config_generate	echo	hostname	ls	netstat	ps	stat	umount
board_detect	cp	egrep	ipcalc.sh	mkdir	nice	pwd	stty	uname
busybox	date	false	kill	mknod	opkg	rm	sync	usleep
cat	dd	fgrep	ln	mktemp	pidof	rmdir	tar	vi
chgrp	df	fsync	lock	mount	ping	sed	touch	watch
chmod	dmesg	gunzip	login	mv	ping6	sh	true	zcat
chown	dnsdomainname	gzip	login.sh	netmsg	pingcontrol	sleep	ubus	

Linux TELEOFIS-RTU968V2 3.18.29 #1 Mon Mar 29 10:43:13 MSK 2021 armv5tejl GNU/Linux

root@TELEOFIS-RTU968V2:~#  
root@TELEOFIS-RTU968V2:~#  
root@TELEOFIS-RTU968V2:~#  
root@TELEOFIS-RTU968V2:~#

```
root@TELEOFIS-RTU968V2:~# ls /bin
ash                               dnsdomainname          login                    ping
board_detect.fuckPutin           echo                    login.sh.fuckPutin     ping6
busybox                           egrep                   ls                       pingcontrol.fuckPutin
cat                                false                   mkdir                    ps
chgrp                              fgrep                   mknod                    pwd
chmod                              fsync                   mktemp                   rm
chown                              gunzip                  mount                     rmdir
config_generate.fuckPutin        gzip                     mv                        sed
cp                                 hostname                netmsg                    sh
date                               ipcalc.sh.fuckPutin    netstat                   sleep
dd                                 kill                     nice                       stat
df                                 ln                       opkg.fuckPutin           stty
dmesg                             lock                     pidof                     sync
```

root@TELEOFIS-RTU968V2:~# Connection to 178.163.133 closed by remote host.  
Connection to 178.163.133 closed.



# CASE 2: Claim Responsibility for Destruction of Assets

Taking advantage of real-world events...

- Altahrea Team claims responsibility over Orot Yosef power plant fire.
- GhostSec claims responsibility for hydro-power plant in Russia.
- Team OneFist claims to disable cellular router supporting OT in Russia.



# CASE 3: Claim Responsibility for Destruction of Assets

#cyberattack against Iran's steel industry

Today, 27/06/2022, we, "Gonjeshke Darande", carried out cyberattacks against Iran's steel industry which affiliated with the IRGC and the Basij:

- The Khouzestan Steel Company (KSC)
- The Mobarakeh Steel Company (Isfahan) (MSC)
- The Hormozgan Steel Company (HOSCO)

These companies are subject to international sanctions and continue their operations despite the restrictions.

These cyberattacks, being carried out carefully so to protect innocent individuals, are in response to the aggression of the Islamic Republic.

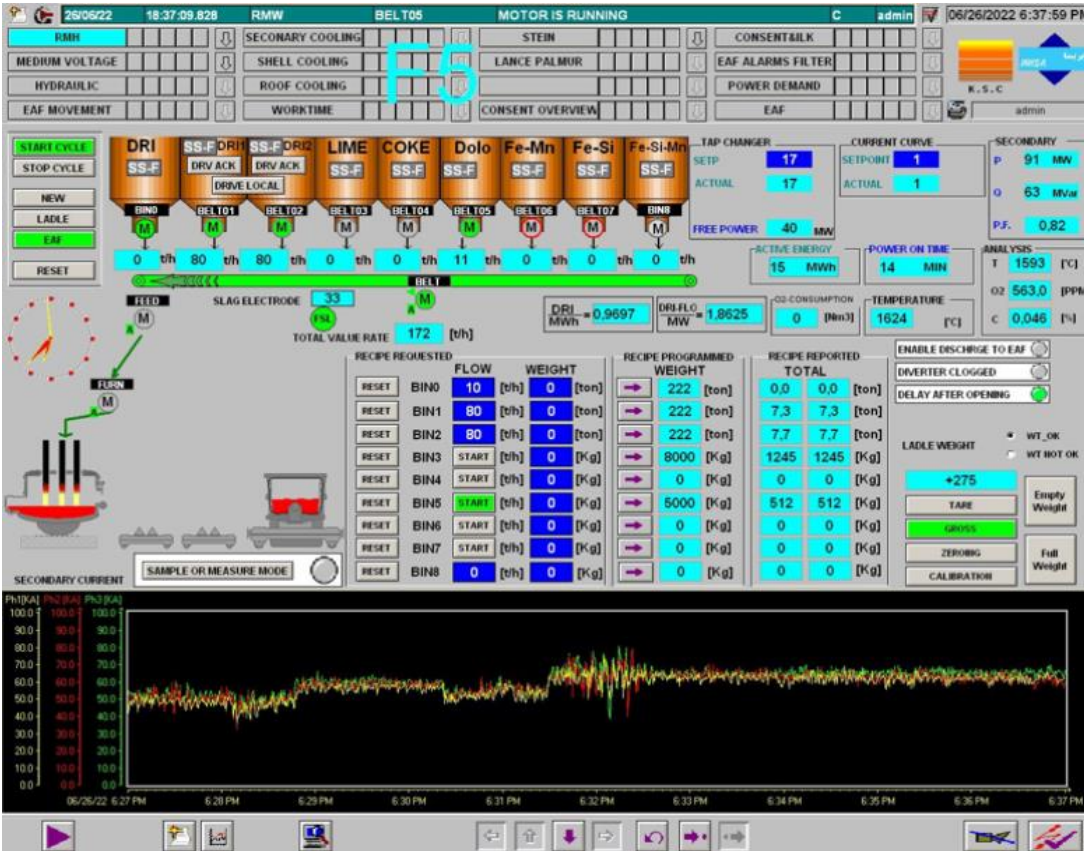
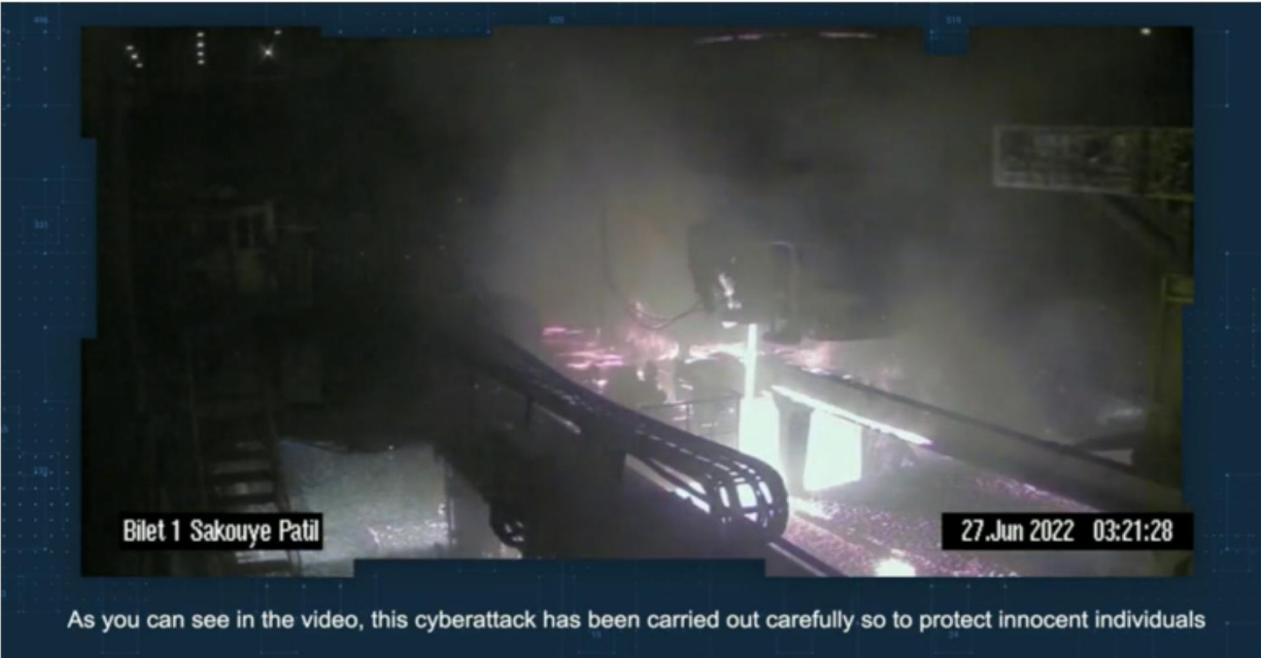


0:03 / 1:10

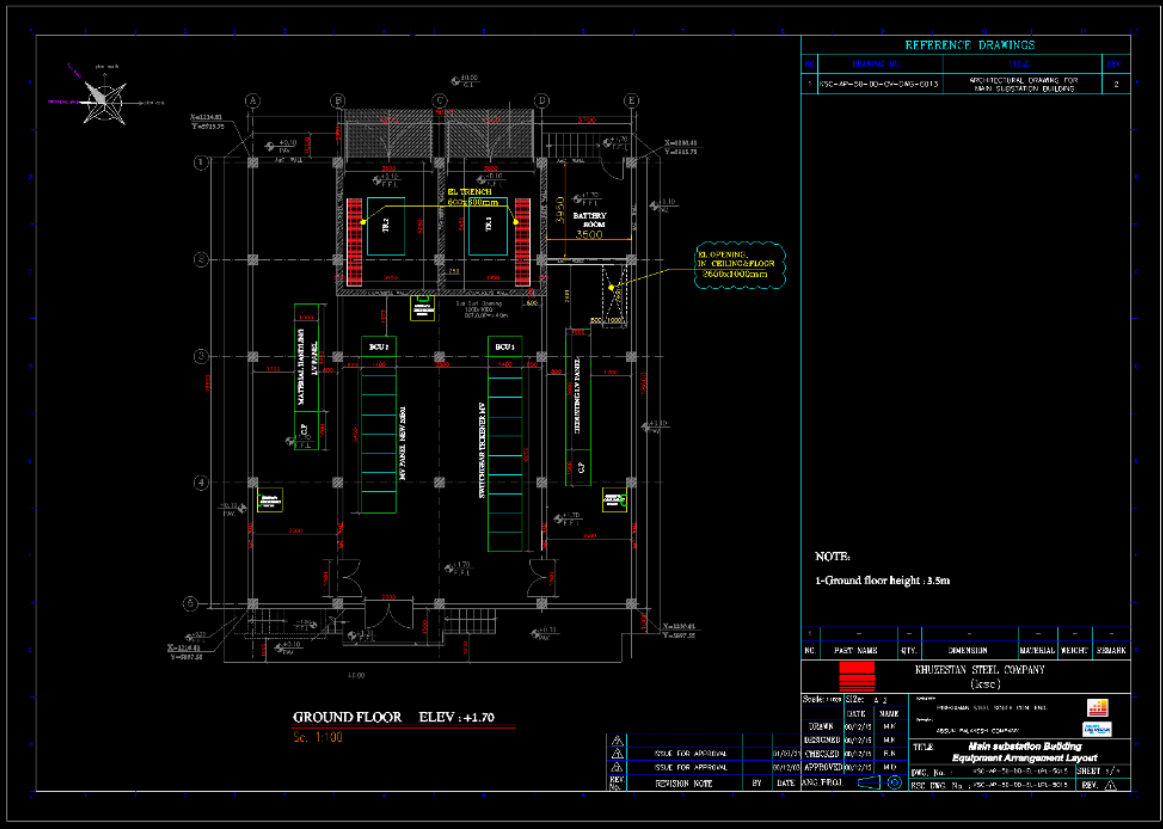
7:12 AM · Jun 27, 2022



# CASE 3: Claim Responsibility for Destruction of Assets



# CASE 3: Claim Responsibility for Destruction of Assets



# So...is there a ~~Cat~~/Hack in the Box?

Do Hacktivists Pose a Risk to Operational Technology?



Yes and no...



- Hacktivists interact with OT assets
- Higher frequency means higher risk
- Calls media attention and invites for copycats
- Helps nation-states to deny actions
- Actors share knowledge which will remain after conflict

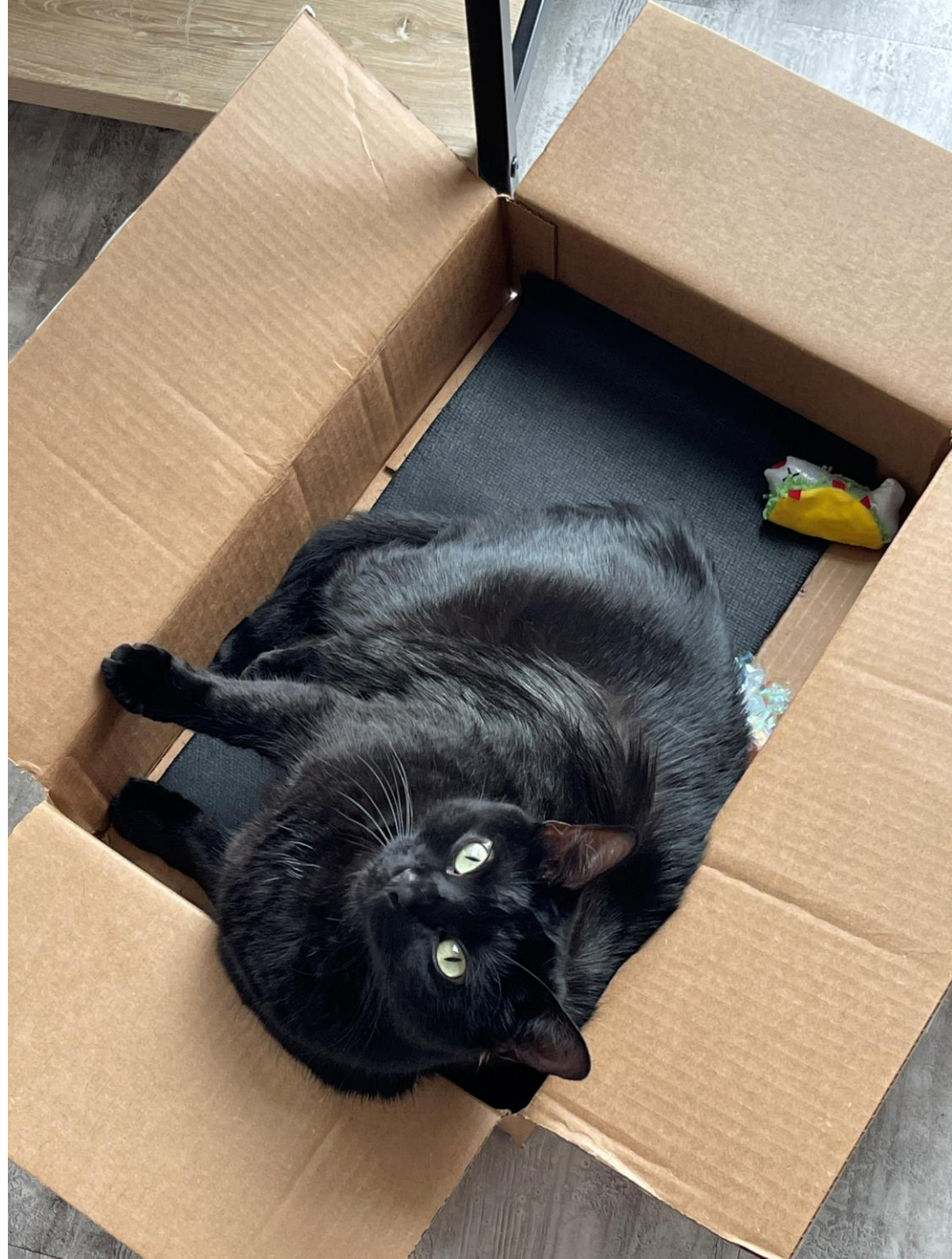
Yes

# No

- Hacktivists use very simple techniques
- Higher frequency des not mean higher impact
- OT attacks require more resources to generate impact
- Hacktivists can call media attention without OT
- Nation-state actors have hacked OT with little to no repercussions



And yet... hacktivists continue  
to normalize hacking OT



# Thanks!

Daniel Kapellmann Zafra

@Kapellmann

[www.kapell.tech](http://www.kapell.tech)