



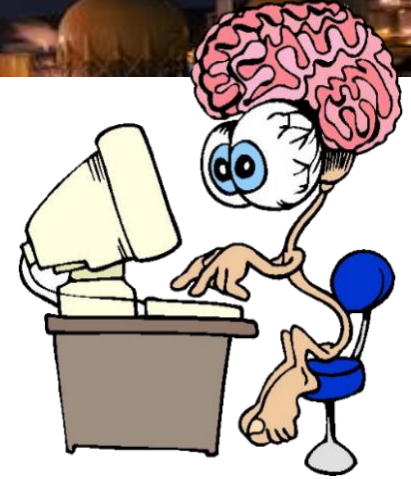
# **Understanding Cyber Threats and Associated Risks for Radioactive Sources**

**Marina Krotofil**

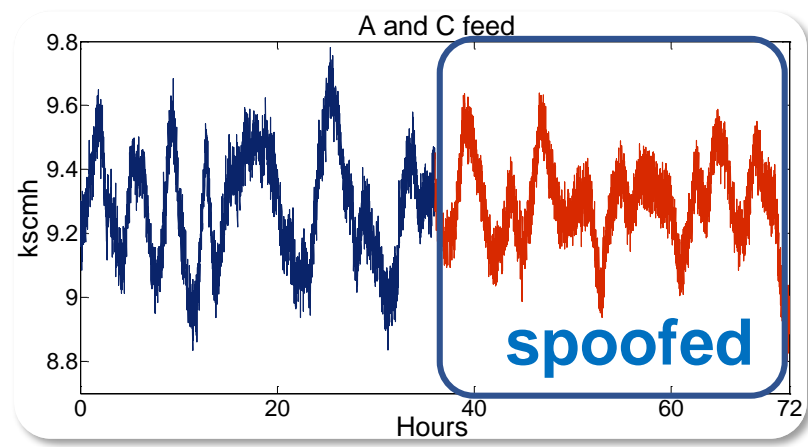
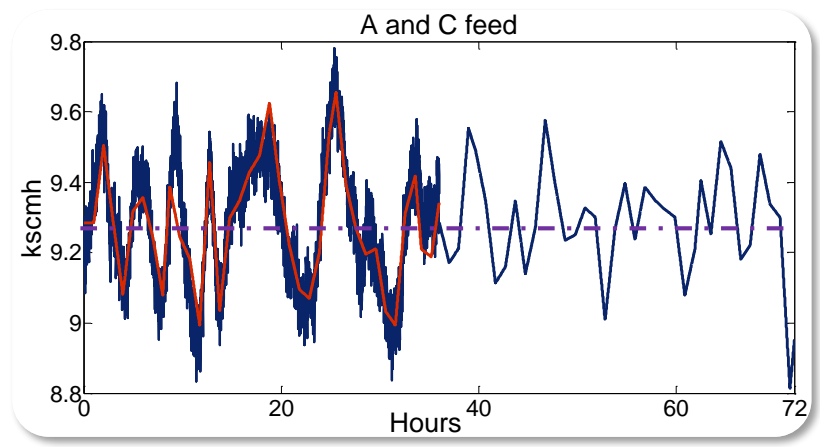
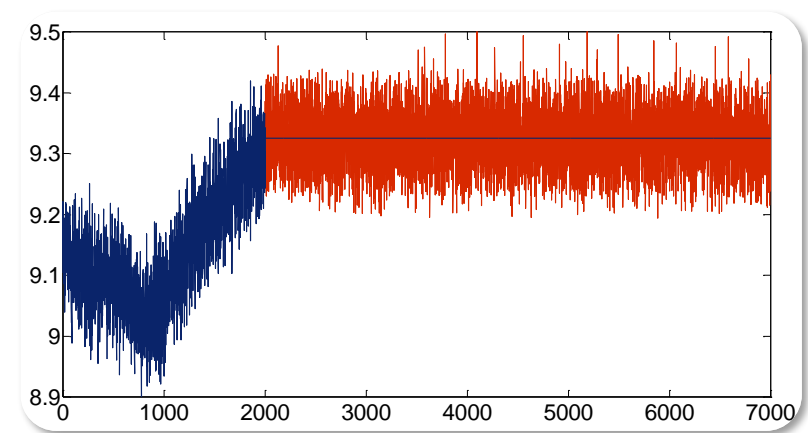
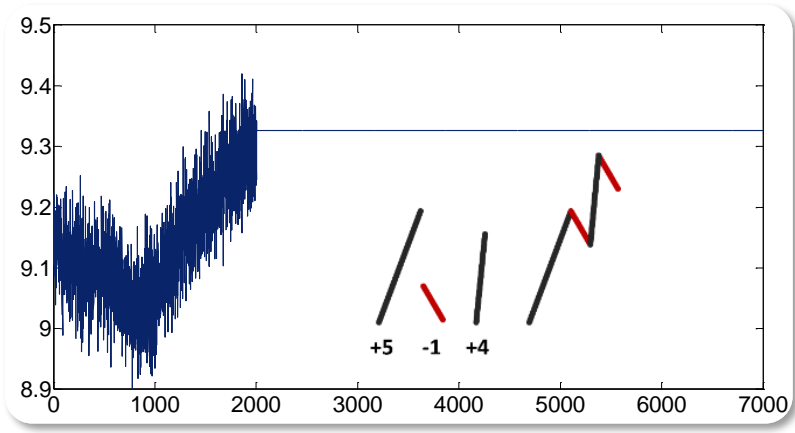
**Round Table on Cybersecurity Best Practices for Users of Radioactive Sources,  
Vienna, Austria, 10.09.2019**

# About myself

- Senior Security Engineer at the large chemical company – defender role
- Specializing in offensive cyber-physical security in Critical Infrastructures
  - **Focus:** Physical damage or how to make something going bad, crash or blow up by means of cyber-attacks



# My only experience with nuclear field



# In this presentation

A nighttime photograph of a city skyline with various buildings and lights. A semi-transparent dark box is overlaid on the top left, containing the title text.

- Evolvement: Threat actors and their motivation
- Current trends: Cyber threat landscape
- Product security: Worrisome State-of-the-Art



# Threat actors evolvemement

# Modernization of the nuclear industry

## How America's First Digitally Operated Reactor Could Push Nuclear Technology Forward

A new kind of nuclear plant is here **Sep 4, 2019**

<https://www.popularmechanics.com/technology/infrastructure/a28912471/digital-nuclear-reactor/>



## References for Cyber Incidents at Nuclear Facilities

December 2014	Korea Hydro and Nuclear Power Company	South Korea	Data theft and release	Intentional	4, 25
February 2015	Japanese Nuclear Material Control Center	Japan	Nuclear facility used as relay point in attack	Unknown	26

<https://www.nti.org/analysis/tools/table/133/>

# (Cyber)Terrorists

- Aim at dramatic effect (Godzilla effect)
- Previously did not showcase strong technical or cyber capabilities
- Currently: actively recruiting members with engineering and cyber background/skills



## Security Guard's Murder Fuels Fears That Nuclear Plants in Belgium Could Be Attacked

A guard's missing security pass to a nuclear power plant in Belgium had to be deactivated after he was found shot to death in his home.

Mar 26 2016,

# (Cyber) Criminals

- (May) use cyber attacks to support criminal activities
  - E.g., stealing/smuggling nuclear materials
- Discovered ways to monetize attacks in infrastructures with critical uptime/availability requirements
  - Extortion attacks (ransomware)
- Participating in the market as a resource for hiring
  - Hackers for hiring
  - Hacking tools for sale






# State-sponsored threat actors

- The build-up of capabilities keep accelerating
  - Leaked NSA catalogue of cyber tools
- Strategic operations to support long-term objectives
  - E.g. espionage, persistence
- Hacking to support national economy
  - E.g., discredit competitor products or subvert production lines

TOP SECRET//COMINT//REL TO USA, FVEY

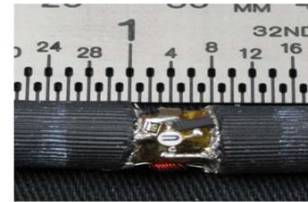


**RAGEMASTER**  
ANT Product Data

24 Jul 2008

(TS//SI//REL TO USA,FVEY) RF retro-reflector that provides an enhanced radar cross-section for VAGRANT collection. It's concealed in a standard computer video graphics array (VGA) cable between the video card and video monitor. It's typically installed in the ferrite on the video cable.

**(U) Capabilities**  
(TS//SI//REL TO USA,FVEY) RAGEMASTER provides a target for RF flooding and allows for easier collection of the VAGRANT video signal. The current RAGEMASTER unit taps the red video line on the VGA cable. It was found that, empirically, this provides the best video return and cleanest readout of the monitor contents.



**(U) Concept of Operation**  
(TS//SI//REL TO USA,FVEY) The RAGEMASTER taps the red video line between the video card within the desktop unit and the computer monitor, typically an LCD. When the RAGEMASTER is illuminated by a radar unit, the illuminating signal is modulated with the red video information. This information is re-radiated, where it is picked up at the radar, demodulated, and passed onto the processing unit, such as a LFS-2 and an external monitor, NIGHTWATCH, GOTHAM, or (in the future) VIEWPLATE. The processor recreates the horizontal and vertical sync of the targeted monitor, thus allowing TAO personnel to see what is displayed on the targeted monitor.

**Unit Cost: \$ 30**

**Status:** Operational. Manufactured on an as-needed basis. Contact POC for availability information.

**POC:** [REDACTED] S32243, [REDACTED], [REDACTED]@nsa.ic.gov

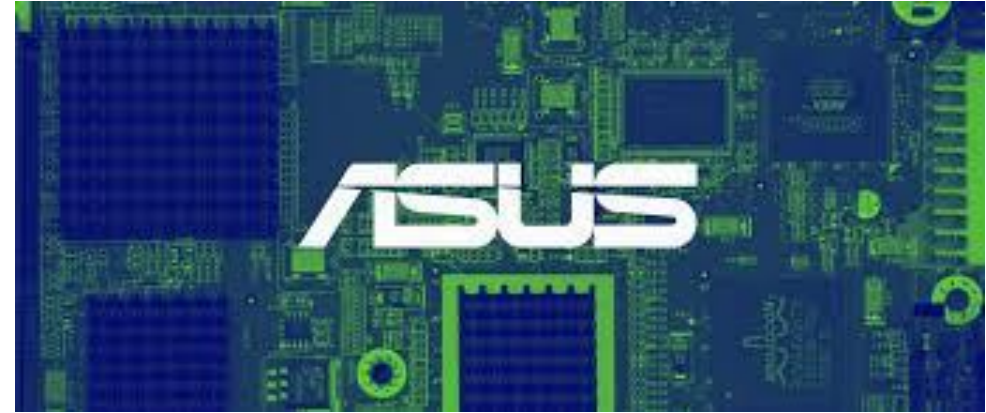
Derived From: NSA/CSSM 1.52  
Dated: 20070108  
Declassify On: 20320108

TOP SECRET//COMINT//REL TO USA, FVEY

# Recent high-profile attacks



Over 500.000 affected devices  
(over 10 brands & 70 models),  
2018



Hackers Targeted 600 MAC Addresses, 2019



Hackers targeted specific records of 20  
individuals, 2019

# Lagging behind threat actors are catching-up

## China's APT3 Pilfers Cyberweapons from the NSA

September 6, 2019



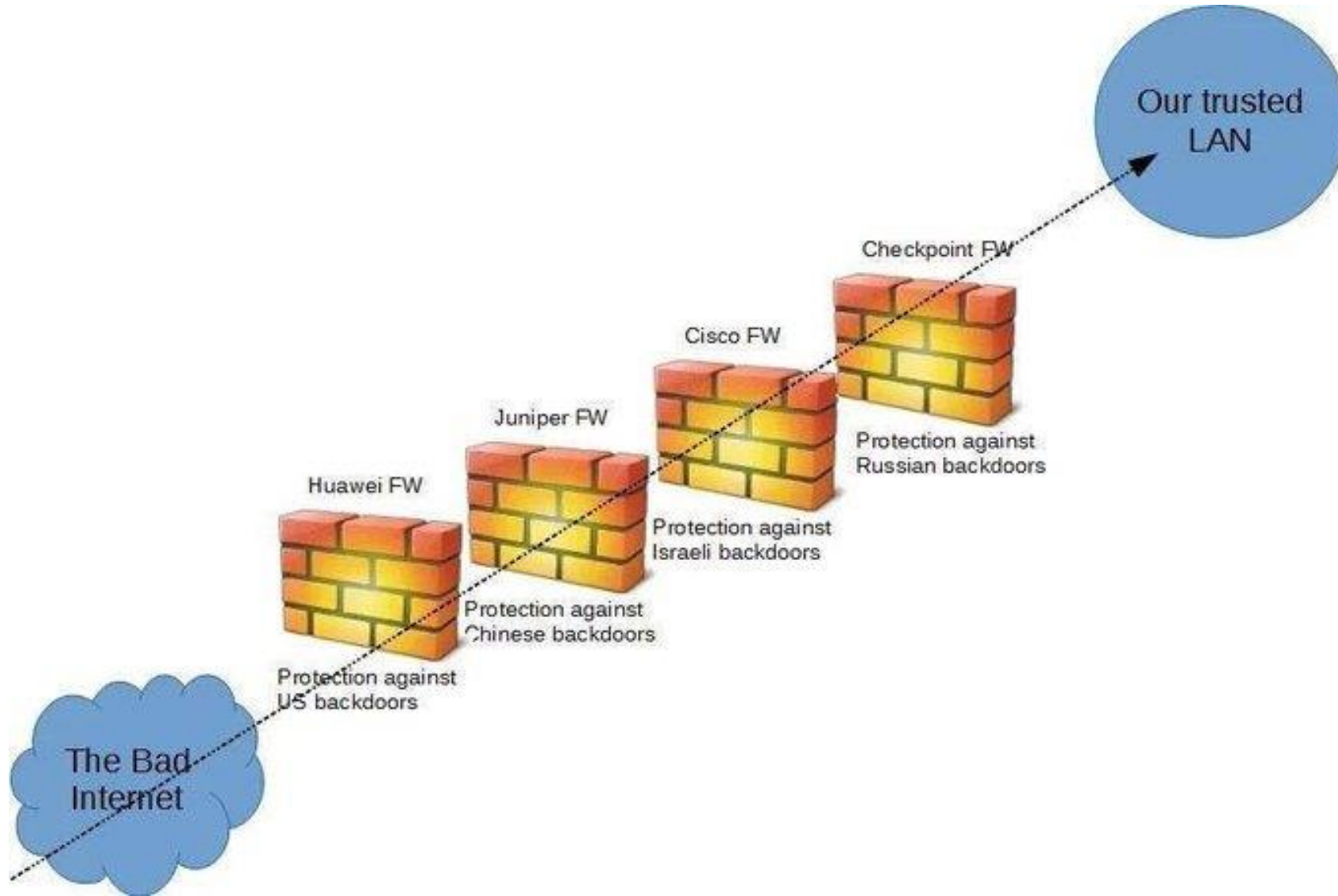
# Threat actors with special privileges

## Playing nice? FireEye CEO says U.S. malware is more restrained than adversaries'

JUN 1, 2018 | CYBERSCOOP

Mandia, for example, told CyberScoop that before publishing a public threat intelligence report, FireEye will typically tip off intelligence officials from the Five Eyes alliance about the release. If FireEye detects malware on a customer's system that researchers think is from the U.S. or an allied country, it will remove it. But Mandia said such malware ought to be stealthier.

# “Defense-in-Depth” in perimeter security



# Accessibility of proprietary information



- Sensitive and confidential documentation is readily available
  - Unprotected repositories
  - Public sources, e.g. Virus Total, Scribd, etc.
  - Purposely leaked data and documentation

<https://www.reuters.com/article/us-nuclear-southkorea-northkorea-idUSKBN0MD0GR20150317>



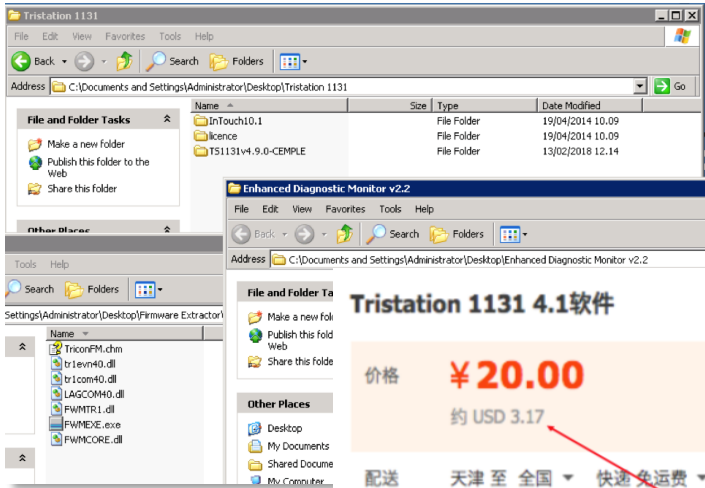
# Easily obtainable hardware & software



- One no longer need rich and legal buyer to obtain equipment
  - Can be purchased on e-commerce platforms
  - Firmware available on GitHub
  - Even source code can be obtained



# Hardware and software for purchase



## Tristation 1131 4.1软件

价格 **¥20.00**  
约 USD 3.17

0 累计评论  
1 交易

配送 天津 至 全国 快速 免运费 24小时内发货

数量  件(库存993件)

立即购买

加入购物车

**3 USD**

支付



## TRICONEX 3008 MODULE

Pre-Owned

**\$1,600.00**

or Best Offer

+\$60.82 s

**12 Sold**



## Triconex User Manuals

New (Other)

**\$740.95**

Buy It Now

+\$55.57 shipping

FIELD NAME	MEMORY LAYOUT	ABSOLUTE LOCATION
4x1024K ROM	TSX ROMs	000000
	TSX system stack	080000
16x256K RAM	TSX Variables RAM	081800
A-field	Diagnostic, comm buf,	08c000
	cpStatus Table,	
	Peers Contexts	
	Input Confidence Bits	
	Discrete Input Data	
	Integer Input Data	
	Real Input Data	
B-field	Discrete Input Data	
C-field	Integer Output Data	
	Real Output Data	
	Discrete Output Data	
no-field	Auxiliary Input Area	
Up Stream A-Field		
Up Stream B-Field		
	Board Fault Data	
	my_config	
	us_config	
	ds_config	

**Source code**



# **Current trends in cyber threats landscape**

# Targeted ransomware

## Norsk Hydro ransomware incident losses reach \$40 million after one week

March 26, 2019



# Cryptomining farms in isolated facilities

## Security News This Week: Cryptocurrency Miners Expose Nuclear Plant to Internet

08.24.2019

<https://www.wired.com/story/nuclear-plant-cryptomining-bec-scam-xbox-security-roundup/>



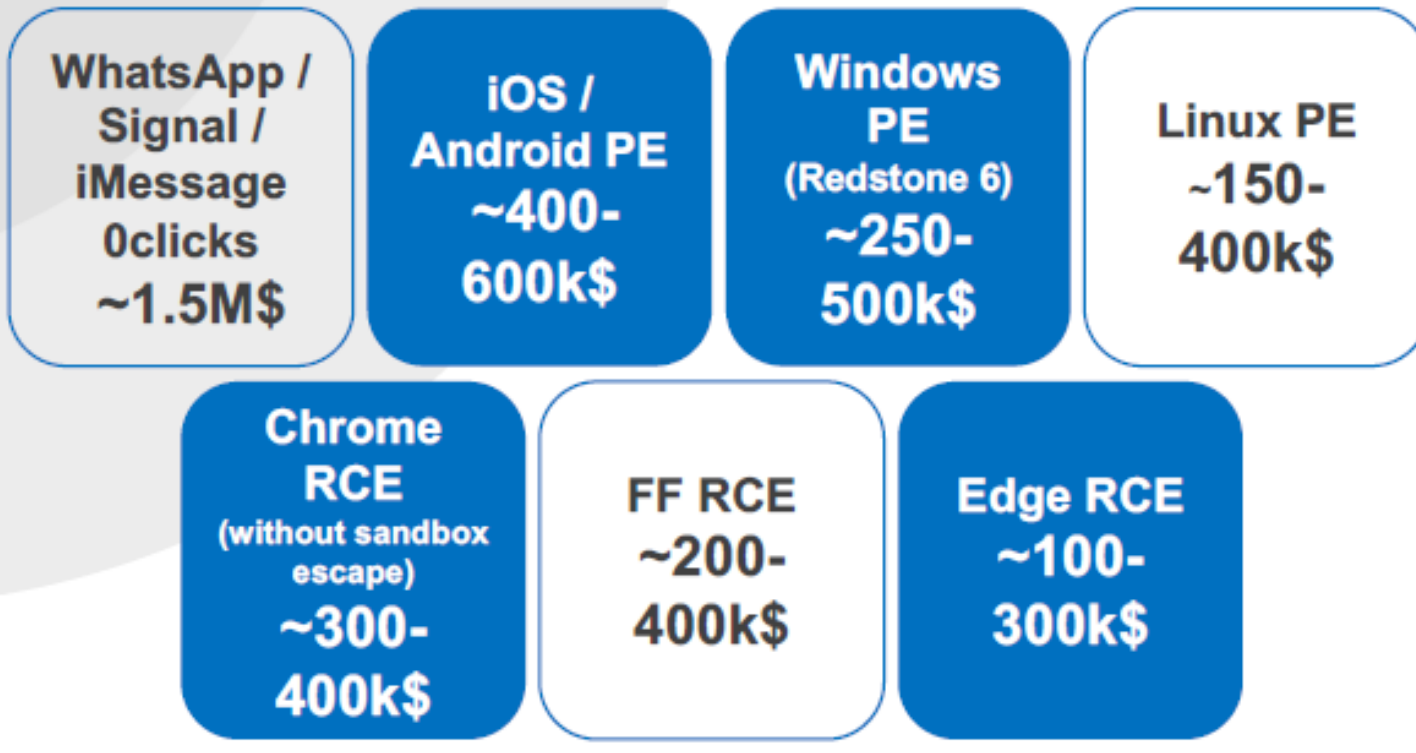
## Russian Scientists Arrested for Crypto Mining at Nuclear Lab

Feb 9, 2018

<https://www.coindesk.com/russian-scientists-arrested-crypto-mining-nuclear-lab>

# Matured zero day & offensive tools market

## Payouts – behind the scenes



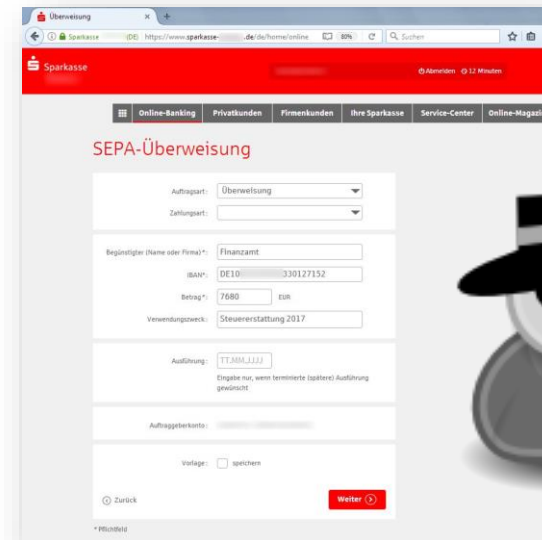
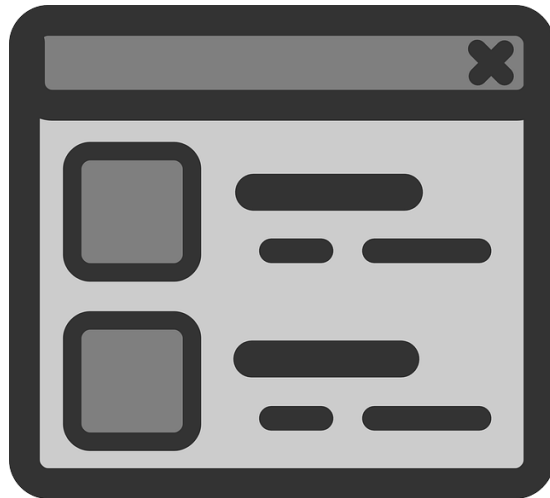
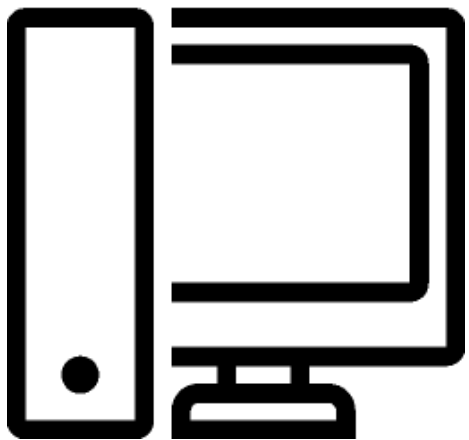
**Main trend in offensive security**

A nighttime photograph of an industrial facility, possibly a refinery or chemical plant, with numerous lit-up towers, pipes, and storage tanks against a dark sky.

**RACE TO THE  
BOTTOM**

Two large, dark grey arrows pointing downwards from the word 'BOTTOM' in the text above, emphasizing the direction of the trend.

# Race-to-the-Bottom in e-commerce



**Business  
processes  
secure by design**

*Currently threat models  
assumes that the e-commerce  
application is “taken” by  
attacker*

# BIOS rootkits



**LoJax: First UEFI rootkit  
found in the wild, courtesy of  
the Sednit group**



27 Sep 2018



# Brief history of cyber-physical attacks

Reconnaissance and weaponization of capabilities

It's happening: Publicly known cyber-physical attacks



**1999**

First active recon & initial intrusion attempts

**2010**

Planned operation to hinder Iran's nuclear program (Stuxnet)

**2013**

First publicly known OT recon activities (HAVEX)

**2015**

Ukraine power grid attack (BlackEnergy)

**2016**

Ukraine power grid attack (Industroyer)

**2017**

**TRITON**

Successful *cyber-physical* experiments



# Purdue network reference architecture

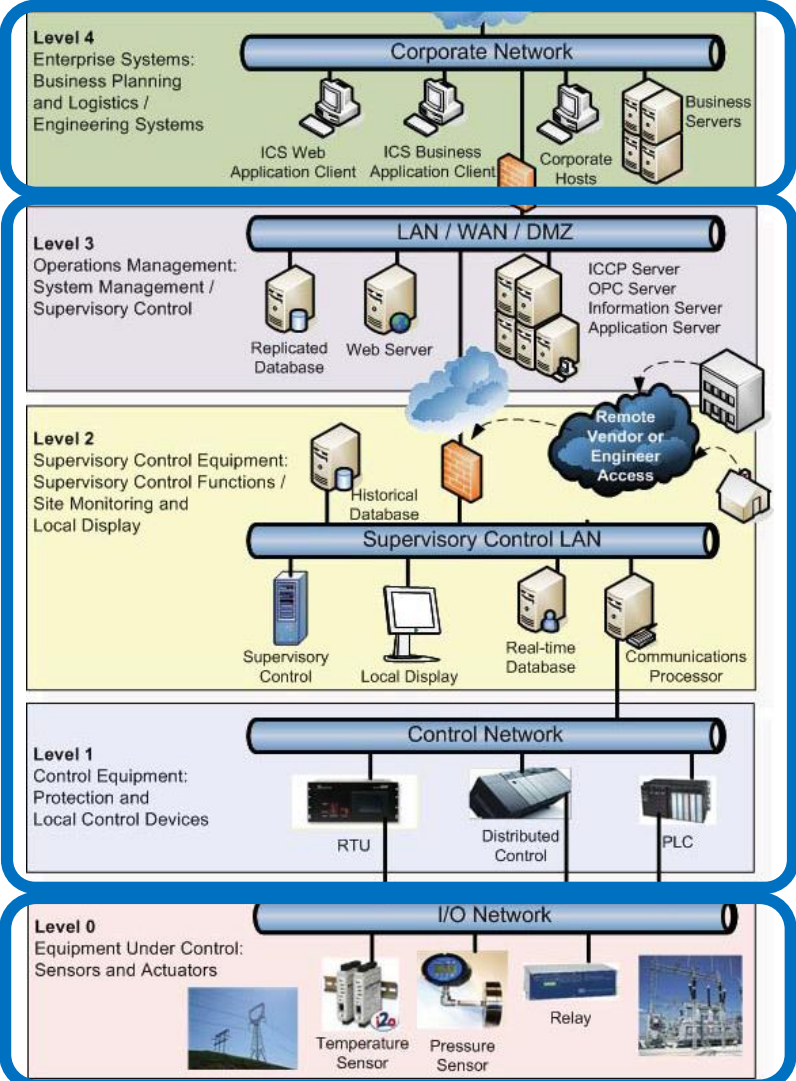
Level 4

Level 3

Level 2

Level 1

Level 0



IT network

OT network

Physical process

# Race-to-the-Bottom when placing exploits

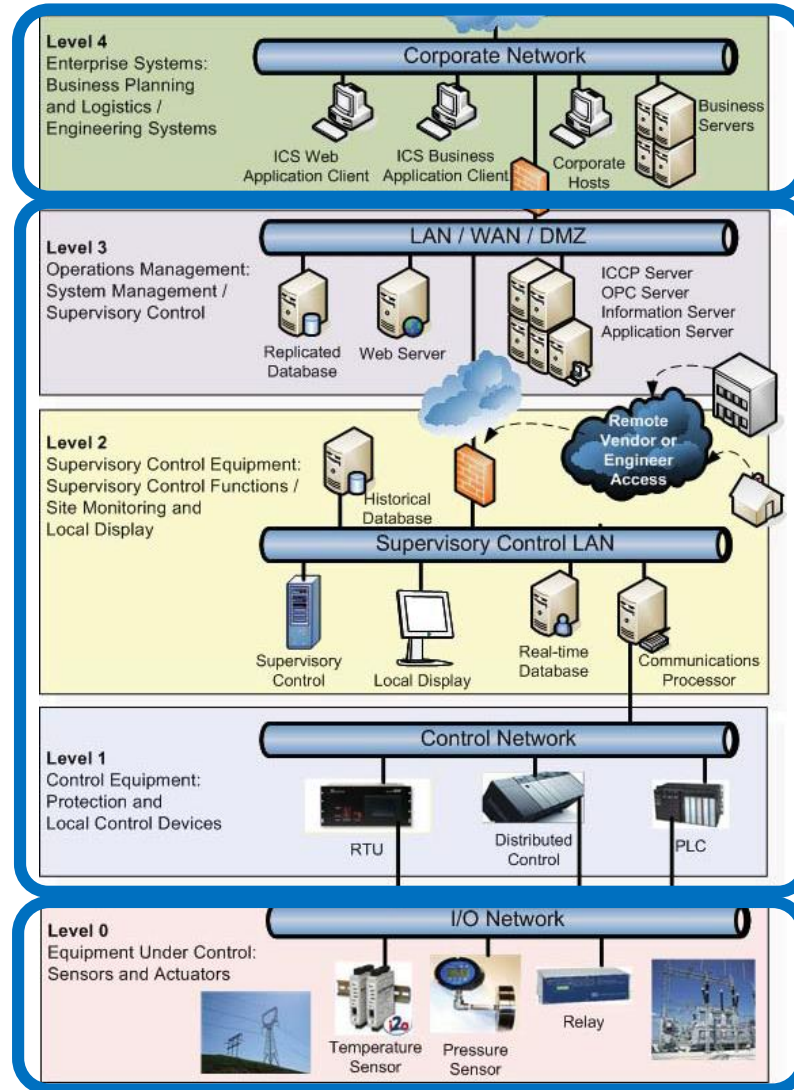
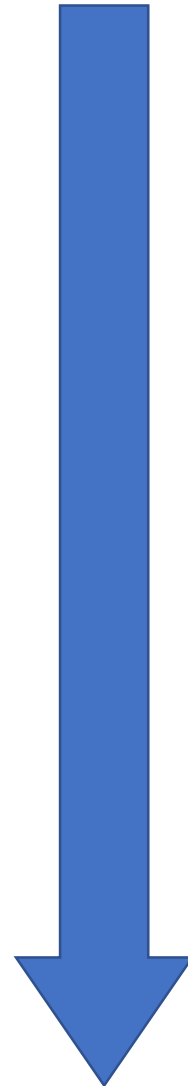
Level 4

Level 3

Level 2

Level 1

Level 0



IT network

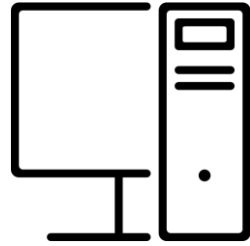
BlackEnergy  
(2015)

Industroyer  
(2016)

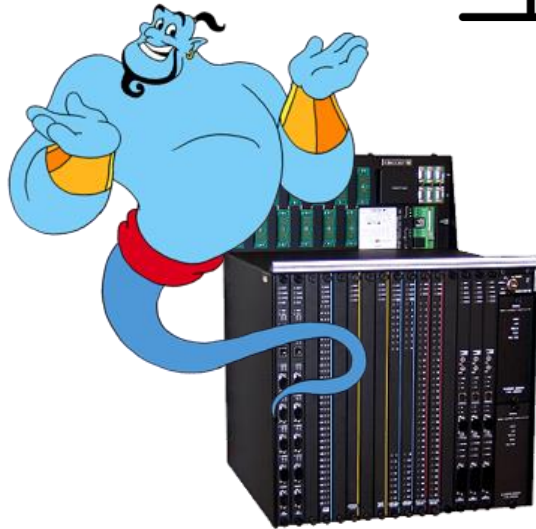
TRITON  
(2017)

Physical process

# TRITON implant



Human operator



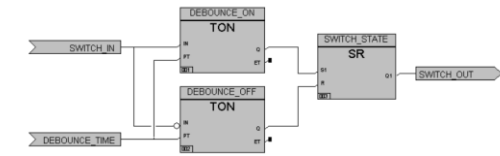
“Your wish is my command”

Triconex

Control logic

Firmware

Triton



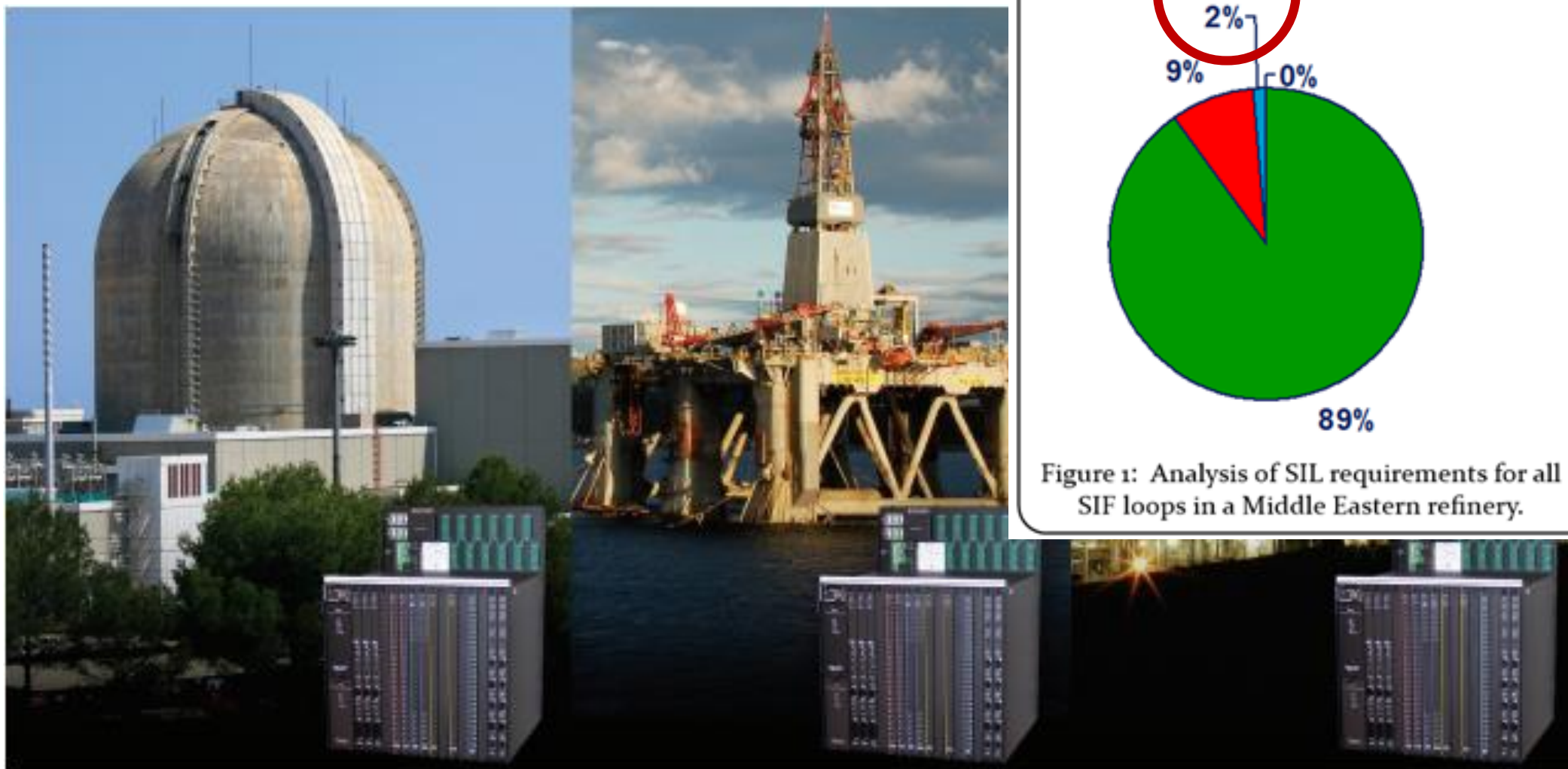
```
_handler:                                # CODE XREF: invoke_syscall:5v
lwz   r11, 0xC(r3) # Load Word and Zero
lis   r10, off_FFB000@ha # Load Immediate Shifted
addi  r11, r11, -1 # Add Immediate
mulli r0, r11, 0x1C # Multiply Low Immediate
addi  r10, r10, off_FFB000@l # Add Immediate
lwz   r6, (off_FFB104 - 0xFFB000)(r10) # FFB104
lhz   r9, (word_FFD232 - 0xFFB000)(r10) # FFD232
add   r12, r6, r0 # Add
addi  r7, r10, 0x174 # 0xFFB174
```

```
// Execute function at address X
case M_EXECUTE:
{
  if (mp >= 0x10)
  {
    function_ptr = arg->field_0;

    if (function_ptr < 0x100000)
    {
      call(function_ptr);
      return_value = 0xA;
    }
    else

```

# TRICONEX: Safety Integrity Level (SIL3)



# Triconex in nuclear field

TRICONEX  
Tricon Version 9-10 Systems

**Planning and Installation Guide**  
for Tricon v9-v10 Systems

Assembly No. 9700077-012



February 2009

TriStation 1131 Developer's Workbench



invensys-  
**TRICONEX**

TRICONEX PRODUCTS - INVENSYS PROCESS SYSTEMS

Project: TRICON v10 NUCLEAR QUALIFICATION PROJECT

## SOFTWARE QUALIFICATION REPORT

Triconex Document No: 9600164-535

Revision 0

July 2007

### MPR ASSOCIATES QUALITY ASSURANCE DOCUMENT

This document has been prepared, reviewed, and approved in accordance with the Quality Assurance requirements of 10 CFR 50, Appendix B, as specified in the MPR Quality Assurance Manual and in accordance with the requirements of Invensys Triconex Purchase Order No. 113803, dated March 23, 2006.

	Name	Signature	Title
Author:	David Herrell	<i>David Herrell</i>	Supervisory Engineer, MPR Assoc.
Reviewer:	Chris Rice	<i>Chris Rice</i>	Lead Engineer, MPR Assoc.
Approval:	Eric Claude	<i>Eric Claude</i>	ICT Group Manager, MPR Assoc.

# Multidisciplinary attack teams

- Origin of one of the attacks attack was narrowed down to ***Central Scientific Research Institute of Chemistry and Mechanics***
- **Unusual/novel *modus operandi*** for offensive operations

<https://www.fireeye.com/blog/threat-research/2018/10/triton-attribution-russian-government-owned-lab-most-likely-built-tools.html>

Федерации Федеральное государственное унитарное предприятие  
«Центральный научно-исследовательский институт химии и механики»  
8(499)611-51-29 8(499)782-23-21ф ОБРАТНАЯ СВЯЗЬ

О предприятии ГНЦ РФ Новости Издания Аспирантура Вакансии Контакты

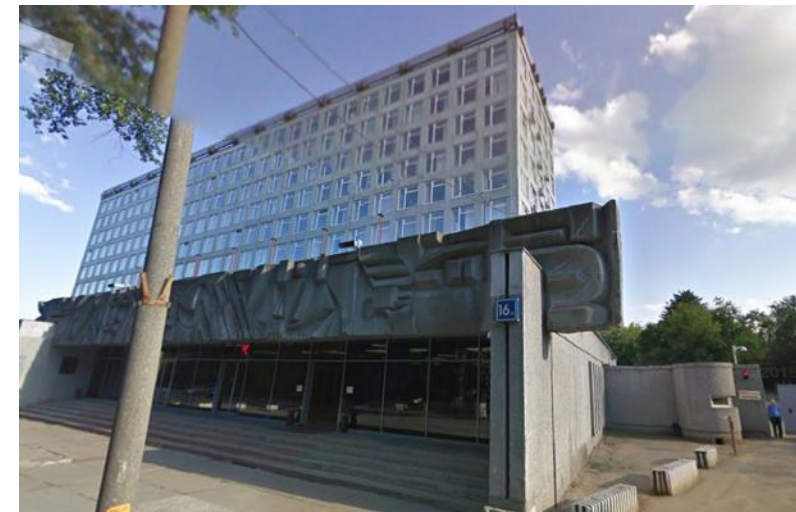
ГНЦ РФ ФГУП "ЦНИИХМ" От познания к передовым технологиям

**Служение науке, защита Отечества**

Государственный научный центр Российской Федерации федеральное государственное унитарное предприятие "Центральный научно-исследовательский институт химии и механики" находится в ведомственном подчинении Федеральной службы по техническому и экспортному контролю (ФСТЭК России).

Институт ведет свою историю с 1894 года. Его рождение напрямую связано с развитием пороховой промышленности России и именем великого русского химика Д.И. Менделеева, внесшего выдающийся вклад в становление этой отрасли...

ФСТЭК России Подробнее



# Current cyber operations in ICS domain

## Alert (TA18-074A)

Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors

Original release date: March 15, 2018 | Last revised: March 16, 2018

<https://www.us-cert.gov/ncas/alerts/TA18-074A>



National Cyber  
Security Centre  
a part of GCHQ

The NCSC is aware of an ongoing attack campaign against multiple companies involved in the CNI supply chain. These attacks have been ongoing since at least March 2017. The targeting is focused on

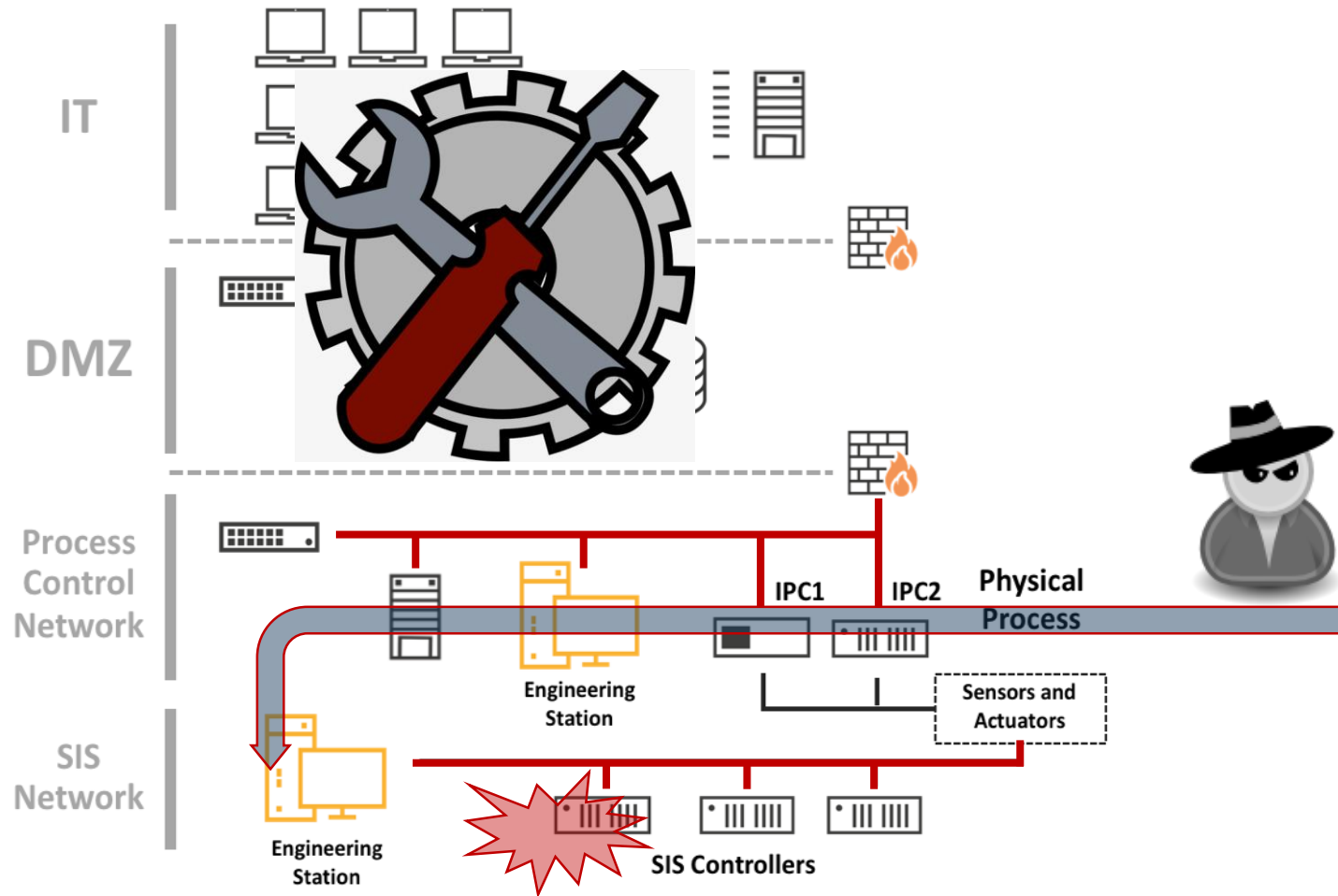
Advisory: Hostile state actors compromising UK organisations with focus on engineering and industrial control companies

**Espionage, PERSISTENCE,  
Reconnaissance**

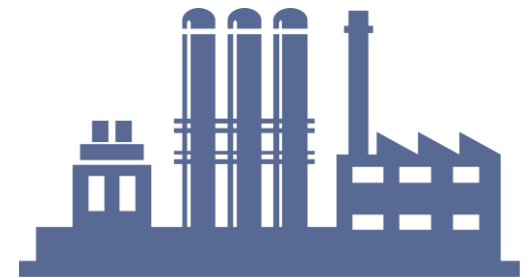
<https://www.ncsc.gov.uk/news/hostile-state-actors-compromising-uk-organisations-focus-engineering-and-industrial-control>



# Intrusion via trusted third-parties



Trusted third-parties:  
subcontractors,  
service providers, etc.



A photograph of an industrial facility, likely a refinery or chemical plant, at night. The scene is illuminated by numerous lights, creating a complex pattern of bright spots and shadows against the dark sky. The facility features various structures, including tall towers and large storage tanks.

# Supply chain compromise (big problem!)

## **EVERYBODY DOES IT: THE MESSY TRUTH ABOUT INFILTRATING COMPUTER SUPPLY CHAINS**

January 24 2019

<https://theintercept.com/2019/01/24/computer-supply-chain-attacks/>

## **There's No Good Fix If the Supply Chain Gets Hacked**

<https://www.wired.com/story/supply-chain-hacks-cybersecurity-worst-case-scenario/>

China's penetration of U.S. supply chain runs deep, says report

<https://fcw.com/articles/2018/04/23/china-supply-chain-cyber.aspx>

# Compromised security controls

- Stolen certificates to sign malware and compromised software
- Compromised malware protection companies
  - Whitelisting service providers
  - Antivirus companies
- Compromised software and firmware updates

**Hackers breached 3 US antivirus companies, researchers reveal**

Source code, network access being sold online by "Fxmisp" collective.

# Contractor threat

производство. В середине октября 2018 года персонал компании SAMSE в полном объеме покинул строительную площадку. ОАО «Светлогорский ЦКК» было вынуждено принять меры по обеспечению безопасности и работоспособности смонтированного оборудования. При этом, компания SAMSE до отъезда с площадки предприняла меры для создания препятствий запуску оборудования без участия китайских специалистов.

*Справочно:* Были извлечены лицензионные ключи с двух серверов цехов производства волокна и производства товарной целлюлозы, была удалена программная логика управления технологическим оборудованием отдельных участков нового завода, демонтирован специальный турбиной.

17.01.2019 специалистами ОАО  
проведении работ по прокладке каб

office life

серверной в здании центрального управления производства  
сульфатной белимой целлюлозы, под фальшиполем указанного  
помещения было обнаружено незакрепленное электронное  
устройство. Проектной документацией указанное устройство не  
предусмотрено.

По предварительной оценке, проведенной специалистами  
ОАО «Светлогорский ЦКК», обнаруженное устройство  
предназначено для дистанционного повреждения оборудования  
серверной путем искусственного создания короткого замыкания с  
целью причинения урона и вреда нормальному функционированию  
нового завода.

По заявлению генерального директора ОАО «Светлогорский ЦКК» Светлогорским РОВД была проведена проверка, по результатам которой принято решение об отказе в возбуждении уголовного дела в связи с отсутствием поводов и оснований для его возбуждения (постановление от 26.03.2019).

Концерн в свою очередь письмом от 04.02.2019 обратился в МВД РБ для оказания содействия в проведении проверки всех энергетических и электронных объектов производства на предмет посторонних устройств.

14.02.2019 от МВД РБ поступил ответ о том, что МВД не имеет соответствующих полномочий, не располагает специалистами и техническими возможностями для проведения такой проверки.

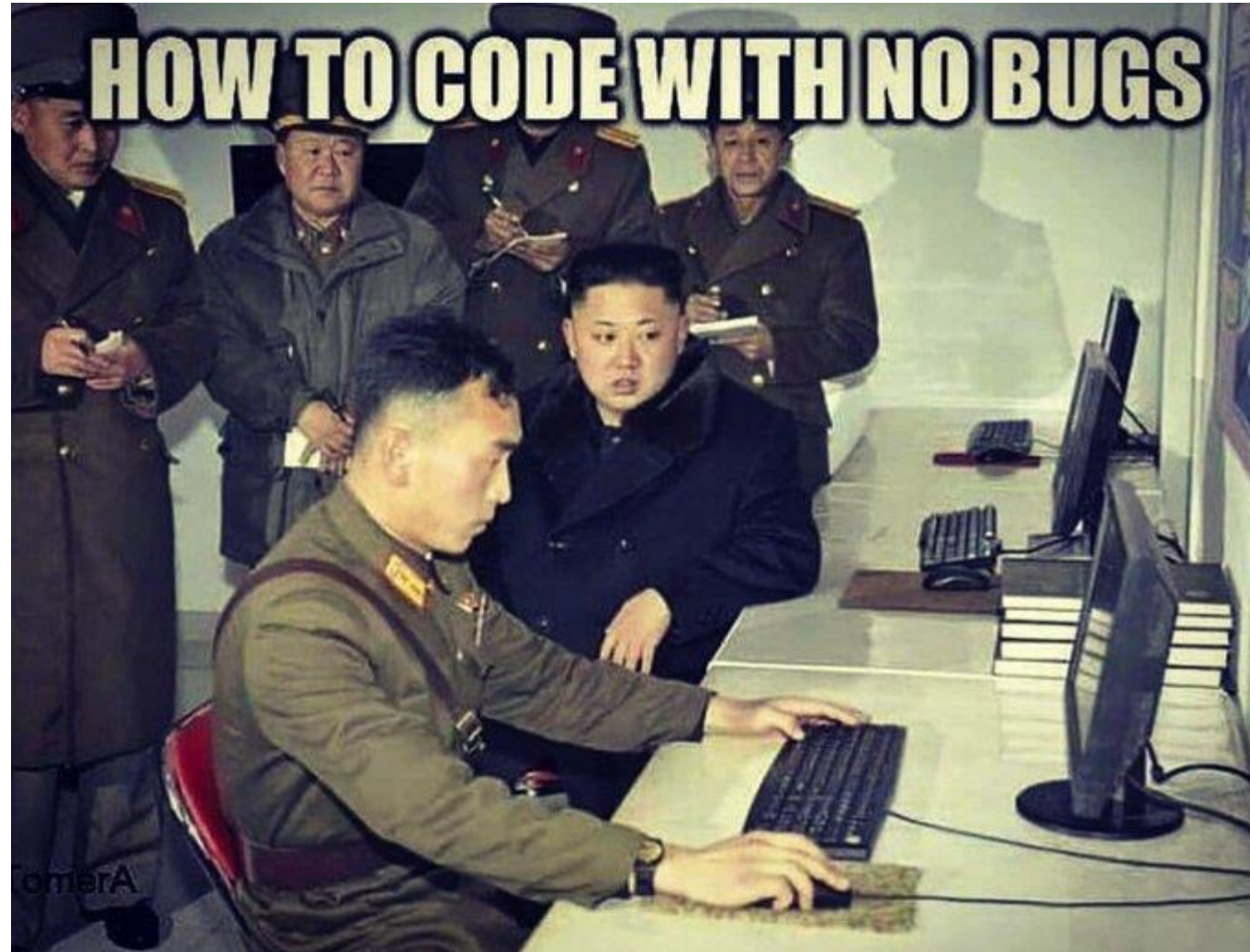
office life





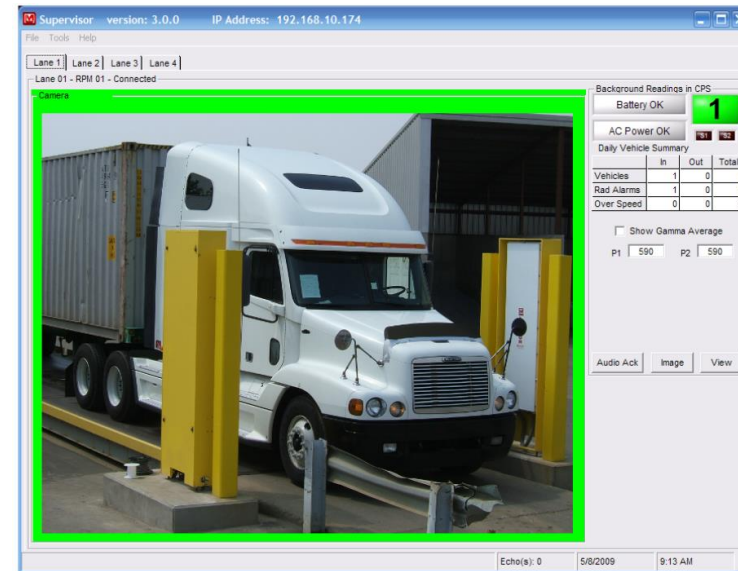
**Product security**

# Urgent need for stricter requirements



# (In)security of Radiation Monitoring Devices

## Go Nuclear: Breaking Radiation Monitoring Devices



```
// Lmi.Sam.Supervisor.Host  
private const string BackDoor = "5147";
```

<https://www.blackhat.com/docs/us-17/wednesday/us-17-Santamarta-Go-Nuclear-Breaking%20Radition-Monitoring-Devices-wp.pdf>

<https://www.wired.com/story/radioactivity-sensor-hacks/>

<https://www.bleepingcomputer.com/news/security/three-vendors-decline-to-patch-vulnerabilities-in-nuclear-radiation-monitors/>

# Insecure medical equipment

## Serious Vulnerabilities Found in Fujifilm X-Ray Devices

April 24, 2019

## Machines In Healthcare Espionage

Apr 23, 2018,



<https://www.forbes.com/sites/thomasbrewster/2018/04/23/x-ray-machines-taken-over-by-healthcare-hackers>

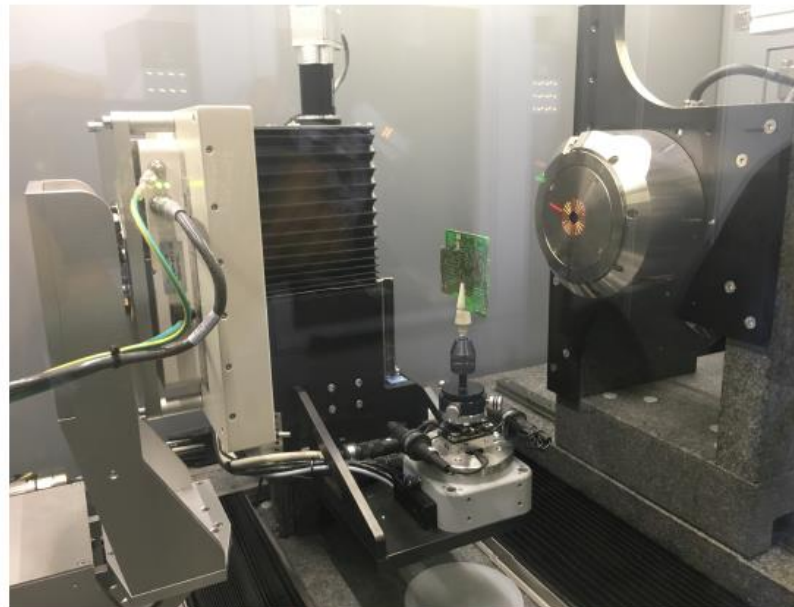
<https://www.securityweek.com/serious-vulnerabilities-found-fujifilm-x-ray-devices>



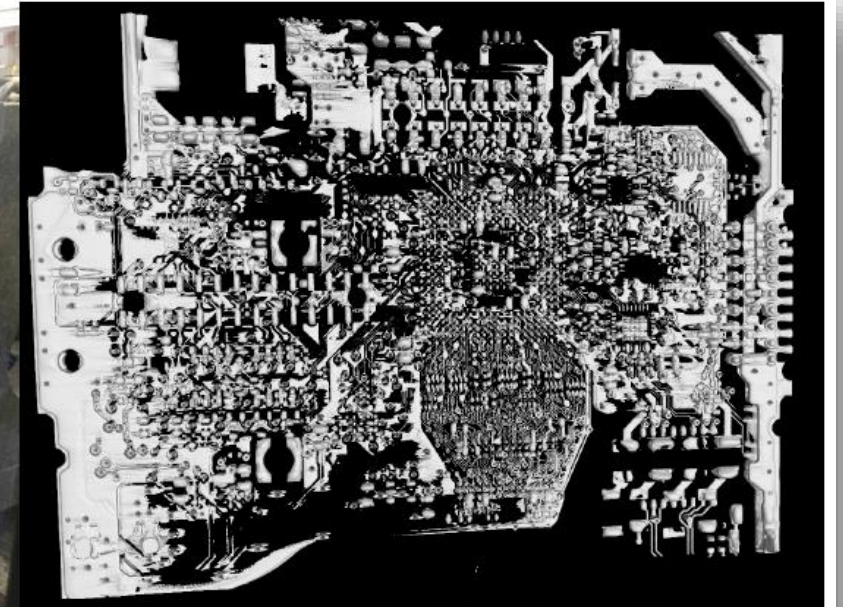
# Hardware backdoors in equipment

## Hardware-based Special Access Implant on Siemens S7-1200 PLCs

March 18, 2019



(a) 3D X-Ray Tomography of the PLC PCB.



(b) Result of 3D X-Ray Tomography of the PLC PCB and mapping entire

# No place to hide



**NSA intercepting Cisco router shipments and installing implants**

<https://arstechnica.com/tech-policy/2014/05/photos-of-an-nsa-upgrade-factory-show-cisco-router-getting-implant/>

# Embedded systems security is very poor

## Siemens S7 PLCs Share Same Crypto Key Pair, Researchers Find

Researchers at Black Hat USA reveal how security authentication weaknesses in popular Siemens ICS family let them control a PLC.



Mitigation	Support Since	Enabled by Default?
Data Execution Prevention (DEP)	6.3.2	X
Address Space Layout Randomization (ASLR)	6.5	X
Stack Canaries	6.5	X
Relocation Read-Only (RELRO)	6.5	X

*No support for:*

- Vtable Protection (eg. VTGuard, VTV)
- CPI / CFI (eg. CFG)
- Kernel Data / Code Isolation (eg. SMAP/PAN, SMEP/PXN)
- Etc.

<https://www.darkreading.com/vulnerabilities---threats/siemens-s7-plcs-share-same-crypto-key-pair-researchers-find-/d/d-id/1335452>

<https://recon.cx/2018/brussels/resources/slides/RECON-BRX-2018-Dissecting-QNX.pdf>

# Product compromise via supply chain

- Supply-chain attacks
  - Allows to bypass multiple levels of security
  - Better scaling of attack efforts

**Industrial transmitter**



**Layers of standardized electronics (for a individual vendors)**



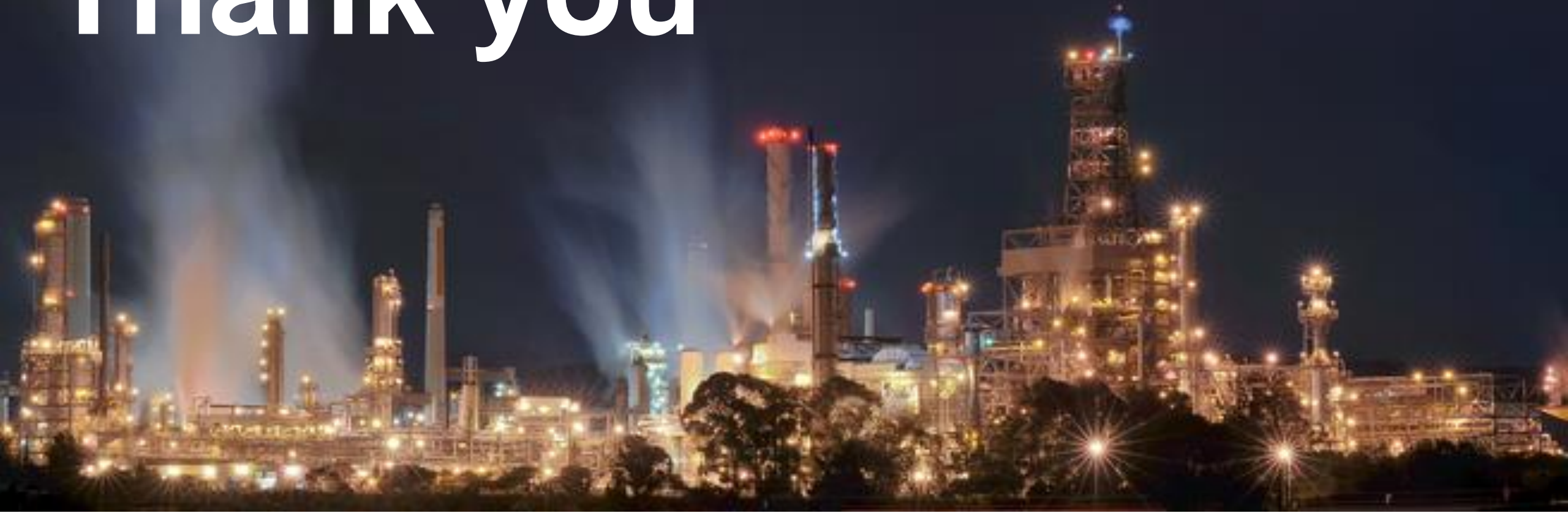
**Concluding remarks**

# Some takeaways



- Accelerated build-up of advanced cyber/cyber-physical capabilities
- Race-to-the-Bottom and supply chain security
- Compromise of security controls/mechanisms

# Thank you



**Marina Krotofil**  
**@marmusha**  
**marmusha@gmail.com**