Check Point
SOFTWARE TECHNOLOGIES LTD

5TH GENERATION CYBER SECURITY

GEN V

IOT/SCADA
S.O.S EMERGENCY CALL

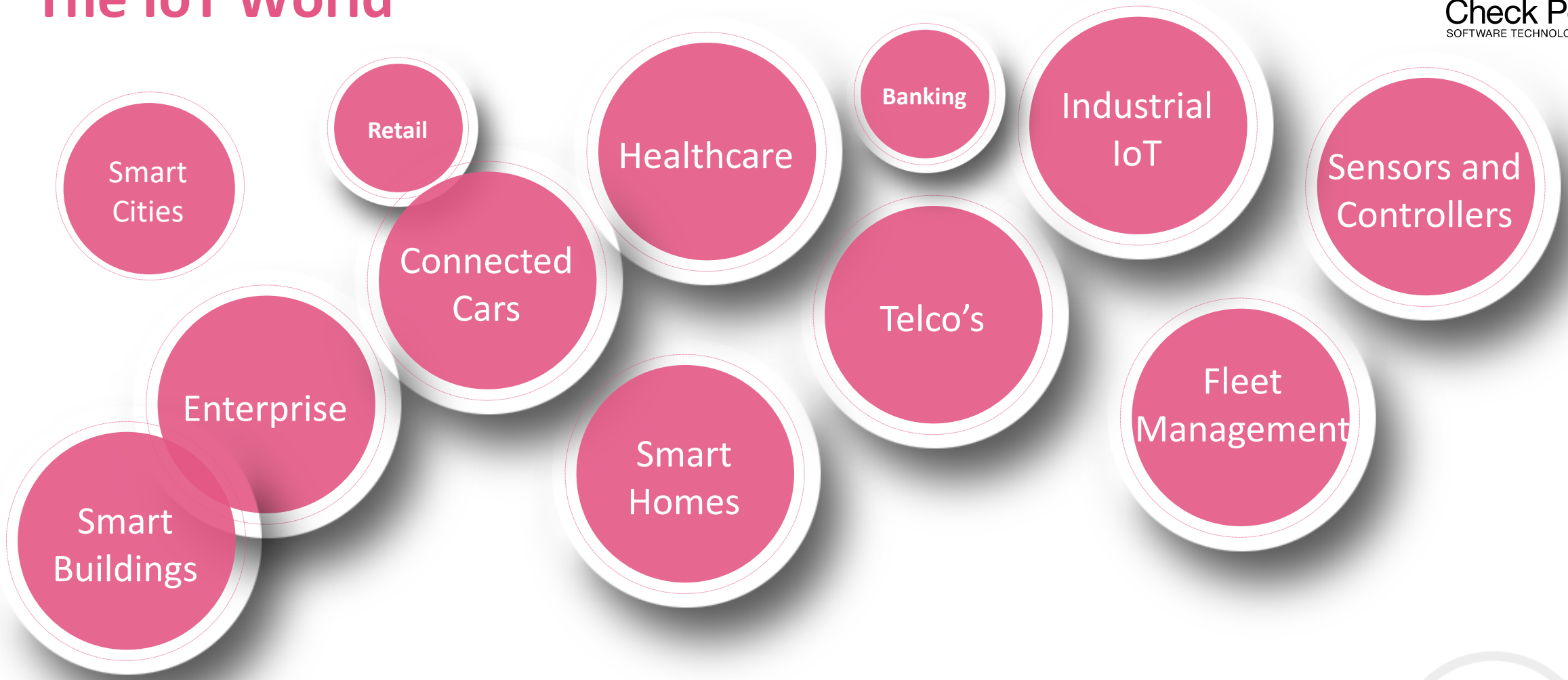
.. --- - -·····- ... . -·-· ..- .-. .. - -·--

... ·-·-·- --- ·-·-·- ... -·-· .- .-.. .-..

Tomas Vobruba | Check Point SE

CPX
CHECK POINT
EXPERIENCE

The IoT World

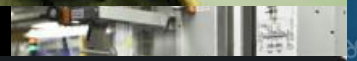
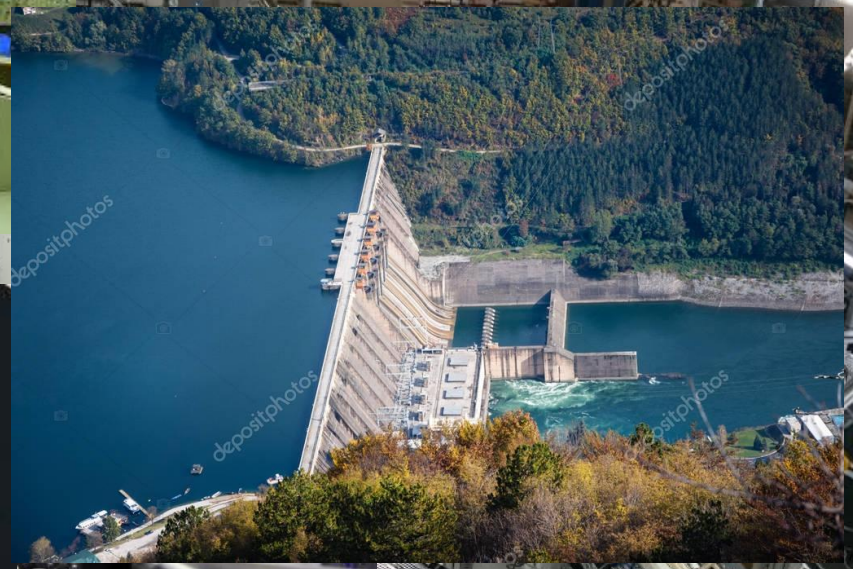



0 / 10

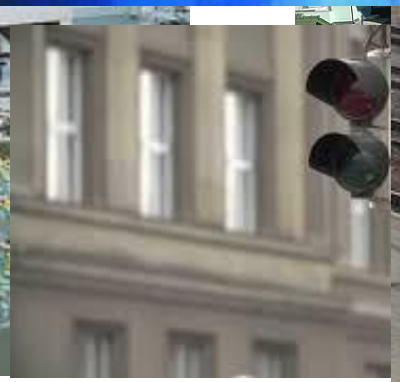



VPKNX
340 - 34
OAL759
400 - 42
400
LBE
AZA473
380 D 37
380
BASUM
AOM818
360 D 35
360
FUA224
380 - 40
380
HLZ
OSN
ROBES
DLE
CFG161
320 - 36
320
GHN231
240 C 37
240
WRB
EDDL
CTH932
122 T 23
GMH
EEDER
NOR
EGGD
NOR
DOM
OSN
BASUM
LBE

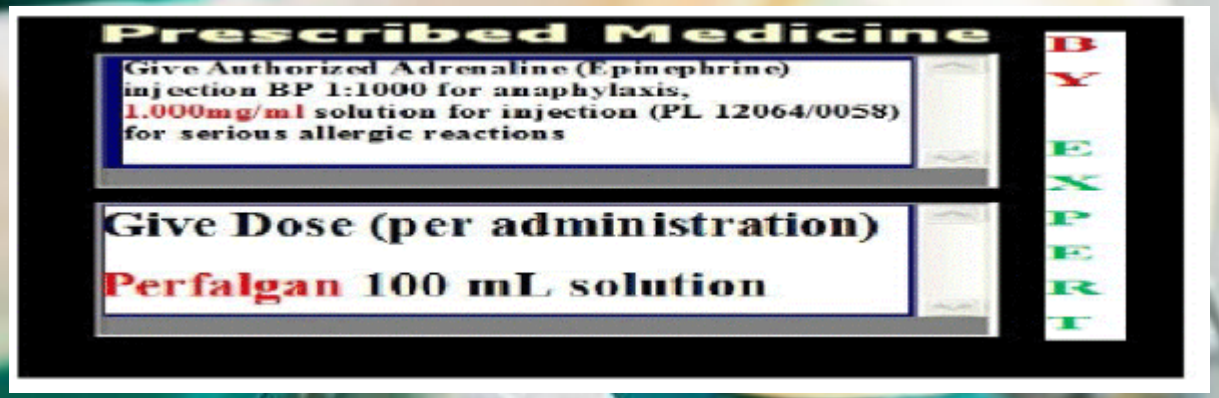




Bohumín



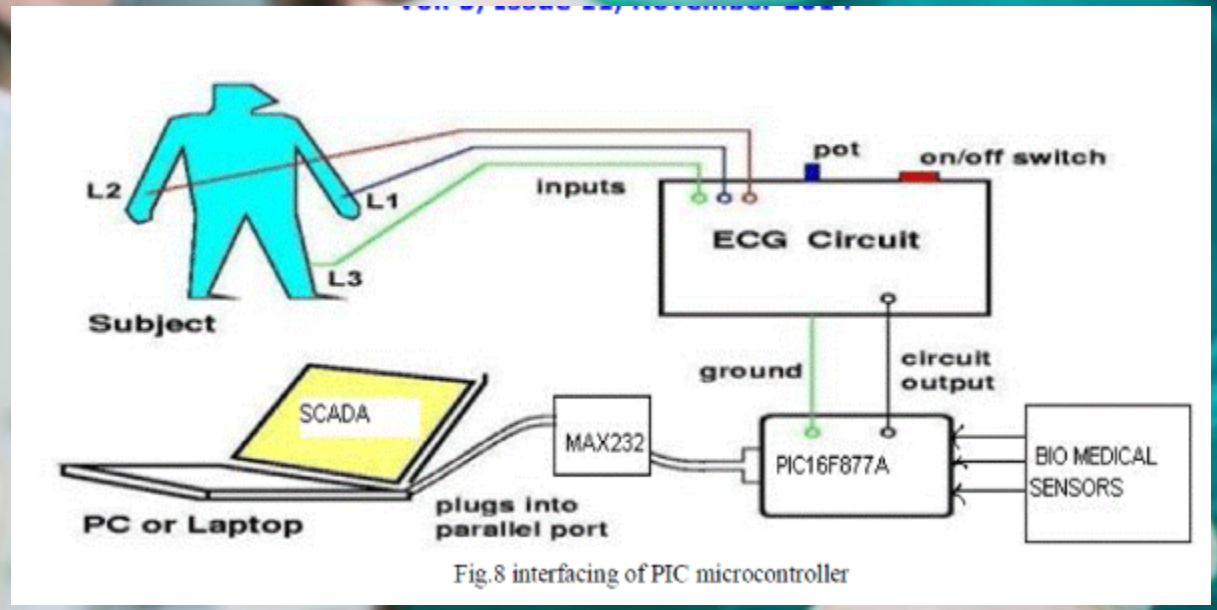


Fig.8 interfacing of PIC microcontroller

Check Point
SOFTWARE TECHNOLOGIES LTD.

- Energy Management
- HVAC
- Lighting
- Elevators
- Access & Security
- Water
- And more…

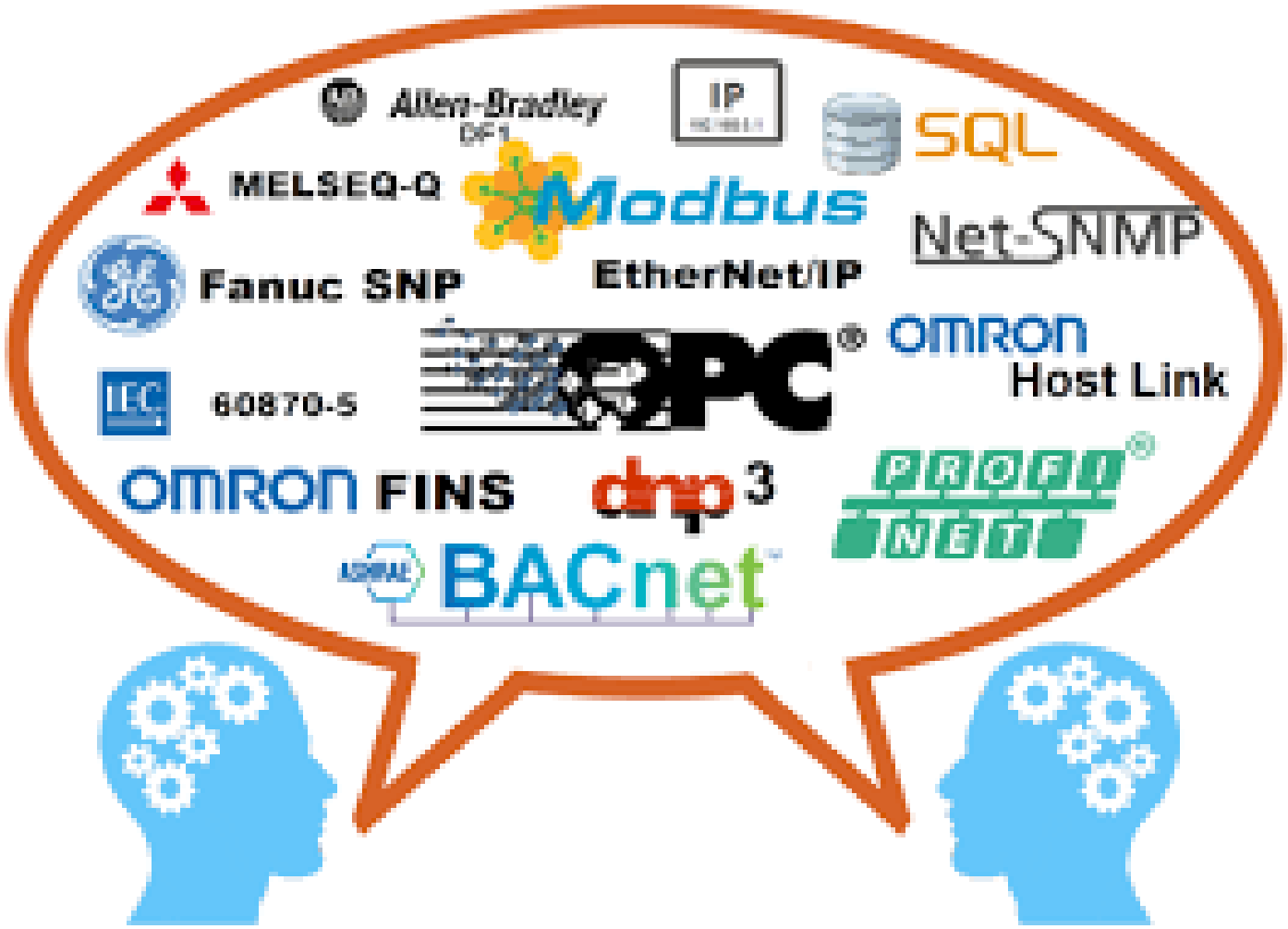
What goes into a Modern Building ??

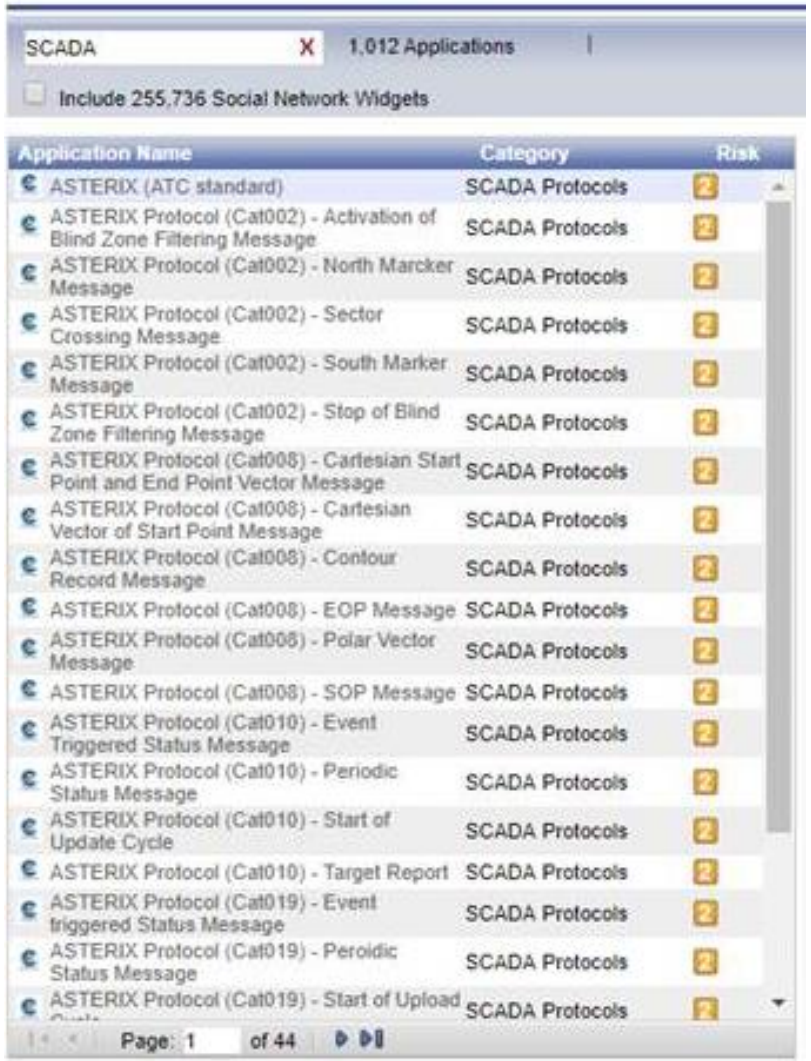
LonMark | BACnet | OPC | Modbus

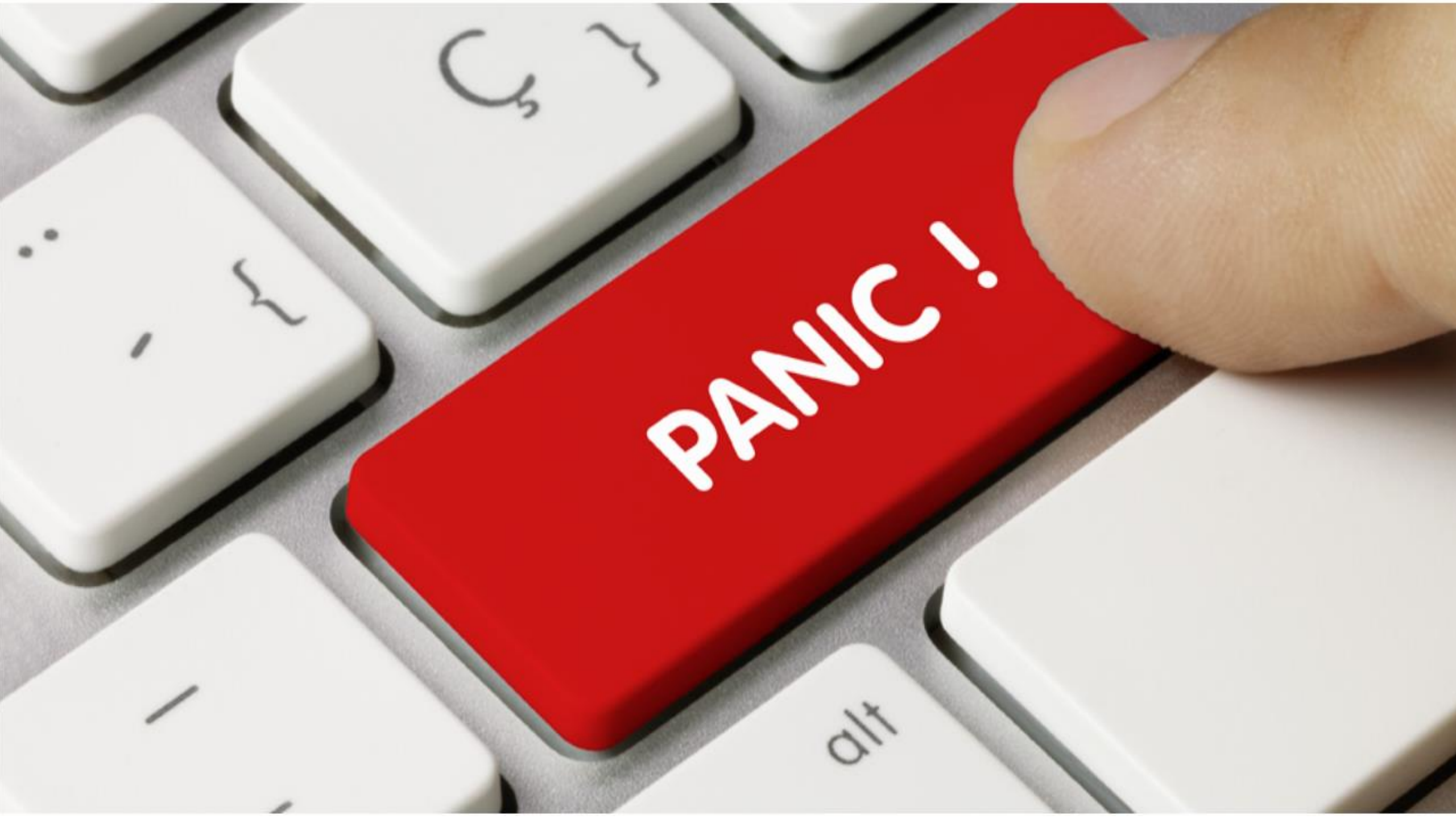
Life Safety Systems	Security Systems	BMS Systems	Utility Services
Fire Detection	Access Control	Chiller Management	DG Set Monitoring
Fire Supp (Wet)	CCTV Systems	HVAC Systems	Elevator Control
Fire Supp (Dry)	Intrusion Systems	Ventilation System	Water Leak Systems
VESDA Systems	Perimeter Protection	Energy Metering	Waste Water Management
Paging System	Gate Automation	Lighting Control	Third Party

Schneider

+1000

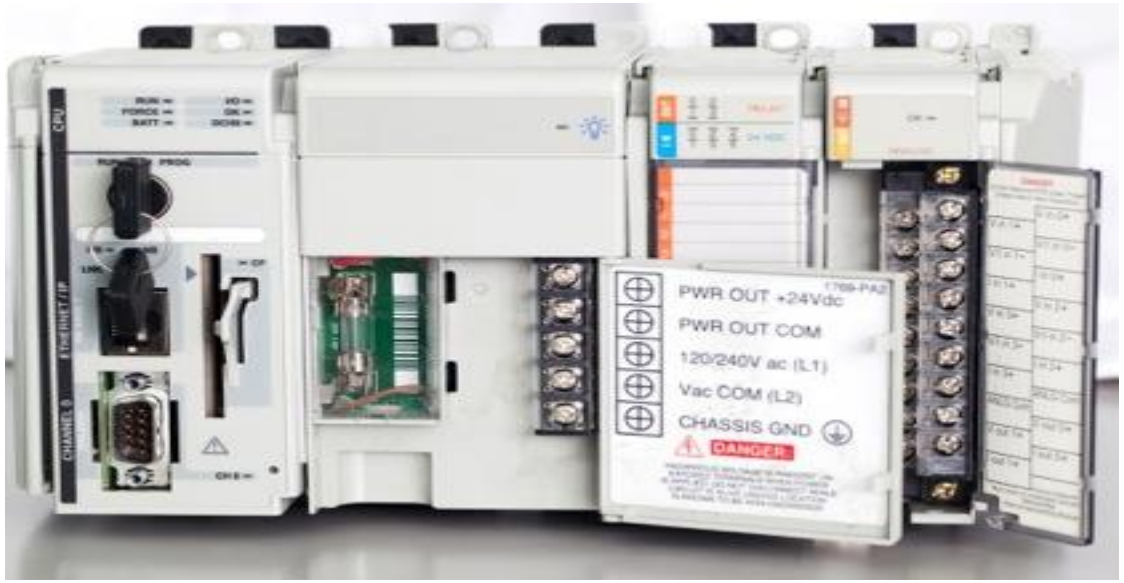





PANIC !
alt

Proč jsou útoky tohoto typu úspěšné?

- SCADA zařízení nejsou designovaná na to aby byla bezpečná a proto jsou zranitelná



Programmable Logic Controller

Příklady PLC zranitelností

	A-B	Schneider Electric	GE	SEL	Koyo
Firmware	!	x	!	!	!
Ladder Logic	!	!	x	!	x
Backdoors	!	x	x	✓	✓
Fuzzing	x	x	x	!	!
Web	!	x	N/A	N/A	x
Best Config	!	!	x	!	!
Exhaustion	✓	✓	x	✓	✓
Undoc Features	!	x	x	!	!

"x" zranitelnost existuje a jednoduše exploitovatelná

“!” zranitelnost existuje, ale neexistuje exploit

“v” systém není zranitelný.

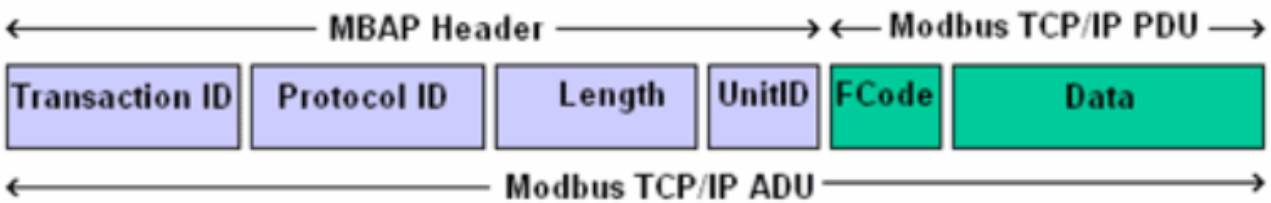
Protokoly a bezpečnost?

- No security
  - No authentication
  - No authorization
  - No encryption
  - No validation
  - **Accessible**
  - **All open**

SCADA Hacking: Modbus

Check Point
SOFTWARE TECHNOLOGIES LTD

SCADA/ICS systems use many different protocols to communicate than your standard IT systems. The most widely used and the de facto standard is the **modbus** protocol. First developed by Modicon (now Schneider Electric) in 1979 as a serial protocol, it has been modified and updated to run over TCP and is often referred to as **Modbus TCP**. You can see a diagram of the two packet structures below.



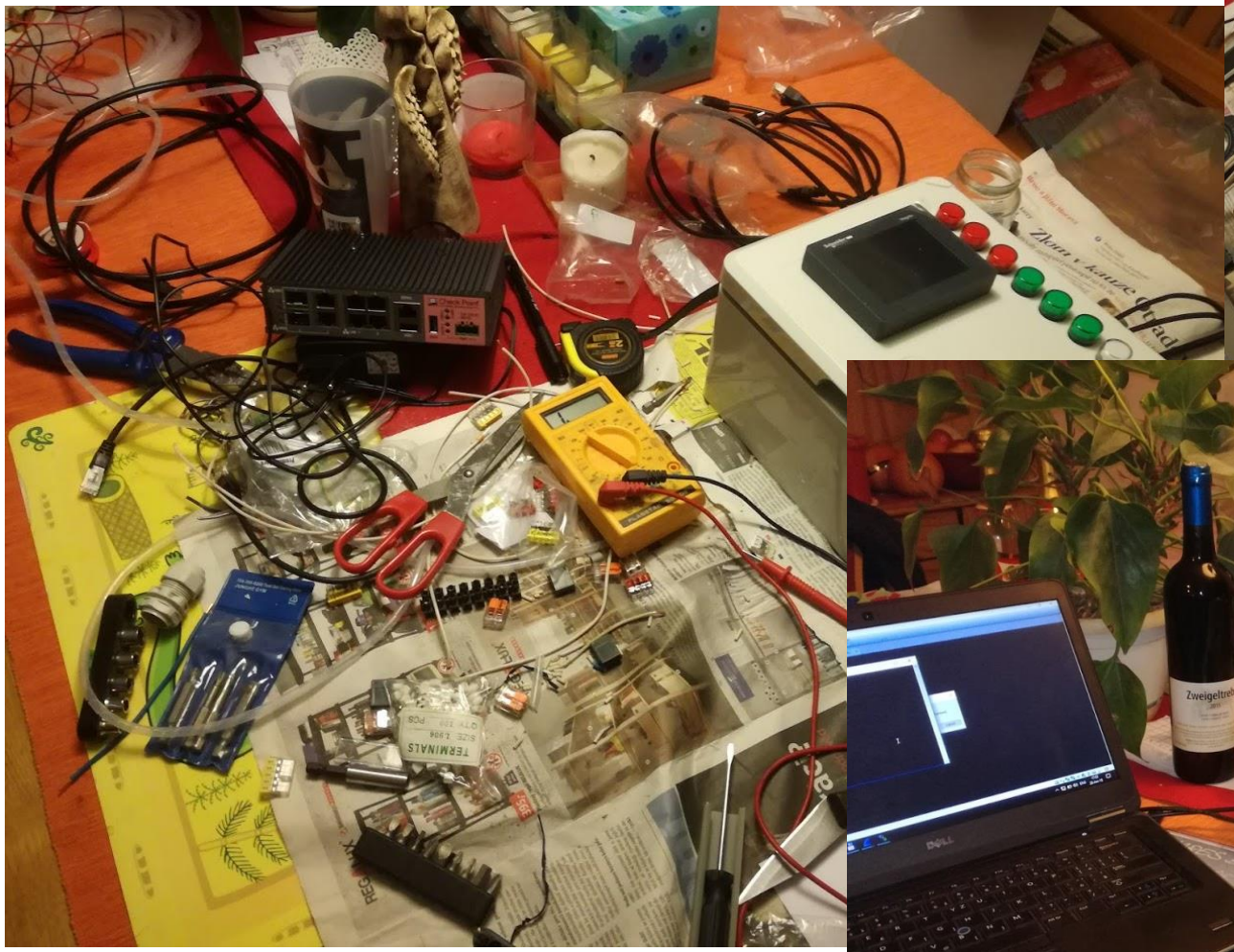
67 1.096342	10.10.10.3	10.10.20.2	Modbus/	67	Response: Trans: 0; Unit: 1, Func: 3: Read Holding Registers
60 1.200043	10.10.20.2	10.10.10.3	TCP	60	13967 → 502 [ACK] Seq=61 Ack=66 Win=8192 Len=0
66 1.345321	10.10.20.2	10.10.10.3	Modbus/	66	Query: Trans: 0; Unit: 1, Func: 3: Read Holding Registers
67 1.346382	10.10.10.3	10.10.20.2	Modbus/	67	Response: Trans: 0; Unit: 1, Func: 3: Read Holding Registers
60 1.400041	10.10.20.2	10.10.10.3	TCP	60	13967 → 502 [ACK] Seq=73 Ack=79 Win=8192 Len=0
66 1.603338	10.10.20.2	10.10.10.3	Modbus/	66	Query: Trans: 0; Unit: 1, Func: 3: Read Holding Registers
67 1.604427	10.10.10.3	10.10.20.2	Modbus/	67	Response: Trans: 0; Unit: 1, Func: 3: Read Holding Registers
60 1.800068	10.10.20.2	10.10.10.3	TCP	60	13967 → 502 [ACK] Seq=85 Ack=92 Win=8192 Len=0
66 1.853311	10.10.20.2	10.10.10.3	Modbus/	66	Query: Trans: 0; Unit: 1, Func: 3: Read Holding Registers
67 1.854468	10.10.10.3	10.10.20.2	Modbus/	67	Response: Trans: 0; Unit: 1, Func: 3: Read Holding Registers

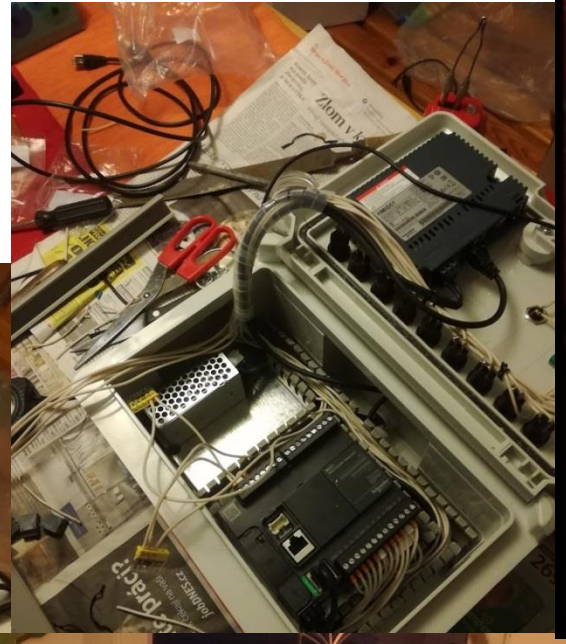
```
⊞ Frame 18: 67 bytes on wire (536 bits), 67 bytes captured (536 bits)
⊞ Ethernet II, Src: CheckPoi_72:b8:75 (00:1c:7f:72:b8:75), Dst: Schneide_2e:7a:5e (00:01:23:2e:7a:5e)
⊞ Internet Protocol Version 4, Src: 10.10.10.3, Dst: 10.10.20.2
⊞ Transmission Control Protocol, Src Port: 502, Dst Port: 13967, Seq: 66, Ack: 73, Len: 13
⊟ Modbus/TCP
    Transaction Identifier: 0
    Protocol Identifier: 0
    Length: 7
    Unit Identifier: 1
⊟ Modbus
    .000 0011 = Function Code: Read Holding Registers (3)
    [Request Frame: 17]
    Byte Count: 4
  ⊟ Register 0 (UINT16): 600
      Register Number: 0
      Register Value (UINT16): 600
  ⊟ Register 1 (UINT16): 63
      Register Number: 1
      Register Value (UINT16): 63
```

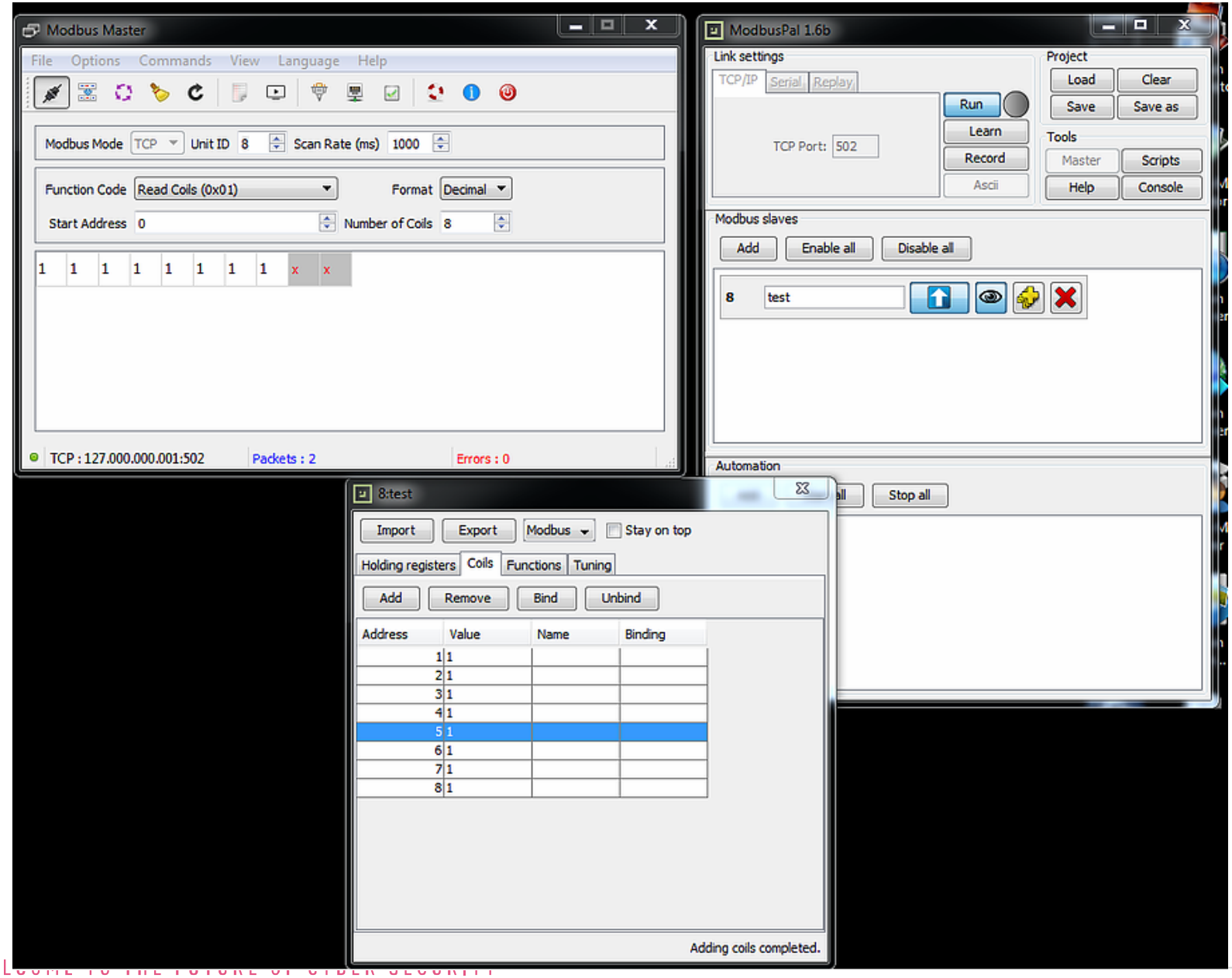
67	4.896985	10.10.10.3	10.10.20.2	Modbus/	67	Response: Trans: 0; Unit: 1, Func: 3: Read Holding Registers
60	5.000221	10.10.20.2	10.10.10.3	TCP	60	13967 → 502 [ACK] Seq=241 Ack=261 Win=8192 Len=0
66	5.150337	10.10.20.2	10.10.10.3	Modbus/	66	Query: Trans: 0; Unit: 1, Func: 3: Read Holding Registers
67	5.151027	10.10.10.3	10.10.20.2	Modbus/	67	Response: Trans: 0; Unit: 1, Func: 3: Read Holding Registers
60	5.200204	10.10.20.2	10.10.10.3	TCP	60	13967 → 502 [ACK] Seq=253 Ack=274 Win=8192 Len=0
69	5.287459	10.10.20.2	10.10.10.3	Modbus/	69	Query: Trans: 0; Unit: 1, Func: 16: Write Multiple Registers
66	5.289058	10.10.10.3	10.10.20.2	Modbus/	66	Response: Trans: 0; Unit: 1, Func: 16: Write Multiple Registers
60	5.400209	10.10.20.2	10.10.10.3	TCP	60	13967 → 502 [ACK] Seq=268 Ack=286 Win=8192 Len=0
66	5.400557	10.10.20.2	10.10.10.3	Modbus/	66	Query: Trans: 0; Unit: 1, Func: 3: Read Holding Registers
67	5.402343	10.10.10.3	10.10.20.2	Modbus/	67	Response: Trans: 0; Unit: 1, Func: 3: Read Holding Registers

```
⊞ Frame 65: 69 bytes on wire (552 bits), 69 bytes captured (552 bits)
⊞ Ethernet II, Src: Schneide_2e:7a:5e (00:01:23:2e:7a:5e), Dst: CheckPoi_72:b8:75 (00:1c:7f:72:b8:75)
⊞ Internet Protocol Version 4, Src: 10.10.20.2, Dst: 10.10.10.3
⊞ Transmission Control Protocol, Src Port: 13967, Dst Port: 502, Seq: 253, Ack: 274, Len: 15
⊟ Modbus/TCP
    Transaction Identifier: 0
    Protocol Identifier: 0
    Length: 9
    Unit Identifier: 1
⊟ Modbus
    .001 0000 = Function Code: Write Multiple Registers (16)
    Reference Number: 0
    Word Count: 1
    Byte Count: 2
  ⊟ Register 0 (UINT16): 444
      Register Number: 0
      Register Value (UINT16): 444
```

Workshop demo





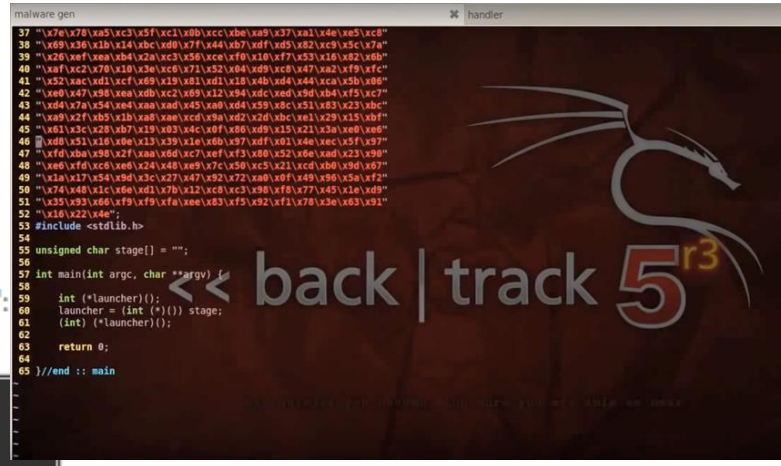


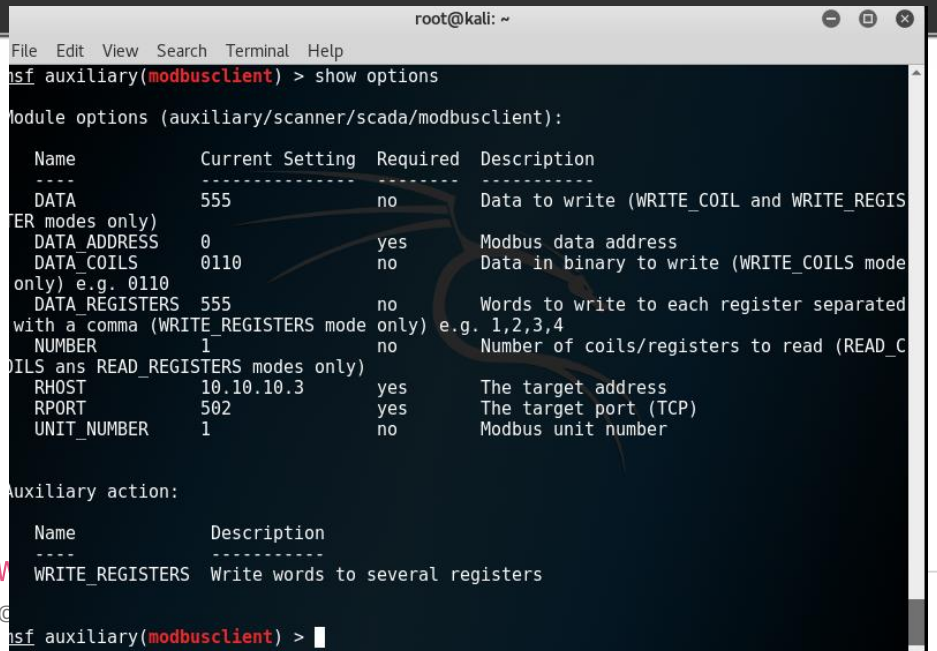
https://www.rapid7.com/db/modules/auxiliary/scanner/scada/modbusclient

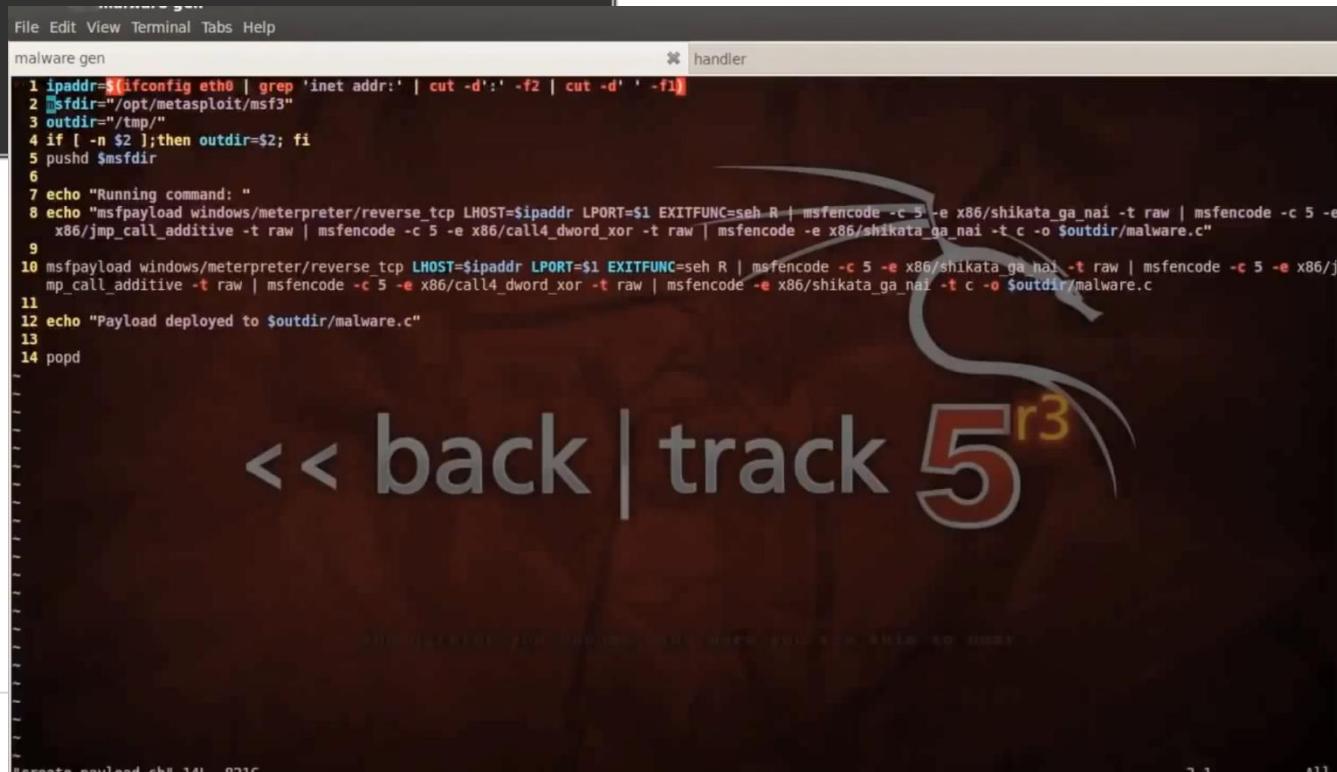
Module Options

To display the available options, load the module within the Metasploit console and run the commands 'show options' or 'show advanced':

```
msf > use auxiliary/scanner/scada/modbusclient
msf auxiliary(modbusclient) > show actions
      ...actions...
msf auxiliary(modbusclient) > set ACTION <action-name>
msf auxiliary(modbusclient) > show options
      ...show and set options...
msf auxiliary(modbusclient) > run
```

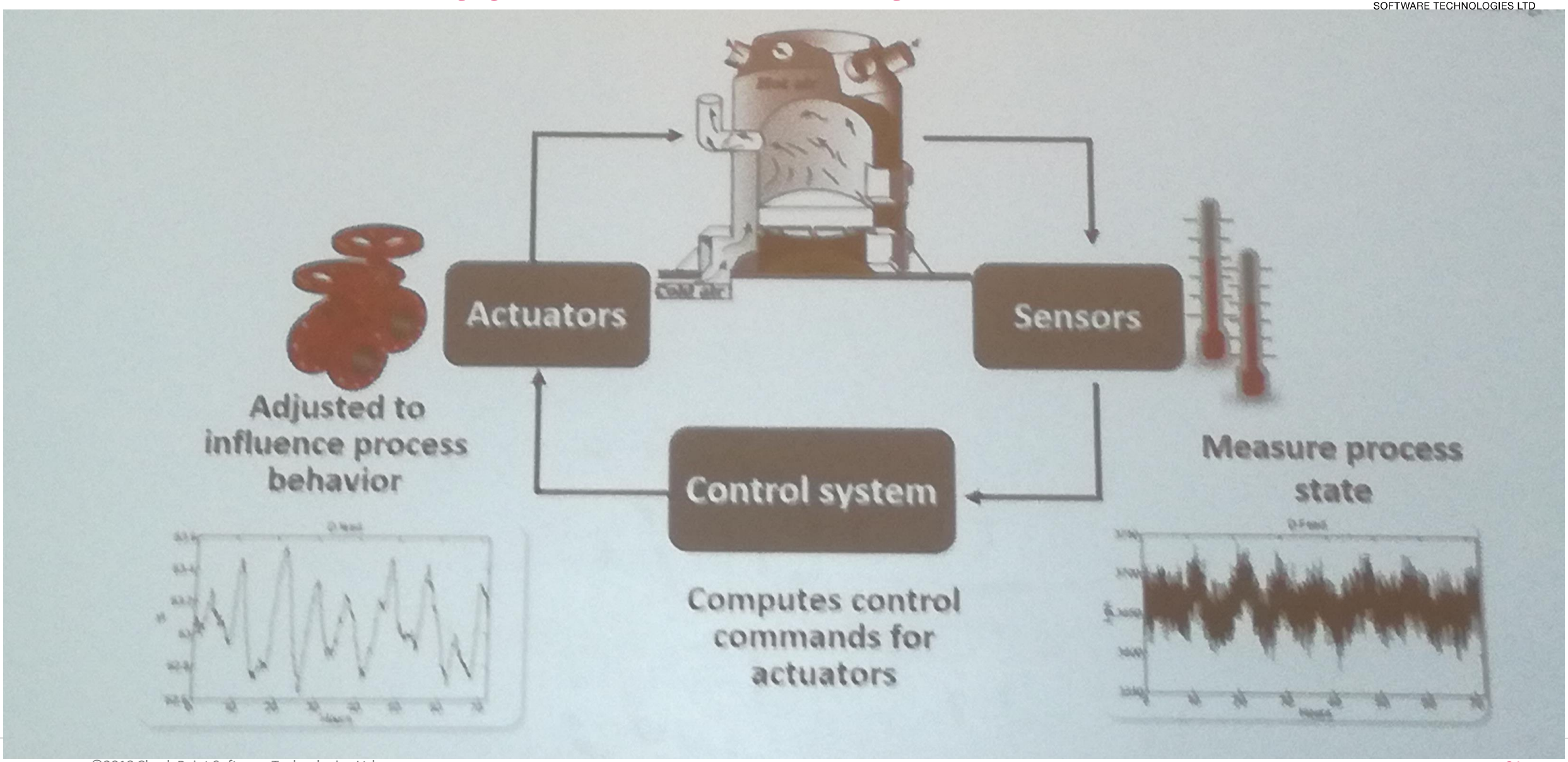


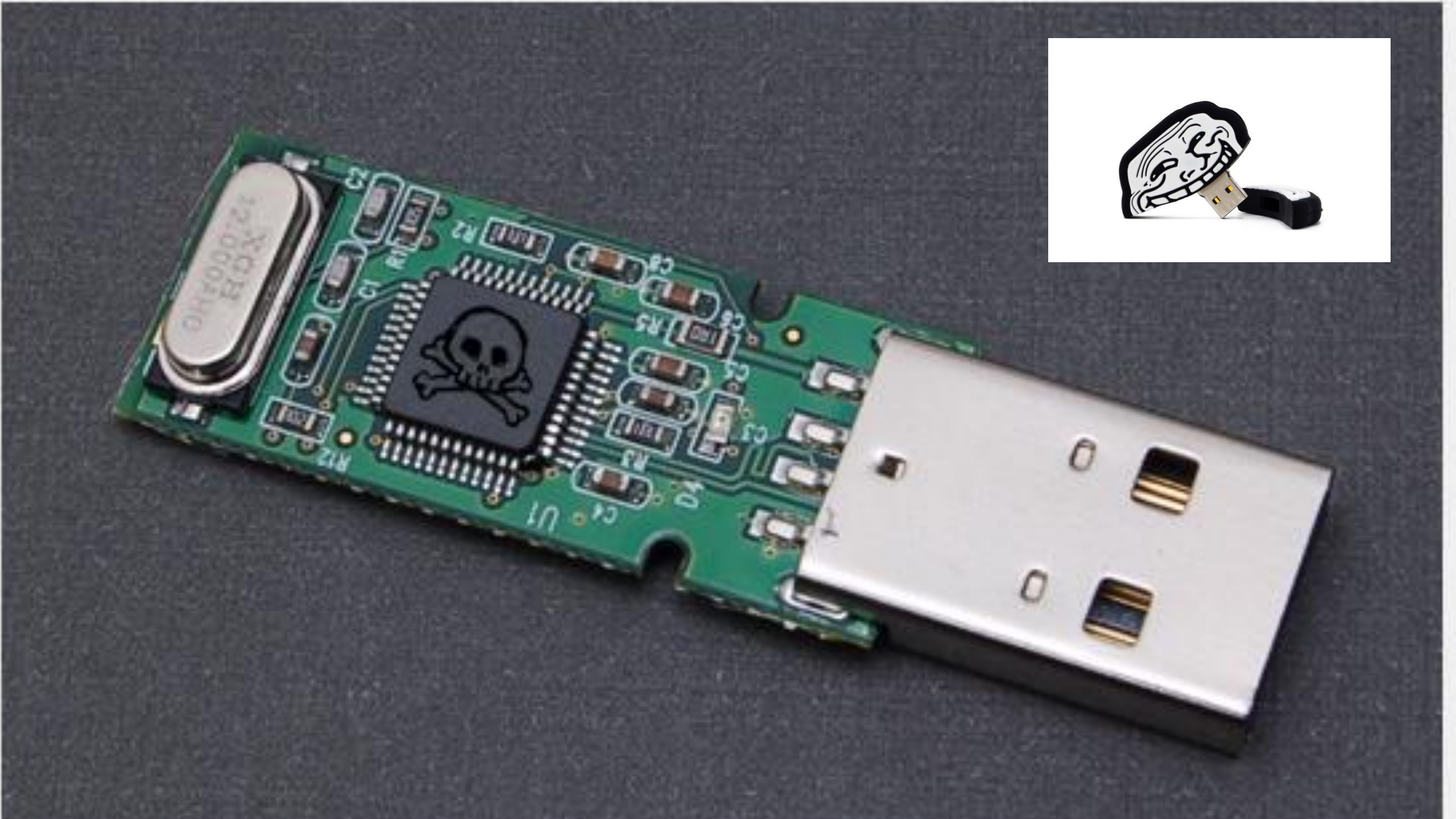




Ransomware

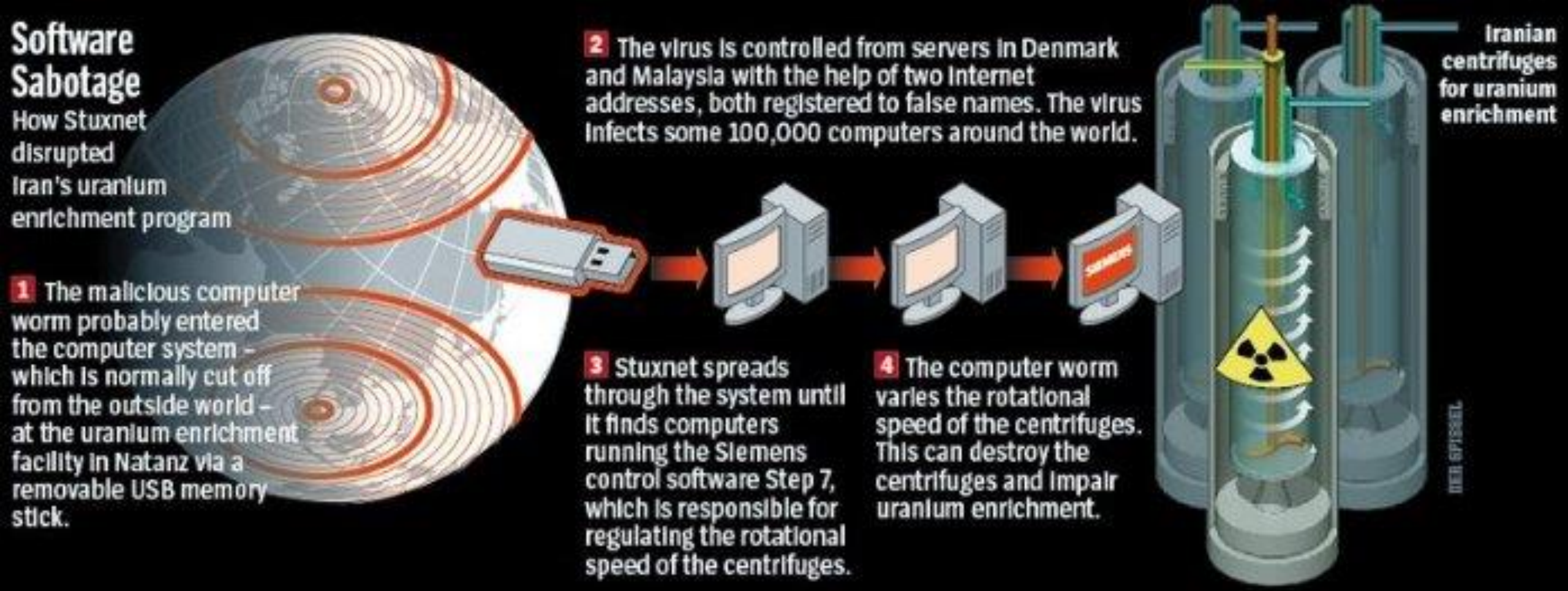
Industriální útoky jsou o kontrole cyklů




U1

Software Sabotage

How Stuxnet disrupted Iran's uranium enrichment program



1 The malicious computer worm probably entered the computer system – which is normally cut off from the outside world – at the uranium enrichment facility in Natanz via a removable USB memory stick.

2 The virus is controlled from servers in Denmark and Malaysia with the help of two Internet addresses, both registered to false names. The virus infects some 100,000 computers around the world.

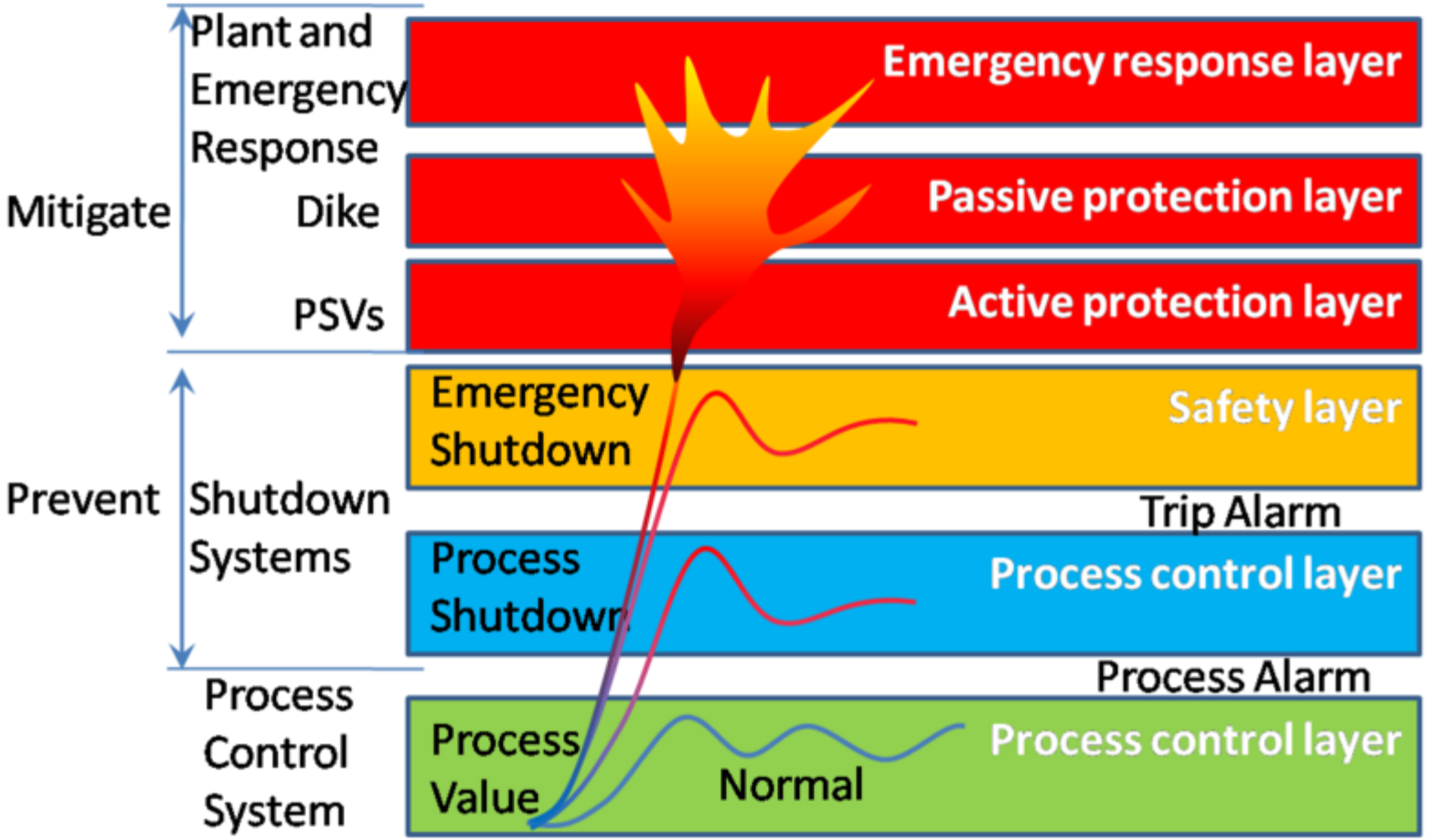
3 Stuxnet spreads through the system until it finds computers running the Siemens control software Step 7, which is responsible for regulating the rotational speed of the centrifuges.

4 The computer worm varies the rotational speed of the centrifuges. This can destroy the centrifuges and impair uranium enrichment.

Iranian centrifuges for uranium enrichment

5 The Stuxnet attacks start in June 2009. From this point on, the number of inoperative centrifuges increases sharply.

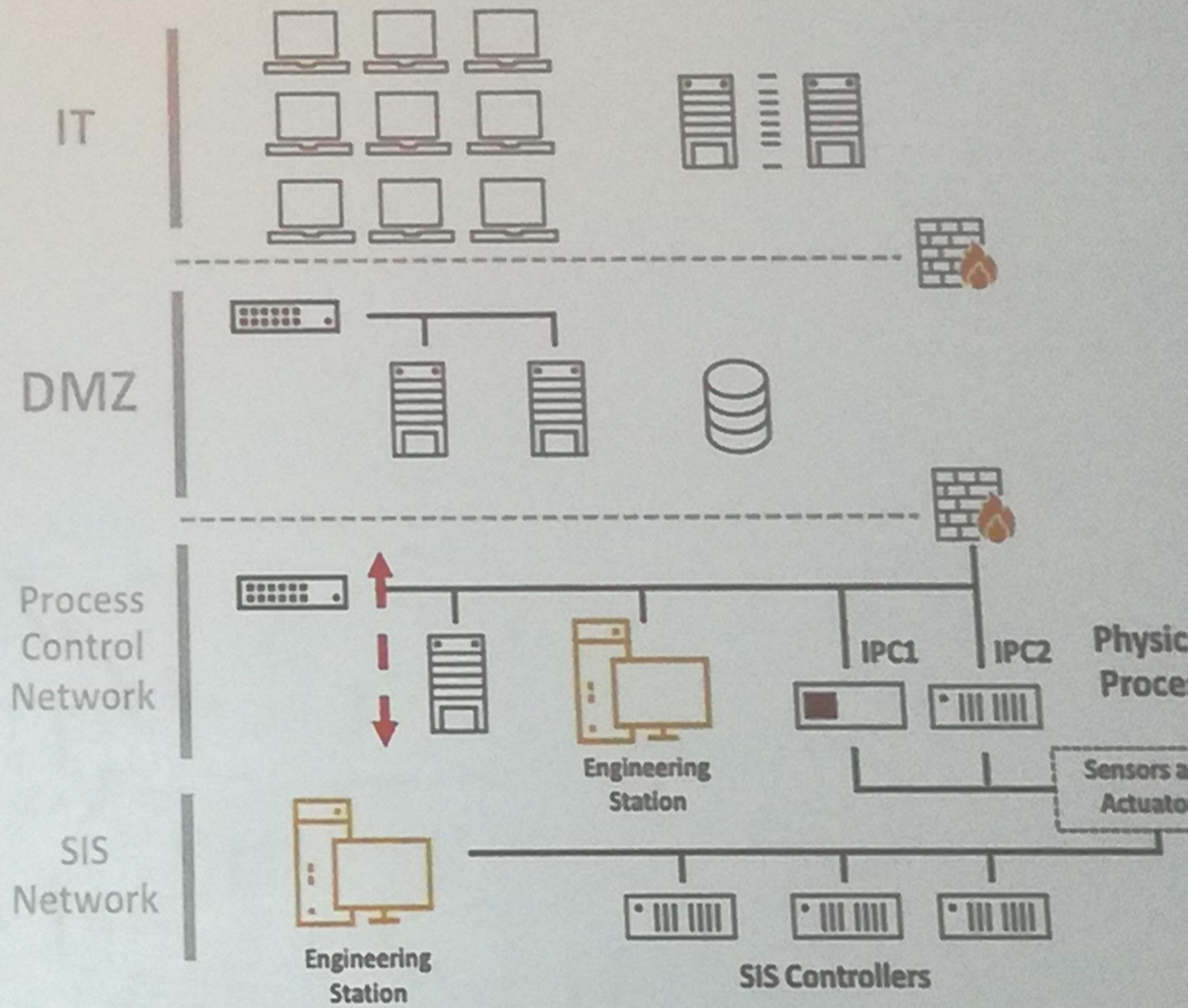
A co hacknutí záchraného tlačítka?



DCS / SIS Network

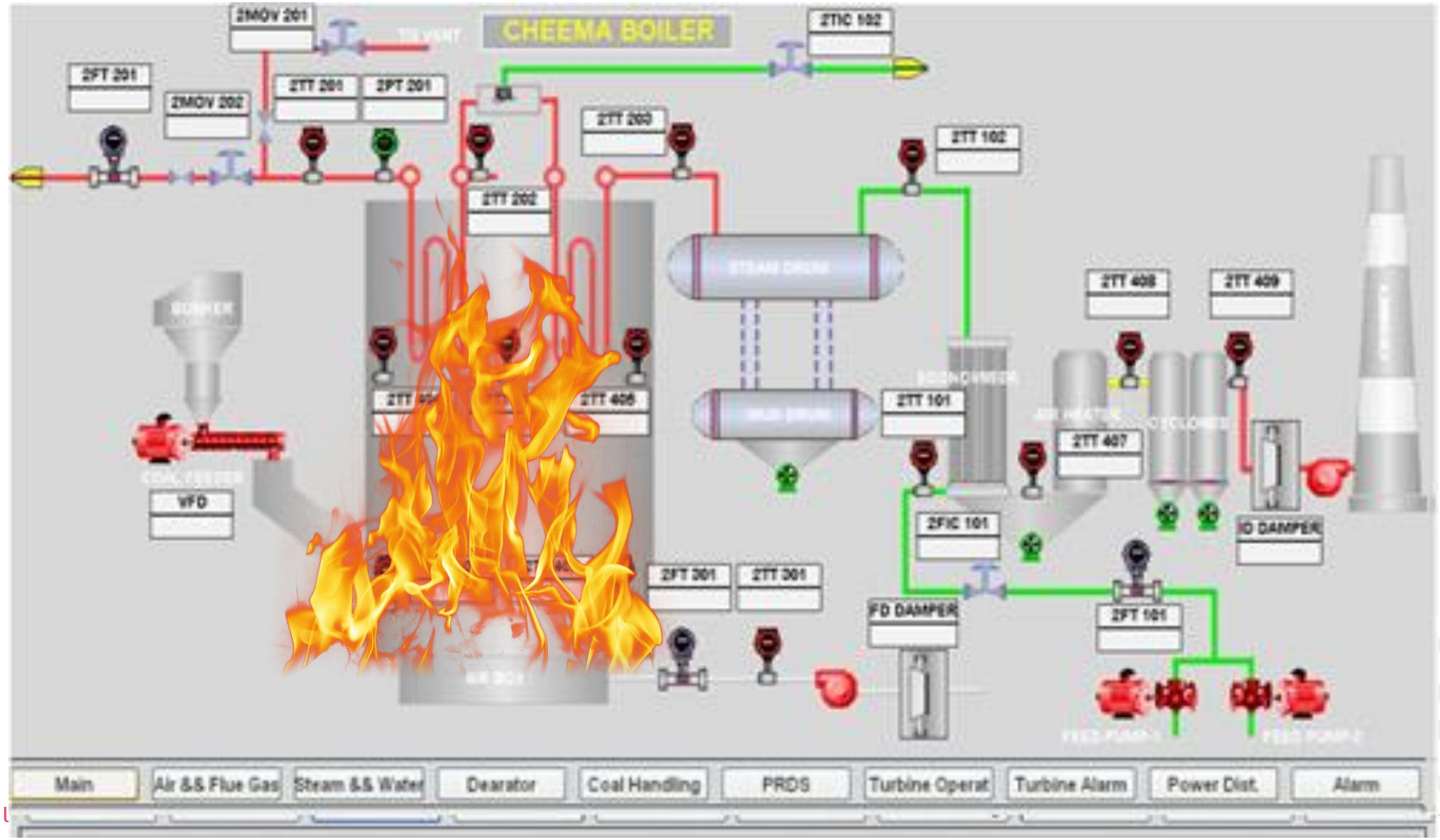
Midnight Blu

An attack on a safety system can cause the MOST DAMAGING outcome of a cyber-physical attack

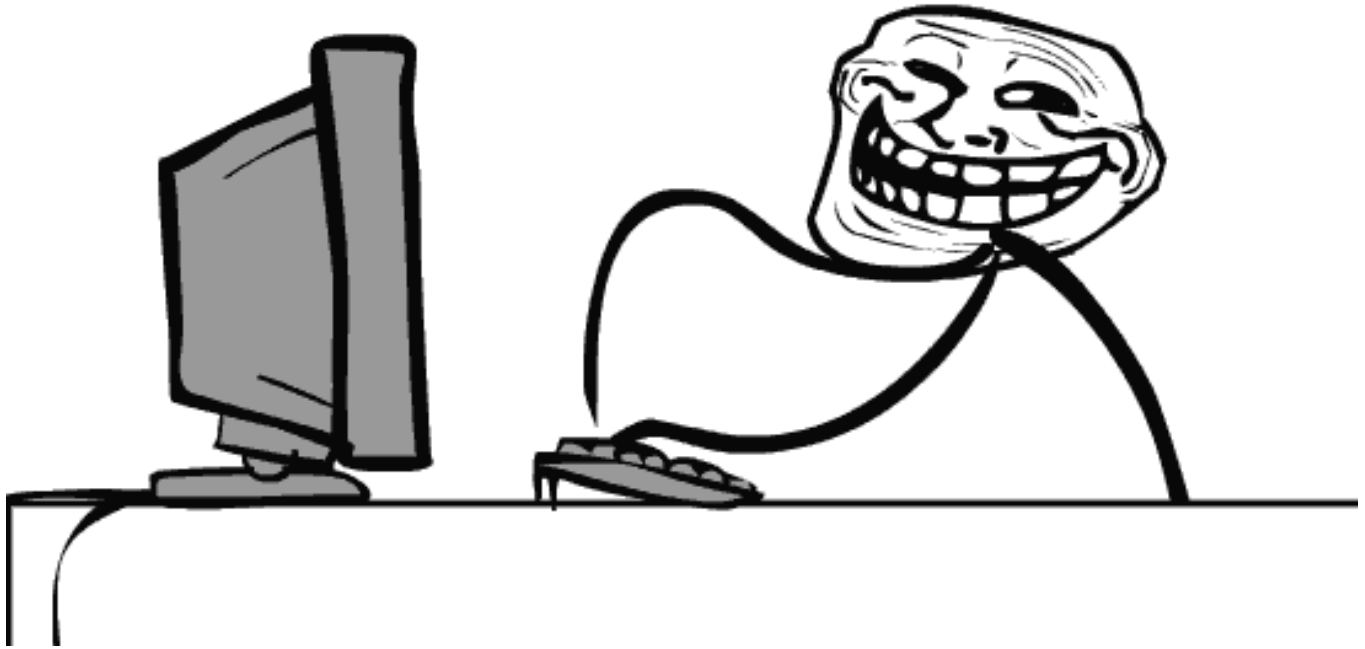


SIS Triconex attack vectors

- Jednoduchý ‘Do not press’ HMI útok



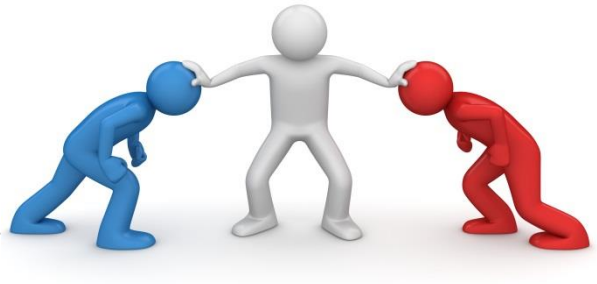
How to solve it?



5 základních mýtů

- Mám oddělenou OT síť
- My to kontrolujeme
- Provoz má přednost
- Nikoho nepovolaného tam nepouštím
- Máme tam IPS a antivirus

- 100% tomu tak není
- 100% nekontrolujete
- Až do doby bezpečnostního incidentu, který způsobí odstávku
- Vy máte veškeré vývojáře a techniky svoje?
- Většinou neumí DPI a nepoznají anomálie

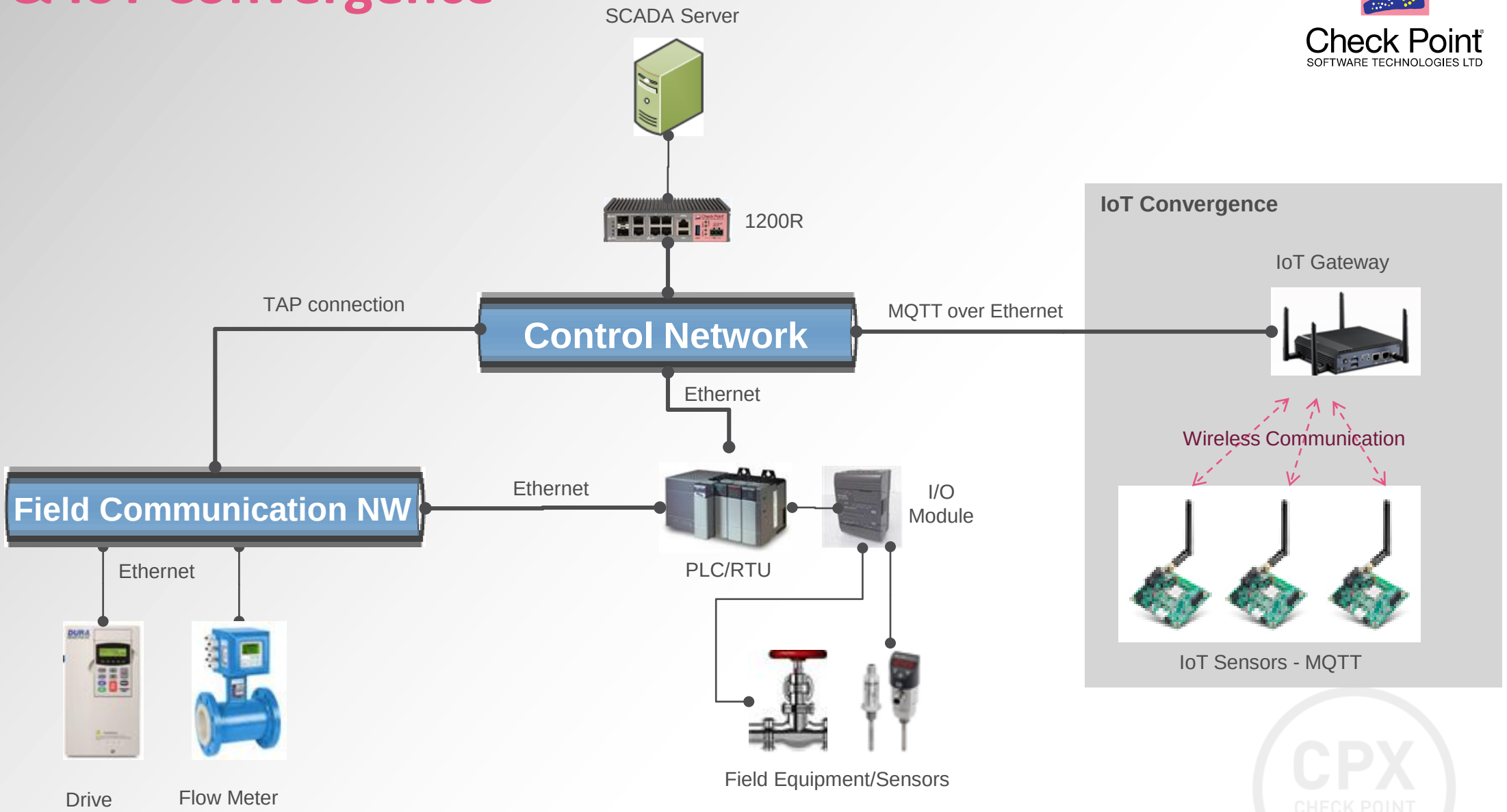


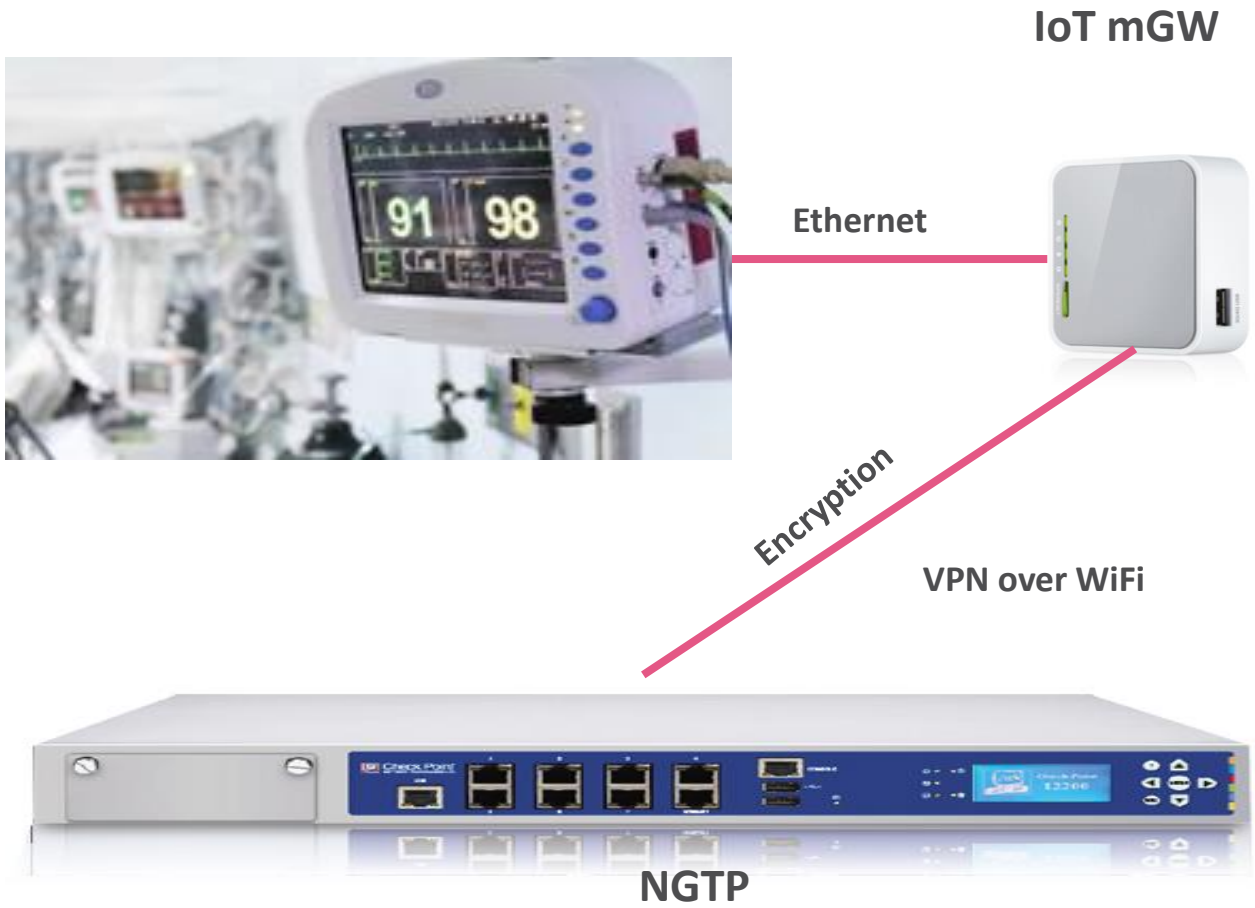
Realita je jiná

- A víte co tu máte za systémy?
- Máte představu jak chcete začít?
- Můžeme se starych systémů zbavit?

- Já nevím, něco jo, něco nevím vůbec. Asi bych to potřeboval zmapovat
- No nějakou mám, chtěl jsem tam nainstalovat antiviry, ale jsou tam Windows XP
- Ježíši jen to ne, toho co to kdysi psal přejela včera tramvaj

SCADA & IoT Convergence





PŘEDCHÁZET A BLOKOVAT

Procesy

Technologie

Take Action

Check Point
SOFTWARE TECHNOLOGIES LTD

1

Začněte se základy

Definujte efektivní perimetrovou i datacentrovou bezpečnost

2

Nebuďte slepí

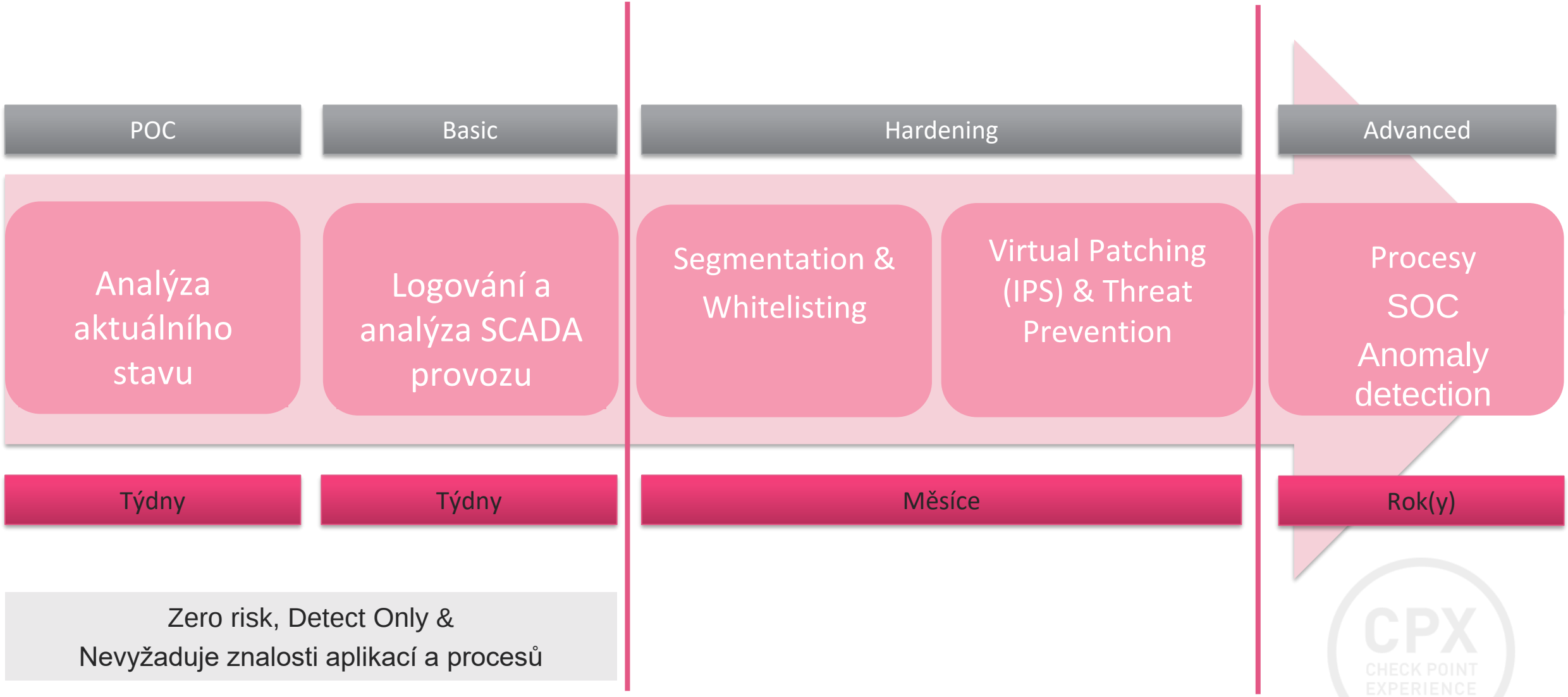
Logujte všechny SCADA aktivity a vytvořte si tzv. baseline (známé/neznámé) a poté detekujte anomálie

3

Udělejte to útočníkům složité

Segmentace, VxPatch management a co není povoleno, je zakázáno

Implementace bezpečnosti



Zero risk, Detect Only &
Nevyžaduje znalosti aplikací a procesů

IT/OT ochrany

Corporate Network	Operational Network	
Segmentace	Segmentace	SCADA Logging, Anomaly Detection, Whitelisting
Firewall	Firewall	Application Control
Hardening	Hardening	SmartEvent
Endpoint Security	Endpoint Security	Advanced Logical SCADA Attacks Detection
Threat Prevention	Threat Prevention	Security Matters
IPS	IPS	
Anti-Virus / Anti-Bot	Anti-Virus / Anti-Bot	
Threat Emulation	Threat Extraction	
Threat Extraction	Threat Emulation	
IntelliStore	IntellStore	
	SCADA Virtual Patching	
	IPS	
Standard Gateways	Standard or Industrial Security Gateways	

Check Point
SOFTWARE TECHNOLOGIES LTD

5TH GENERATION CYBER SECURITY

GEN V

THANK YOU

With optimism…

Tomas Vobruba | SE Slovakia

CPX
CHECK POINT
EXPERIENCE