TREND MICRO™

POLITECNICO MILANO 1863

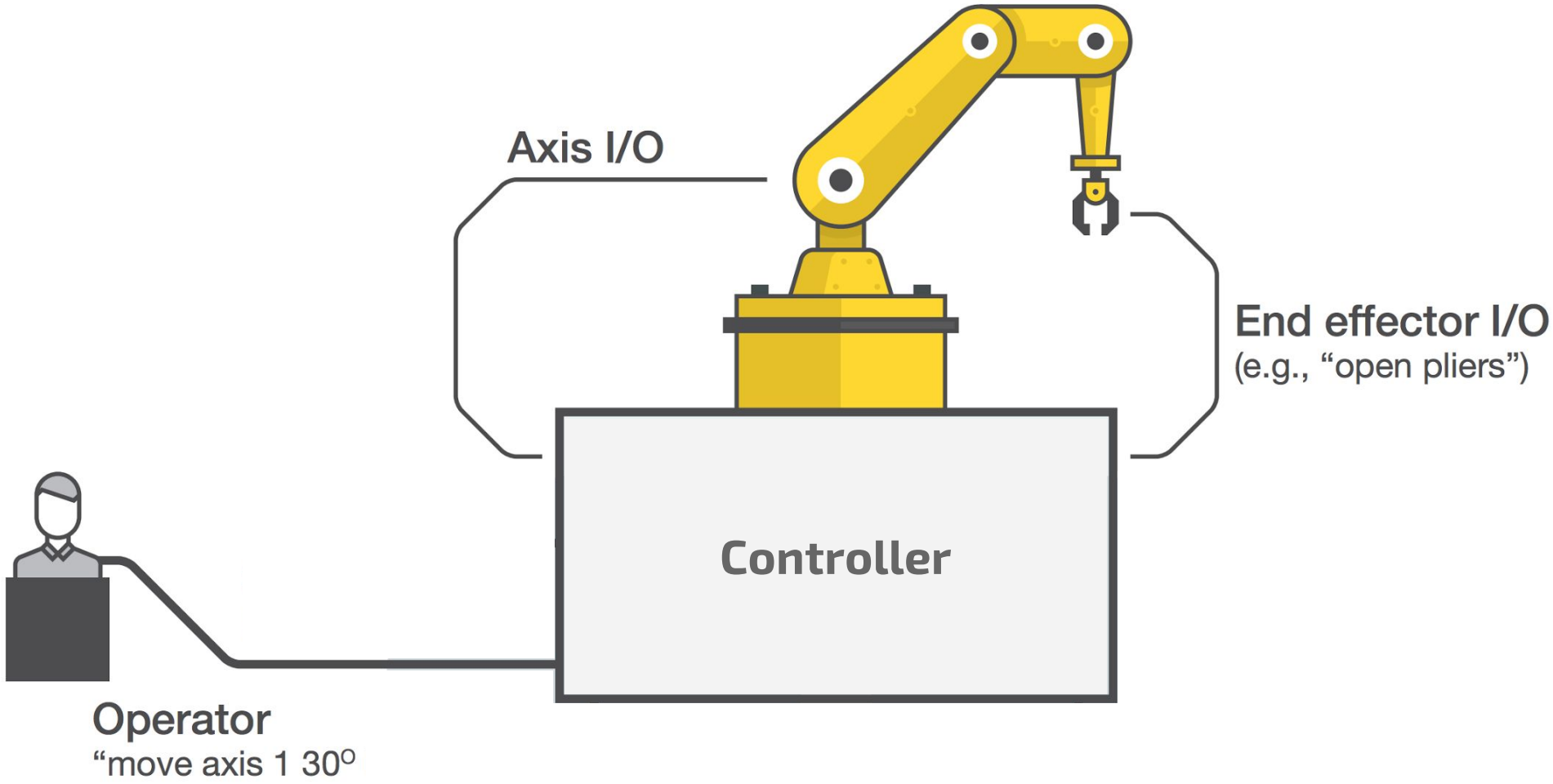
DIPARTIMENTO DI ELETTRONICA INFORMAZIONE E BIOINGEGNERIA

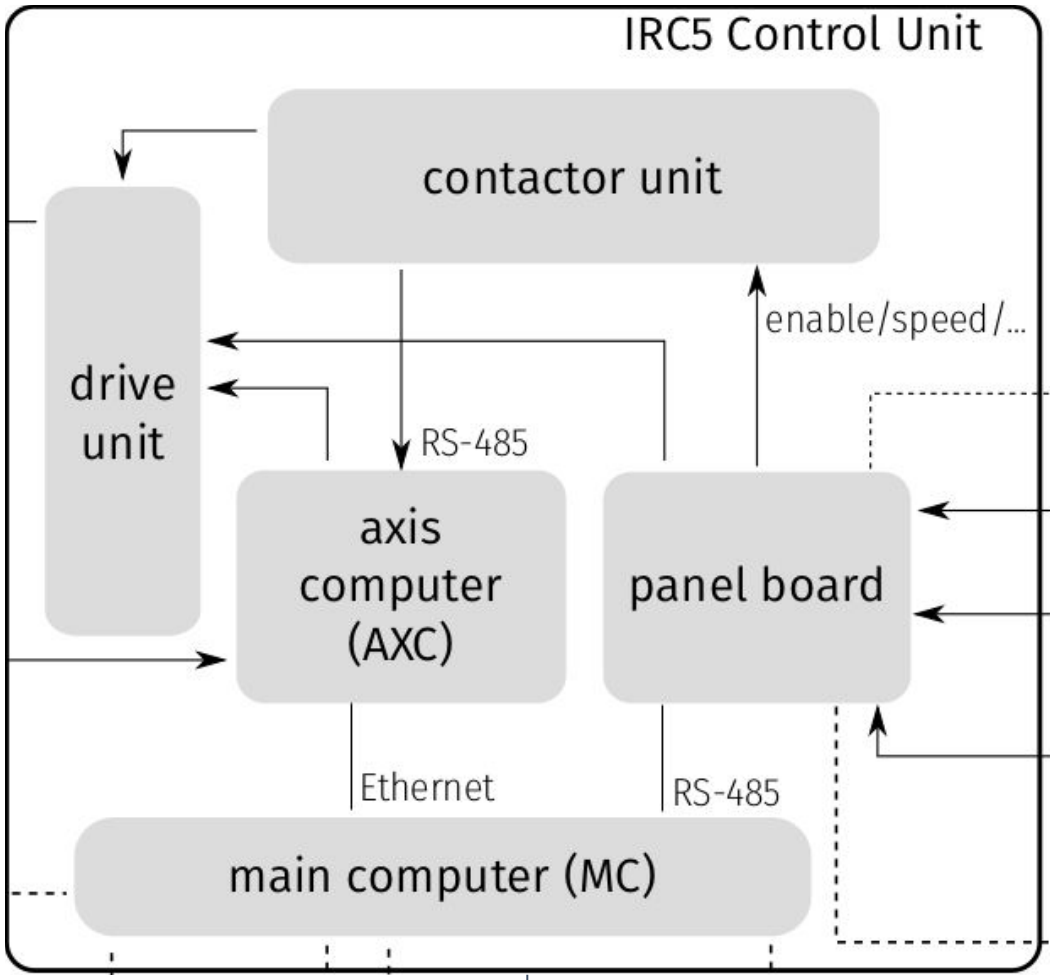
Breaking the Laws of Robotics
Attacking Industrial Robots

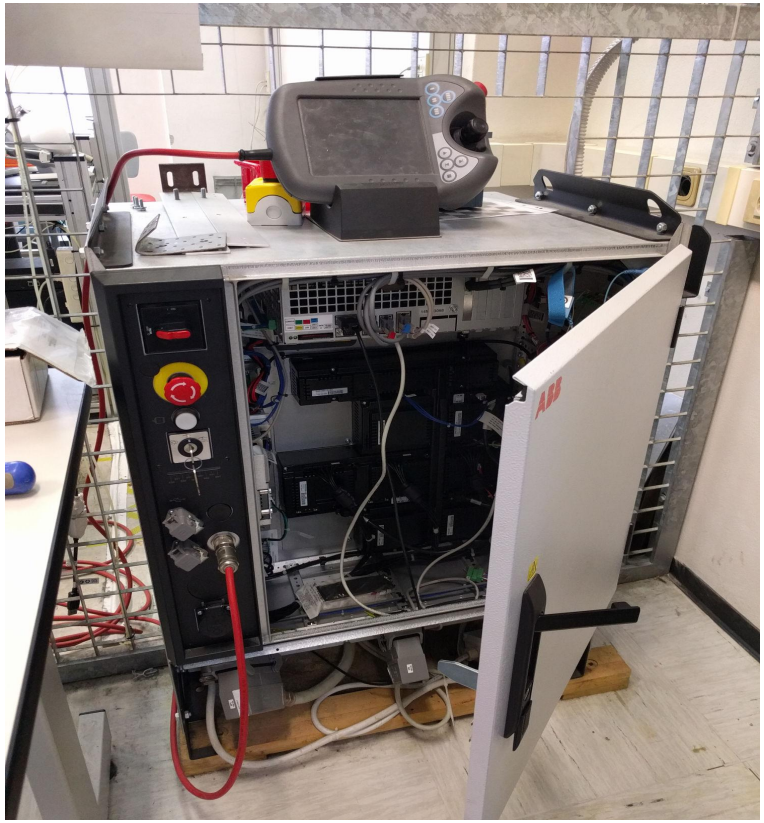
Davide Quarta, **Marcello Pogliani**, Mario Polino, **Federico Maggi**,
Andrea M. Zanchettin, Stefano Zanero

Industrial robots?

Industrial Robot Architecture (Standards)



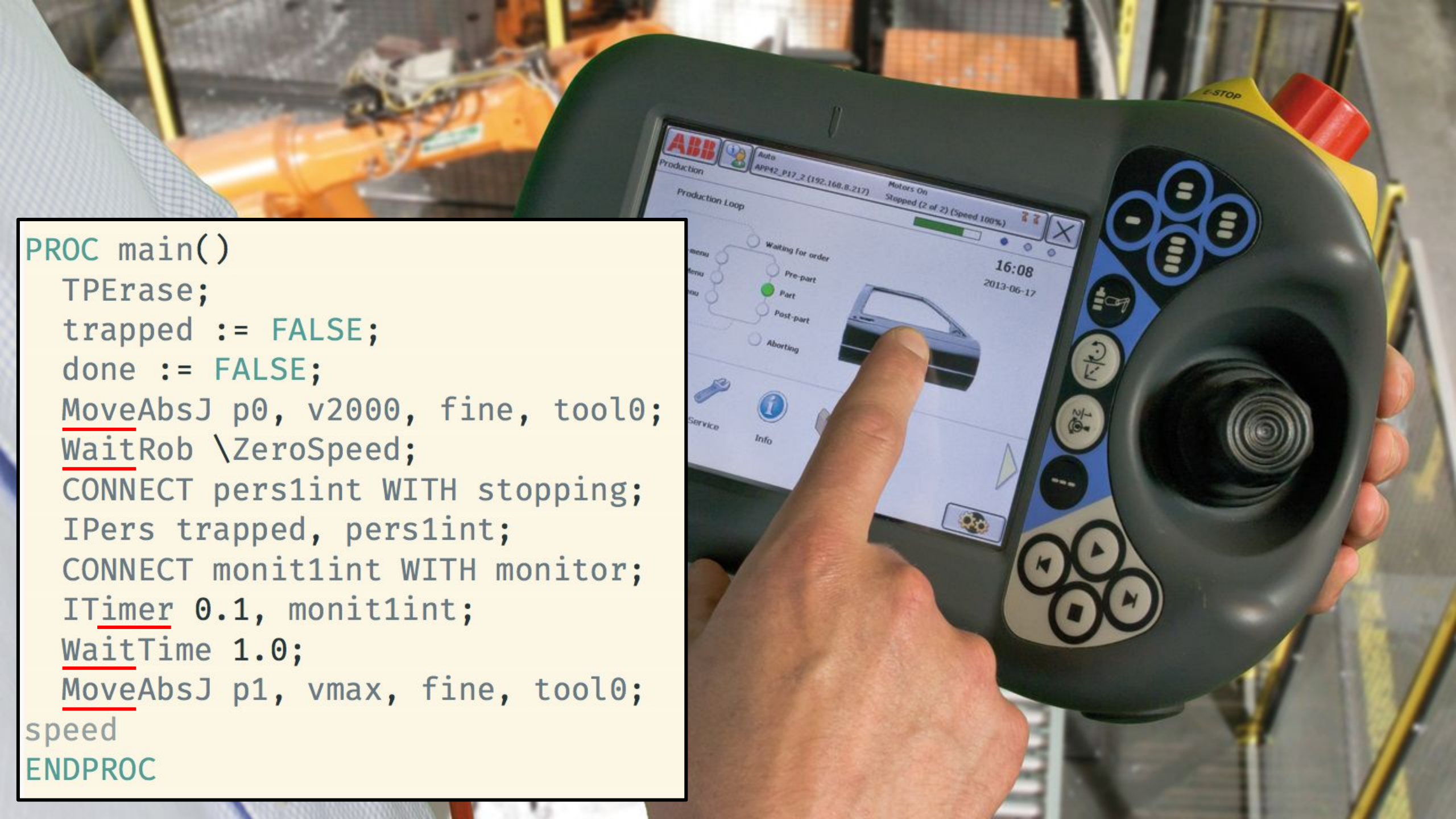

IRC5 Control Unit
contactor unit
drive unit
enable/speed/...
RS-485
axis computer (AXC)
panel board
Ethernet
RS-485
main computer (MC)



Flexibly programmable

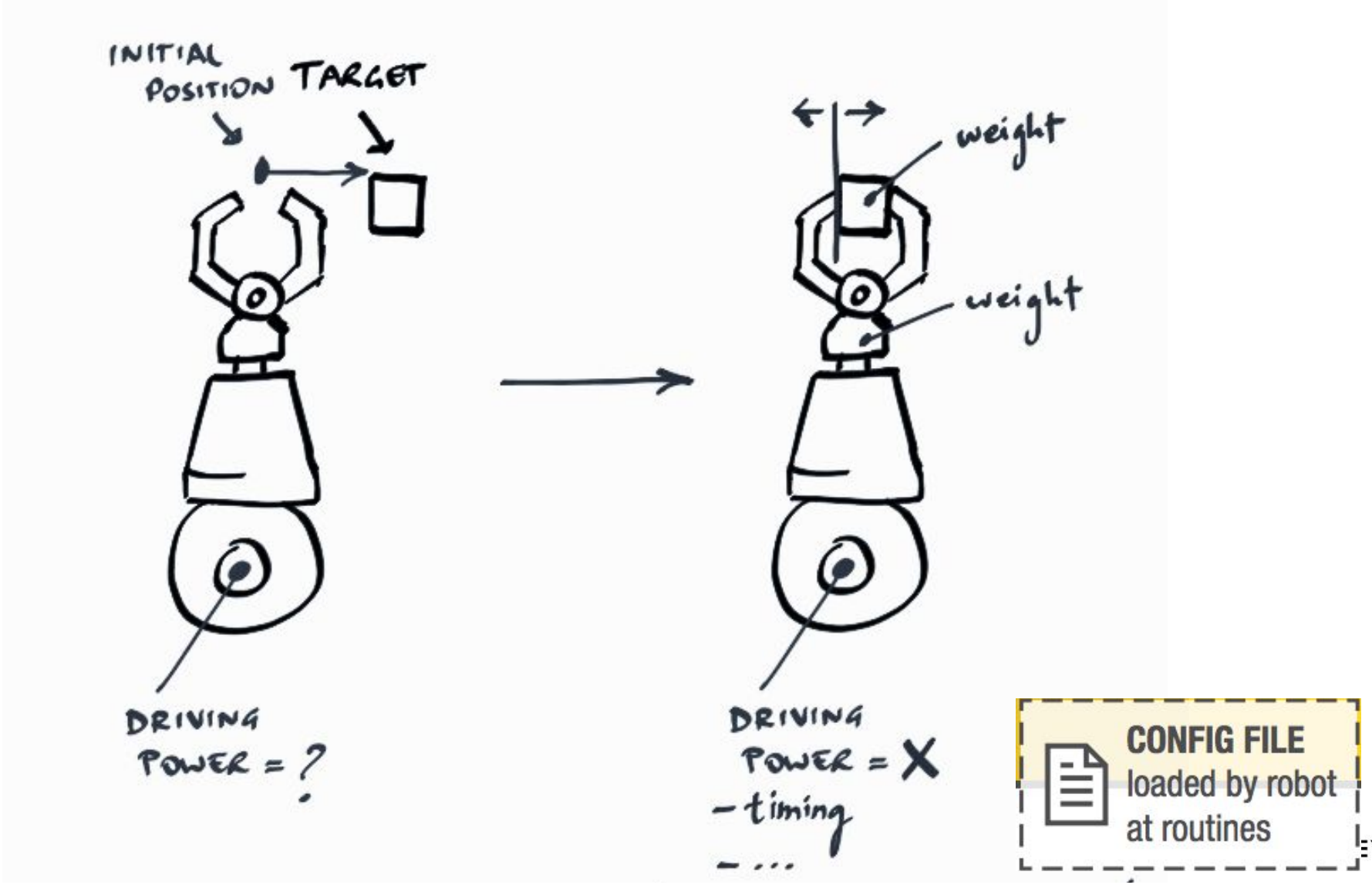
&

Connected




```
PROC main()
  TPErase;
  trapped := FALSE;
  done := FALSE;
  MoveAbsJ p0, v2000, fine, tool0;
  WaitRob \ZeroSpeed;
  CONNECT pers1int WITH stopping;
  IPers trapped, pers1int;
  CONNECT monit1int WITH monitor;
  ITimer 0.1, monit1int;
  WaitTime 1.0;
  MoveAbsJ p1, vmax, fine, tool0;
speed
ENDPROC
```

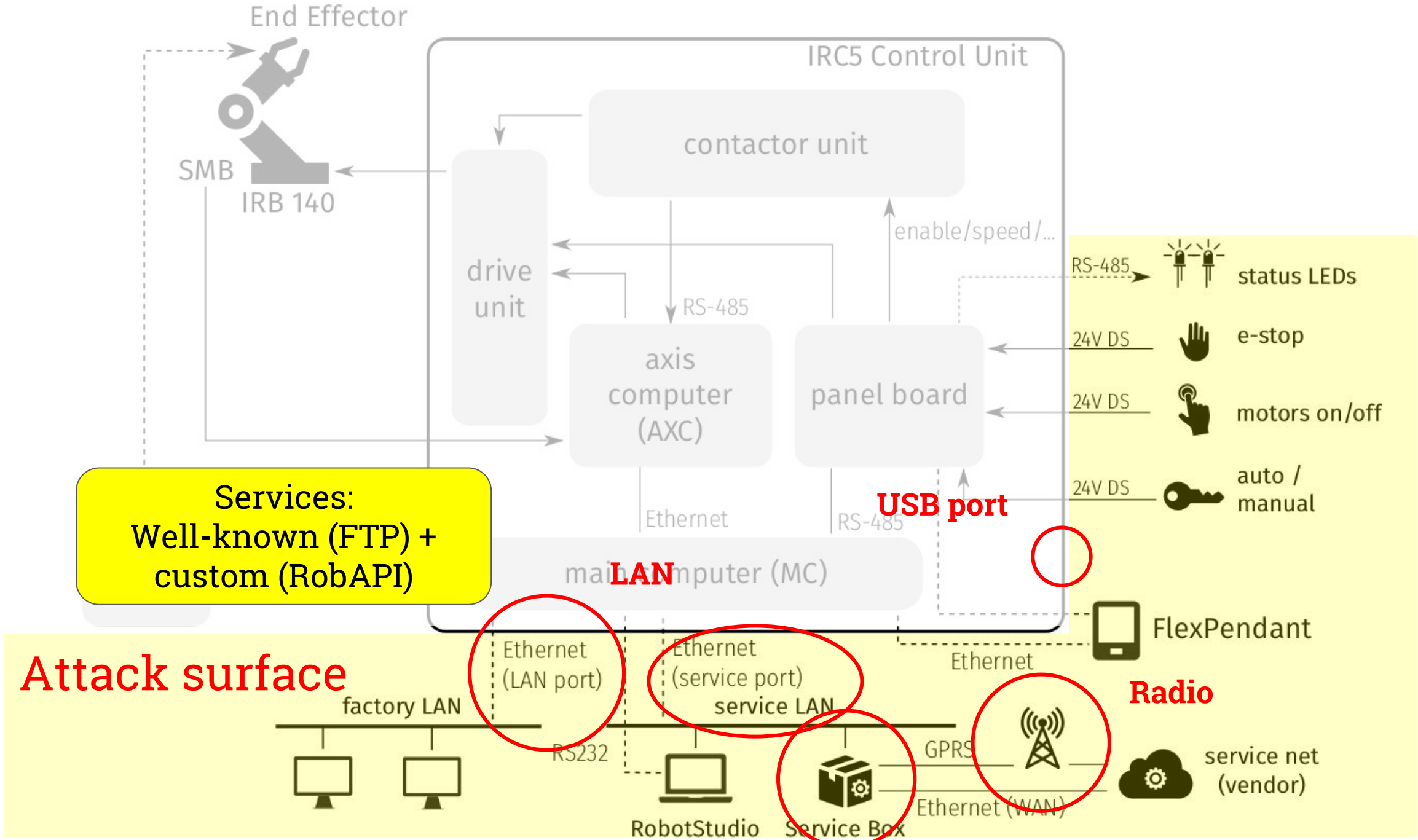
"Implicit" parameters



Flexibly programmable
&
Connected
(Part 1)

Connected Robots

- **Now:** monitoring & maintenance ISO 10218-2:2011
- **Near future:** active production planning and control
  - some vendors expose REST-like APIs
  - … up to the use of mobile devices for commands
- **Future:** app/library stores
  - “Industrial” version of robotappstore.com?


End Effector
SMB
IRB 140
IRC5 Control Unit
contactor unit
drive unit
RS-485
enable/speed/...
axis computer (AXC)
panel board
RS-485
status LEDs
24V DS
e-stop
24V DS
motors on/off
24V DS
auto / manual
Ethernet
RS-485
main computer (MC)
USB port
LAN
Services:
Well-known (FTP) +
custom (RobAPI)
FlexPendant
Ethernet
Attack surface
Ethernet (LAN port)
Ethernet (service port)
factory LAN
service LAN
Radio
RS232
GPRS
service net (vendor)
RobotStudio
Service Box
Ethernet (WAN)

They are *already* meant to be connected

17.3 Sending/receiving e-mails on C4G Controller

A PDL2 program called "email" is shown below ("email" program): it allows to send and receive e-mails on C4G Controller.

DV4_CNTRL Built-In Procedure is to be used to handle such functionalities.

See DV4_CNTRL Built-In Procedure in Chap. BUILT-IN Routines List section for further information about the e-mail functionality parameters.

17.3.1 "email" program

```
PROGRAM email NOHOLD, STACK = 10000
CONST ki_email_cnfg = 20
  ki email send = 21
```

17.4 Sending PDL2 commands via e-mail

The user is allowed to send PDL2 commands to the C4G Controller Unit, via e-mail. To do that, the required command is to be inserted in the e-mail title with the prefix 'CL' and the same syntax of the strings specified in SYS_CALL built-in. Example: if the required

.fm

COMAU ROBOTICS

Connected?

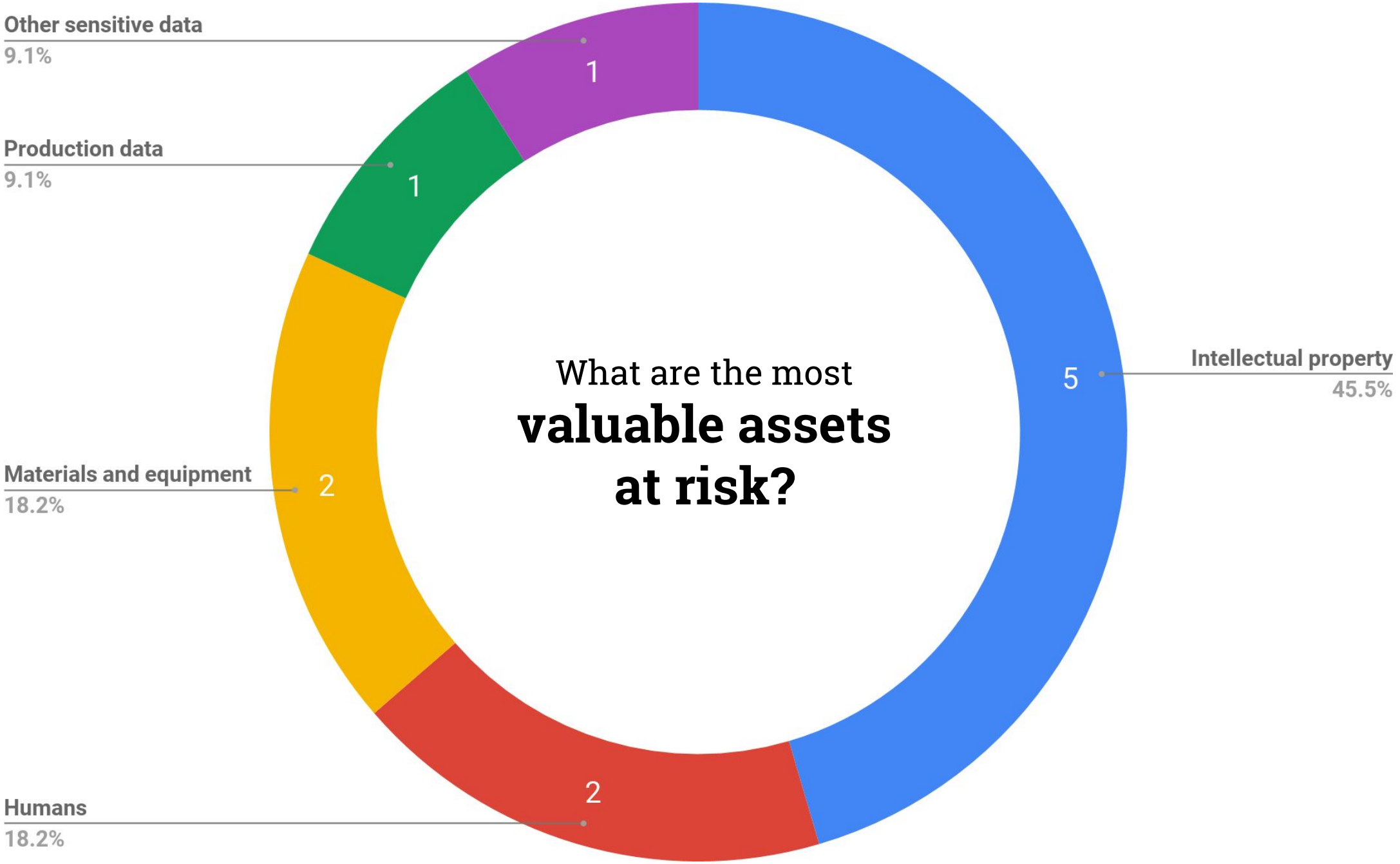
Do you consider

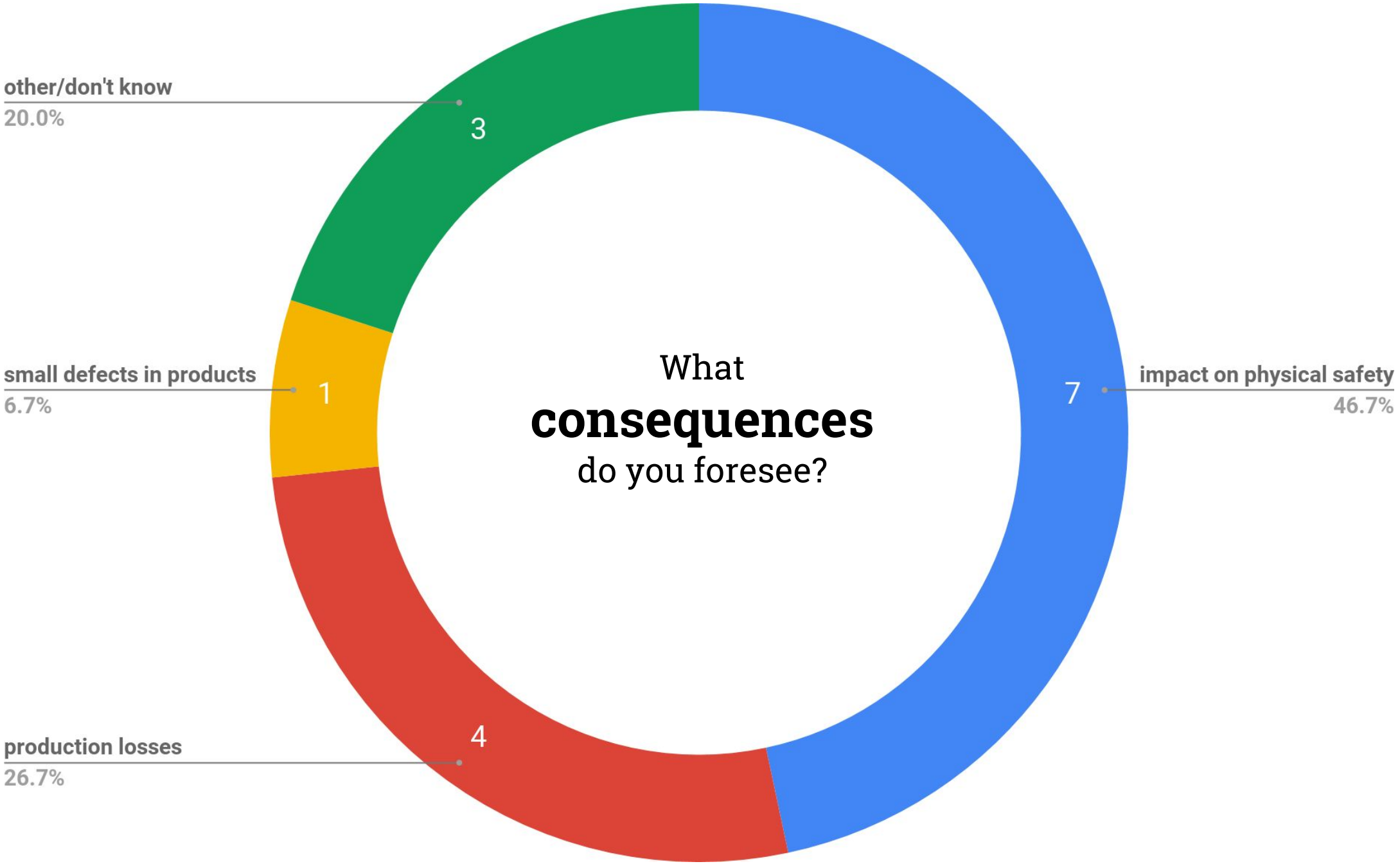
cyber attacks

against robots a

realistic threat?


Do you consider
cyber attacks
against robots a
realistic threat?
No
52.9%
9
8
Yes
47.1%


Other sensitive data
9.1%
1
Production data
9.1%
1
What are the most
valuable assets
at risk?
Intellectual property
45.5%
5
Materials and equipment
18.2%
2
Humans
18.2%
2


other/don't know
20.0%
3
small defects in products
6.7%
1
production losses
26.7%
4
impact on physical safety
46.7%
7
What
consequences
do you foresee?

impact is much more important than the **vulnerabilities** alone.

How do we assess the impact of an attack against industrial robots?

We assess **impact** by reasoning on **requirements**

Requirements: "Laws of Robotics"

Safety

Accuracy

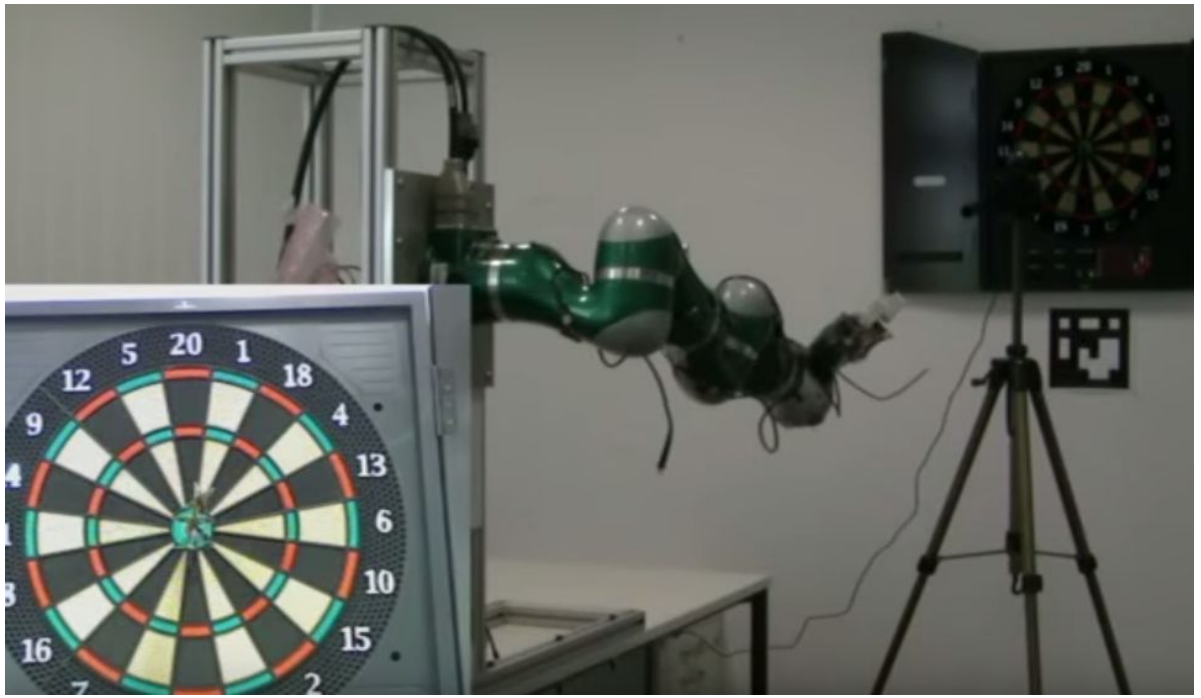
Integrity

Requirements: "Laws of Robotics"

Safety

Accuracy

Integrity



Acknowledgements T.U. Munich, YouTube -- Dart Throwing with a Robotic Manipulator

Requirements: "Laws of Robotics"

Safety

Accuracy

Integrity

Robot-Specific Attack

Safety

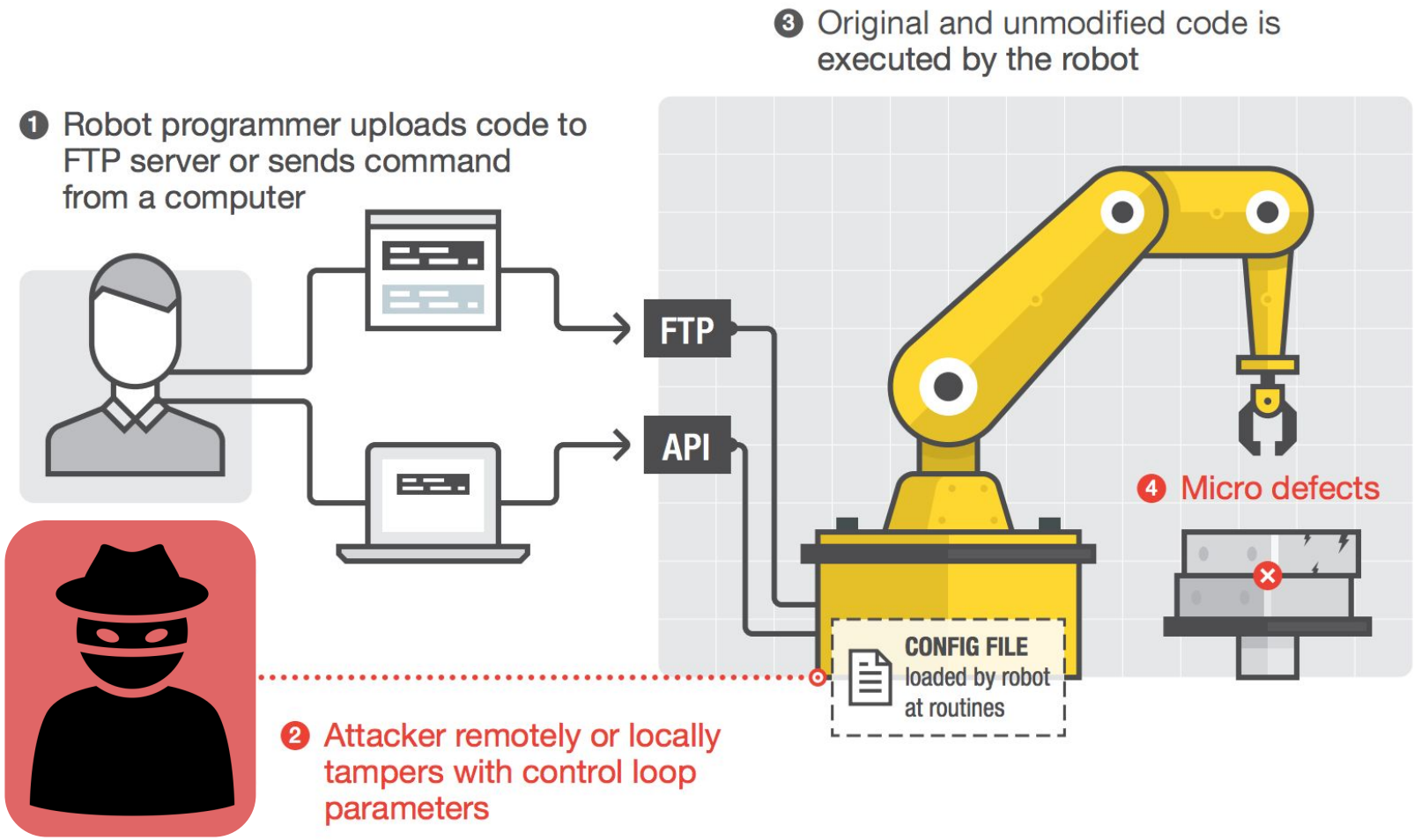
Accuracy

Integrity

→ **violating any of these requirements via a digital vector**

5 robot-specific attacks

Control Loop Alteration

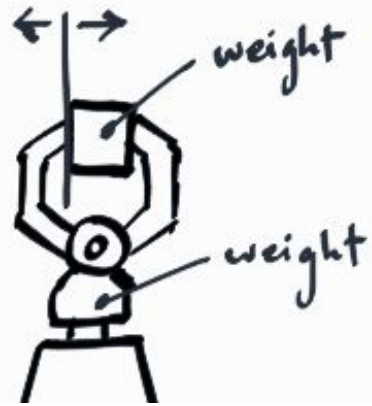


Attack 1

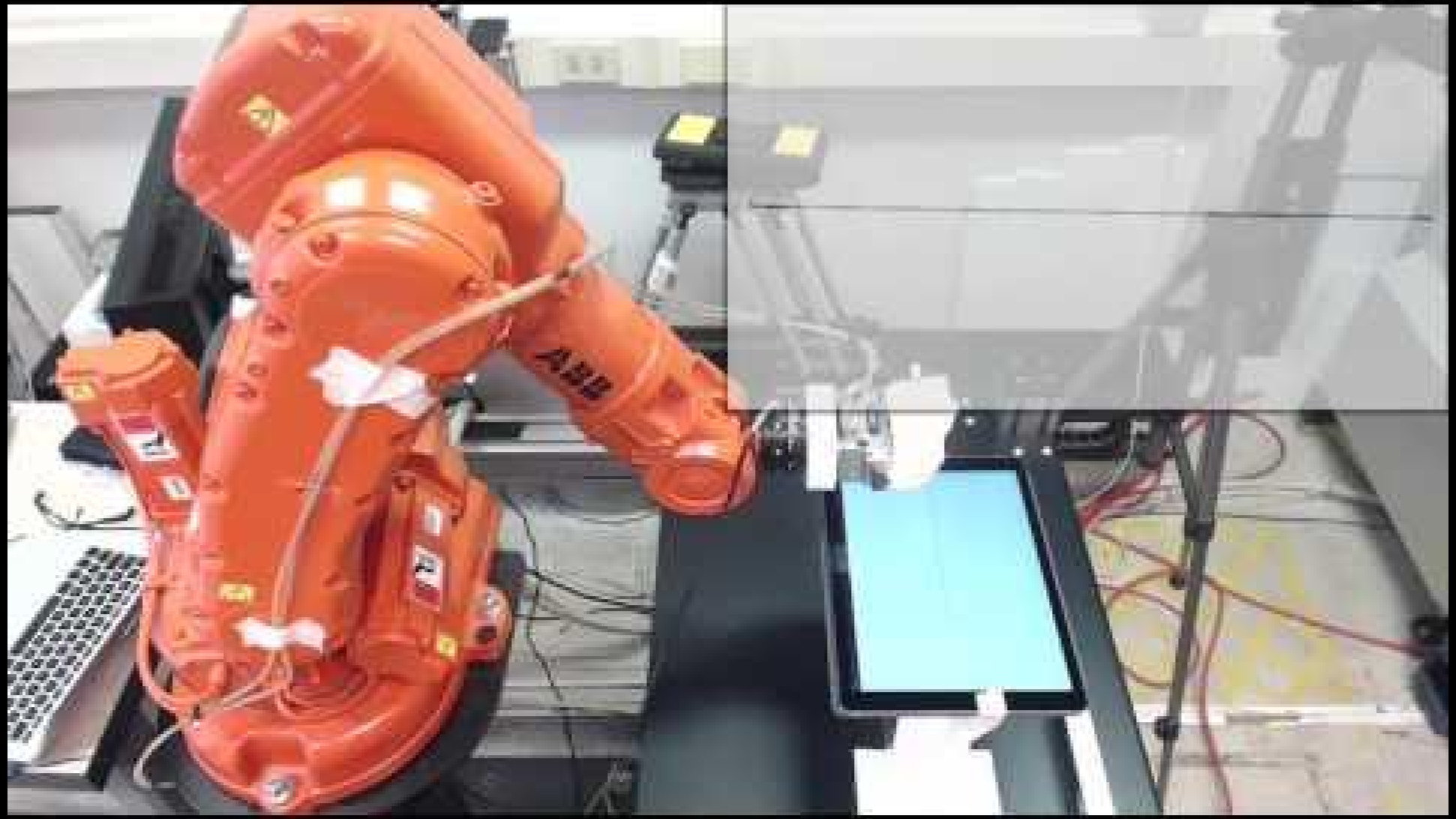
Safety

Accuracy

Integrity

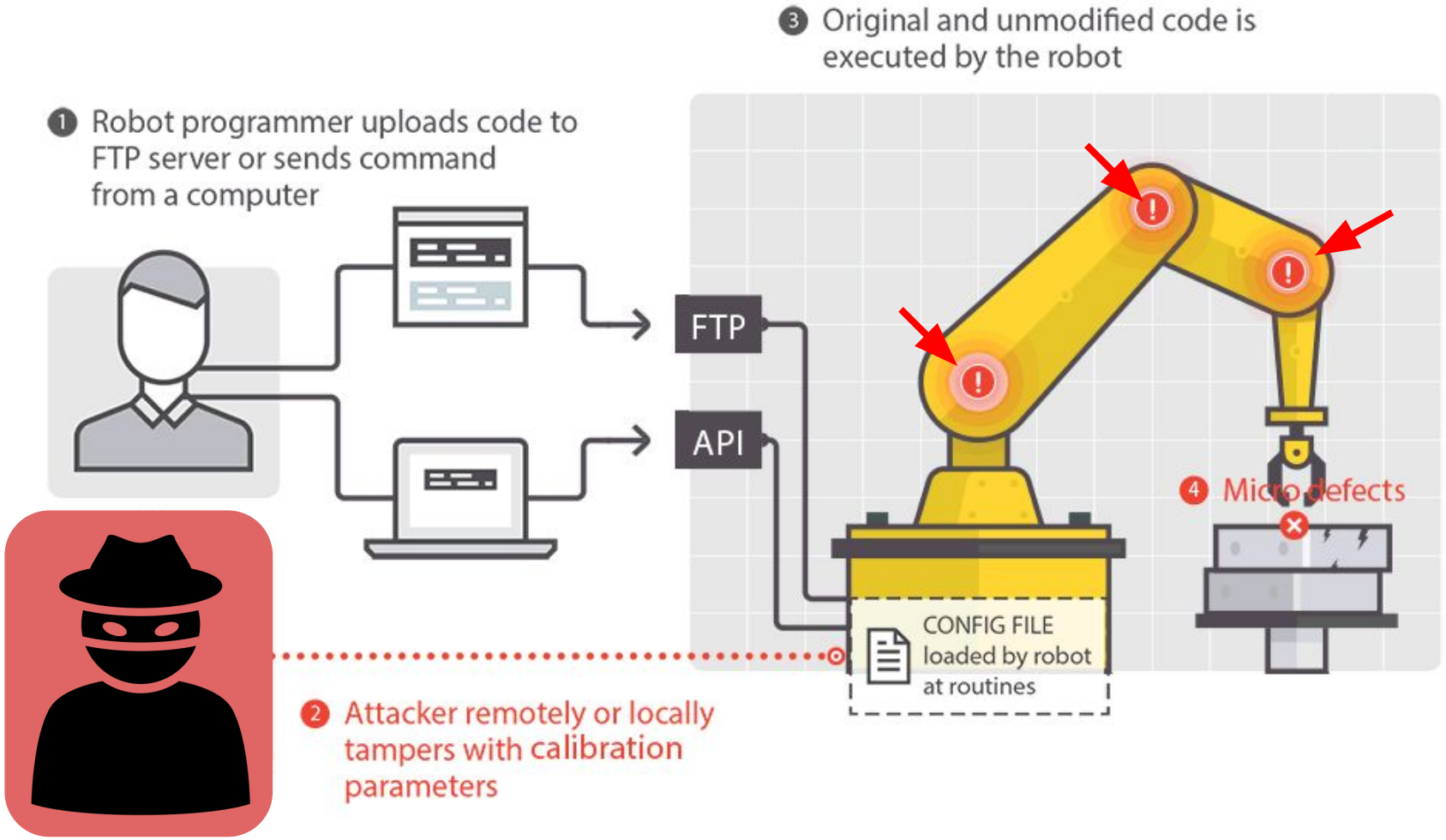


DEMO



ABB

Calibration Tampering



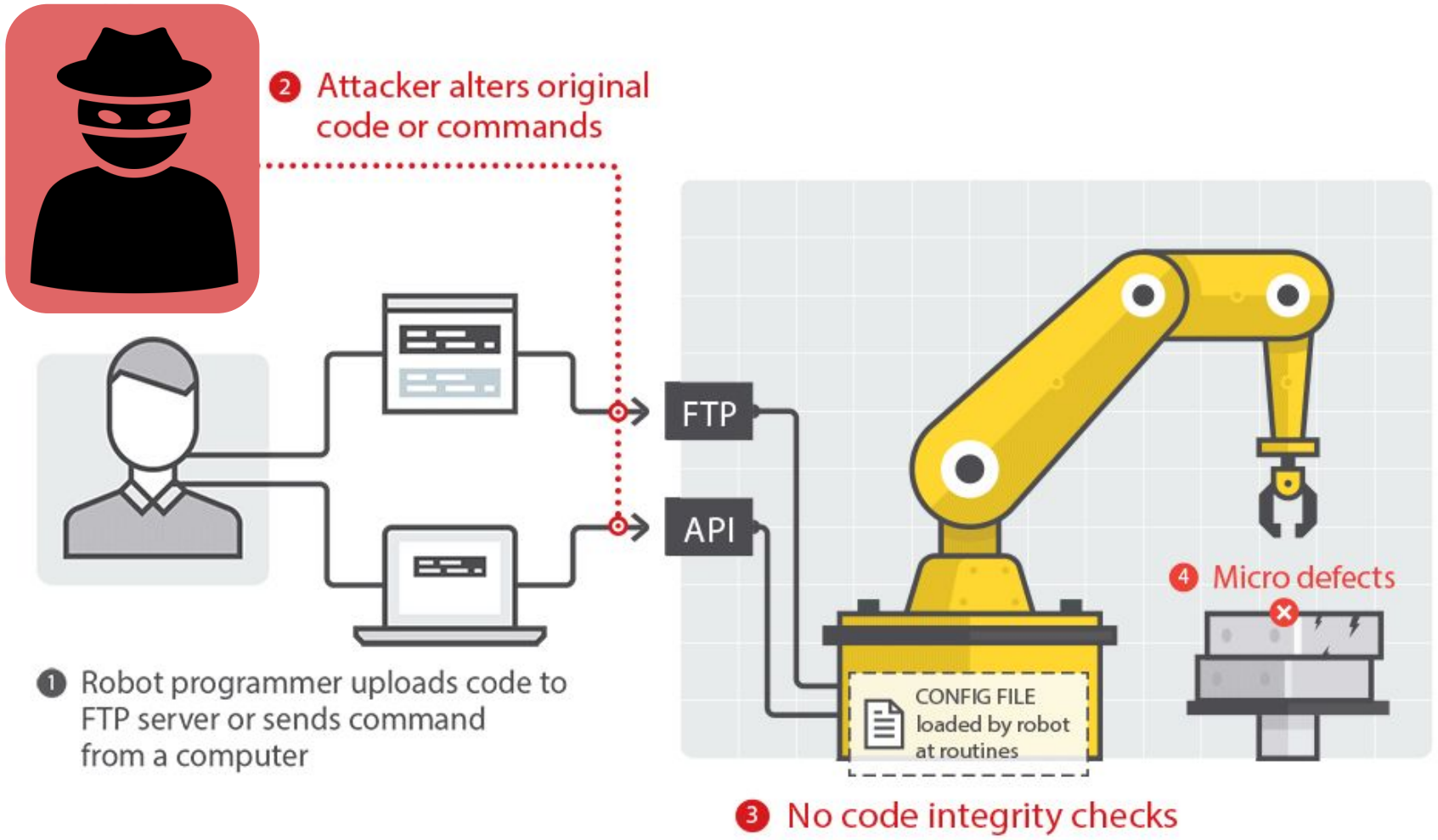
Attack 2

Safety

Accuracy

Integrity

Production Logic Tampering



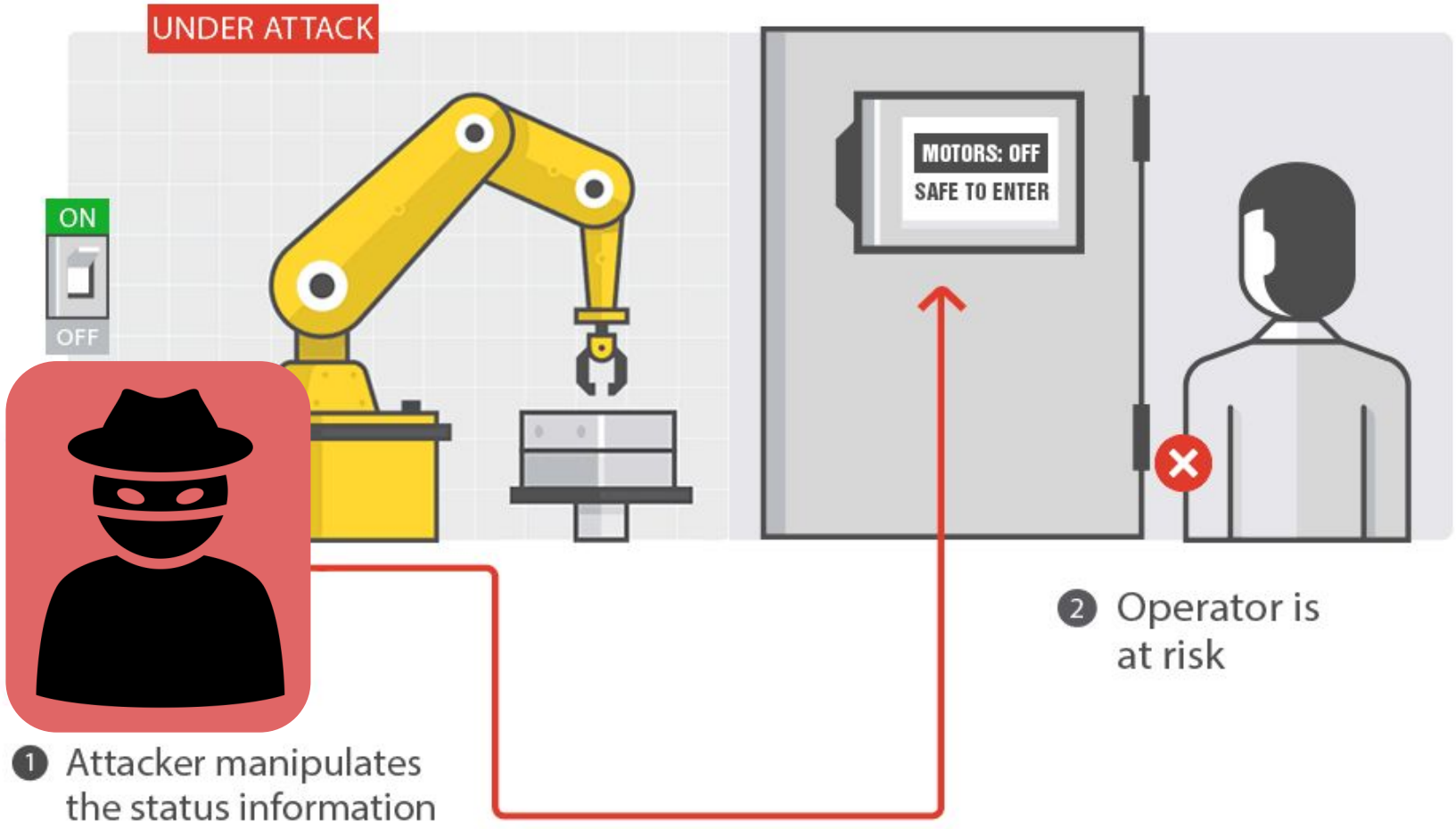
Attack 3

Safety

Accuracy

Integrity

(Perceived) State Alteration



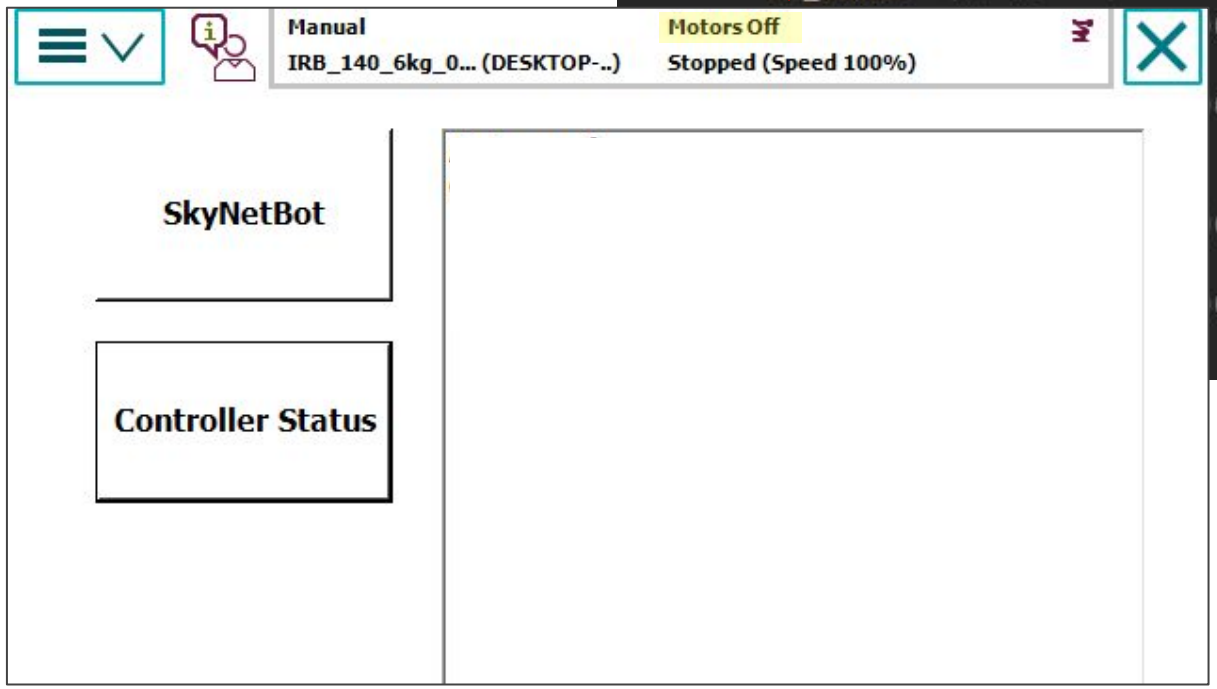
Attack 4+5
Safety
Accuracy
Integrity

Perceived State Alteration PoC

Malicious DLL

Teach Pendant

```
        IL_025c:  /* 03   |                    */ ldarg.1
        IL_025d:  /* 6F   | (0A)000028         */ callvirt   instance class [System.Drawing/*23000
() /* 0A000028 */
        //IL_0262:  /* 02   |                    */ ldarg.0
        //IL_0263:  /* 7B   | (04)0000A8         */ ldfld      string ABB.Robotics.Tps.Controls.St
        ldstr "Motors Off"
    »   IL_0268:  /* 02   |                    */ ldarg.0
        IL_0269:  /* 7B   | (04)0000B2         */ ldfld      class [System.Drawing/*23000007*/]Sys
        IL_026e:  /* 02   |                    */ ldarg.0
                                                0000B0      */ ldfld      class [System.Drawing/*23000007*/]Sys
                                                            */ ldloca.s   V_1
                                                000169      */ call       instance int32 [System.Drawing/*23000
                                                            */ conv.r4
                                                            */ ldloca.s   V_1
                                                0000DF      */ call       instance int32 [System.Drawing/*23000
                                                            */ conv.r4
                                                0000AD      */ callvirt   instance void [System.Drawing/*230000
```

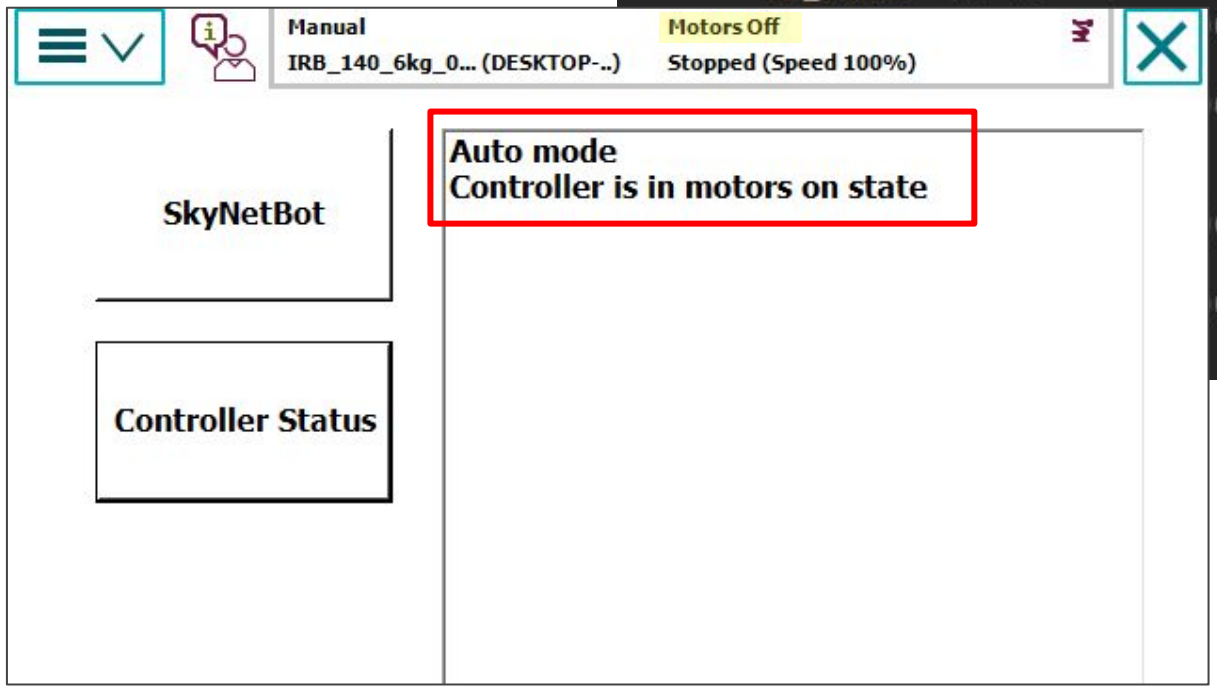


Perceived State Alteration PoC

Malicious DLL

Teach Pendant

```
        IL_025c:  /* 03   |                    */ ldarg.1
        IL_025d:  /* 6F   | (0A)000028         */ callvirt   instance class [System.Drawing/*23000
() /* 0A000028 */
        //IL_0262:  /* 02   |                    */ ldarg.0
        //IL_0263:  /* 7B   | (04)0000A8         */ ldfld      string ABB.Robotics.Tps.Controls.St
        ldstr "Motors Off"
    »   IL_0268:  /* 02   |                    */ ldarg.0
        IL_0269:  /* 7B   | (04)0000B2         */ ldfld      class [System.Drawing/*23000007*/]Sys
        IL_026e:  /* 02   |                    */ ldarg.0
                                                 0000B0      */ ldfld      class [System.Drawing/*23000007*/]Sys
                                                             */ ldloca.s   V_1
                                                 000169      */ call       instance int32 [System.Drawing/*23000
                                                             */ conv.r4
                                                             */ ldloca.s   V_1
                                                 0000DF      */ call       instance int32 [System.Drawing/*23000
                                                             */ conv.r4
                                                 0000AD      */ callvirt   instance void [System.Drawing/*230000
```

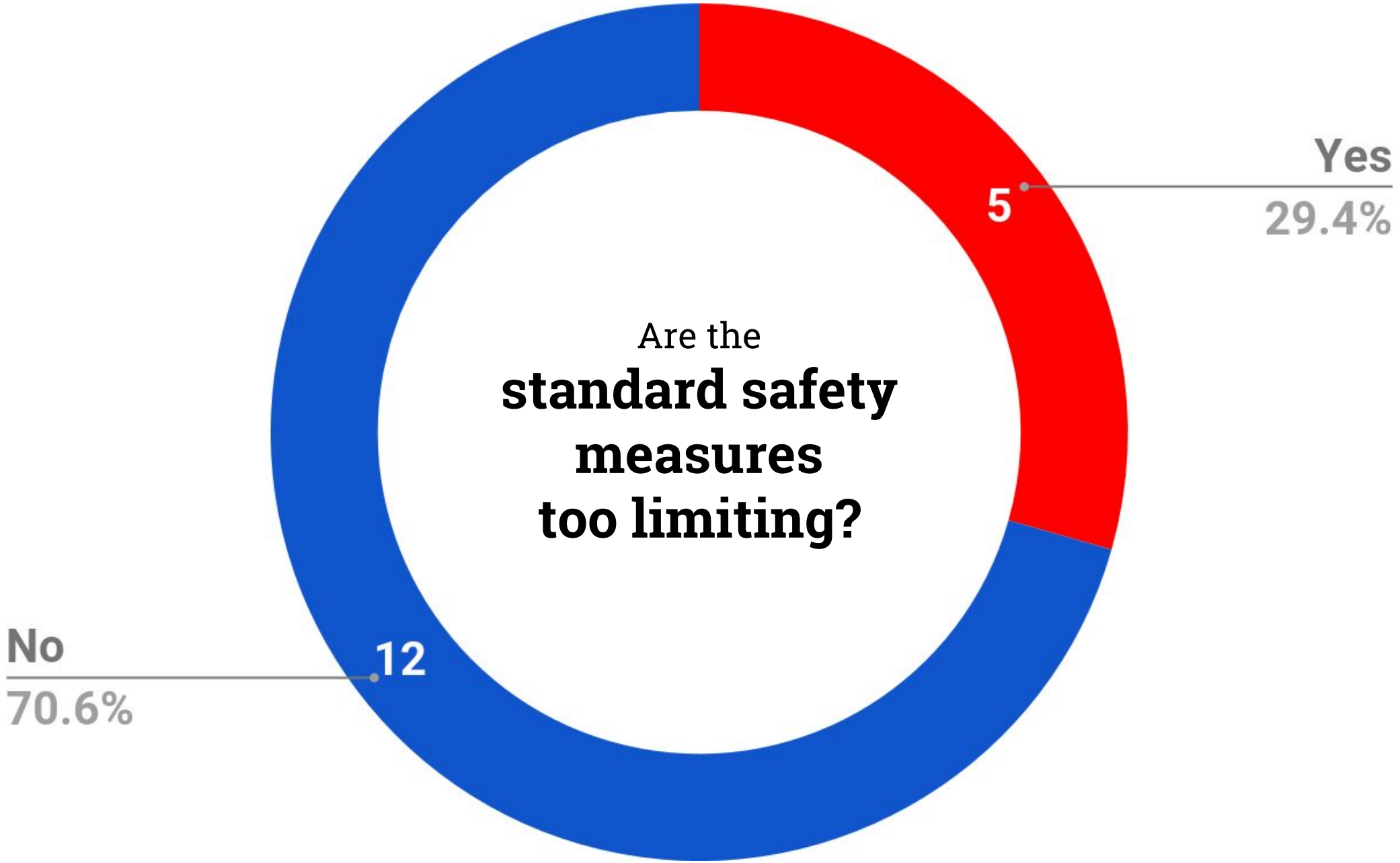


Is the Teach Pendant part of the safety system?

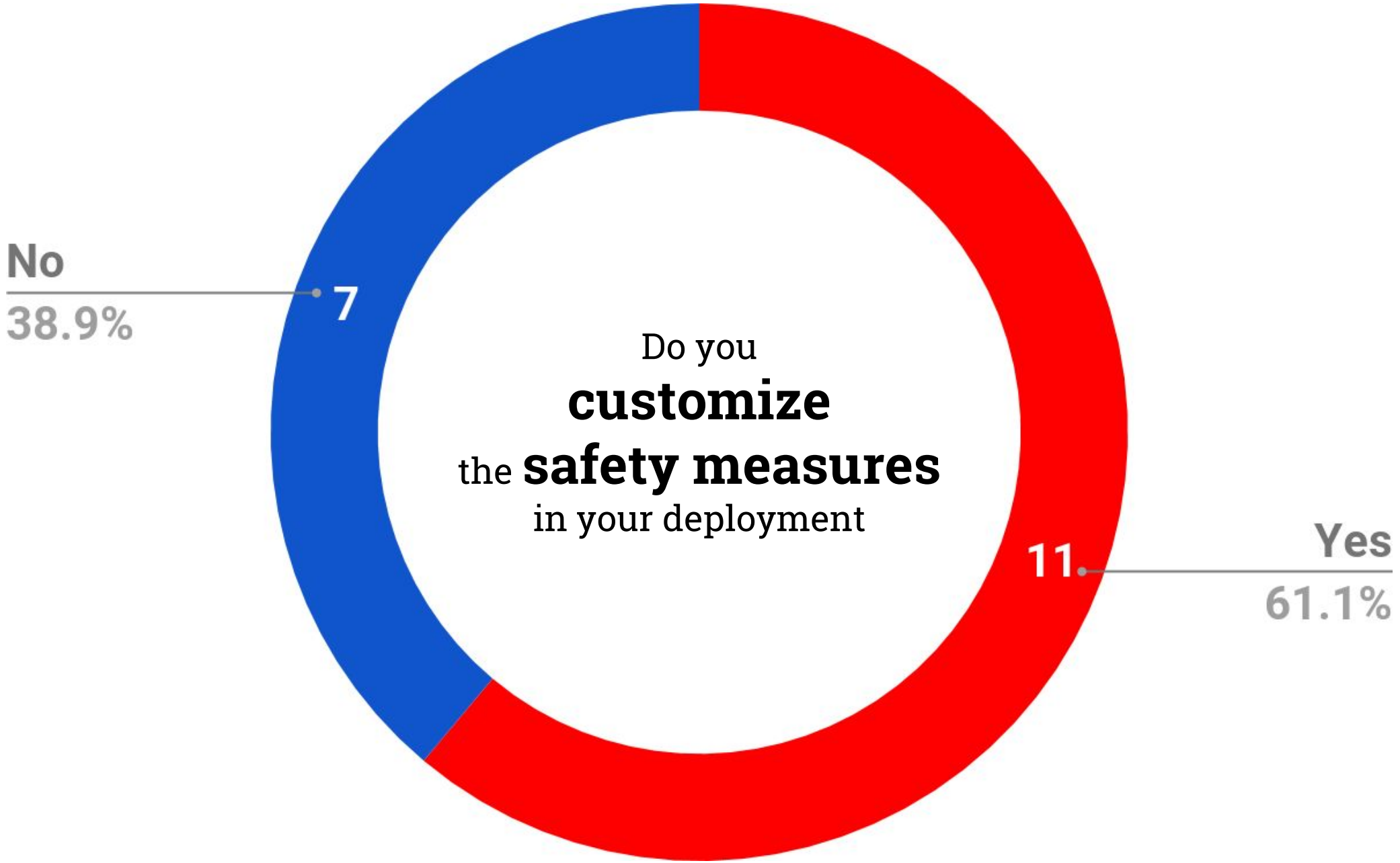
Is the Teach Pendant part of the safety system?

NO

Are the
standard safety measures too limiting?


Are the
standard safety
measures
too limiting?
Yes
29.4%
5
No
70.6%
12

Do you
customize
the **safety measures**
in your deployment


No
38.9%
7
Do you
customize
the safety measures
in your deployment
11
Yes
61.1%

Standards & Regulations vs. Real World

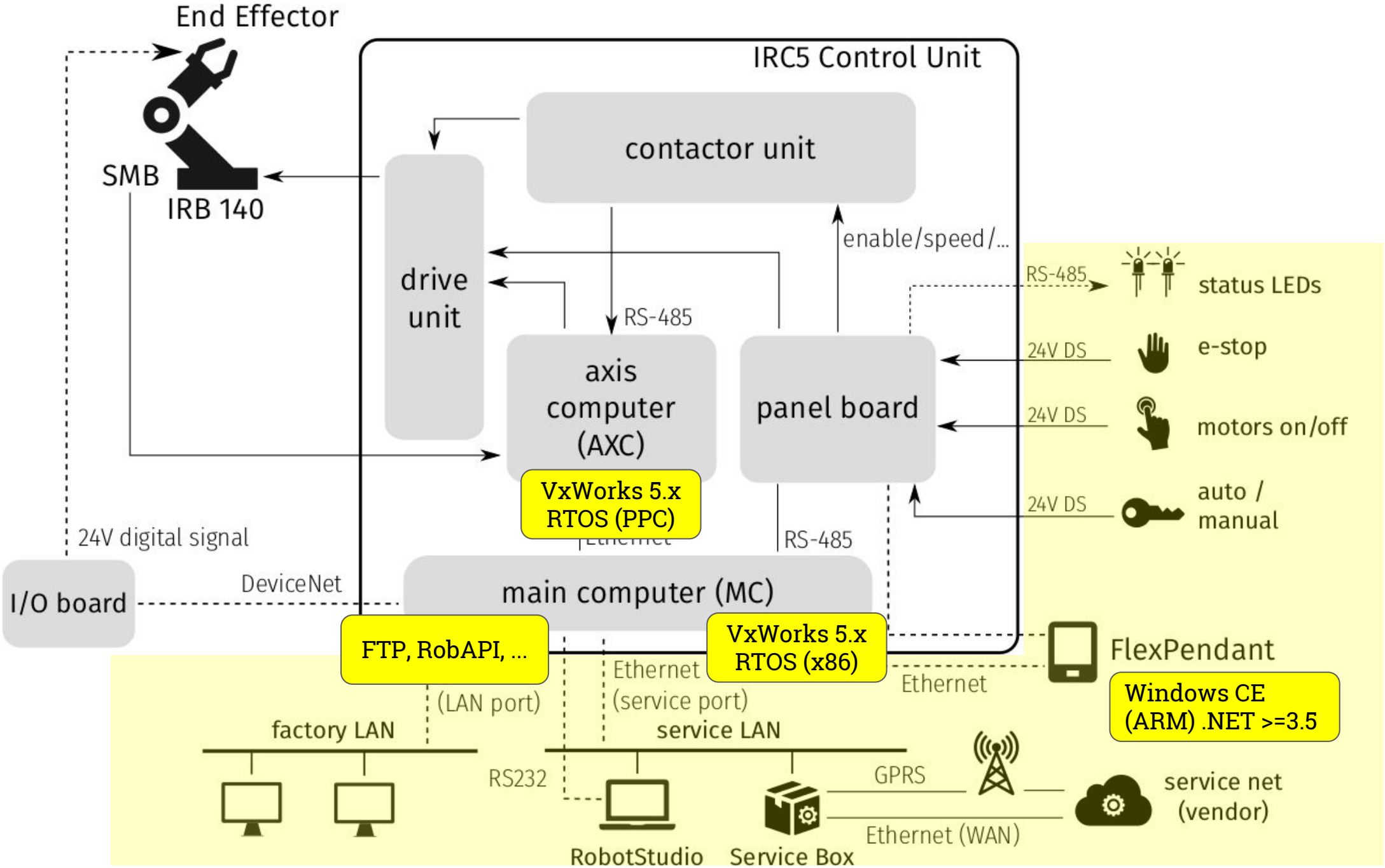
Fwd: [redacted] Researchers hijack a 220-pound industrial robotic arm

[redacted] to [redacted]

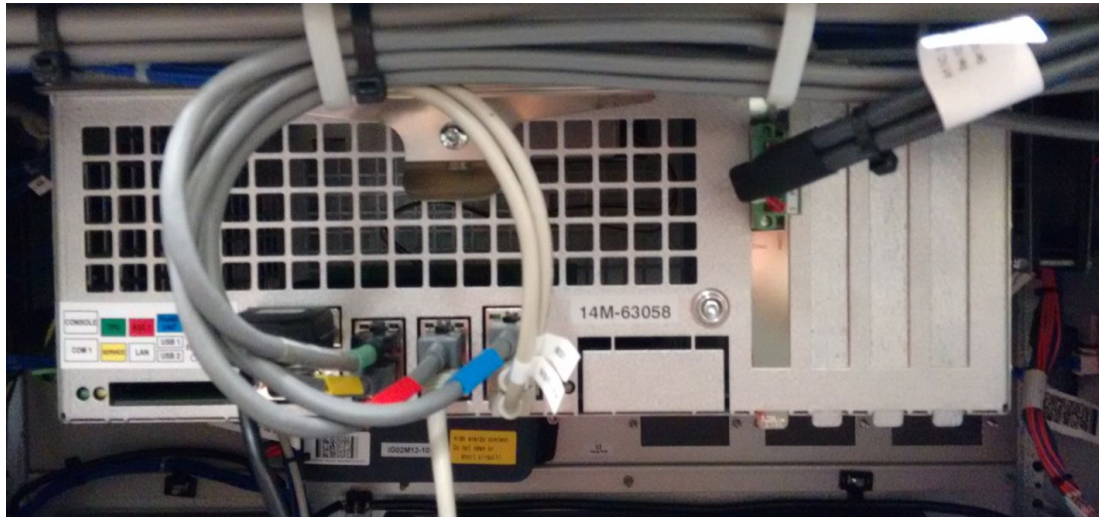
[redacted] has long had a robotics program and laboratories with larger robot arms than the one shown. These were the kind of robot arms where the lab floor had a red line to show the swing distance - inside that line and you could be struck by the arm, potentially fatally. Some of the early models were controlled by PCs connected to the corporate network. When powered down, the arms and their controllers were supposed to be safed. However, the COTS computers had a wake-on-LAN function. The internal security folks ran nmap with ping and happened to include the robotics labs' LAN. The PC woke up, automatically ran the robotics control program, and the arm extended to full length and swung around its full arc. This was witnessed by workers in the lab who, fortunately, were behind the red line.

...so far, we assumed the attacker has already compromised the controller...

… let's compromise the controller!


End Effector
IRC5 Control Unit
SMB
IRB 140
contactor unit
drive unit
enable/speed/...
RS-485
axis computer (AXC)
panel board
VxWorks 5.x RTOS (PPC)
RS-485
RS-485
status LEDs
24V DS
e-stop
24V DS
motors on/off
24V DS
auto / manual
24V digital signal
I/O board
DeviceNet
main computer (MC)
FTP, RobAPI, ...
VxWorks 5.x RTOS (x86)
FlexPendant
Windows CE (ARM) .NET >=3.5
Ethernet
Ethernet (service port)
(LAN port)
factory LAN
service LAN
RS232
GPRS
service net (vendor)
Ethernet (WAN)
RobotStudio
Service Box

Wearing the pentester's hat



- Statically-linked RTOS
- Custom peripherals
  - No fuzzing :(
- Firmware online or MMC
  - yay, with symbols!
- Simulator for Windows
  - "Virtual controller"
  - Not an exact replica

User Authorization System

User $\in$ roles $\rightarrow$ grants

Authentication: username + password

Used for FTP, RobAPI, …

By the way, documentation seems to advise against changing the default user's permissions

Let's boot!

- How do you update such a complex system?
  - Just update the main computer's MMC!
  - Other components (teach pendant, axis computer) fetch their software via FTP at boot.

- FTP? Credentials? Any credential **is OK** during boot!

- No integrity check on firmware, no signatures, nothing

ABBVU-DMRO-124644

Autoconfiguration is magic!

Service box auto-configures itself via FTP

Hard-coded FTP credentials (again…)

They're restricted to `/command`

ABBVU-DMRO-124642

Enter `/command`

FTP GET `/command/whatever` read, e.g., env. vars

FTP PUT `/command/file` execute “commands”

ABBVU-DMRO-124642

Enter `/command`

FTP GET `/command/whatever` read, e.g., env. vars

FTP PUT `/command/file` execute “commands”

```
shell reboot
shell uas_disable
```

Pair this with the default, hard-coded credentials for WAN access → **remote command execution**.

ABBVU-DMRO-124642

Enter /command

There's more! Let's look at **`cmddev_execute_command`**:

`shell` → **`sprintf(buf, "%s", param)`**

other commands → **`sprintf(buf, "cmddev_%s", arg)`**

tl;dr; whatever the command is, **we overflow `buf`**, who is on the stack → **remote code execution**

ABBVU-DMRO-128238

Other buffer overflows

Ex. 1: RobAPI

- Unauthenticated API endpoint
- Unsanitized `strcpy()`

→ **remote code execution**

Ex. 2: Flex Pendant (`TpsStart.exe`)

- FTP write `/command/timestampAAAAAAA.....AAAAAAA`
- file name > 512 bytes ~> Flex Pendant DoS

ABBVU-DMRO-124641, ABBVU-DMRO-124645

Takeaways

Mostly **logical vulnerabilities**

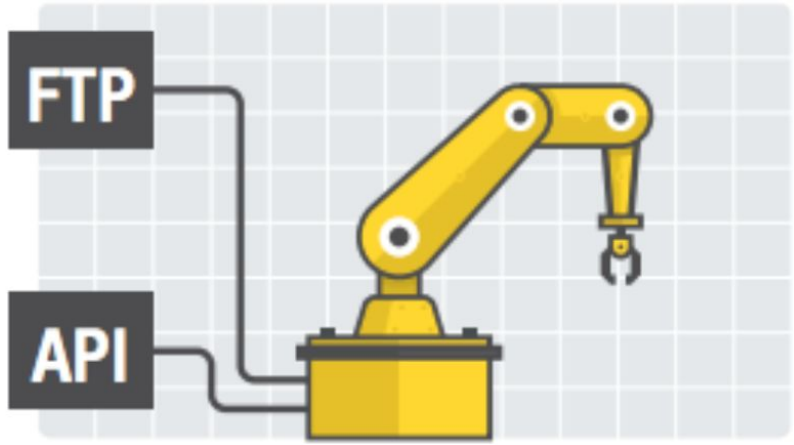
Some **memory corruption**

All the components blindly **trust** the **main computer (lack of isolation)**

Complete attack chain (1)

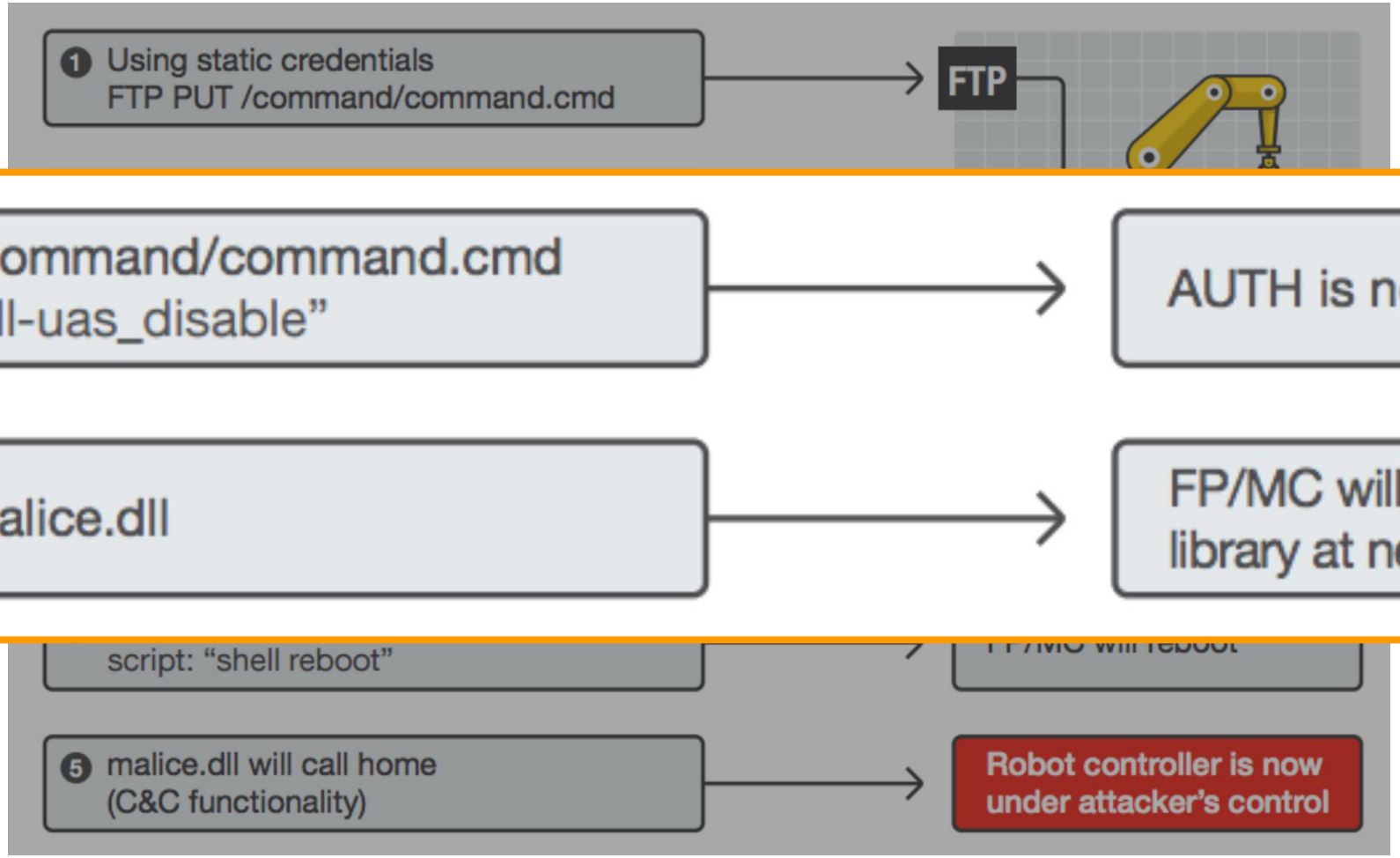
1. Using static credentials
   FTP PUT /command/command.cmd

1. (Alternatively) DHROOT RobAPI request
   (no auth) with buffer overflow exploit

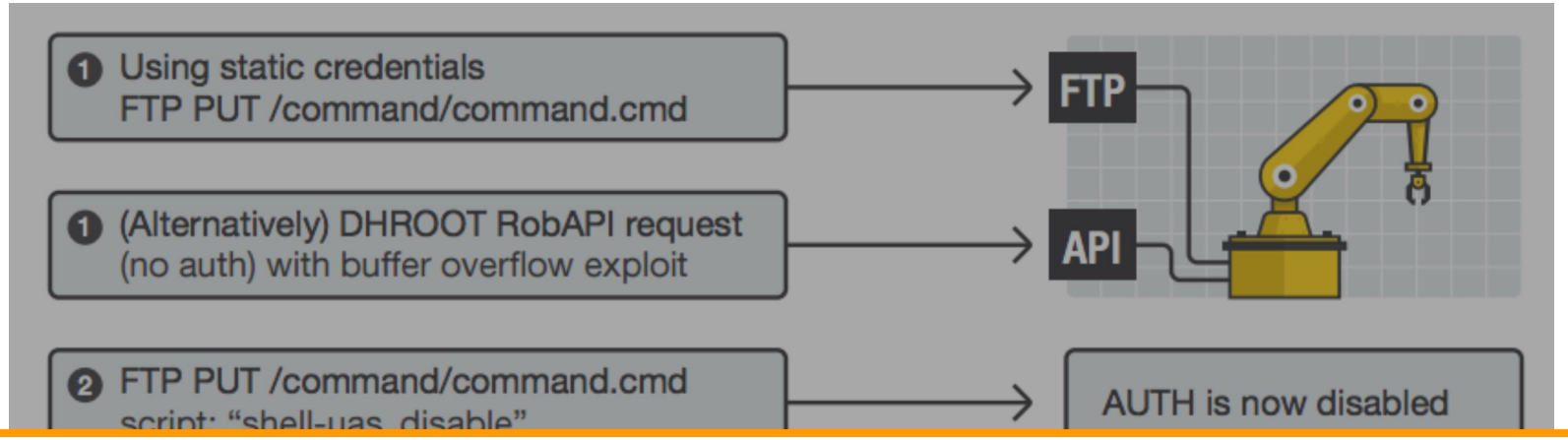


3. FTP PUT malice.dll → FP/MC will load malicious library at next boot
4. FTP PUT /command/command.cmd
   script: "shell reboot" → FP/MC will reboot
5. malice.dll will call home
   (C&C functionality) → **Robot controller is now under attacker's control**

Complete attack chain (2)



Complete attack chain (3)



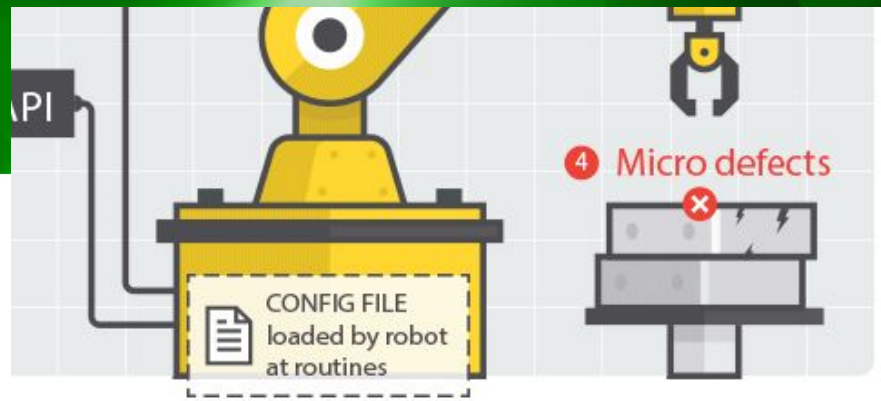
4 FTP PUT /command/command.cmd
script: "shell reboot"

FP/MC will reboot

5 malice.dll will call home
(C&C functionality)

Robot controller is now under attacker's control

File protection



“Sensitive” files:

- Users’ credentials and permissions
- Sensitive configuration parameters (e.g., PID)
- Industry secrets (e.g., workpiece parameters)

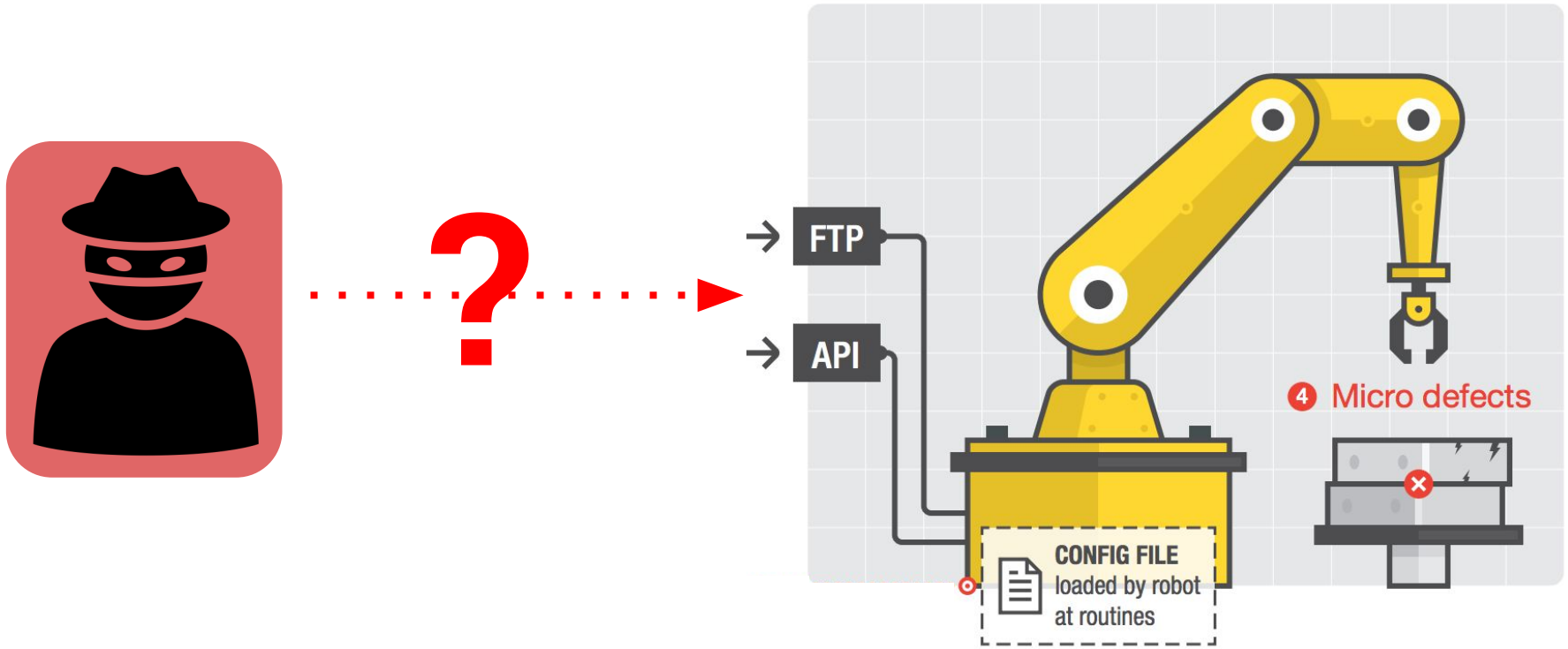
Obfuscation: bitwise XOR with a random key.

Key is derived from the file name. Or from the content. Or …

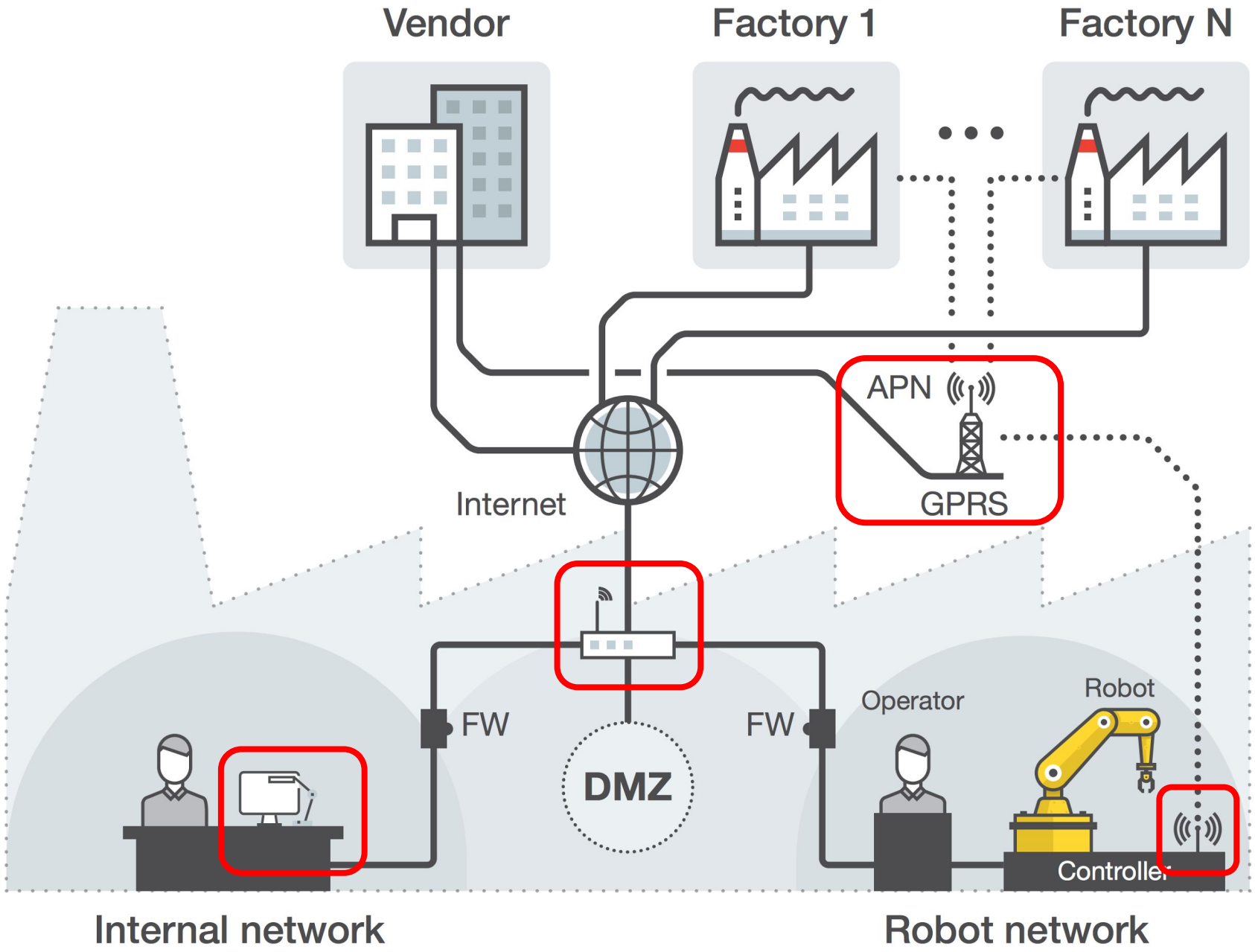
black hat USA 2017

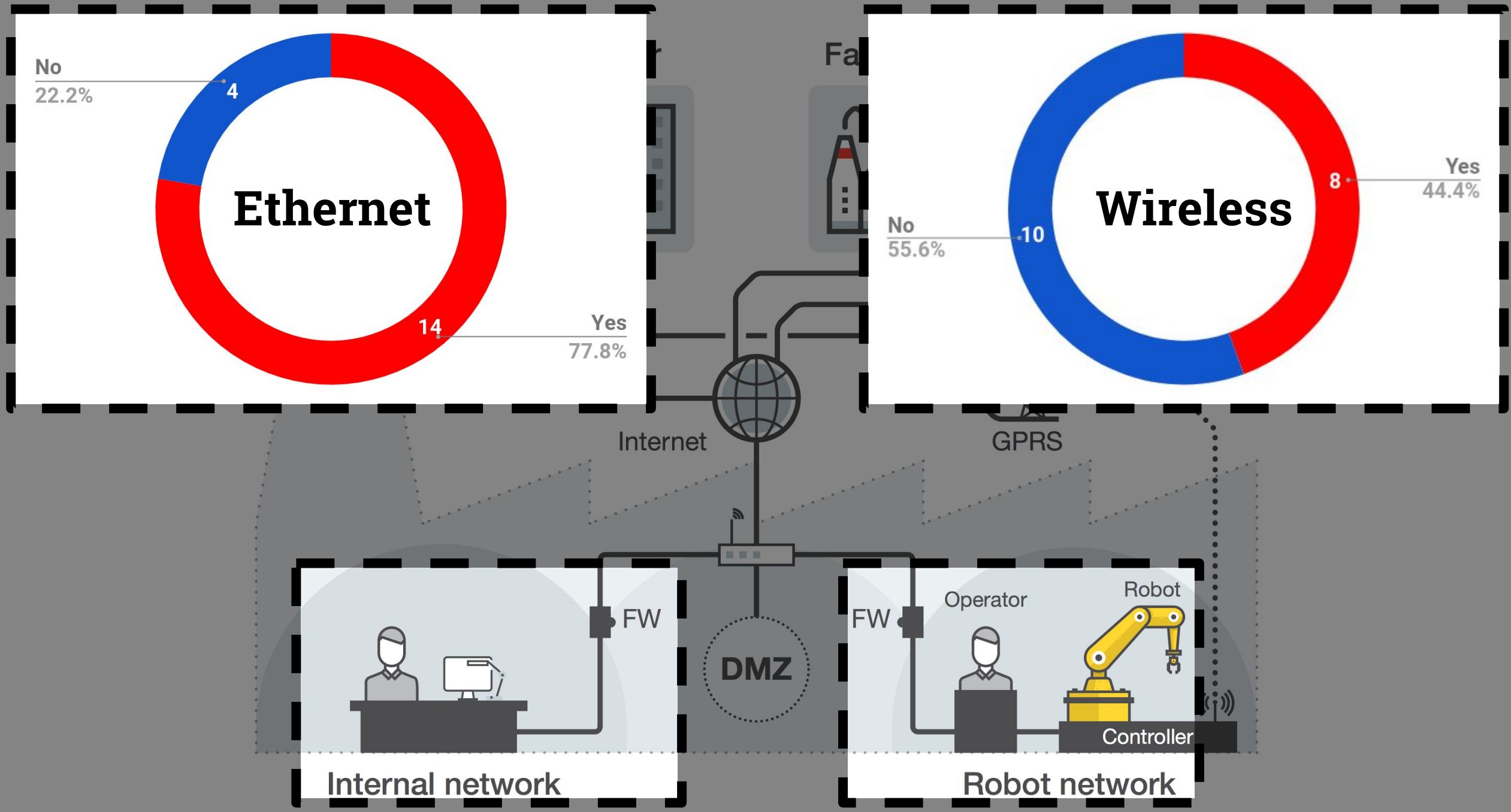
That's how we implemented the attacks

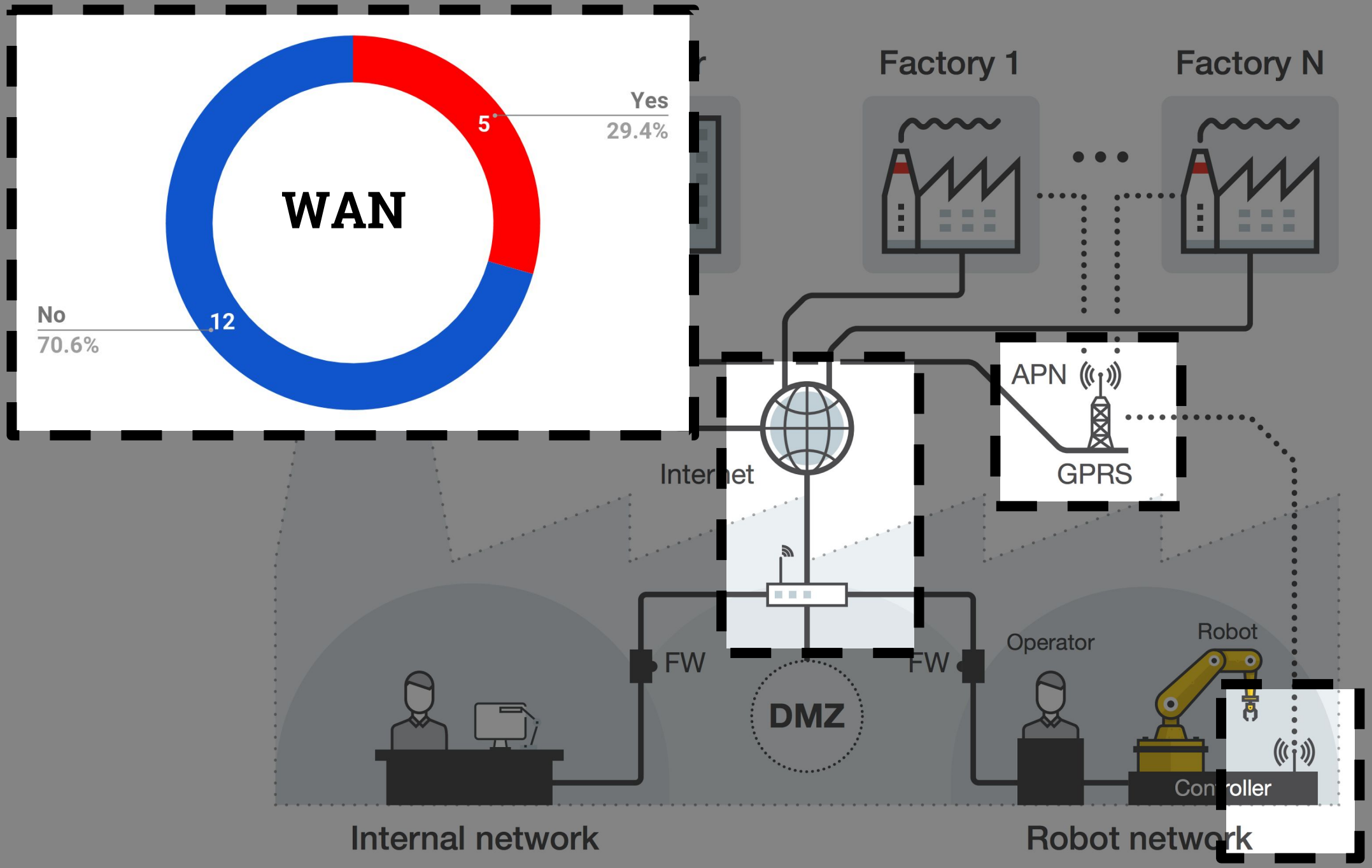
Attack Surface



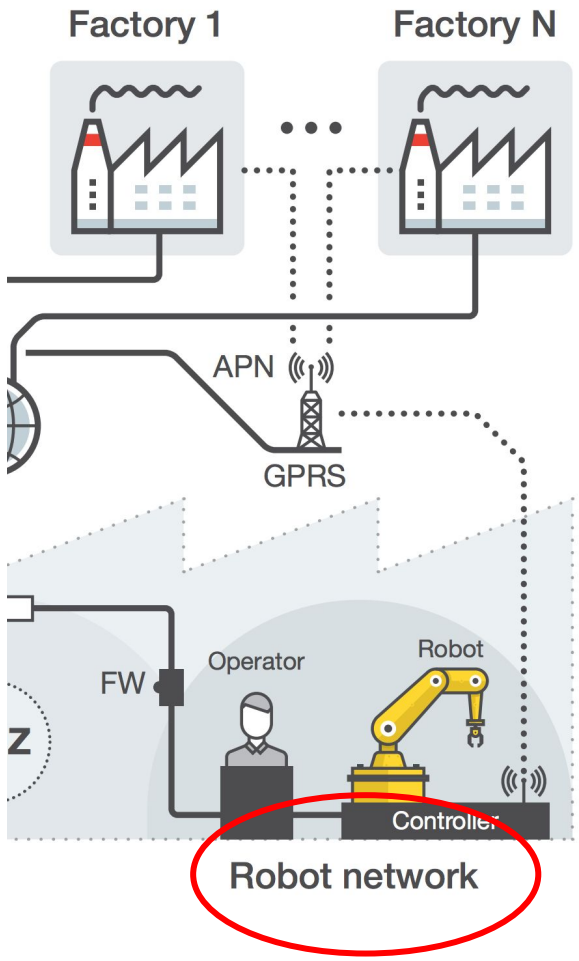
Flexibly programmable
&
Connected
(Part 2)


Vendor
Factory 1
Factory N
APN
GPRS
Internet
FW
FW
DMZ
Operator
Robot
Controller
Internal network
Robot network


No
22.2%
4
Ethernet
14
Yes
77.8%
No
55.6%
10
Wireless
8
Yes
44.4%
Internet
GPRS
FW
DMZ
Internal network
FW
Operator
Robot
Controller
Robot network


WAN
Yes
29.4%
5
No
70.6%
12
Factory 1
Factory N
APN
GPRS
Internet
FW
FW
DMZ
Operator
Robot
Controller
Internal network
Robot network

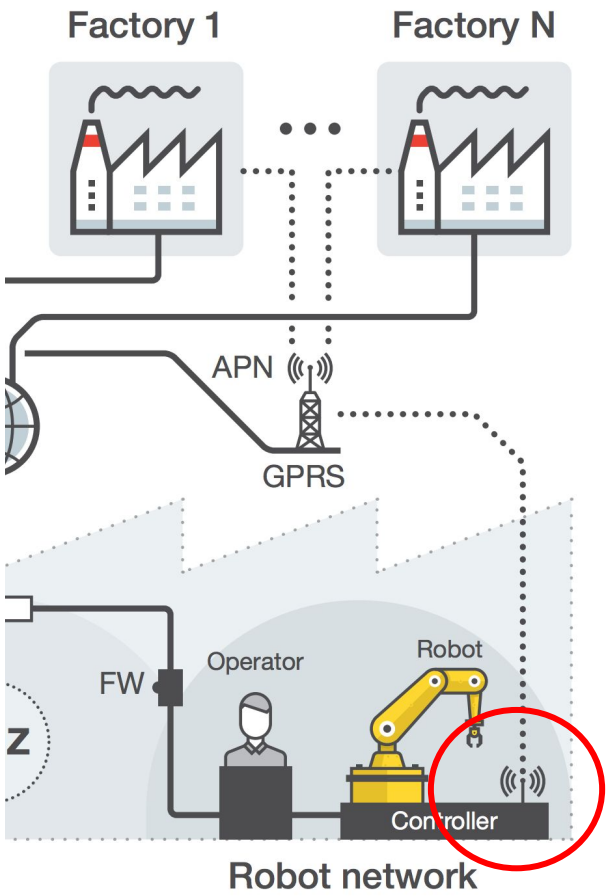
Remote Exposure of Industrial *Robots*



Search	Entries	Country
ABB Robotics	5	DK, SE
FANUC FTP	9	US, KR, FR, TW
Yaskawa	9	CA, JP
Kawasaki E Controller	4	DE
Mitsubishi FTP	1	ID
Overall	**28**	**10**

Not so many…

Remote Exposure of Industrial *Routers*



Brand	Exposed Devices	No Authentication
Belden	956	
Eurotech	160	
eWON	6,219	1,160
Digi	1,200	
InHand	883	
Moxa	12,222	2,300
NetModule	886	135
Robustel	4,491	
Sierra Wireless	50,341	220
Virtual Access	209	
Welotec	25	
Westermo	6,081	1,200
TOTAL	83,673	5,105

...way many more!

Unknown which routers are actually robot-connected

Typical Issues

Information Disclosure and "Fingerprintability"

- Verbose banners (beyond brand or model's name)
- Detailed technical material on vendor's website
  - Technical manual: All vendors inspected
  - Firmware: 7/12 vendors

If you have concerns or questions about this notice please contact our suppor
department via telephone at 801-765-9885 or visit us online at
http://www.digi.com/support/eservice/ to submit a request.

[redacted]

Added on 2017-07-12 10:26:48 GMT

United States

Details

[redacted] Ser#:[redacted]

Software Build Ver[redacted] Sep 24 2012 06:22:23 WW

ARM Bios Ver [redacted] v[redacted] 454MHz [redacted],0 MAC:[redacted]

Typical Issues (1)

Outdated Software Components

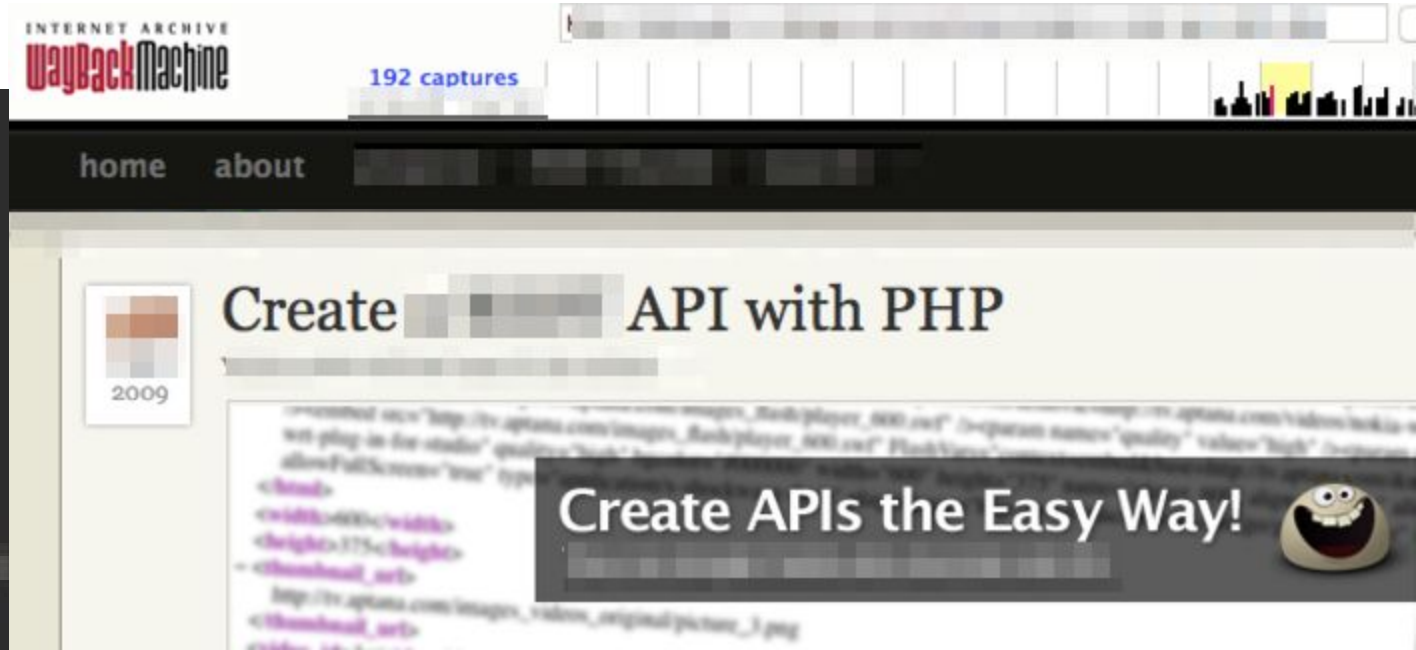
- Application software (e.g., DropBear SSH, BusyBox)
- Libraries (including crypto libraries)
- Compiler & kernel
- Baseband firmware

Typical Issues (2)

Insecure Web Interface

- Poor input sanitization
- E.g., code coming straight from a "beginners" blog

```
19  switch ($request_method)
20  {
21    //
22    case 'get':
23      $data = $_GET;
24      break;
25      //
26    case 'post':
27
28      $data = array_merge($_GET, $_POST);
```



Bottom line

Connect your robots with care

Conclusions

Black Hat Sound Bytes

Robots are increasingly being **connected**

Robot-specific class of attacks

Barrier to entry: **quite high**, budget-wise

What should we do now?

Vendors are very **responsive**

As a **community** we really need
to **push hard for countermeasures**

Hints on Countermeasures

Short term

Attack detection and deployment hardening

Medium term

System hardening

Long term

New standards, beyond safety issues

black hat USA 2017

Questions?

Davide Quarta
davide.quarta@polimi.it
@_ocean

Marcello Pogliani
marcello.pogliani@polimi.it
@mapogli

Federico Maggi
federico_maggi@trendmicro.com
@phretor

Papers, slides, and FAQ @ **robosec.org**

TREND MICRO™

POLITECNICO MILANO 1863

DIPARTIMENTO DI ELETTRONICA INFORMAZIONE E BIOINGEGNERIA

Breaking the Laws of Robotics
Attacking Industrial Robots

Davide Quarta, **Marcello Pogliani**, Mario Polino, **Federico Maggi**,
Andrea M. Zanchettin, Stefano Zanero