black hat USA 2017

JULY 22-27, 2017

MANDALAY BAY / LAS VEGAS

TREND MICRO

POLITECNICO MILANO 1863

DIPARTIMENTO DI ELETTRONICA
INFORMAZIONE E BIOINGEGNERIA

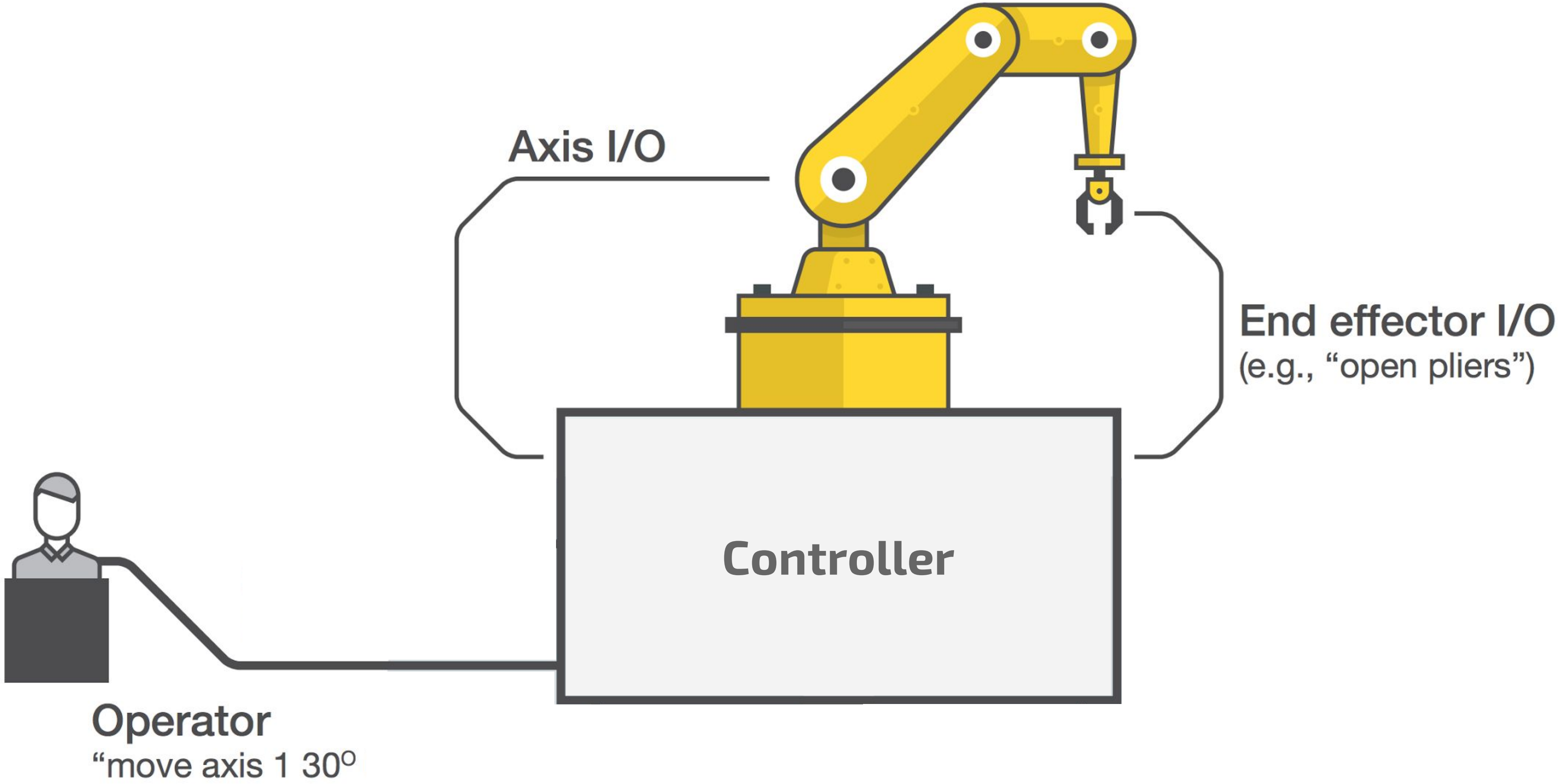
Breaking the Laws of Robotics

Attacking Industrial Robots

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

Industrial robots?

Industrial Robot Architecture (Standards)

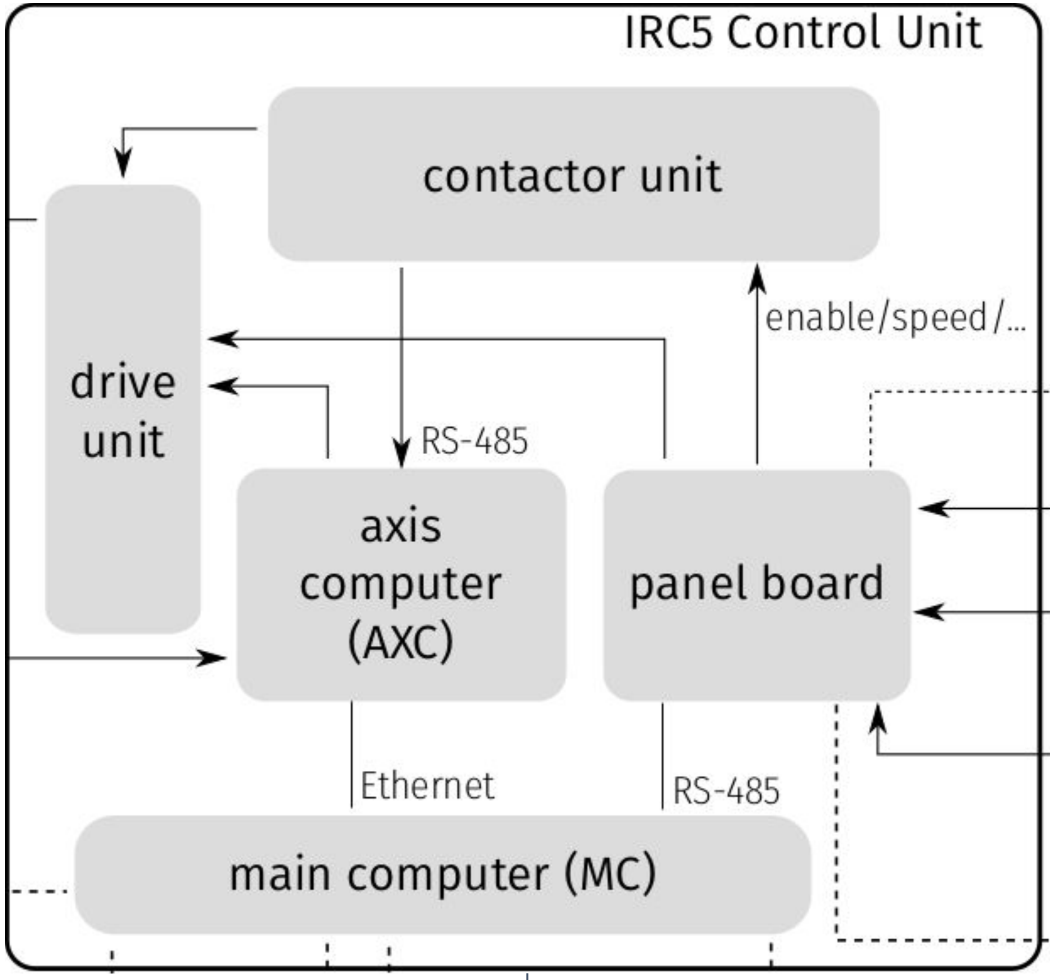


Axis I/O

End effector I/O
(e.g., “open pliers”)

Controller

Operator
“move axis 1 30^{o}



IRC5 Control Unit

contactor unit

drive unit

enable/speed/...

RS-485

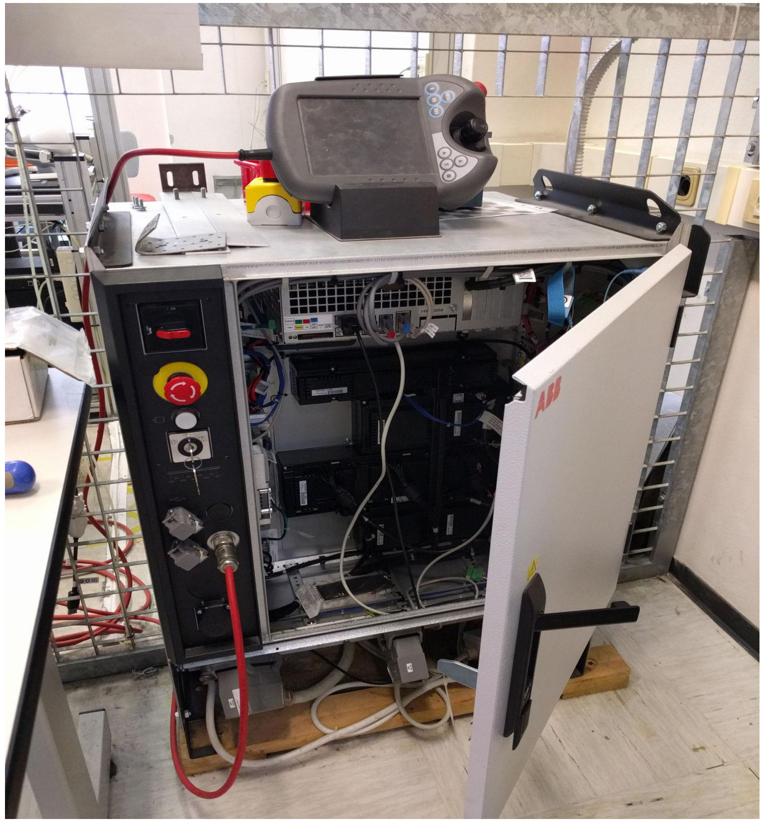
axis computer (AXC)

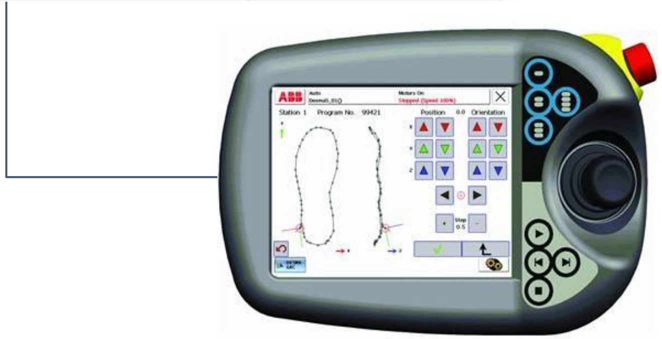
panel board

Ethernet

RS-485

main computer (MC)

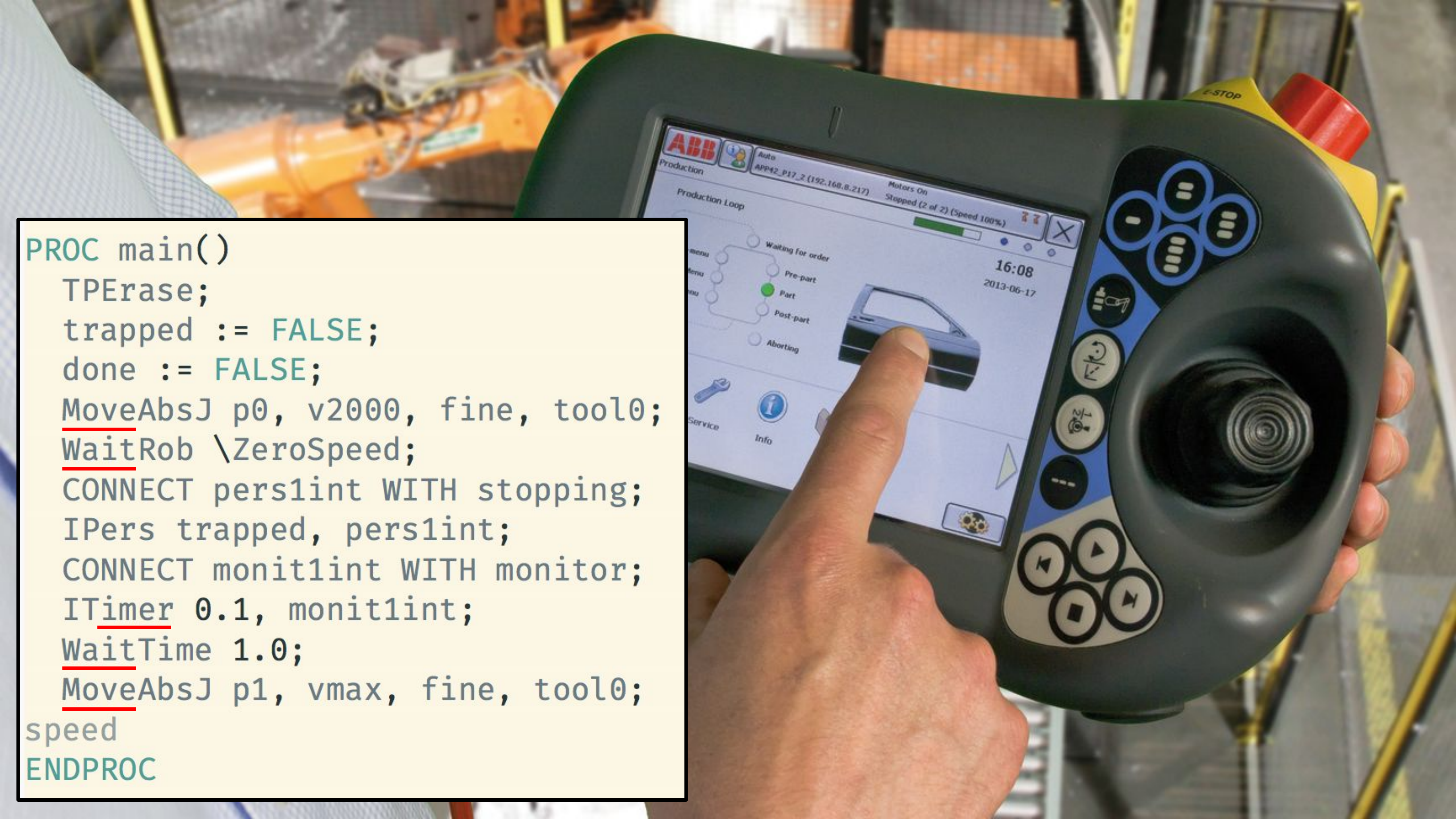




Flexibly programmable

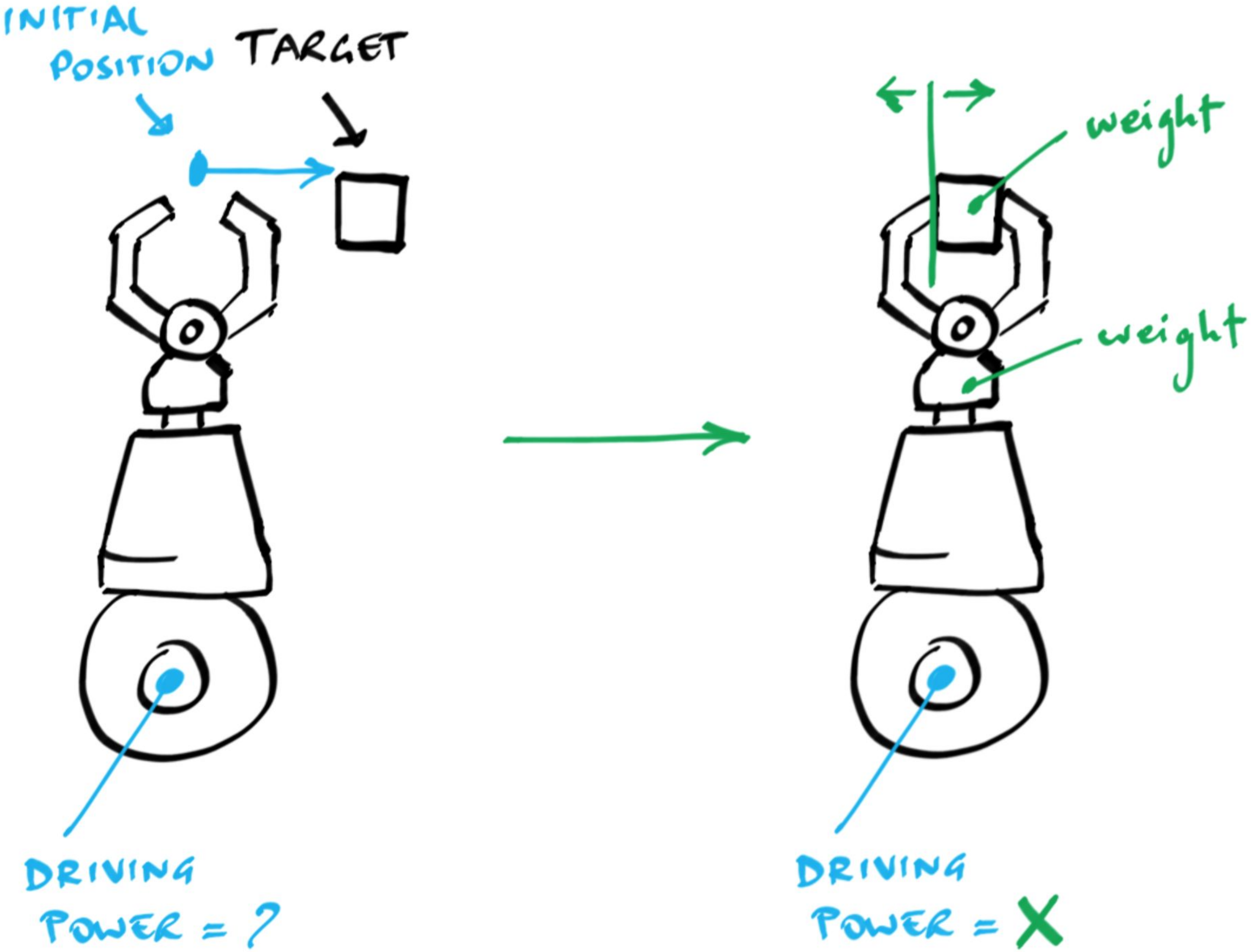
&

Connected



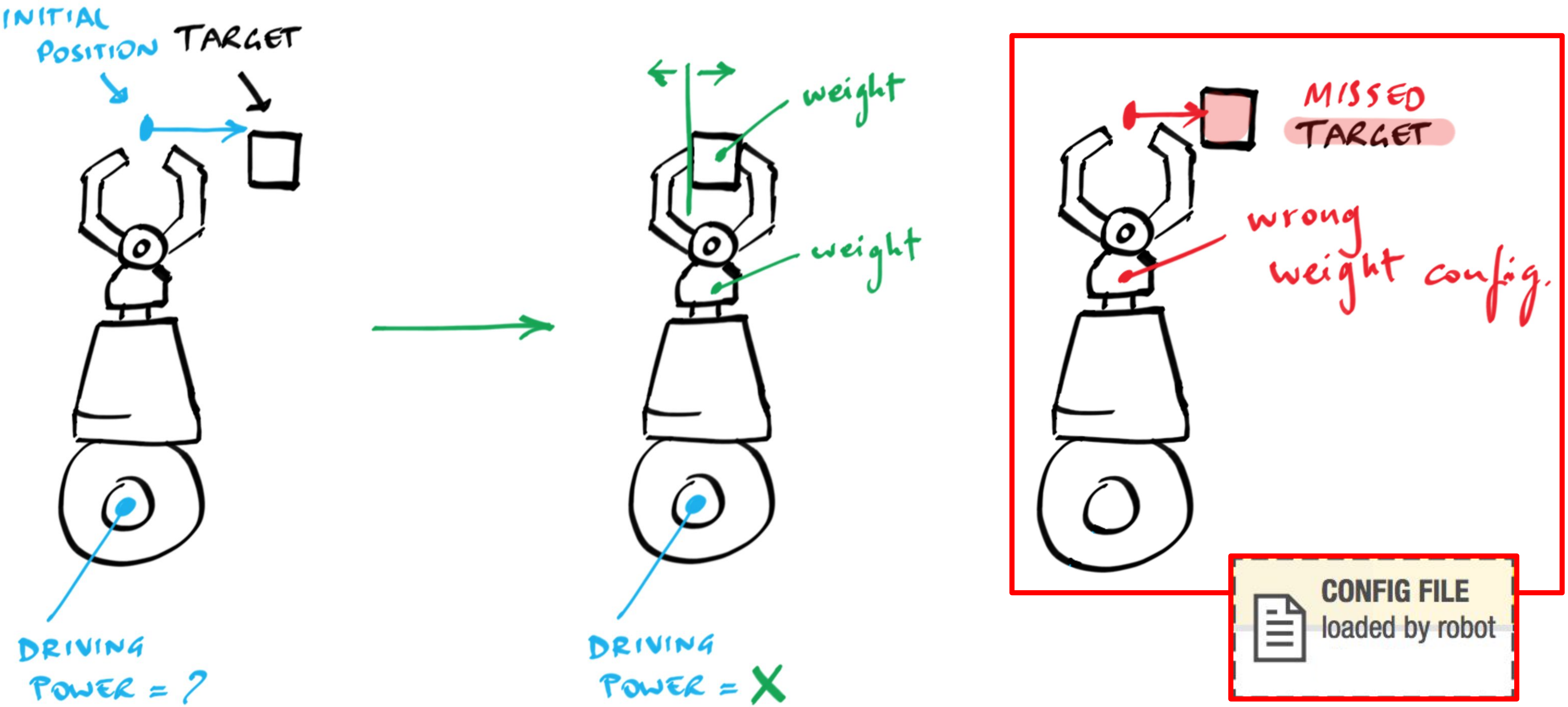
```
PROC main()
  TPErase;
  trapped := FALSE;
  done := FALSE;
  MoveAbsJ p0, v2000, fine, tool0;
  WaitRob \ZeroSpeed;
  CONNECT pers1int WITH stopping;
  IPers trapped, pers1int;
  CONNECT monit1int WITH monitor;
  ITimer 0.1, monit1int;
  WaitTime 1.0;
  MoveAbsJ p1, vmax, fine, tool0;
speed
ENDPROC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

“Implicit” parameters



CONFIG FILE
loaded by robot

“Implicit” parameters



CONFIG FILE
loaded by robot

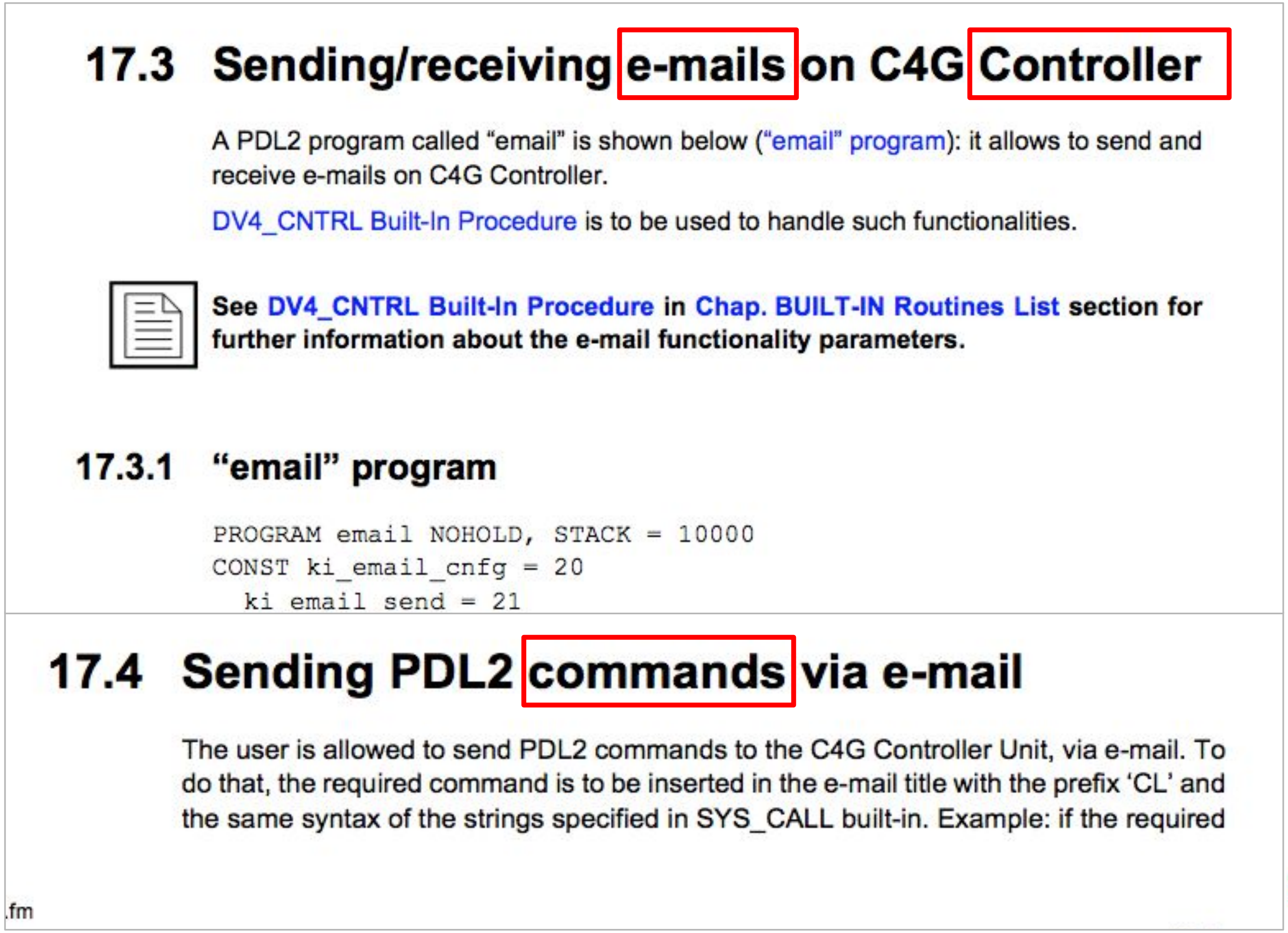
Flexibly programmable

&

Connected

(Part 1)

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

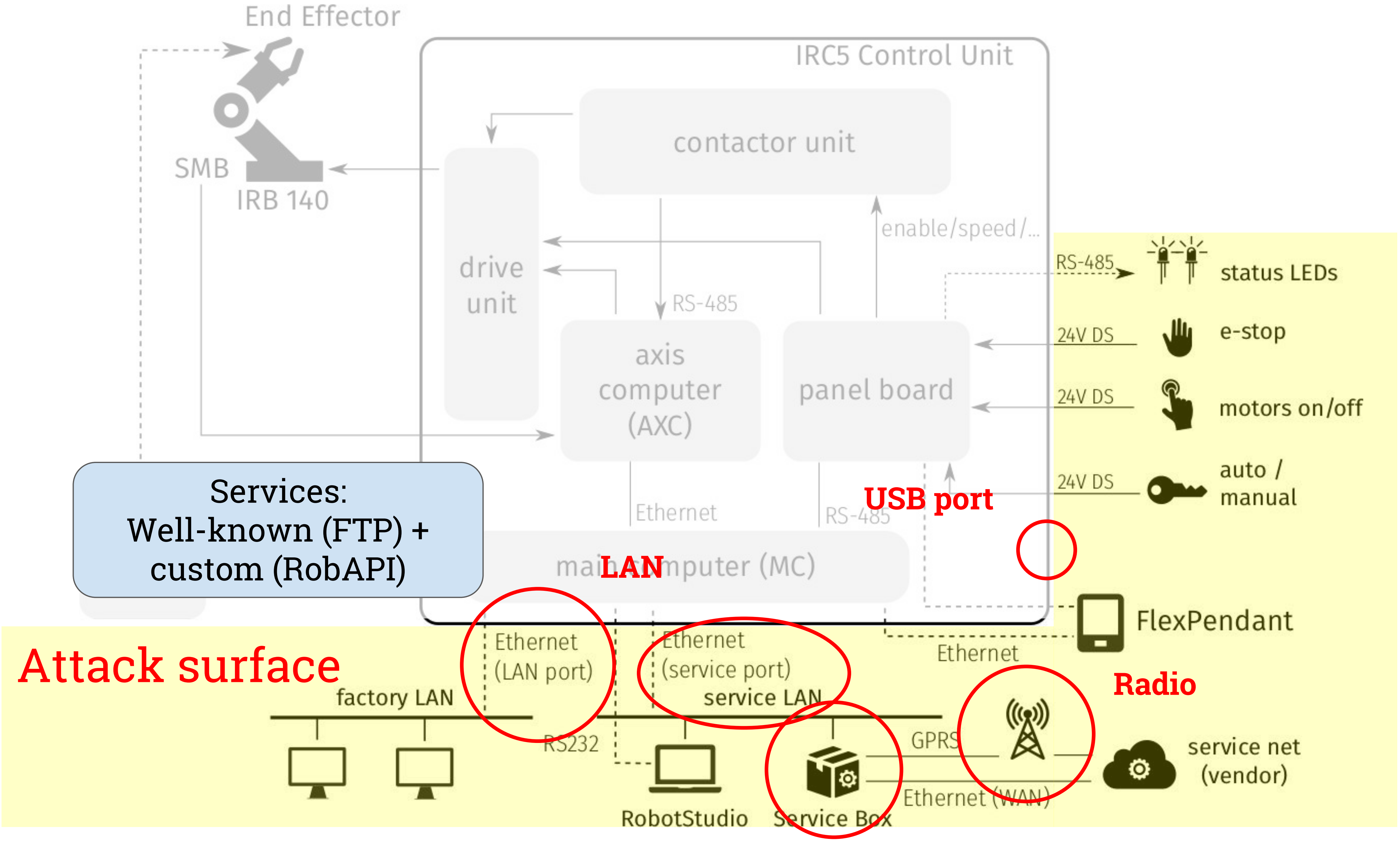
The user is allowed to send PDL2 commands to the C4G Controller Unit, via e-mail. To do that, the required command is to be inserted in the e-mail title with the prefix 'CL' and the same syntax of the strings specified in SYS_CALL built-in. Example: if the required

.fm

COMAU ROBOTICS

Services:
Well-known (FTP) +
custom (RobAPI)

Attack surface



Connected Robots: Why?

- **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?

Connected?

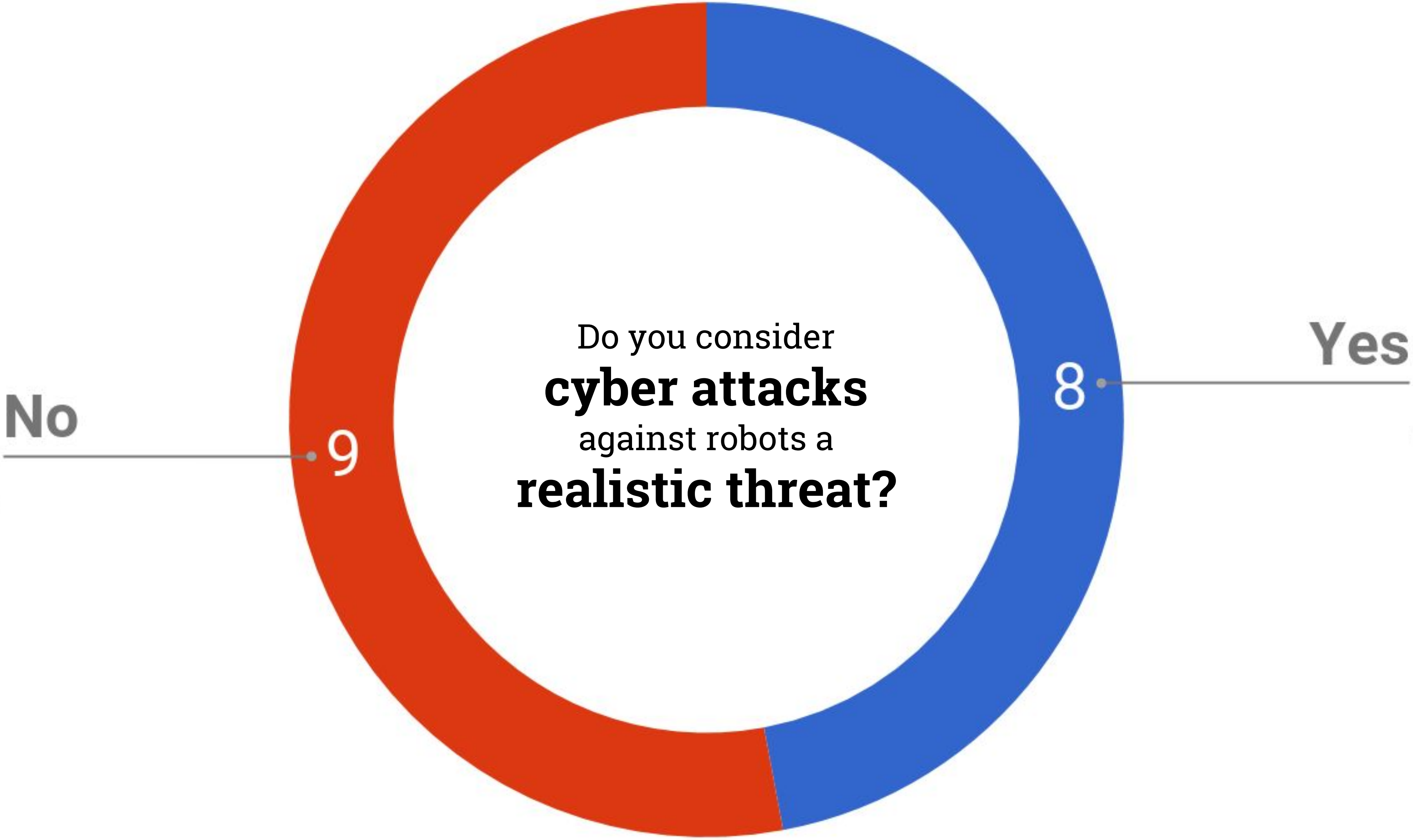
↓

Do you consider

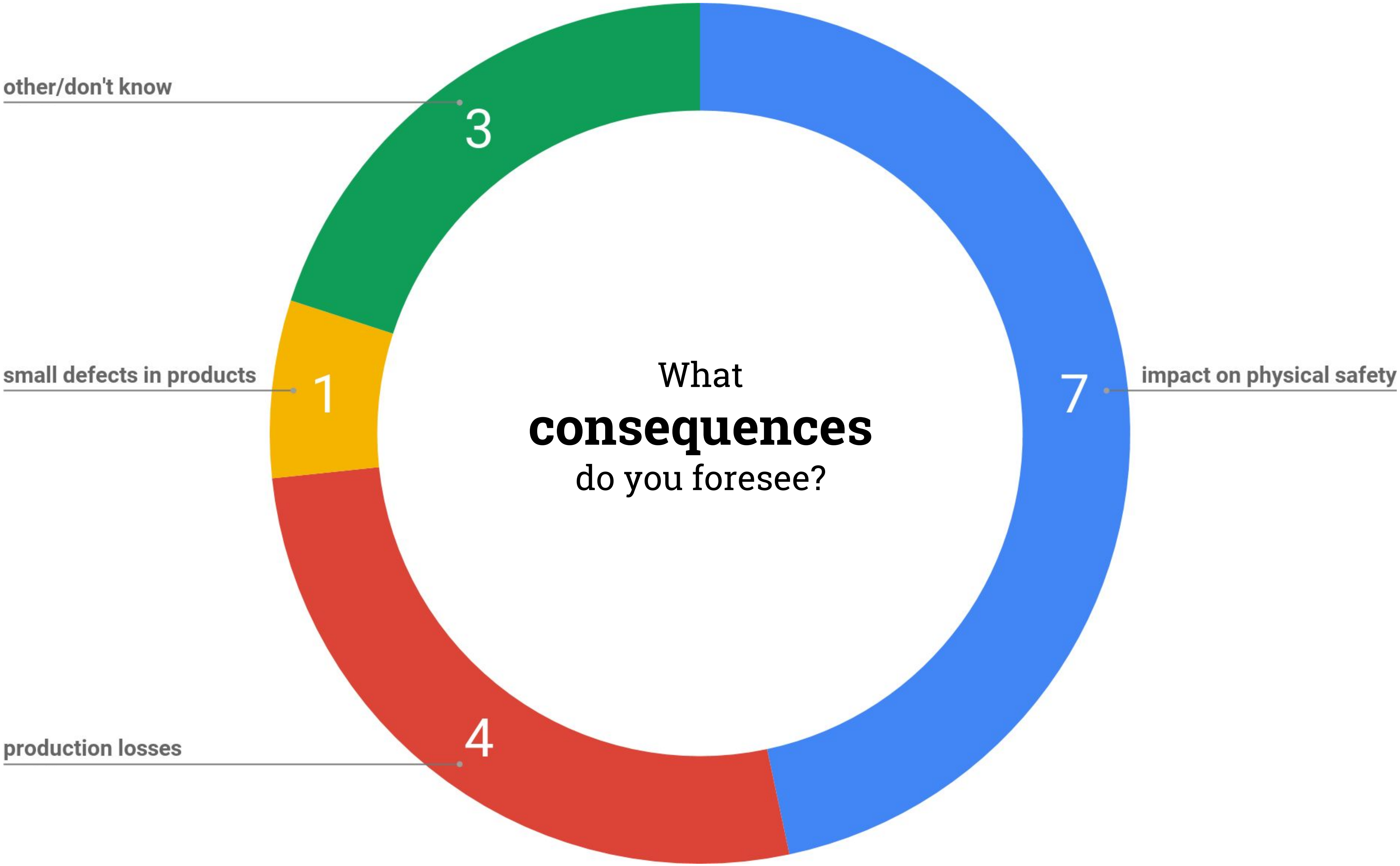
cyber attacks

against robots a

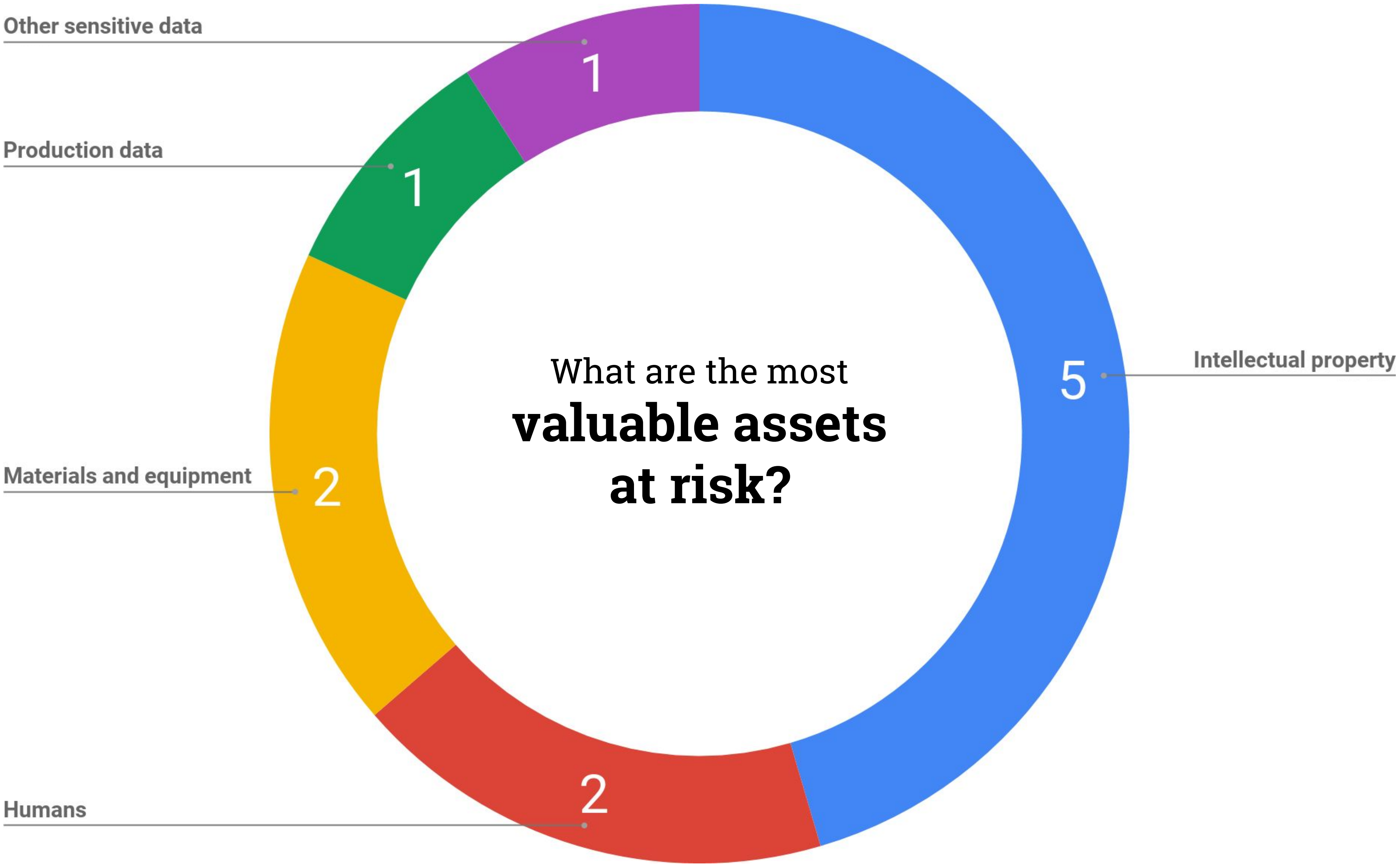
realistic threat?



Do you consider **cyber attacks** against robots a **realistic threat?**



What **consequences** do you foresee?



What are the most **valuable assets at risk?**

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

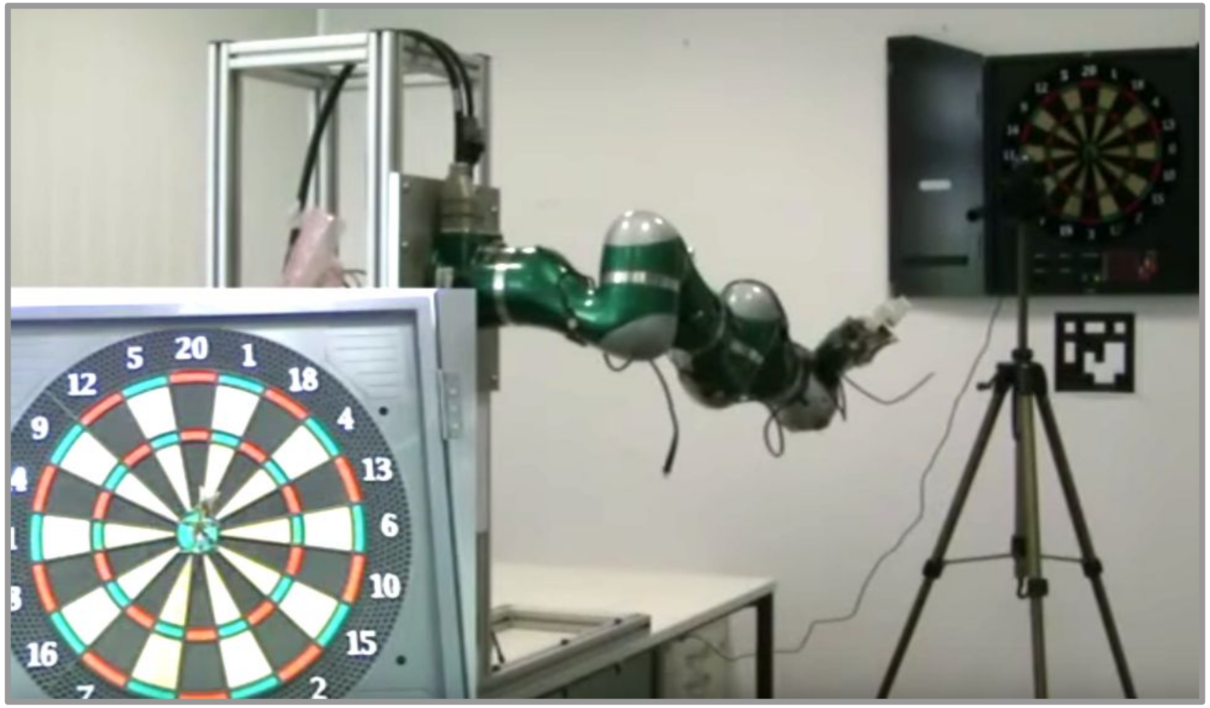
Integrity

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

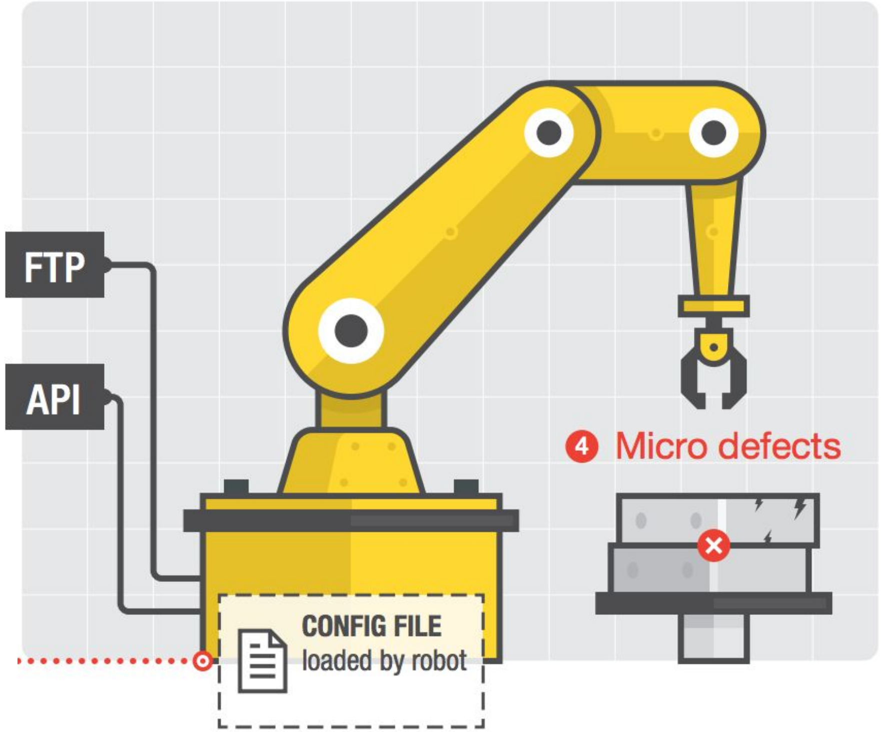
Robot-Specific Attack

Safety

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

Integrity

Control Loop Alteration



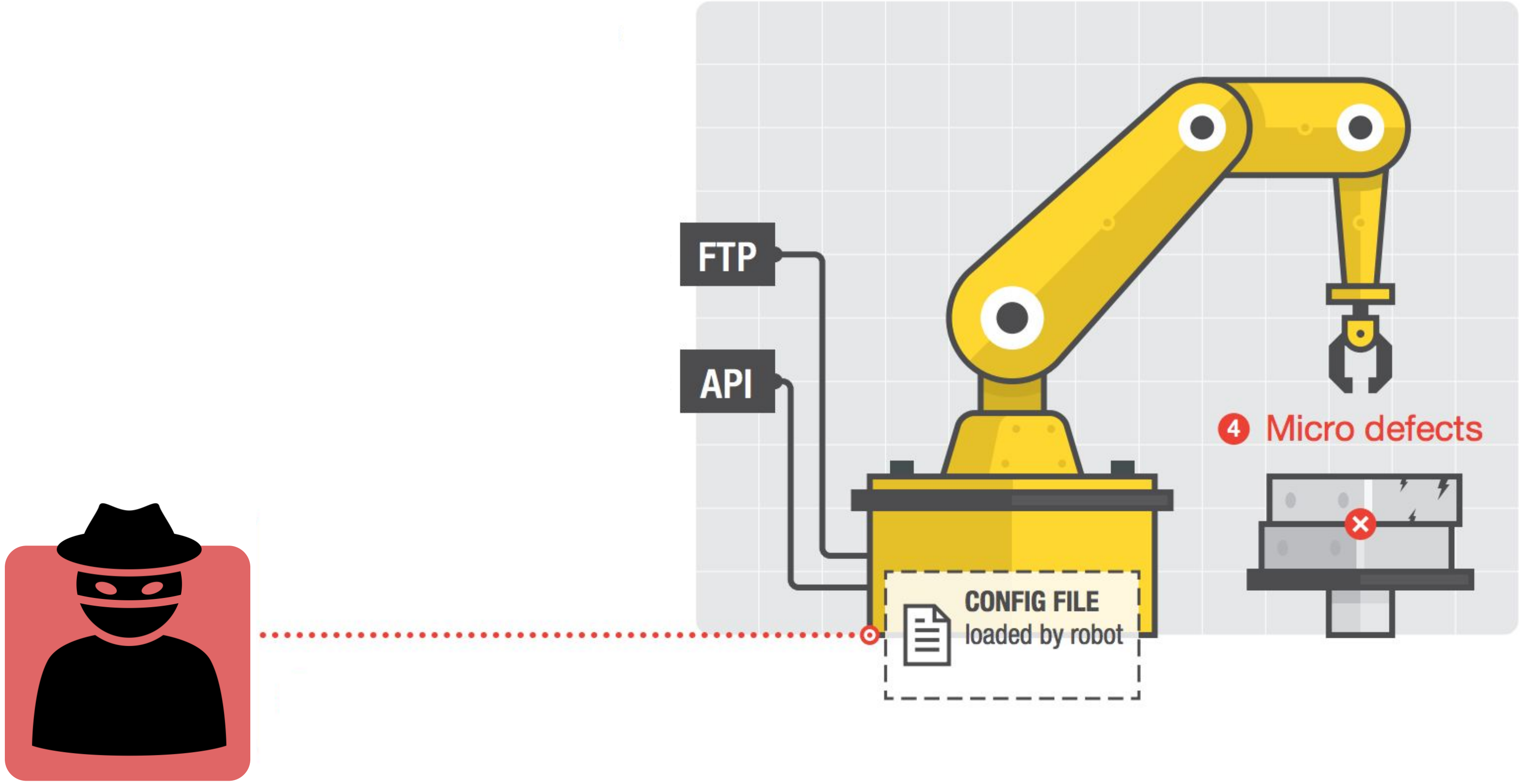
Attack 1

Safety

Accuracy

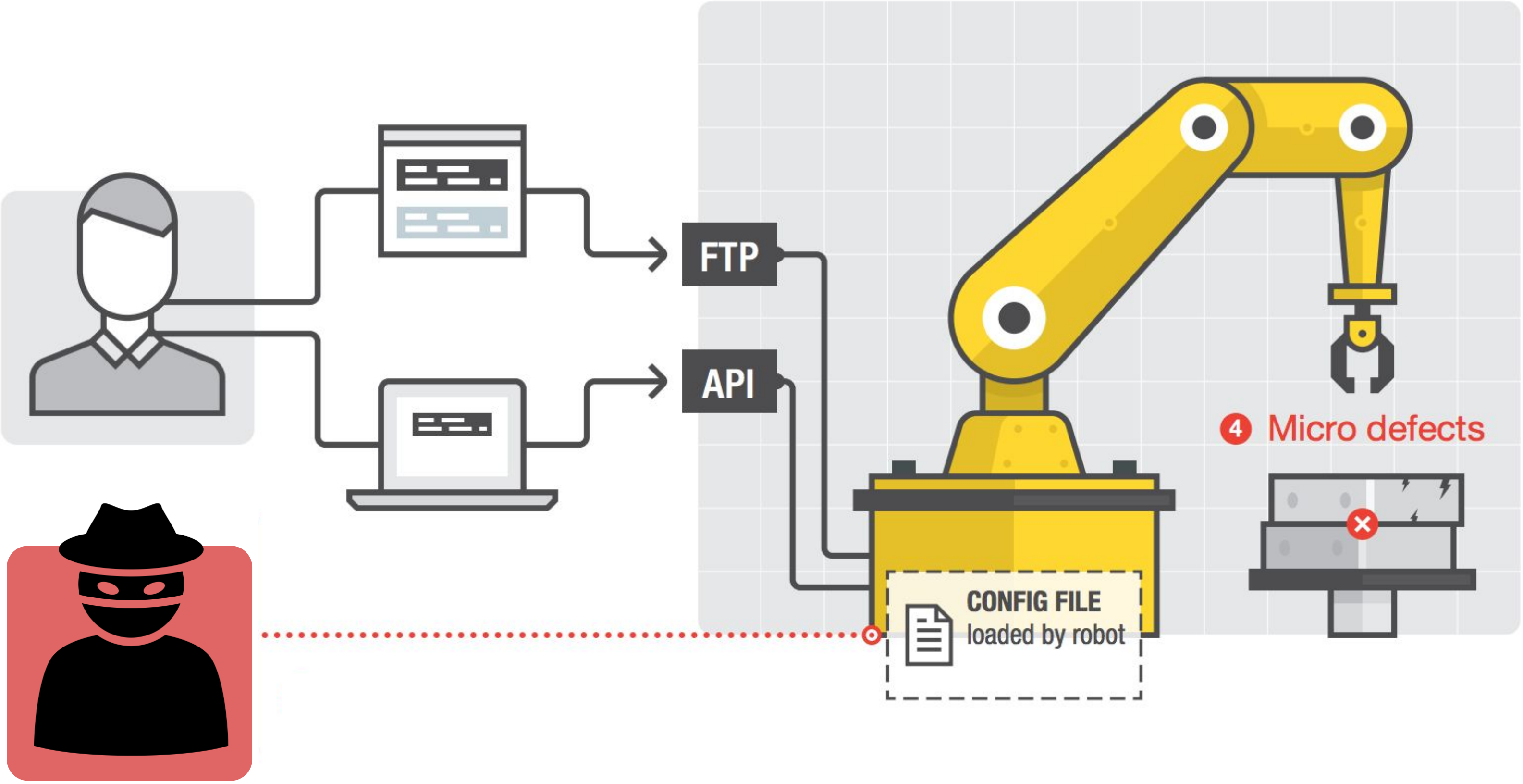
Integrity

Control Loop Alteration



Attack 1
Safety
Accuracy
Integrity

Control Loop Alteration



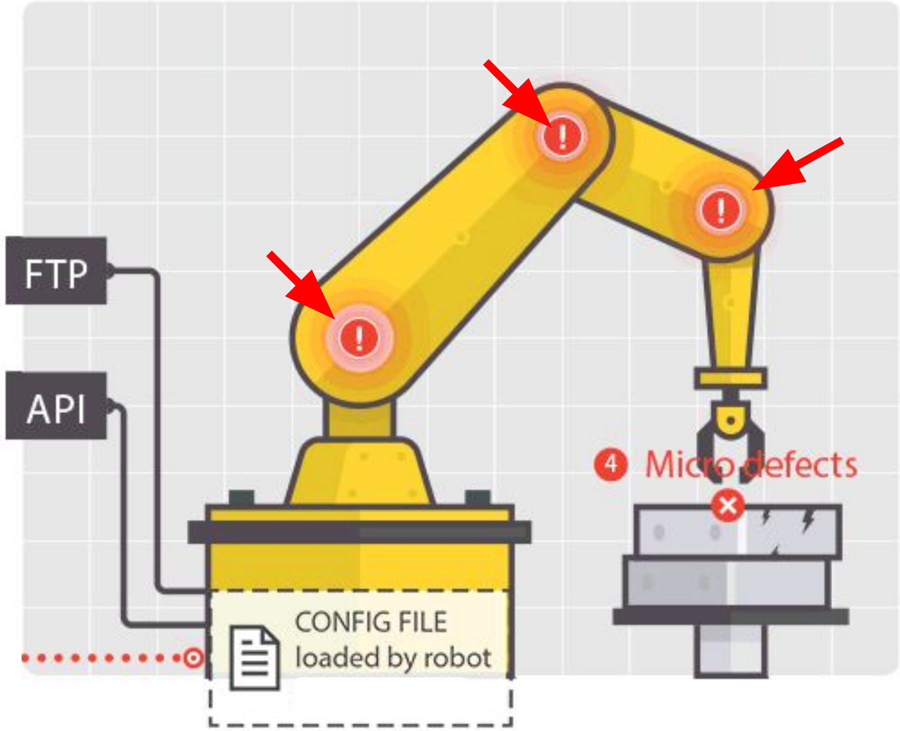
Attack 1

Safety

Accuracy

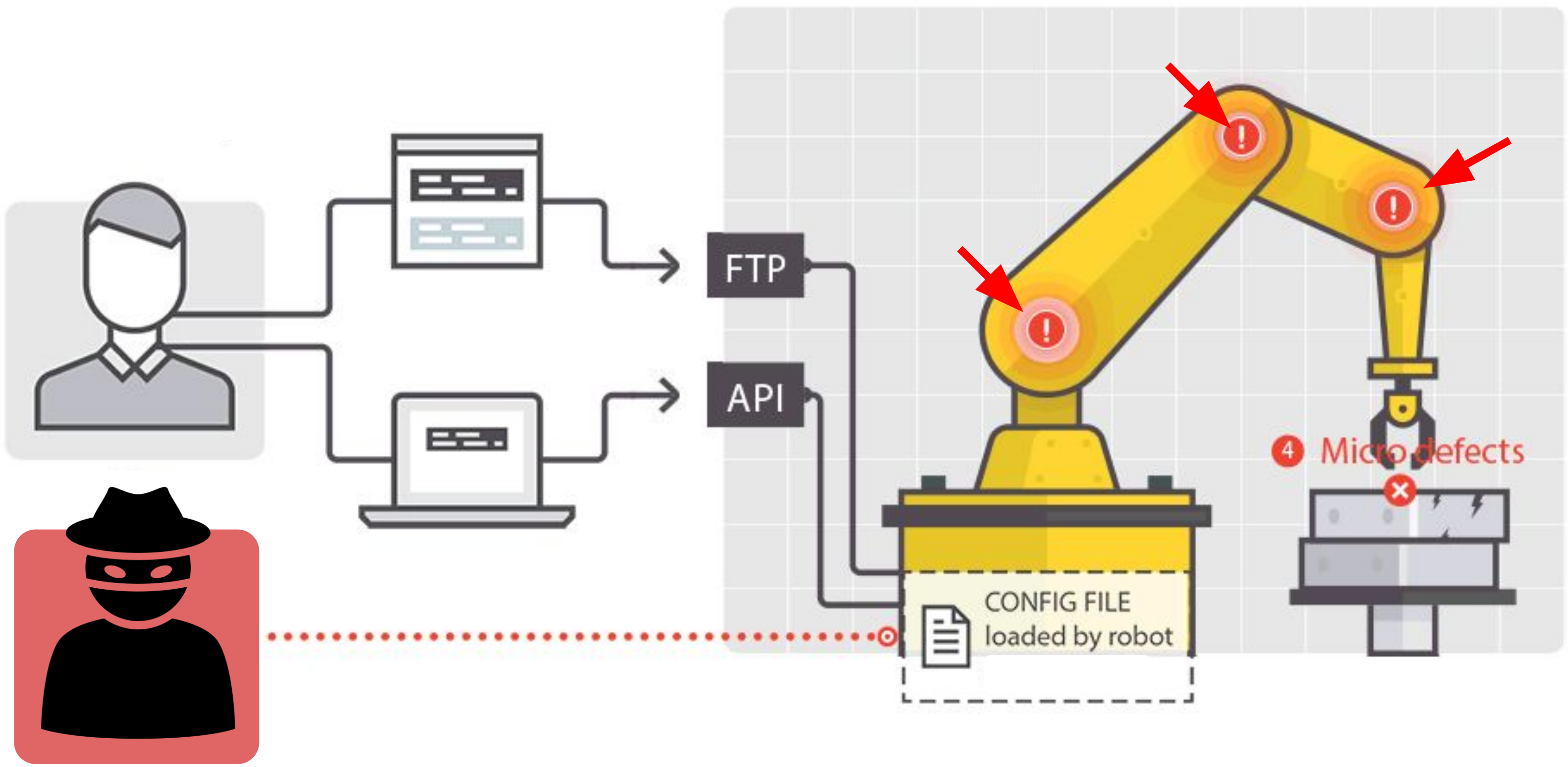
Integrity

Calibration Tampering



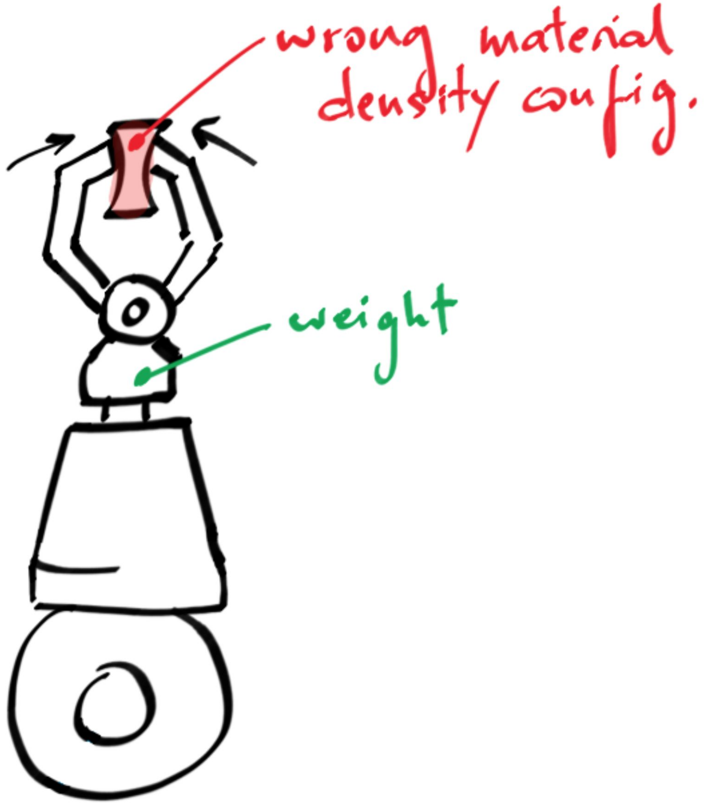
Attack 2
Safety
Accuracy
Integrity

Calibration Tampering



Attack 2
Safety
Accuracy
Integrity

Production Logic Tampering



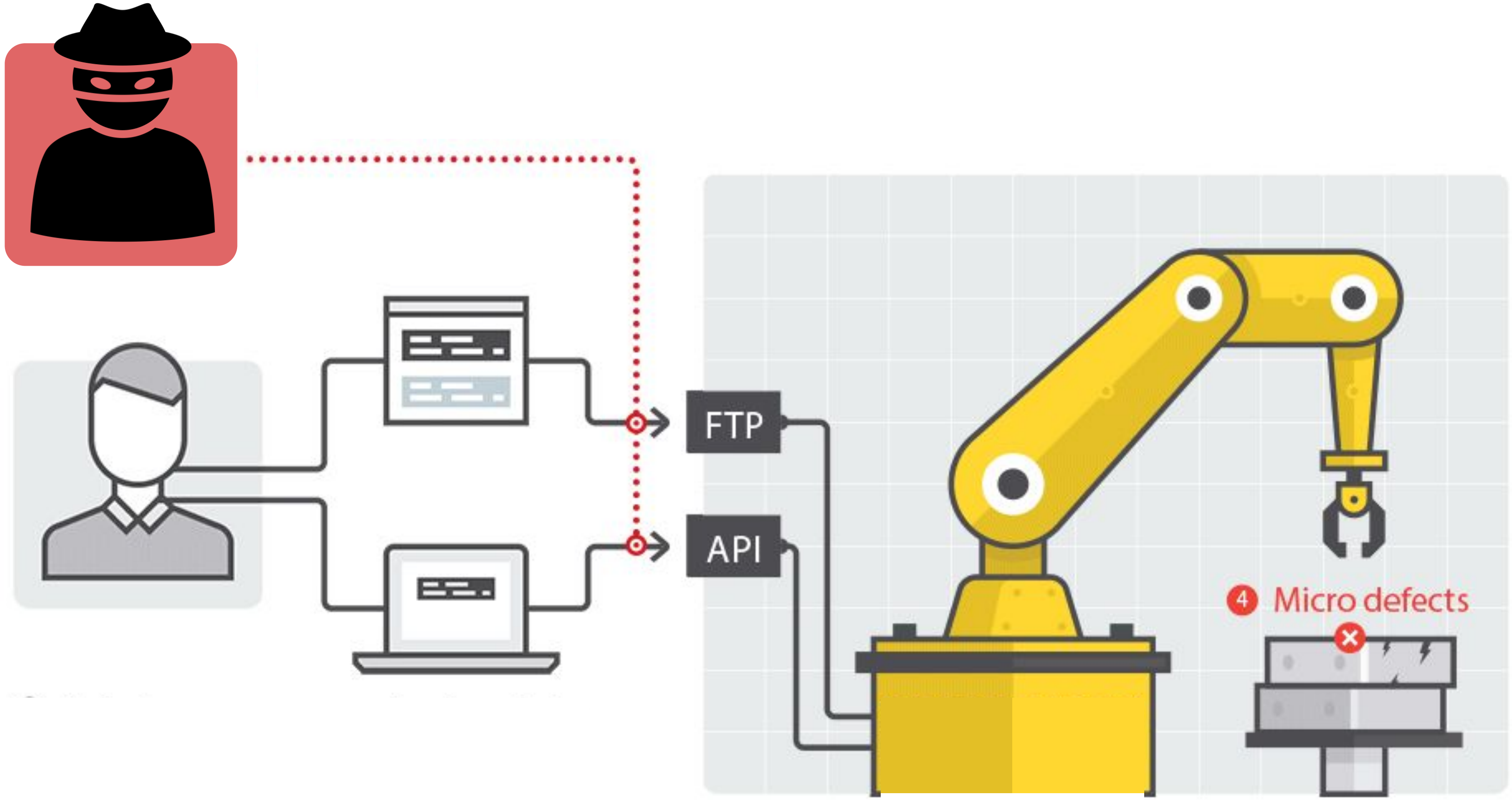
Attack 3

Safety

Accuracy

Integrity

Production Logic Tampering



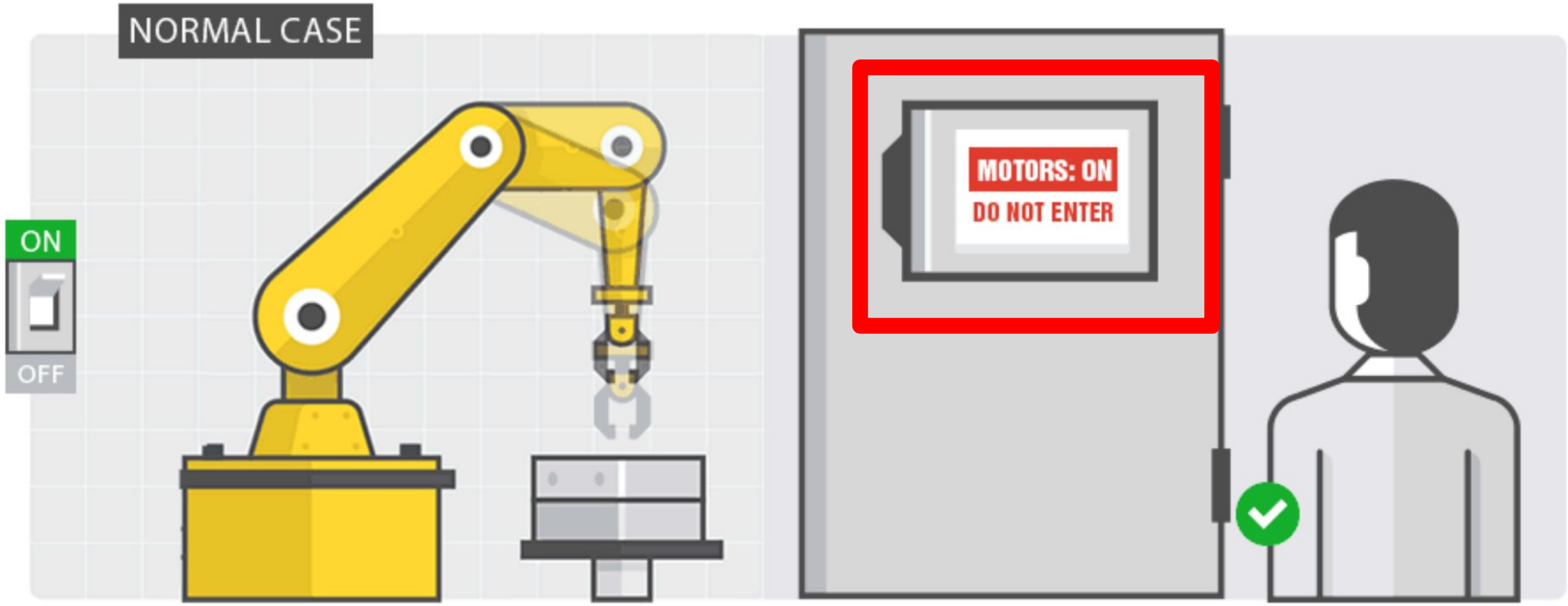
Attack 3

Safety

Accuracy

Integrity

Displayed or Actual State Alteration



Operator is safe

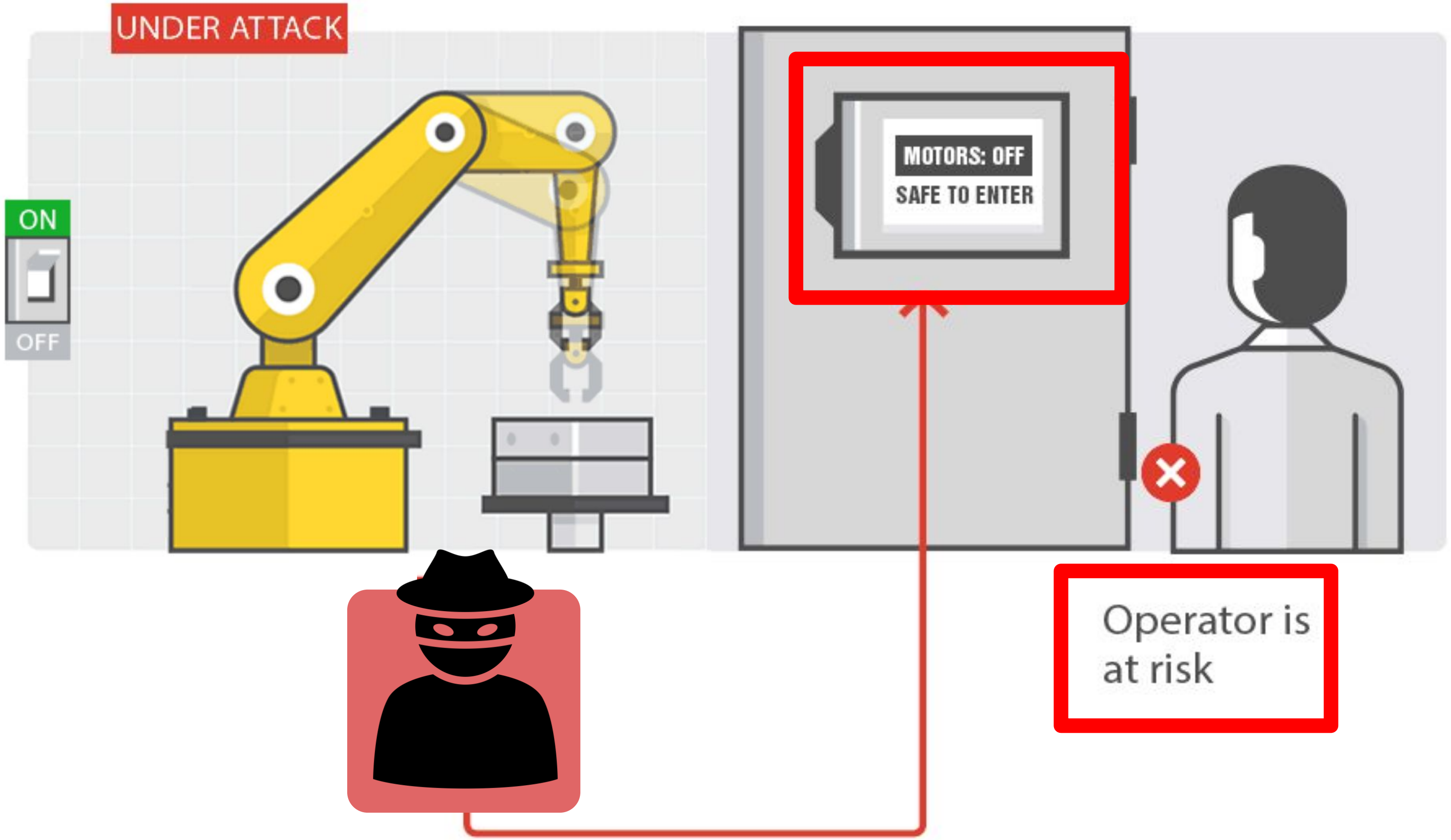
Attacks 4+5

Safety

Accuracy

Integrity

Displayed or Actual State Alteration



Operator is at risk

Attacks 4+5

Safety

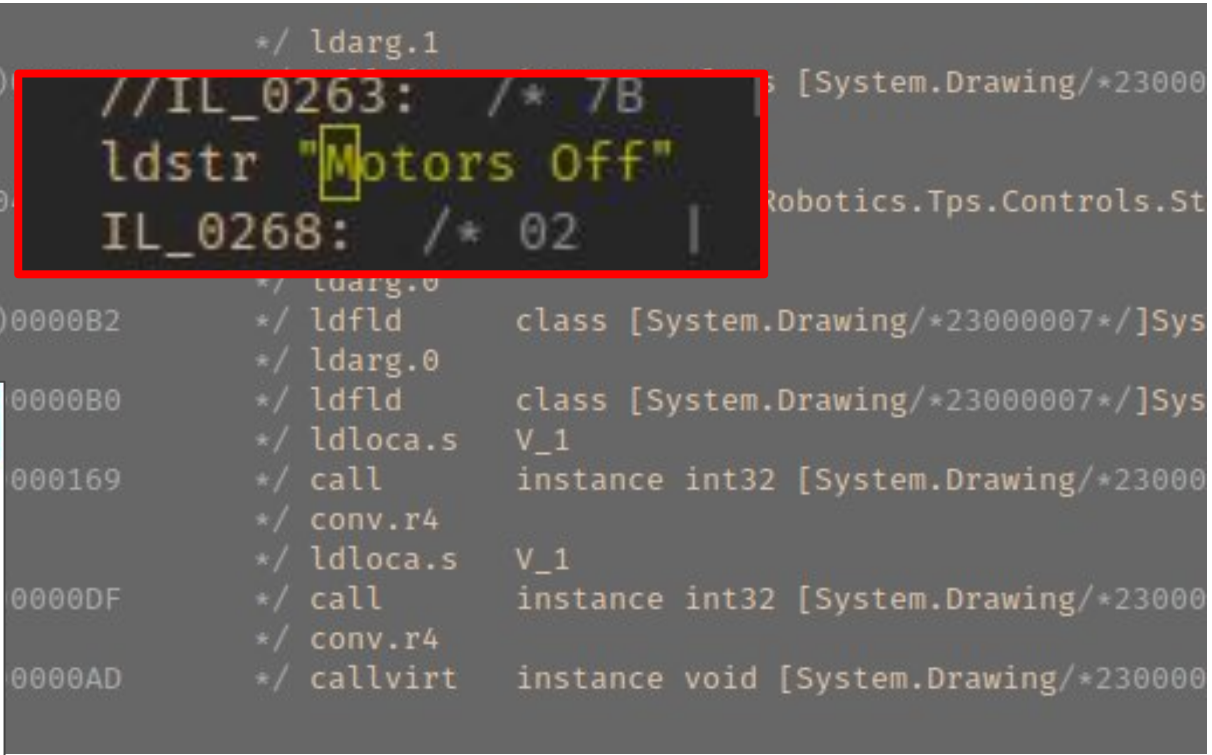
Accuracy

Integrity

Displayed State Alteration PoC

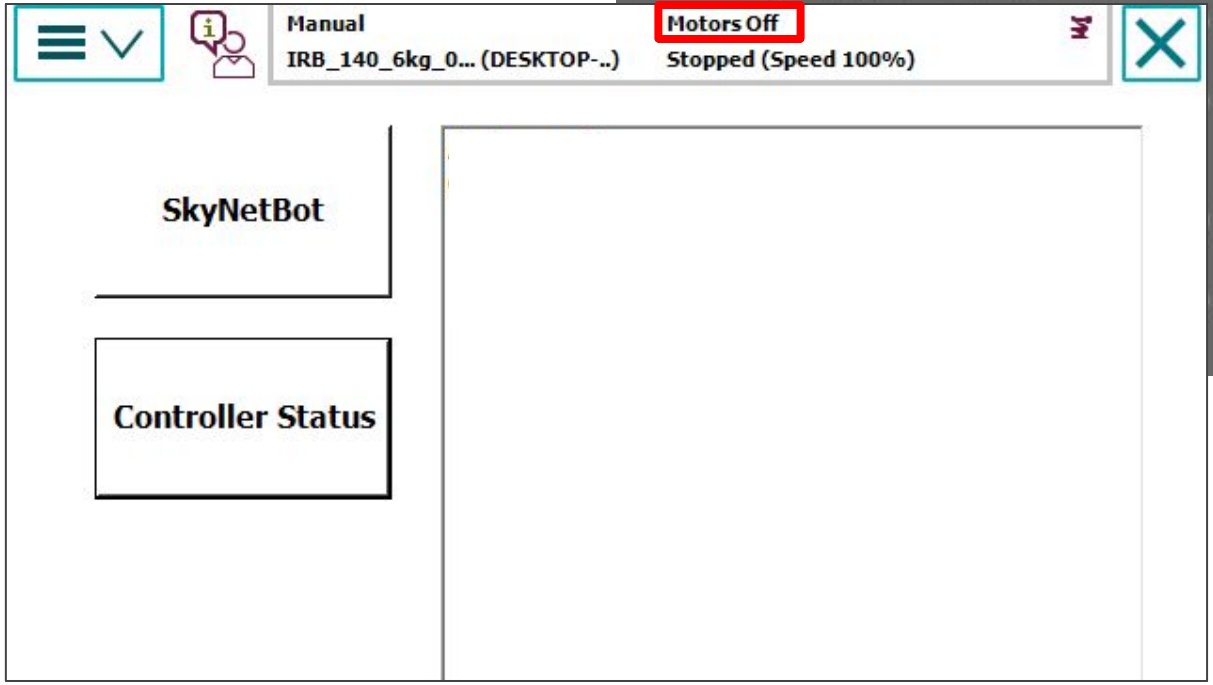
Malicious DLL

Teach Pendant



```
        IL_025c:  /* 03   |                         */ ldarg.1
        IL_025d:  /* 6F   | (0A)                                   s [System.Drawing/*23000
-() /* 0A000028 */
        //IL_0262:  /* 02   |
        //IL_0263:  /* 7B   | (0                                   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
```

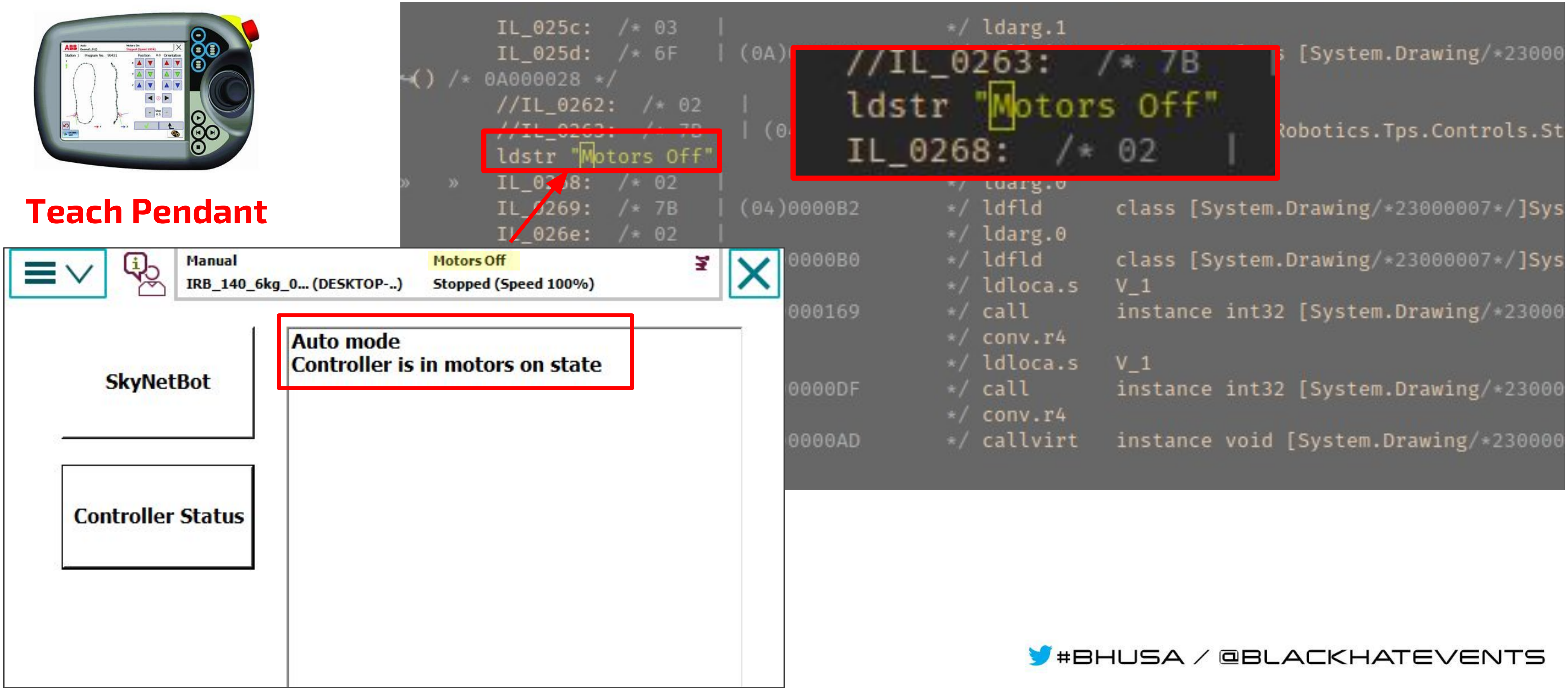
```
//IL_0263:  /* 7B
ldstr "Motors Off"
IL_0268:  /* 02   |
```



Manual
IRB_140_6kg_0... (DESKTOP-..)

Motors Off
Stopped (Speed 100%)

Displayed State Alteration PoC



Malicious DLL

Teach Pendant

```
        IL_025c:  /* 03   |                      */ ldarg.1
        IL_025d:  /* 6F   | (0A)                                     [System.Drawing/*23000
-() /* 0A000028 */
        //IL_0262:  /* 02   |
        //IL_0263:  /* 7B   | (0                                     Robotics.Tps.Controls.St
        ldstr "Motors Off"
»    »  IL_0268:  /* 02   |
        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
```

```
//IL_0263:  /* 7B
ldstr "Motors Off"
IL_0268:  /* 02   |
```

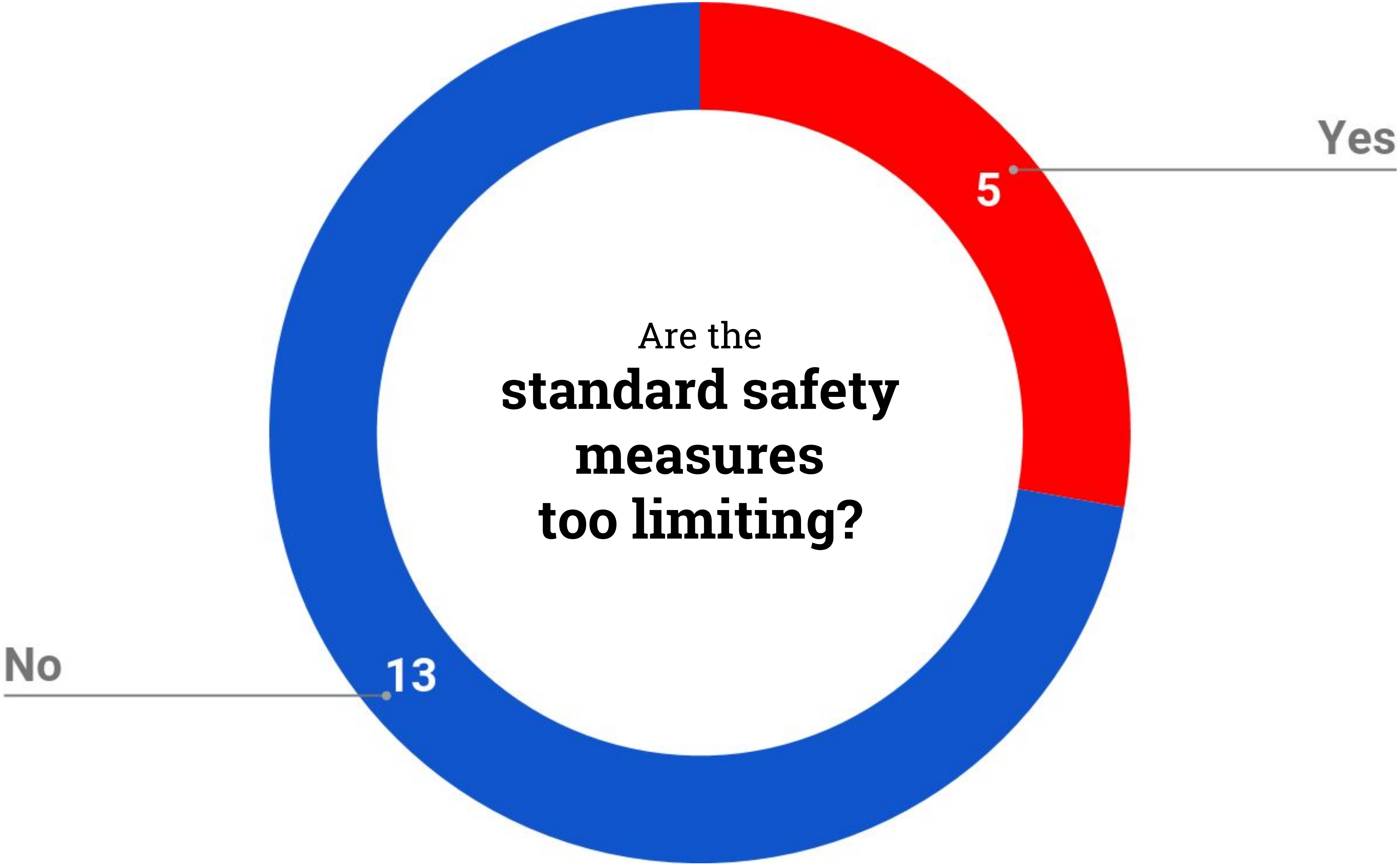
Manual | Motors Off
IRB_140_6kg_0... (DESKTOP-..) | Stopped (Speed 100%)

Auto mode
Controller is in motors on state

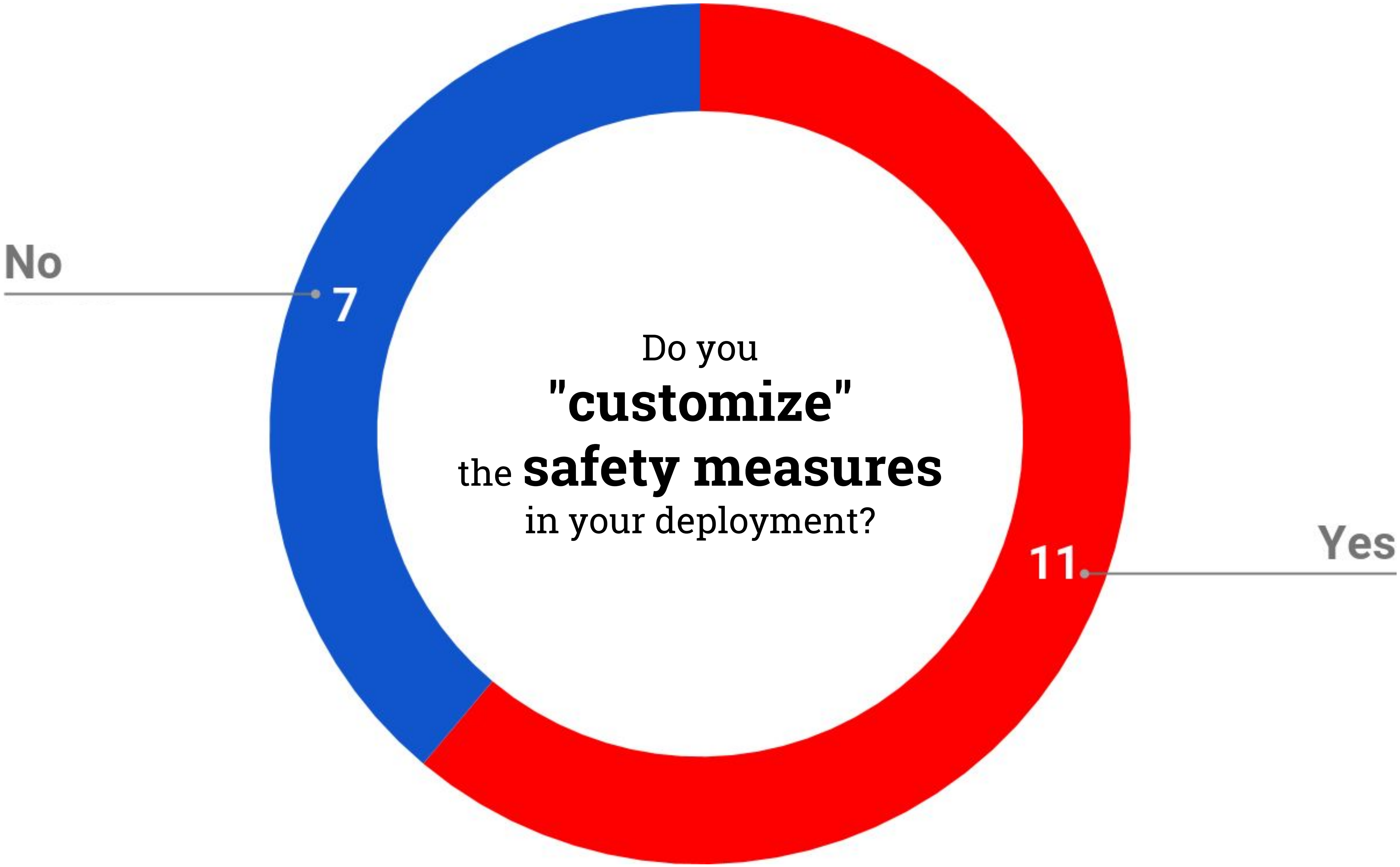
Is the Teach Pendant part of the safety system?

Is the Teach Pendant part of the safety system?

NO

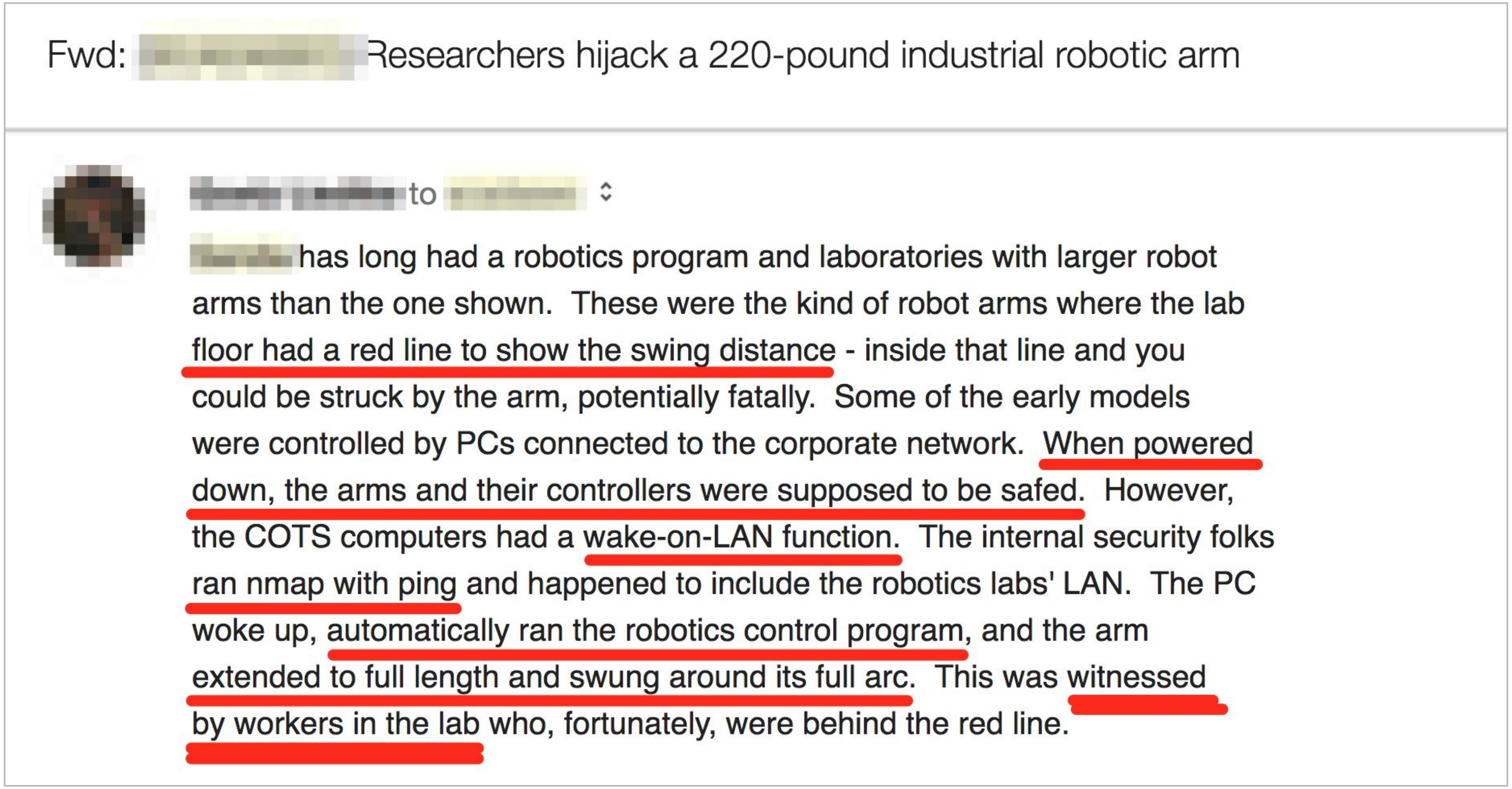


Are the **standard safety measures too limiting?**



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

Standards & Regulations vs. Real World



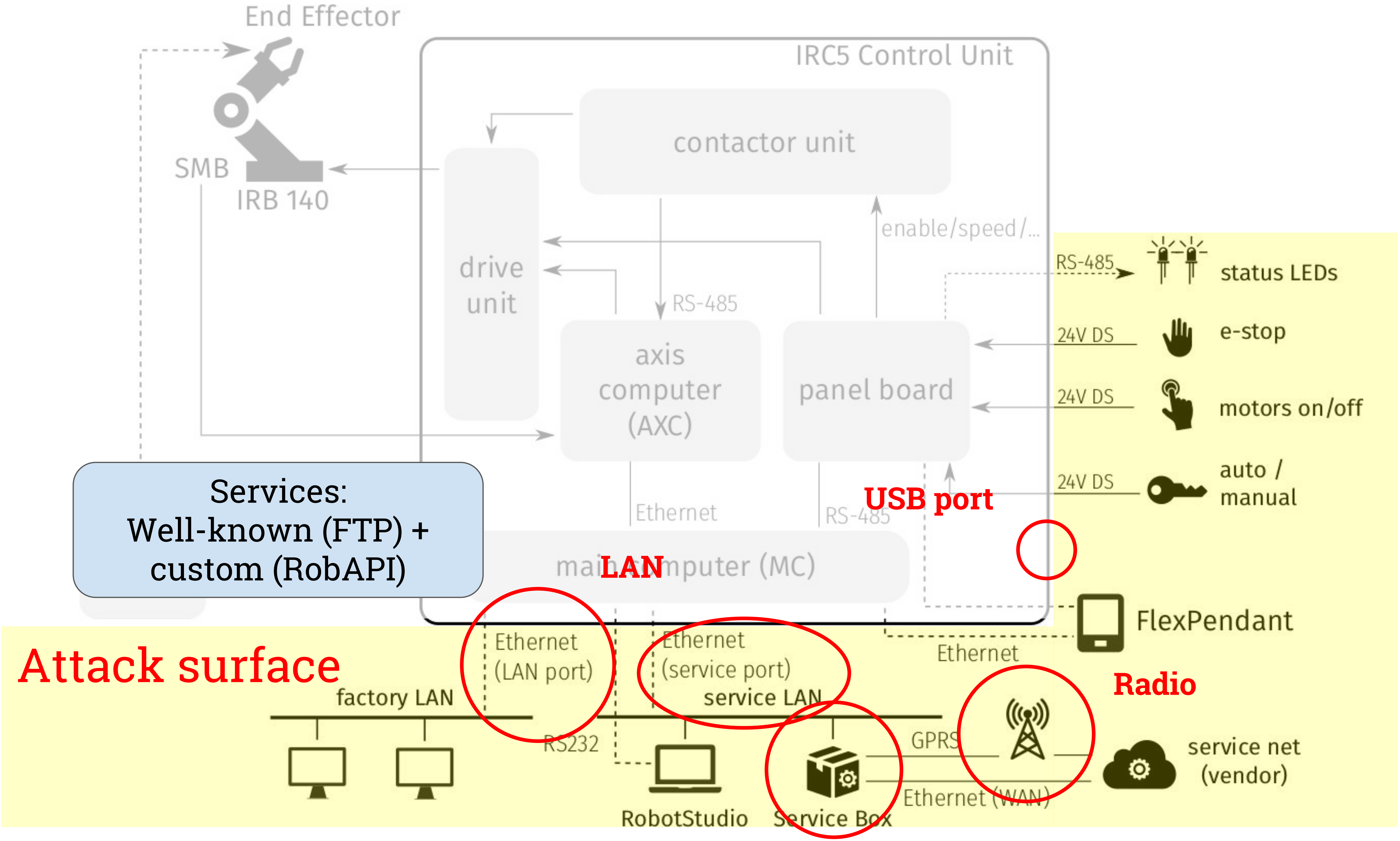
Fwd: [redacted] Researchers hijack a 220-pound industrial robotic arm

[redacted] to [redacted]

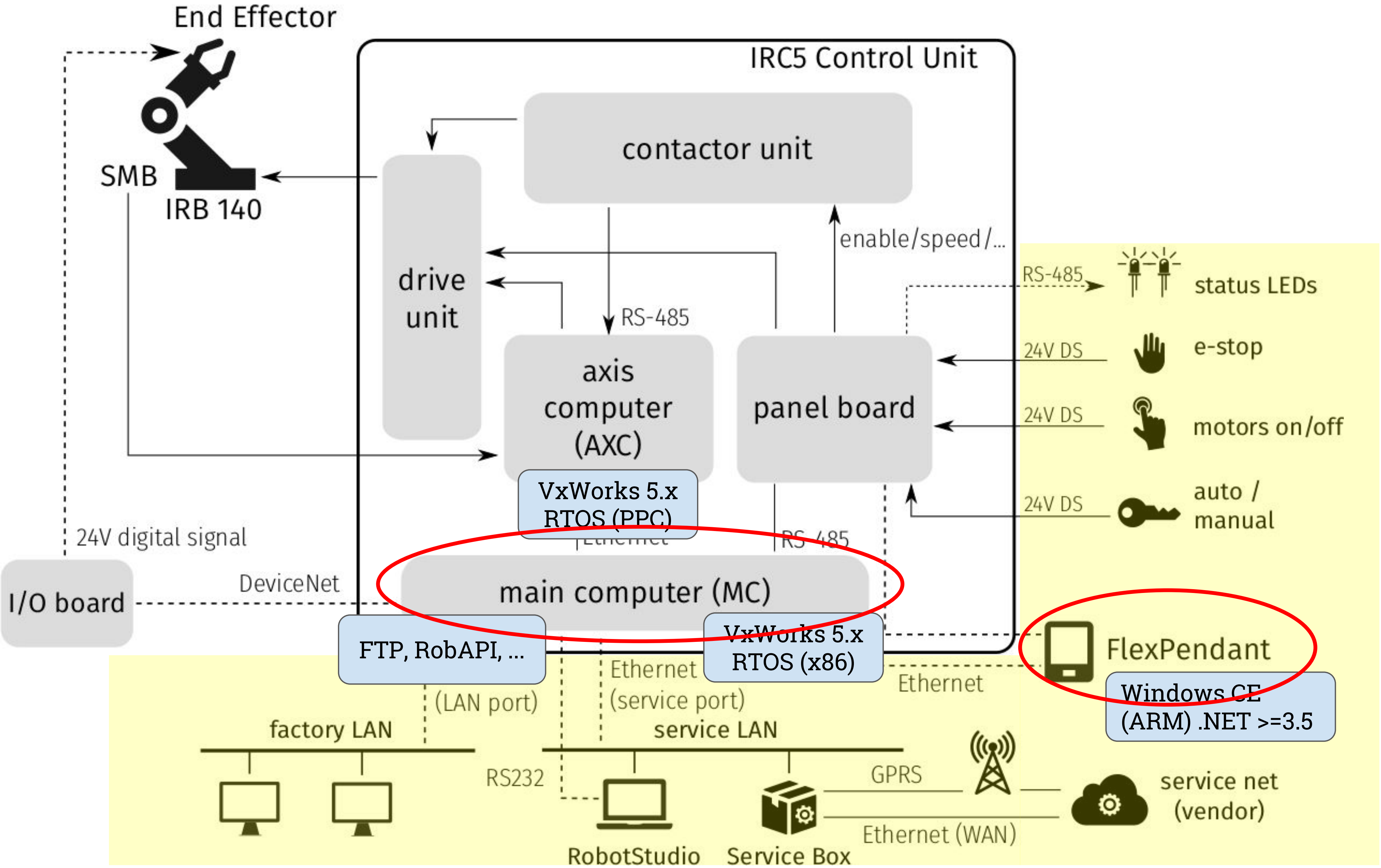
[redacted] has long had a robotics program and laboratories with larger robot arms than the one shown. These were the kind of robot arms where the lab floor had a red line to show the swing distance - inside that line and you could be struck by the arm, potentially fatally. Some of the early models were 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!



Services:
Well-known (FTP) +
custom (RobAPI)

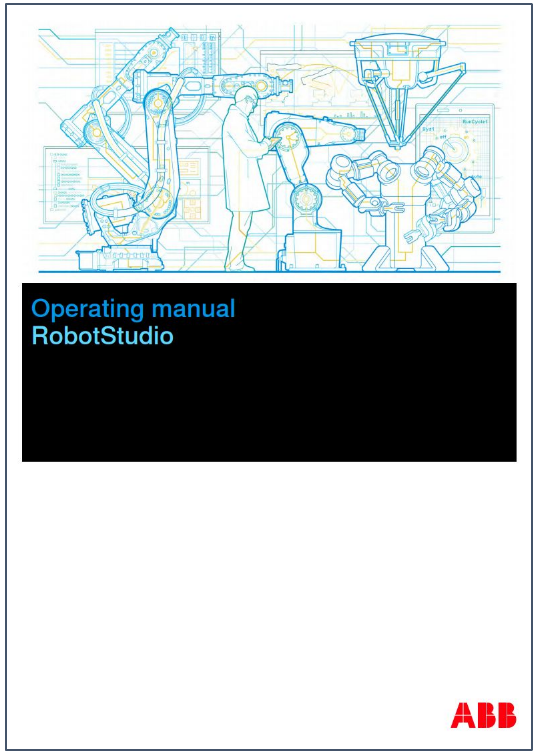

End Effector
IRC5 Control Unit
contactor unit
SMB
IRB 140
drive unit
enable/speed/...
RS-485
status LEDs
RS-485
axis computer (AXC)
panel board
24V DS
e-stop
24V DS
motors on/off
VxWorks 5.x RTOS (PPC)
24V DS
auto / manual
24V digital signal
Ethernet
RS-485
DeviceNet
I/O board
main computer (MC)
FTP,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

User Authorization System

User ∈ roles → grants

Authentication: username + password

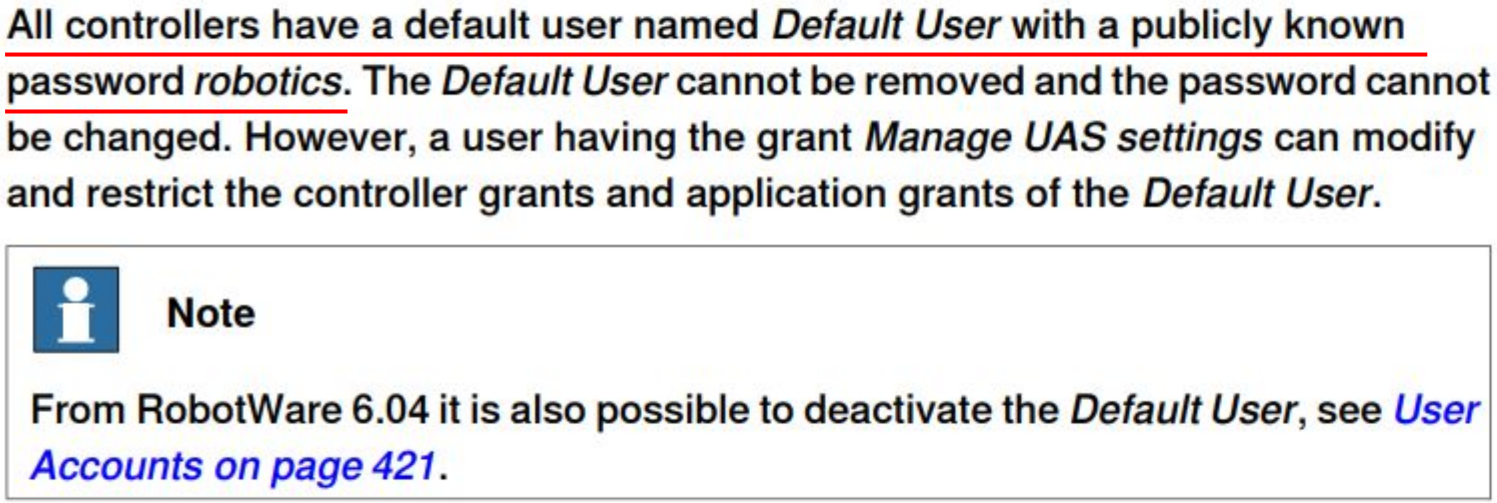
Used for FTP, RobAPI, …



Operating manual
RobotStudio

ABB

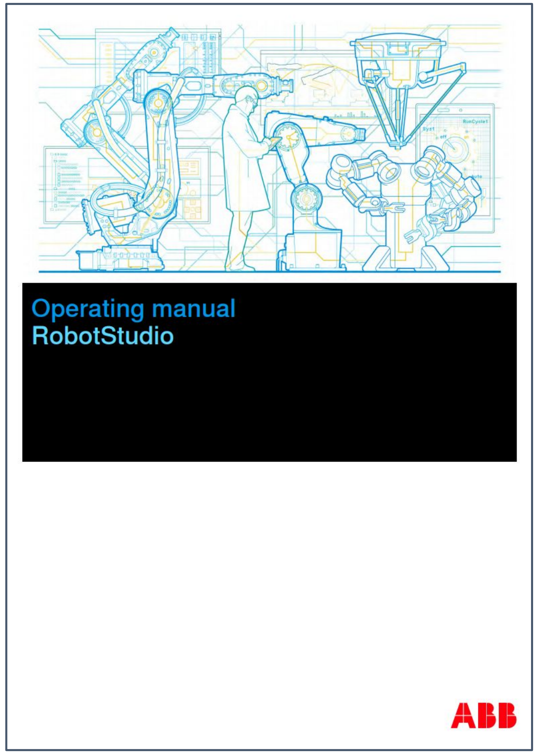
User Authorization System



All controllers have a default user named *Default User* with a publicly known password *robotics*. The *Default User* cannot be removed and the password cannot be changed. However, a user having the grant *Manage UAS settings* can modify and restrict the controller grants and application grants of the *Default User*.

Note

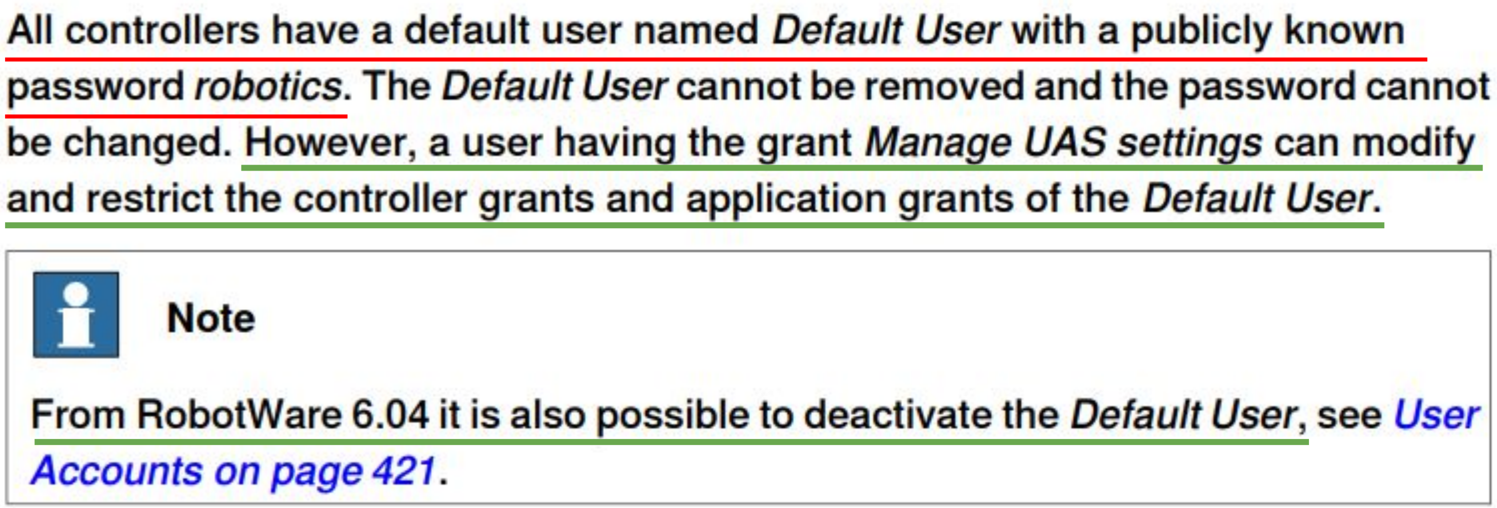
From RobotWare 6.04 it is also possible to deactivate the *Default User*, see *User Accounts on page 421*.



Operating manual
RobotStudio

ABB

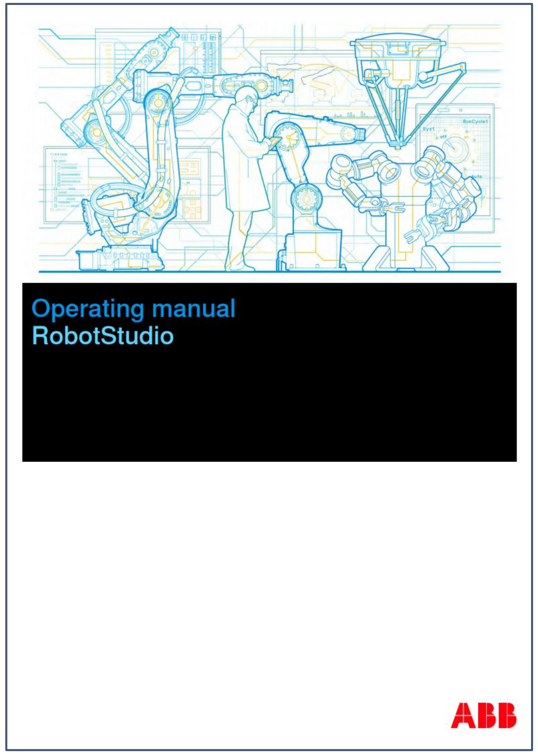
User Authorization System



All controllers have a default user named *Default User* with a publicly known password *robotics*. The *Default User* cannot be removed and the password cannot be changed. However, a user having the grant *Manage UAS settings* can modify and restrict the controller grants and application grants of the *Default User*.

Note

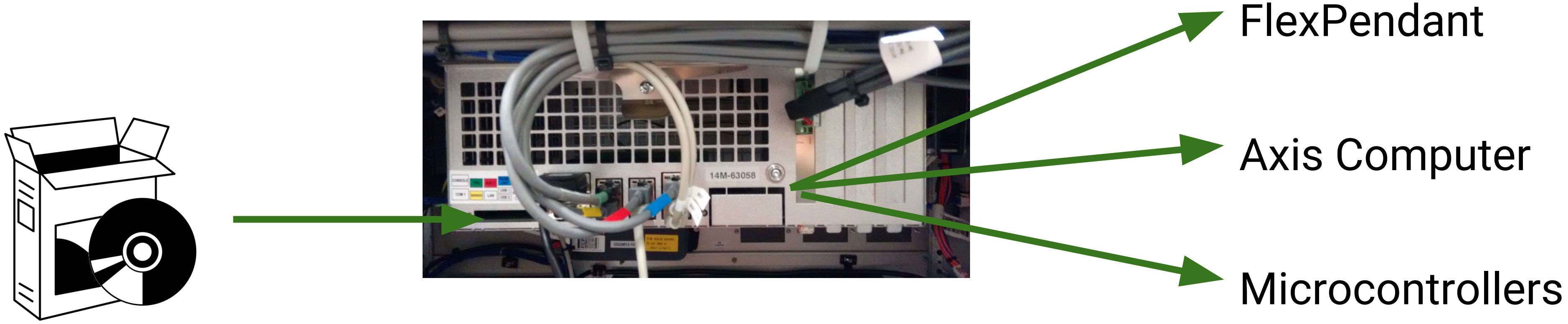
From RobotWare 6.04 it is also possible to deactivate the *Default User*, see *User Accounts on page 421*.



Operating manual
RobotStudio

tl;dr; read deployment guidelines
& deactivate the default user

Update problems

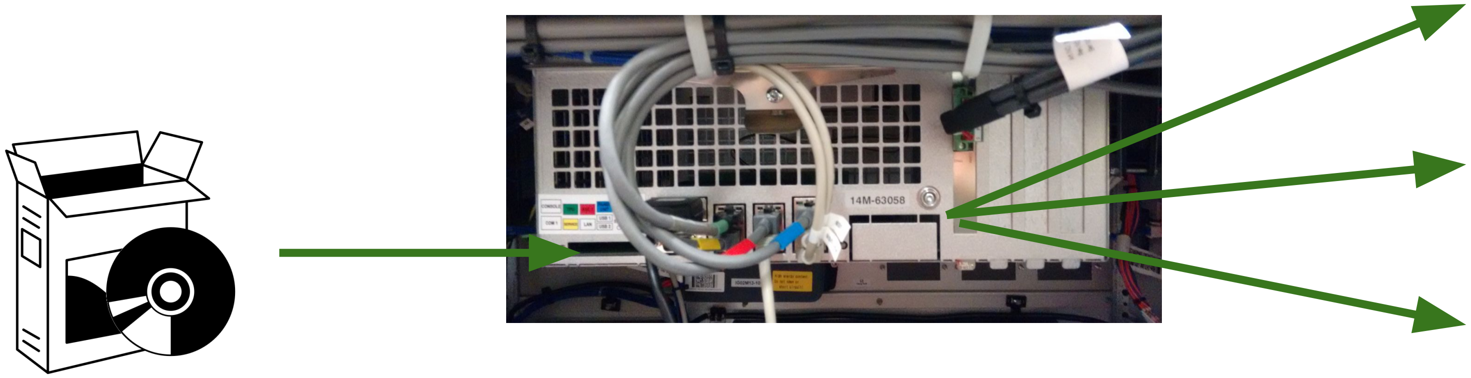


FlexPendant

Axis Computer

Microcontrollers

Update problems

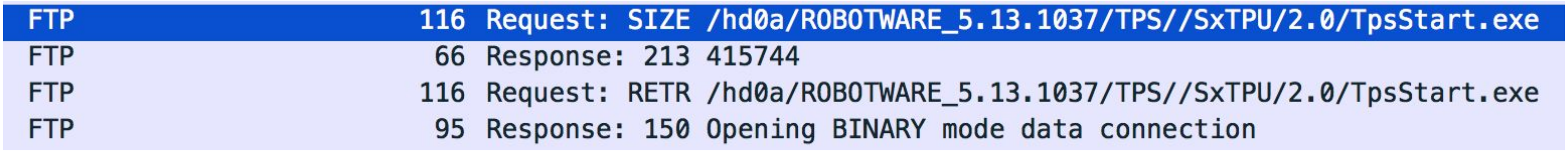


FlexPendant

Axis Computer

Microcontrollers

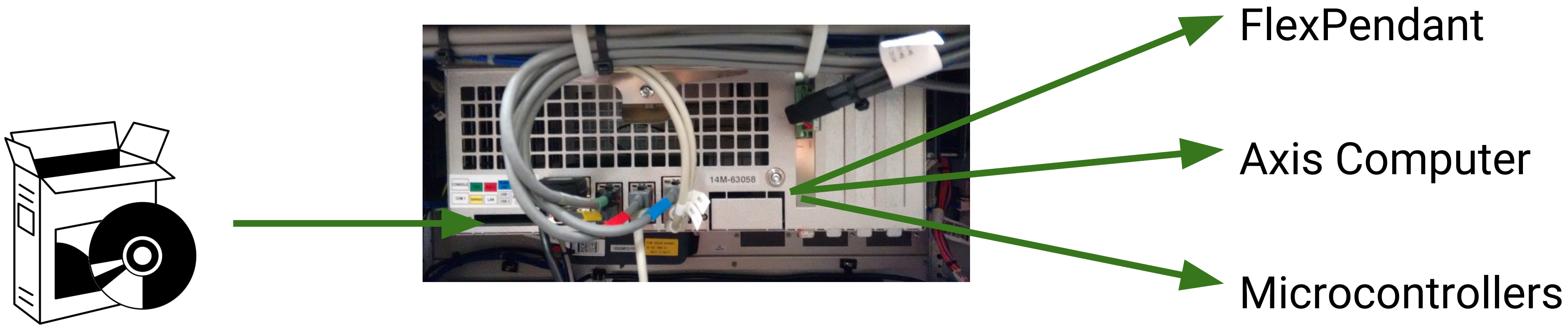
How? FTP at **boot**



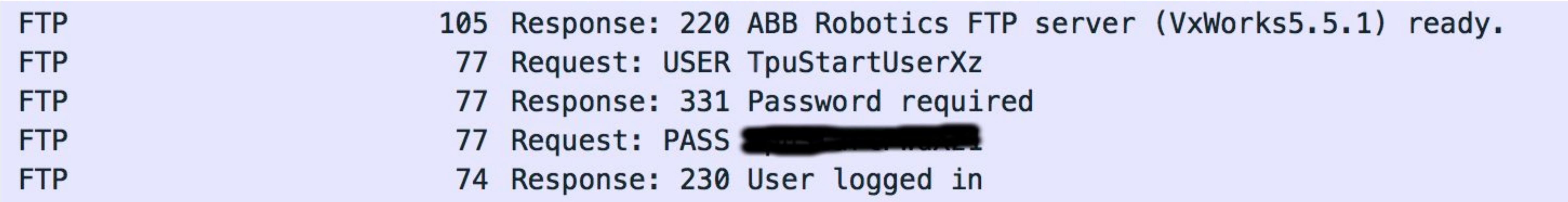
```
FTP                    116  Request: SIZE /hd0a/ROBOTWARE_5.13.1037/TPS//SxTPU/2.0/TpsStart.exe
FTP                     66  Response: 213 415744
FTP                    116  Request: RETR /hd0a/ROBOTWARE_5.13.1037/TPS//SxTPU/2.0/TpsStart.exe
FTP                     95  Response: 150 Opening BINARY mode data connection
```

.... plus, no code signing, nothing

Update problems



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

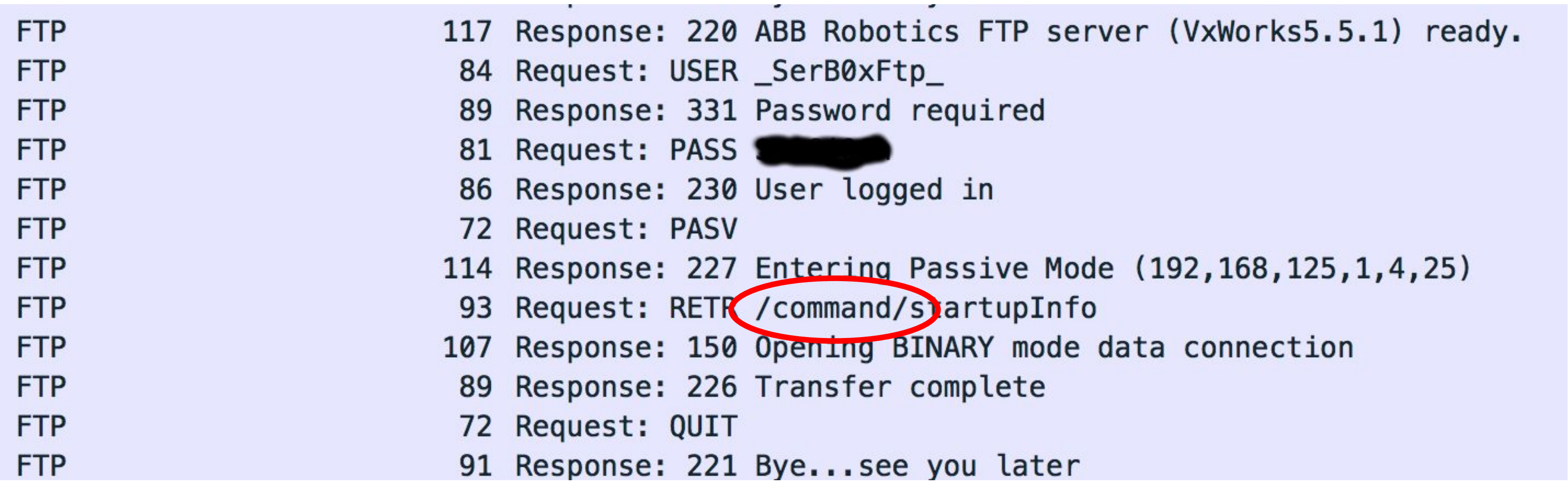


```
FTP                         105 Response: 220 ABB Robotics FTP server (VxWorks5.5.1) ready.
FTP                          77 Request: USER TpuStartUserXz
FTP                          77 Response: 331 Password required
FTP                          77 Request: PASS [redacted]
FTP                          74 Response: 230 User logged in
```

ABBVU-DMRO-124644

Autoconfiguration is magic!

Autoconfiguration is magic!



```
FTP                       117  Response: 220 ABB Robotics FTP server (VxWorks5.5.1) ready.
FTP                        84  Request: USER _SerB0xFtp_
FTP                        89  Response: 331 Password required
FTP                        81  Request: PASS [redacted]
FTP                        86  Response: 230 User logged in
FTP                        72  Request: PASV
FTP                       114  Response: 227 Entering Passive Mode (192,168,125,1,4,25)
FTP                        93  Request: RETR /command/startupInfo
FTP                       107  Response: 150 Opening BINARY mode data connection
FTP                        89  Response: 226 Transfer complete
FTP                        72  Request: QUIT
FTP                        91  Response: 221 Bye...see you later
```

ABBVU-DMRO-124642

Enter /command

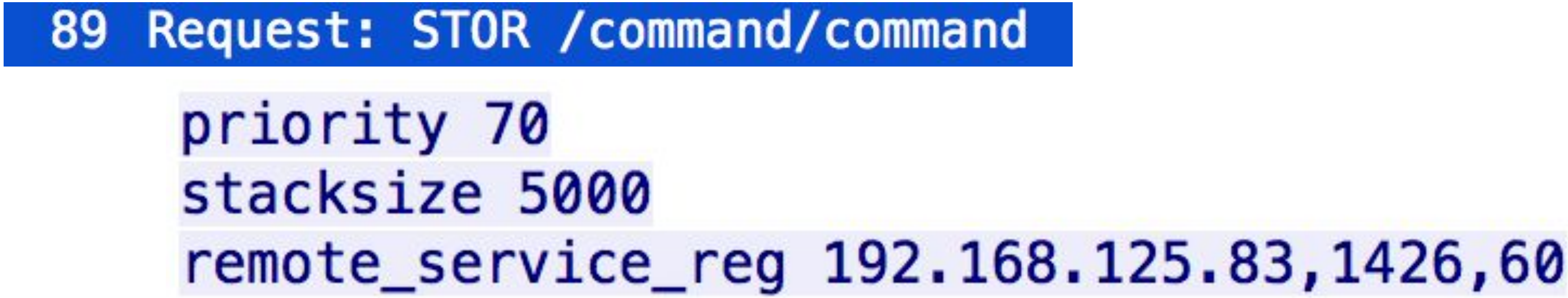
FTP RETR `/command/whatever` read system info

FTP STOR `/command/command` execute “commands”

Enter /command

FTP RETR `/command/whatever` read system info

FTP STOR `/command/command` execute “commands”



```
89 Request: STOR /command/command
```

```
priority 70
stacksize 5000
remote_service_reg 192.168.125.83,1426,60
```

Enter /command

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

FTP PUT `/command/command` execute "commands"

```
    shell reboot
    shell uas_disable
```

+ hard-coded credentials? → **remote command execution**

Enter `/command`

Let’s look at **`cmddev_execute_command`**:

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

overflow **`buf`** (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/timestamp`AAAAAAA`....`AAAAAAA
- file name > 512 bytes ~> Flex Pendant DoS

ABBVU-DMRO-124641, ABBVU-DMRO-124645

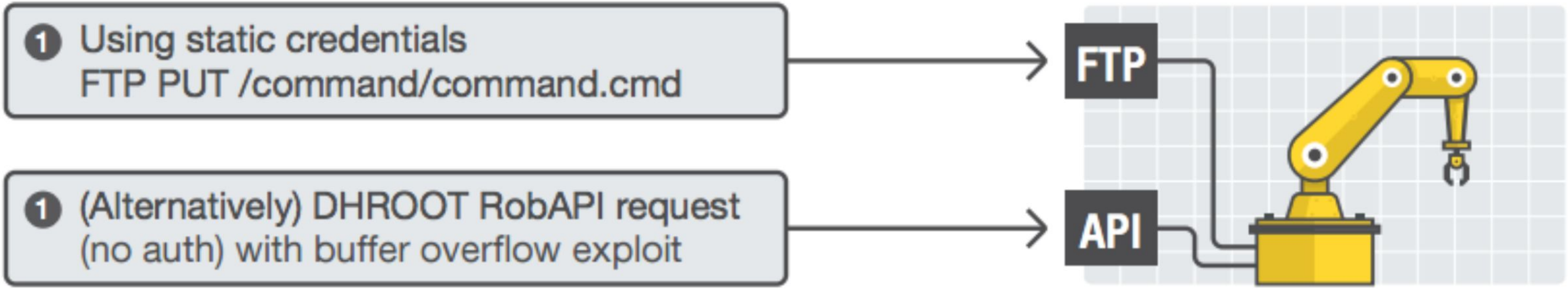
Takeaways

Some **memory corruption**

Mostly **logical vulnerabilities**

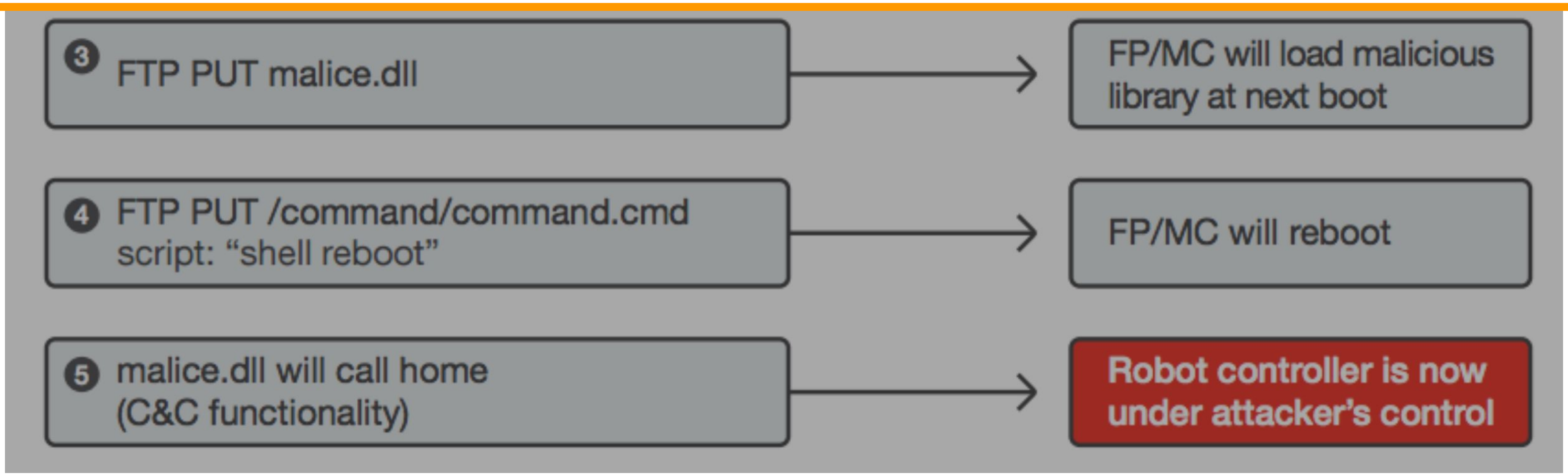
⚠ All the components blindly **trust** the **main computer (lack of isolation)**

Complete attack chain (1)



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

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

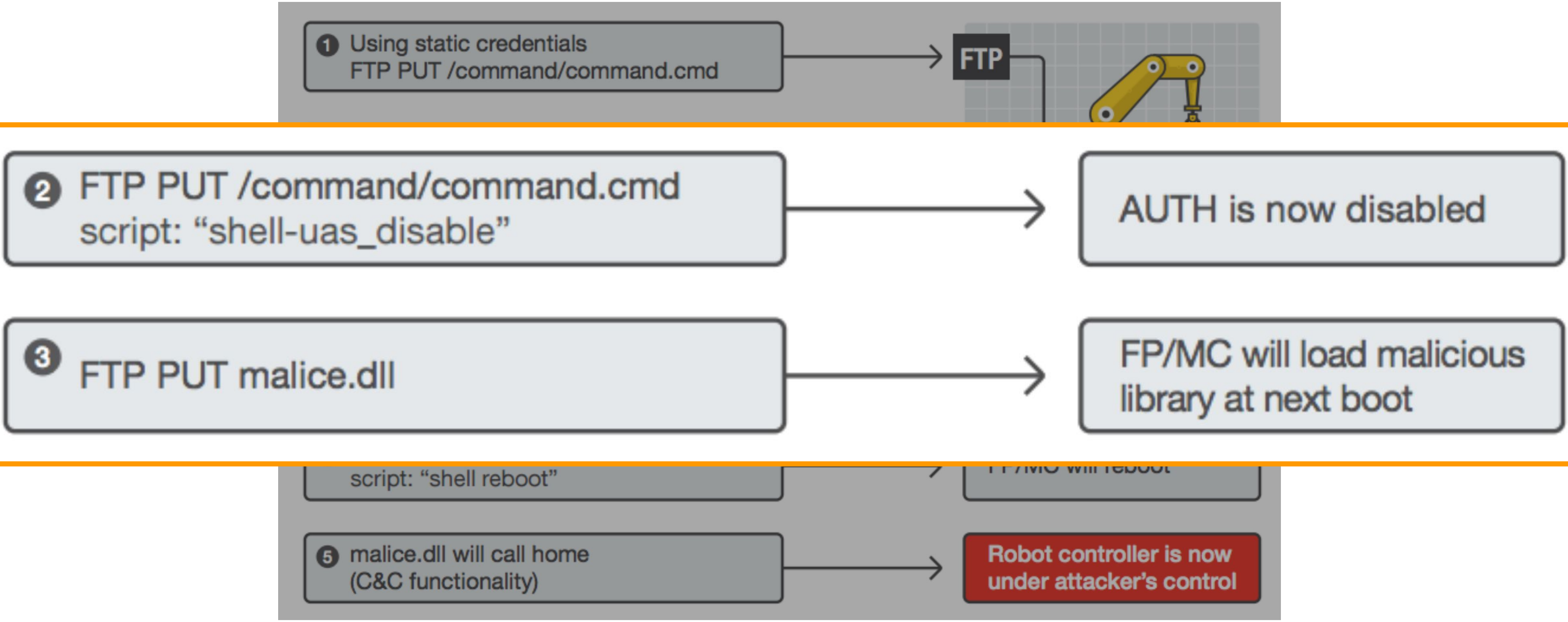


3 FTP PUT malice.dll → FP/MC will load malicious library at next boot

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)



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

2 FTP PUT /command/command.cmd
script: “shell-uas_disable”

AUTH is now disabled

3 FTP PUT malice.dll

FP/MC will load malicious library at next boot

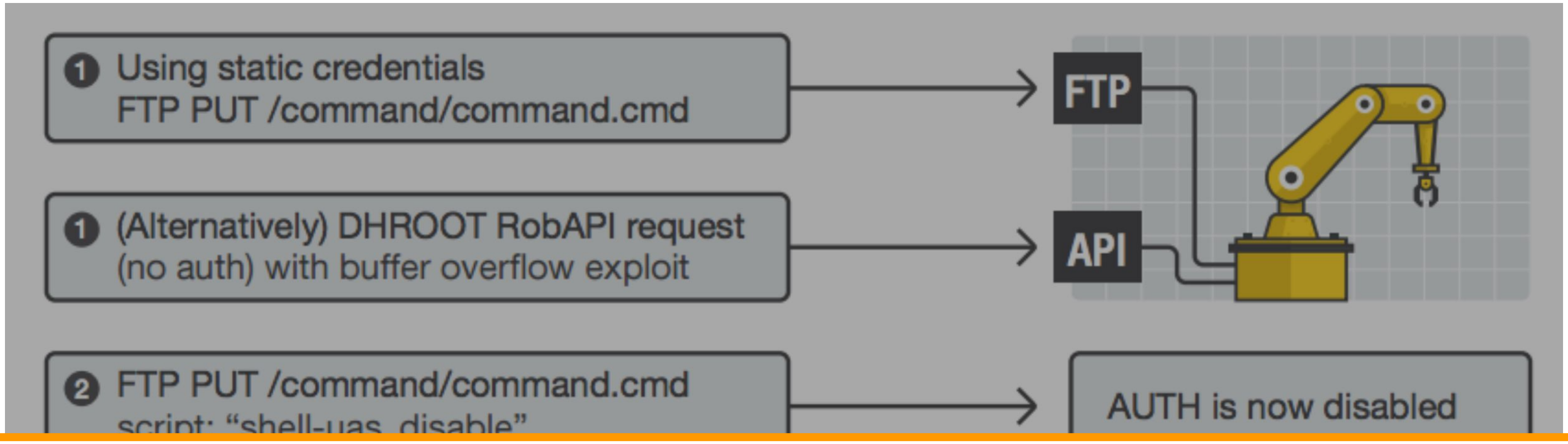
script: “shell reboot”

FP/MC will reboot

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

Robot controller is now under attacker’s control

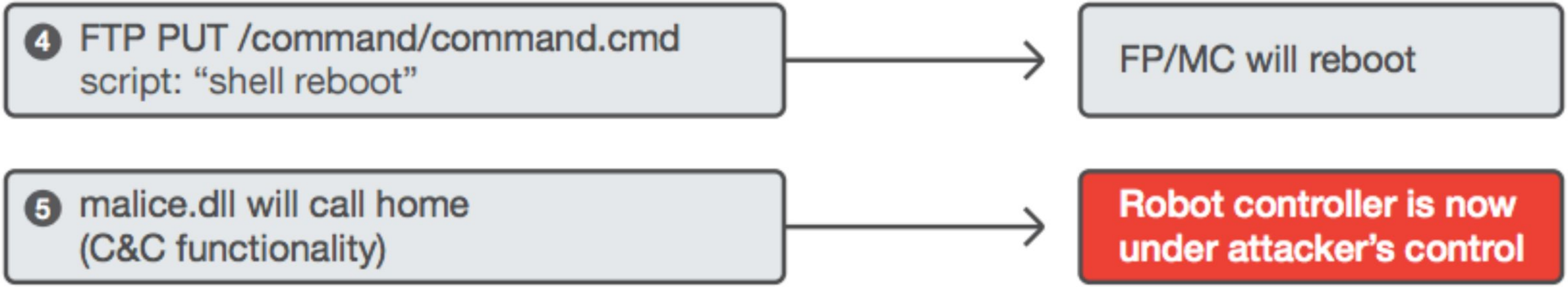
Complete attack chain (3)



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

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

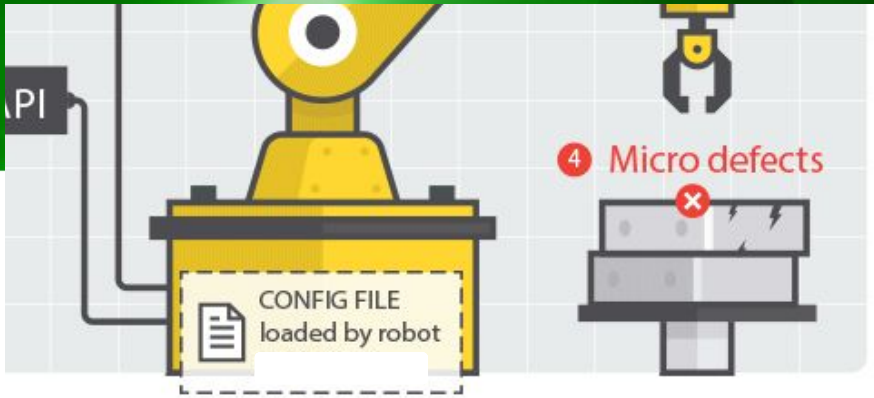
2 FTP PUT /command/command.cmd
script: “shell-uas disable” → AUTH is now disabled



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

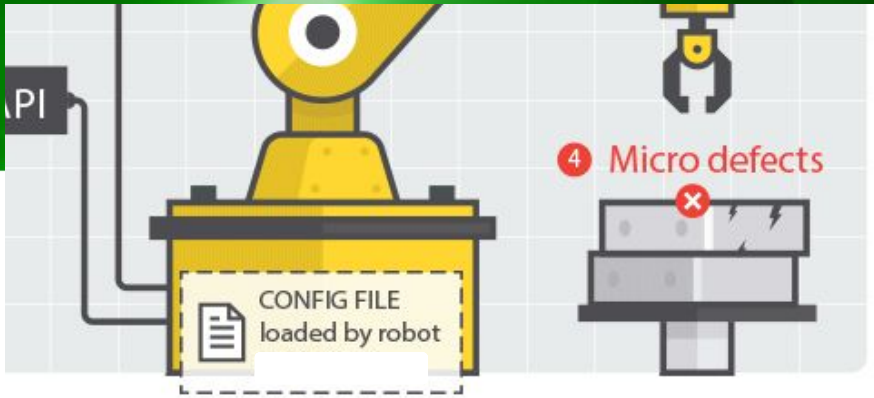
File protection



“Sensitive” files:

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

File protection



“Sensitive” files:

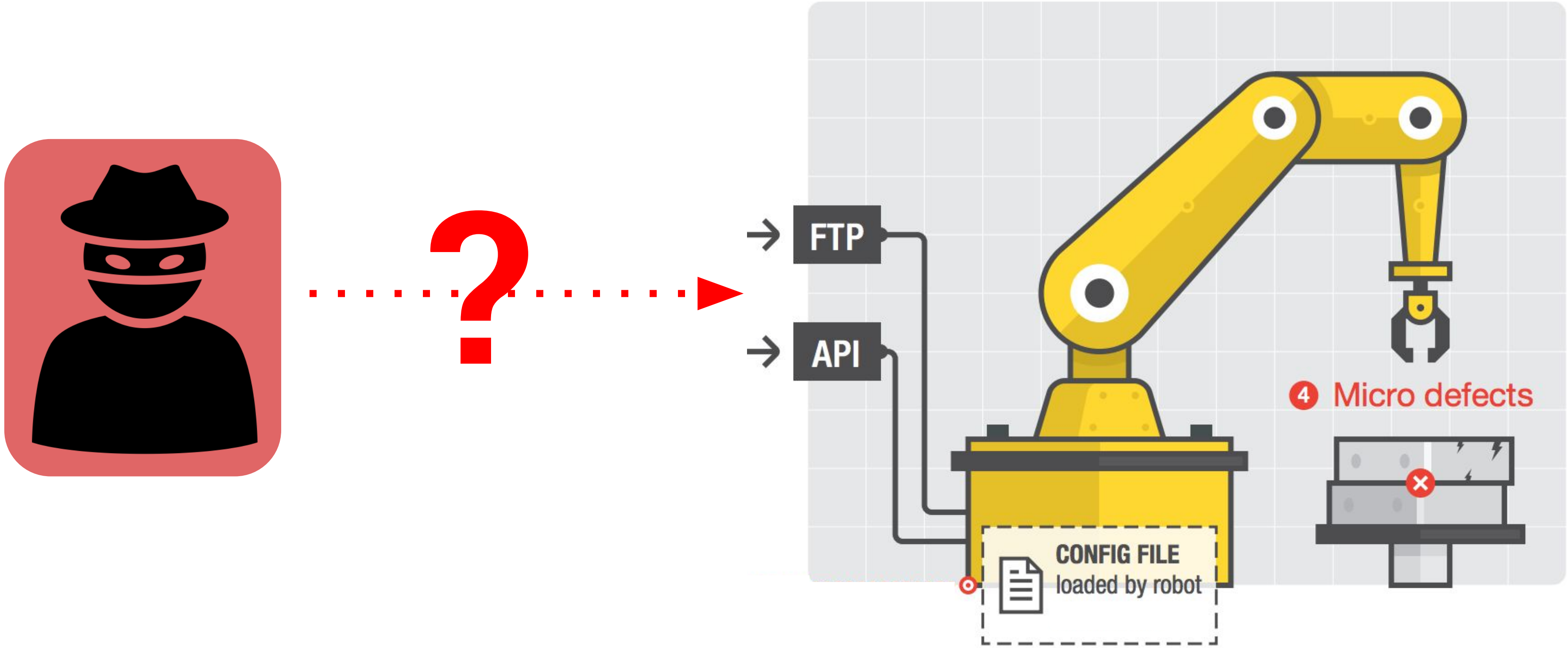
- Users’ credentials and permissions
- Sensitive configuration parameters (e.g., PID)
- Industry secrets (e.g., workpiece parameters)

Obfuscation: bitwise XOR with a “random” key.

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

That’s how we implemented the attacks

Attack Surface

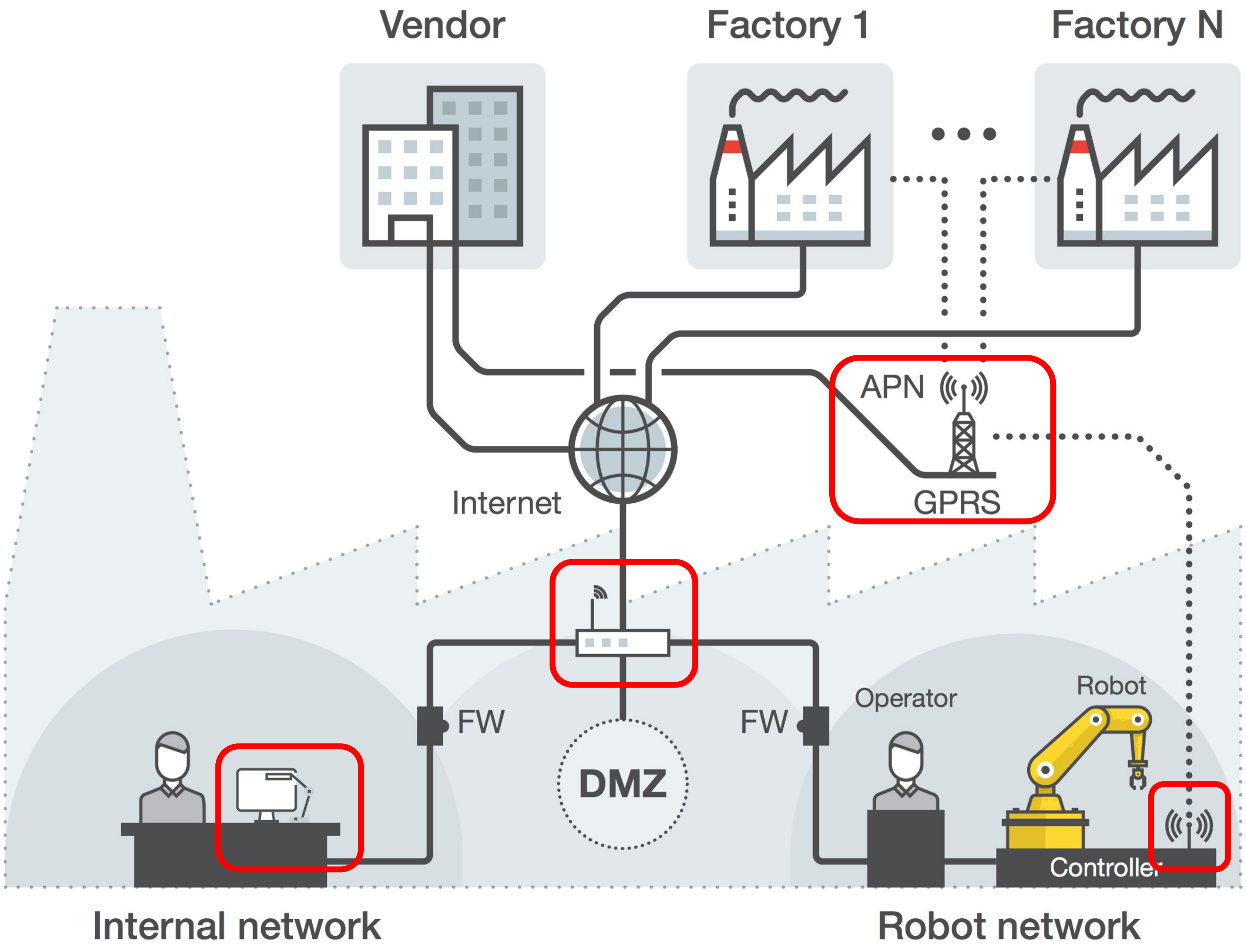


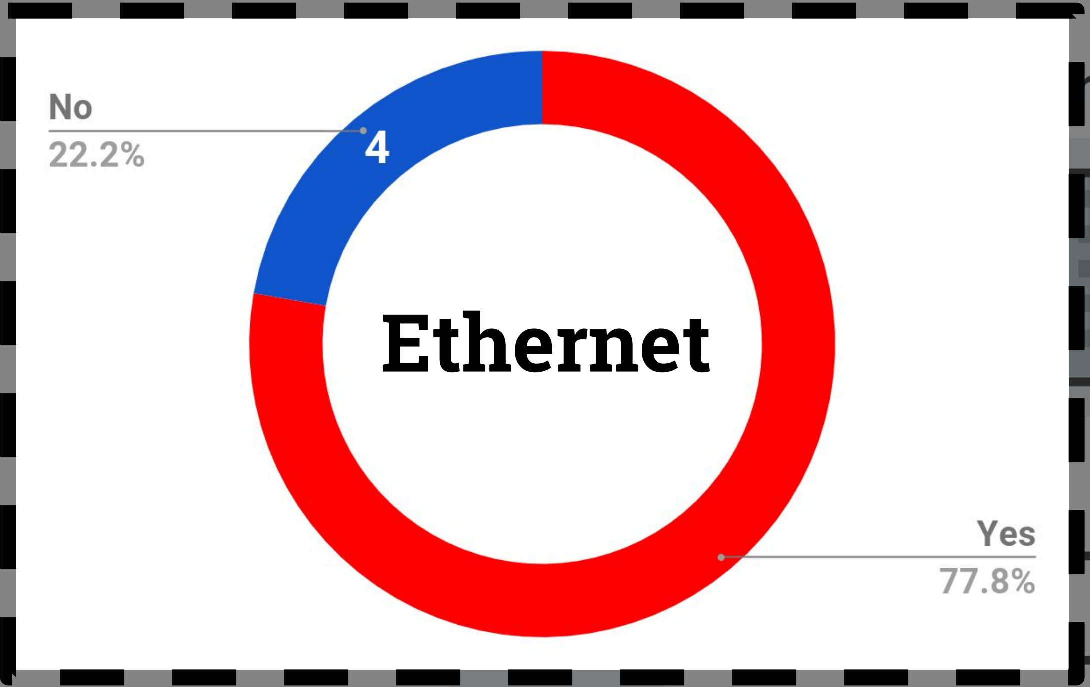
Flexibly programmable

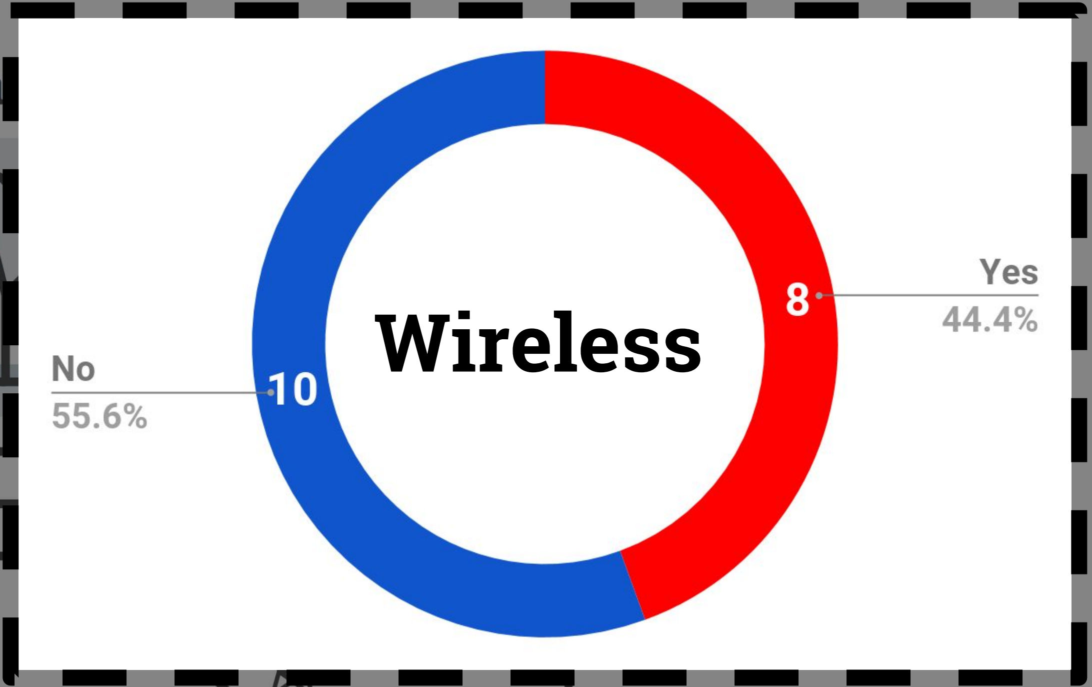
&

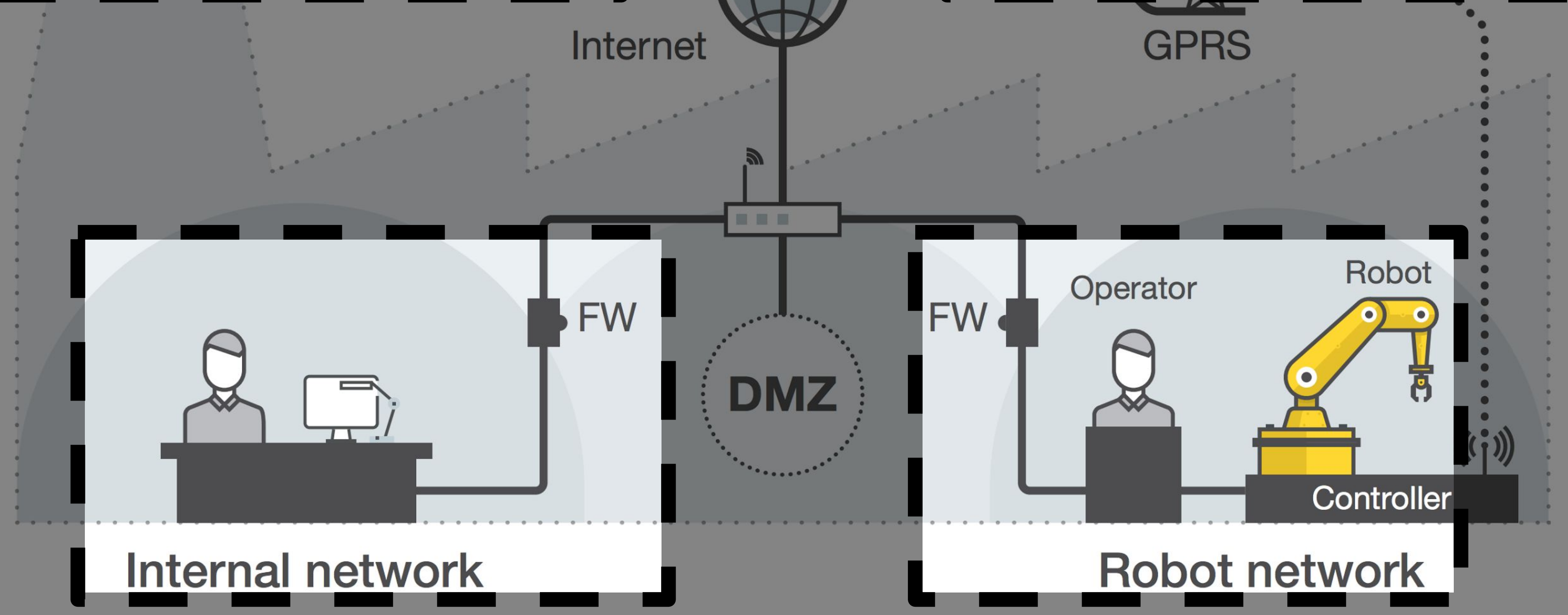
Connected

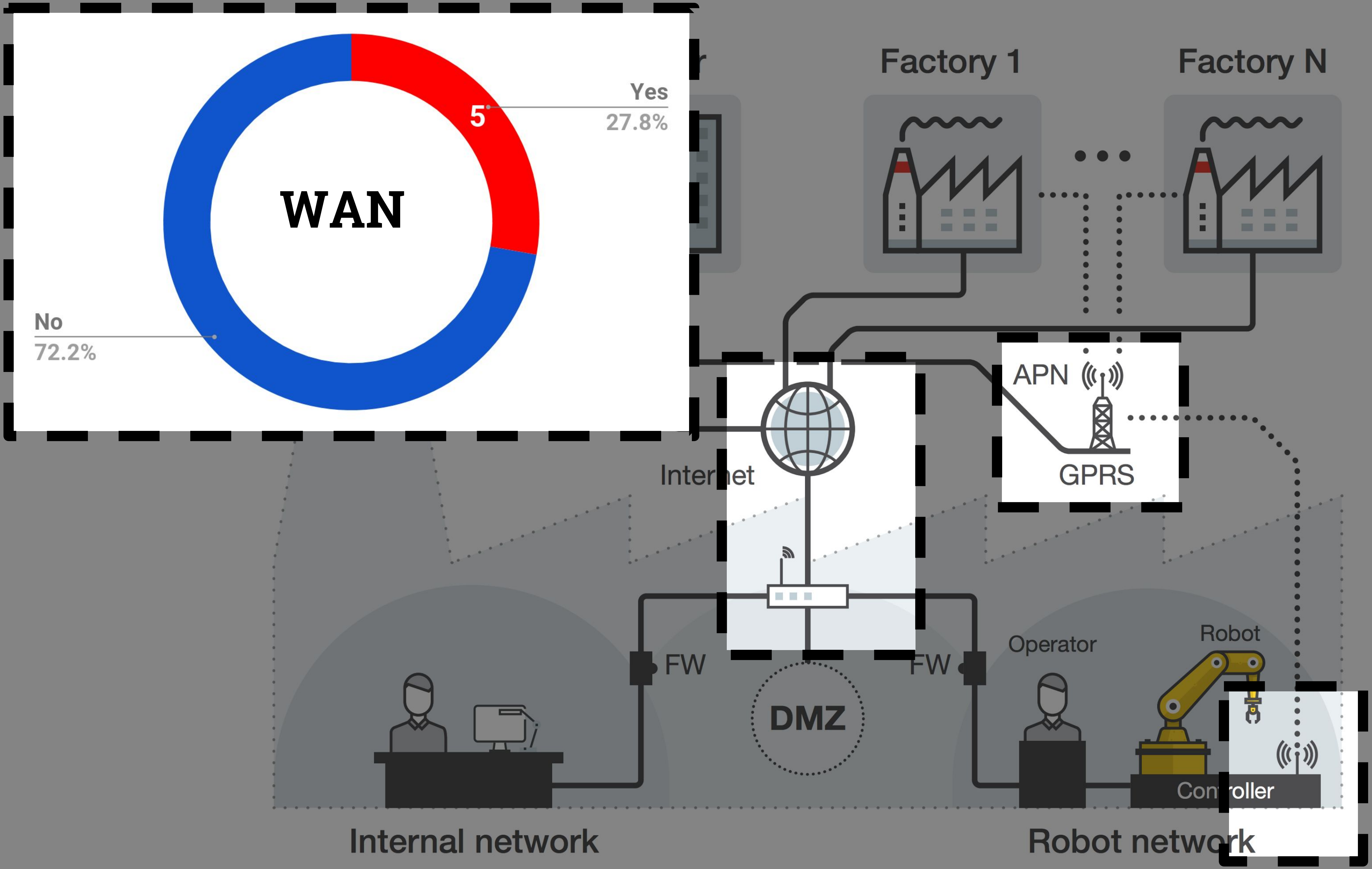
(Part 2)


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

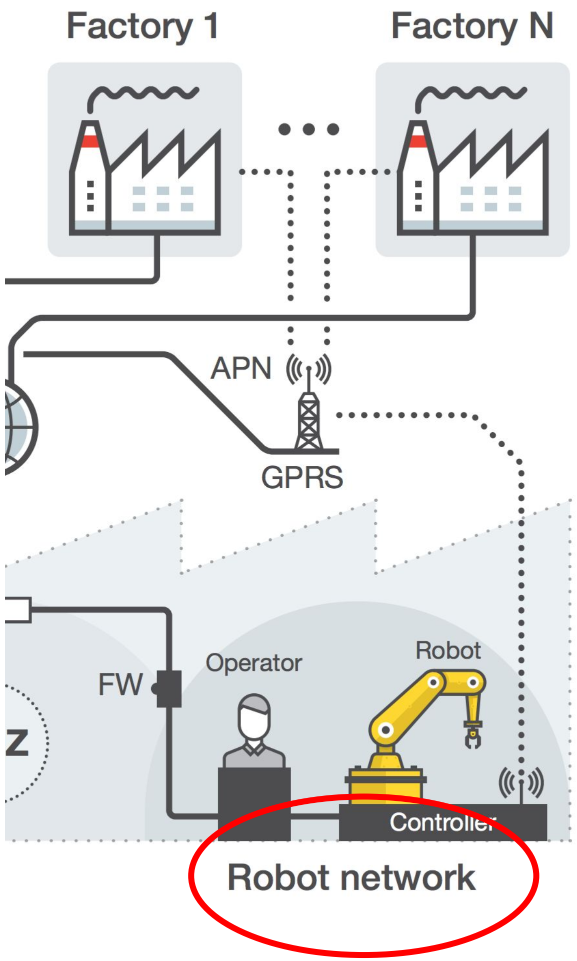

Ethernet
No
22.2%
4
Yes
77.8%


Wireless
Yes
44.4%
8
No
55.6%
10


Internet
GPRS
FW
FW
DMZ
Operator
Robot
Controller
Internal network
Robot network


WAN
Yes
5
27.8%
No
72.2%
Factory 1
Factory N
APN
GPRS
Internet
FW
DMZ
FW
Operator
Robot
Controller
Internal network
Robot network

Remote Exposure of Industrial *Robots*

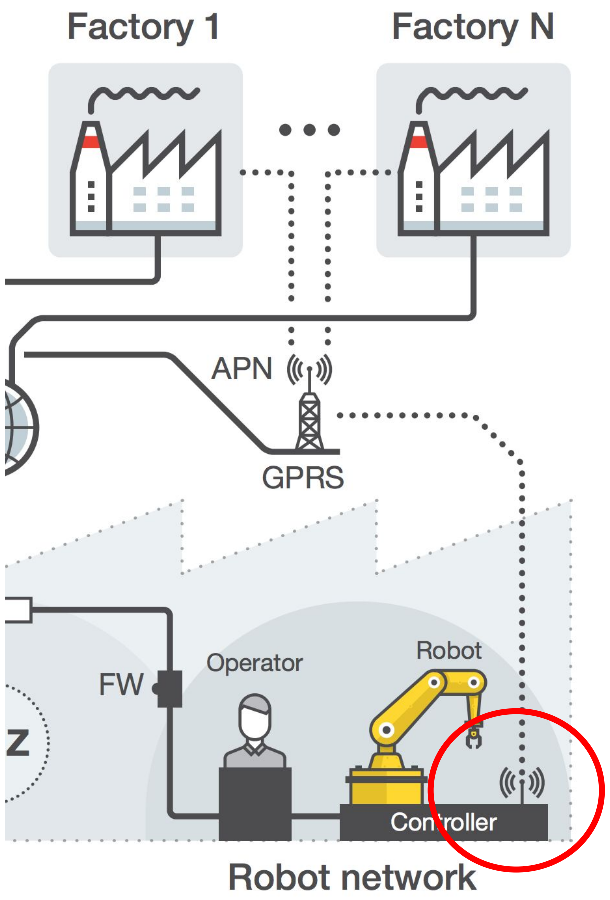


Search	Entries	Country
ABB Robotics	5	DK, SE
FANUC FTP	9	US, KR, FR, TW
Yaskawa	9	CA, JP
Kawasaki E Controller	4	DE
Mitsubishi FTP	1	ID
Overall	**28**	**10**

Not so many...

(yesterday I've just found 10 more)

Remote Exposure of Industrial *Routers*



...way many more!

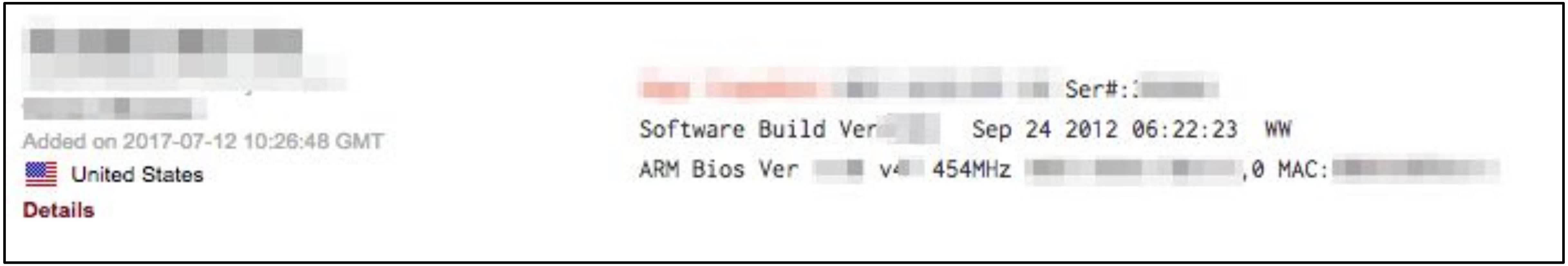
Brand	Exposed Devices	No Authentication
Belden	956	
Eurotech	160	
eWON	6,219	1,160
Digi	1,200	
InHand	883	
Moxa	12,222	2,300
NetModule	886	135
Robustel	4,491	
Sierra Wireless	50,341	220
Virtual Access	209	
Welotec	25	
Westermo	6,081	1,200
TOTAL	83,673	5,105

Unknown which routers are actually robot-connected black hat USA 2017

Typical Issues

Trivially "Fingerprintable"

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



[redacted]

[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)

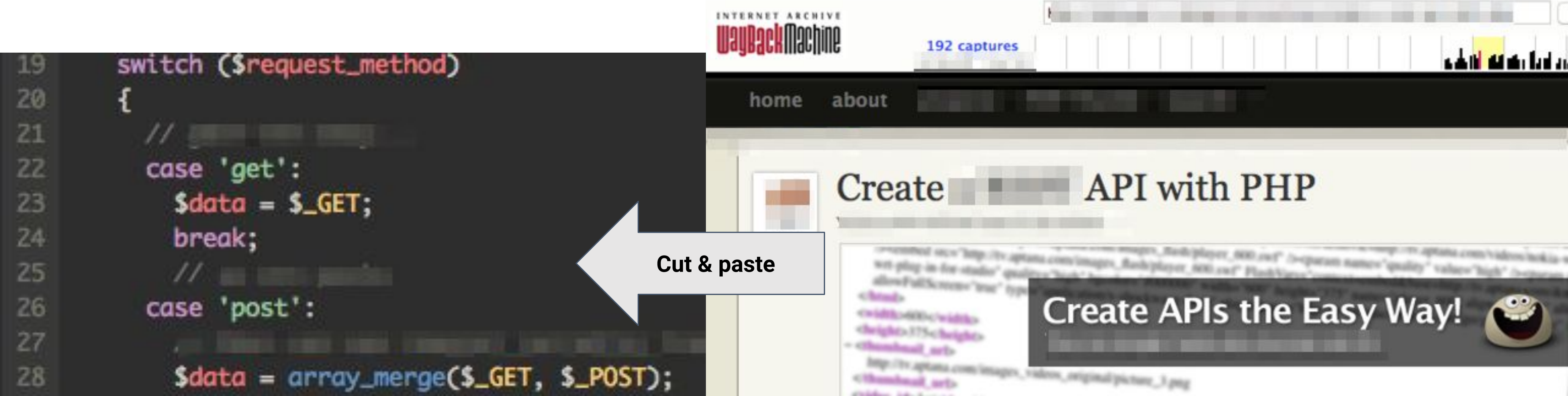
Outdated Software Components

- 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



```
switch ($request_method)
{
  // [redacted]
  case 'get':
    $data = $_GET;
    break;
    // [redacted]
  case 'post':
    [redacted]
    $data = array_merge($_GET, $_POST);
```

Cut & paste

Create [redacted] API with PHP

Create APIs the Easy Way!

Bottom line

Connect your robots with care

(follow security best practices & your robot vendor’s guidance)

Conclusions

Black Hat Sound Bytes

Robots are increasingly being **connected**

Industrial 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

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
http://robosec.org – http://bit.ly/2qy29oq

Questions?

An Experimental Security Analysis of an Industrial Robot Controller

Davide Quarta*, Marcello Pogliani*, Mario Polino*,
Federico Maggi*†, Andrea Maria Zanchettin*, and Stefano Zanero*
*Dipartimento di Elettronica, Informazione e Bioingegneria – Politecnico di Milano, Italy
{davide.quarta, marcello.pogliani, mario.polino, andreamaria.zanchettin, stefano.zanero}@polimi.it
†Trend Micro Inc.
federico_maggi@trendmicro.com

Abstract—Industrial robots, automated manufacturing, and efficient logistics processes are at the heart of the upcoming fourth industrial revolution. While there are seminal studies on the vulnerabilities of cyber-physical systems in the industry, as of today there has been no systematic analysis of the security of industrial robot controllers.

We examine the standard architecture of an industrial robot and analyze a concrete deployment from a systems security standpoint. Then, we propose an attacker model and confront it with the minimal set of requirements that industrial robots should honor: precision in sensing the environment, correctness in execution of control logic, and safety for human operators.

Following an experimental and practical approach, we then show how our modeled attacker can subvert such requirements through the exploitation of software vulnerabilities, leading to consequences that are unique to the robotics domain.
discussing safety standards and security

that, in the future, a manufacturer could leverage these attack opportunities to affect the reputation of a compe not to mention the possibility that enemy nations cou each others' factories manufacturing critical goods

A further exacerbating factor is that robot contro be promptly patched, since updates may require downtime, or even introduce regressions and bugs that render the software unusable. This " lem" makes the exploitation window of a vu longer, eventually increasing the impact of

Taking advantage of new interconnecti devices originally designed to work in already observed, for instance, in the a industrial control system (ICS) sectors. successful attacks have been recentl attack on a German steel mill ca down a blast furnace. In 2015, 2 to the U.S. ICS CERT [systems. Shodan quer

Rogue Robots: Testing the Limits of an Industrial Robot's Security

Federico Maggi
Trend Micro Forward-Looking Threat Research

Davide Quarta, Marcello Pogliani, Mario Polino, Andrea M. Zanchettin, and Stefano Zanero
Politecnico di Milano

A TrendLabs Research Pa

black hat® USA 2017

JULY 22-27, 2017
MANDALAY BAY / LAS VEGAS

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