POLITECNICO
MILANO 1863

NECST laboratory

Hacking Robots

Lessons learned, current research and new perspectives

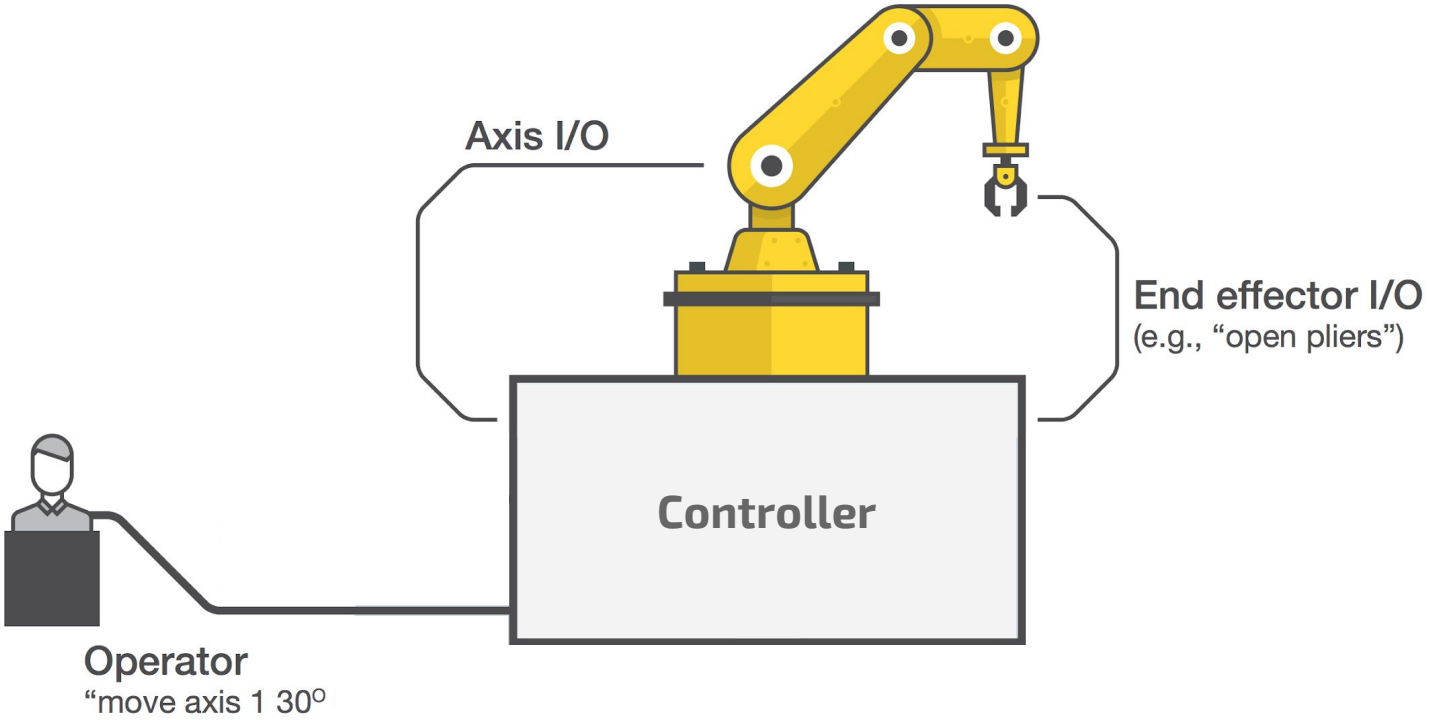
Stefano Zanero

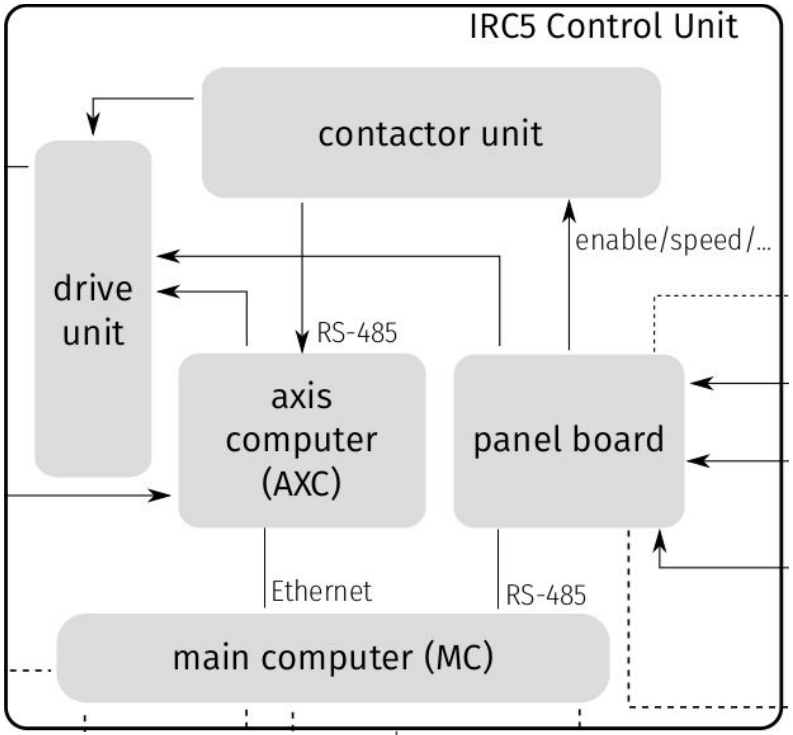
Associate Professor, Politecnico di Milano

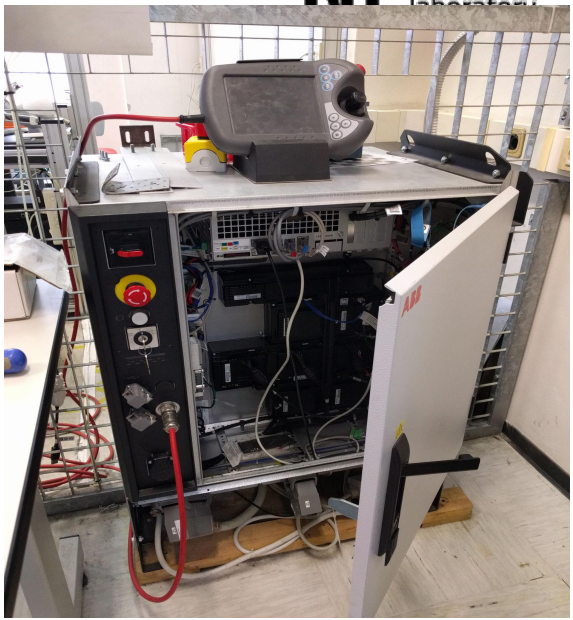
Joint work with: Davide Quarta, Marcello Pogliani, Mario Polino, Federico Maggi, Andrea M. Zanchettin

Industrial robots?

Industrial Robot Architecture (Standards)

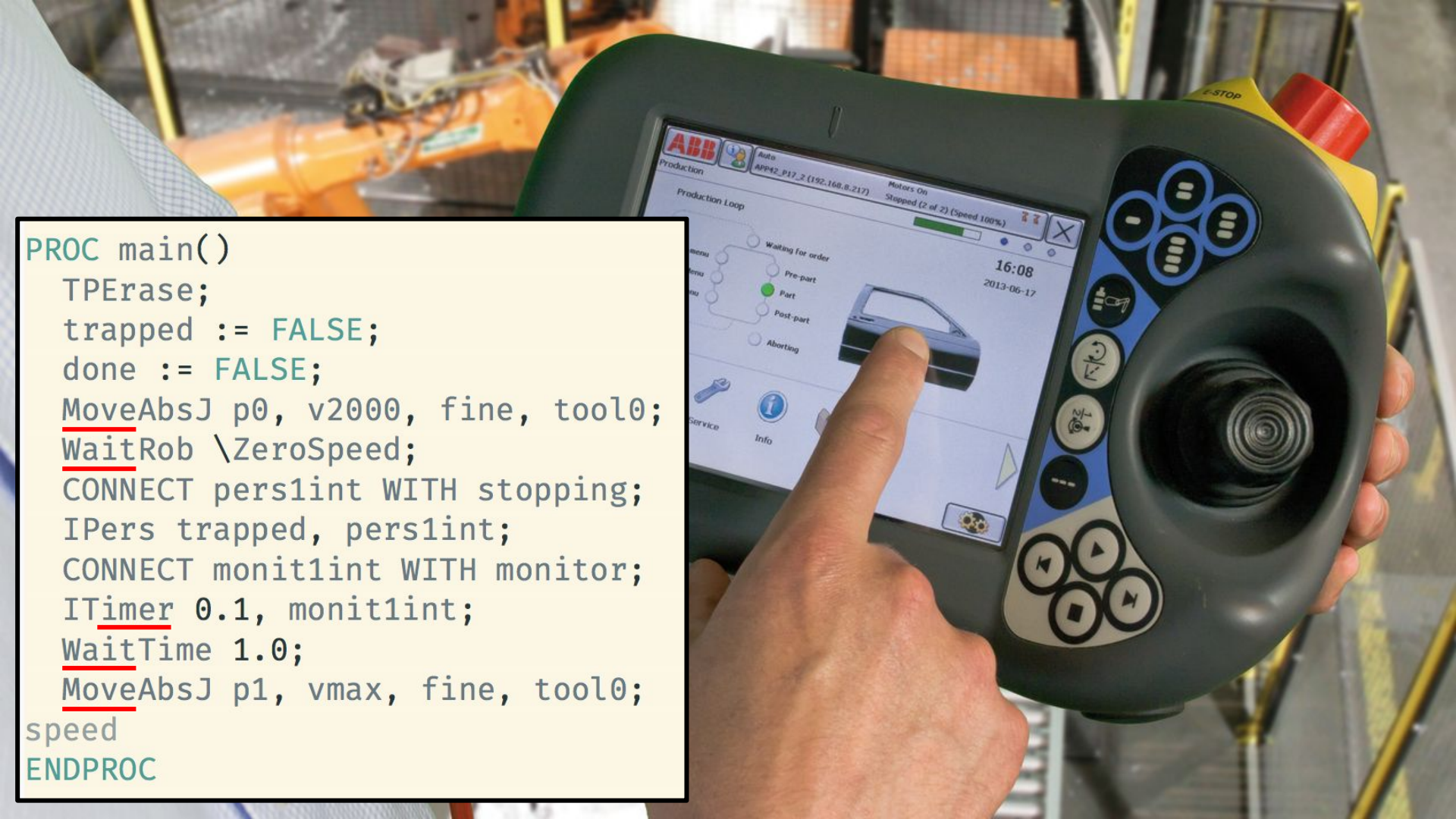



IRC5 Control Unit
contactor unit
drive unit
enable/speed/...
RS-485
axis computer (AXC)
panel board
Ethernet
RS-485
main computer (MC)



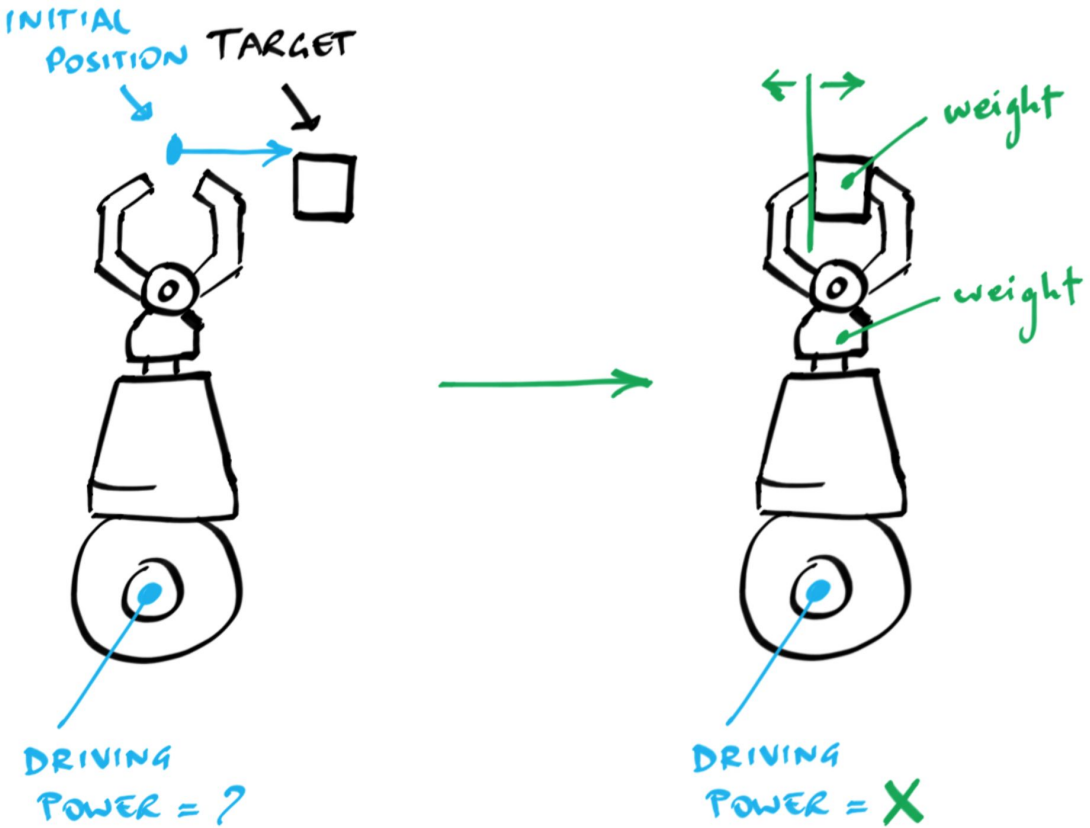
POLITECNICO MILANO 1863
NECST laboratory

Flexibly programmable



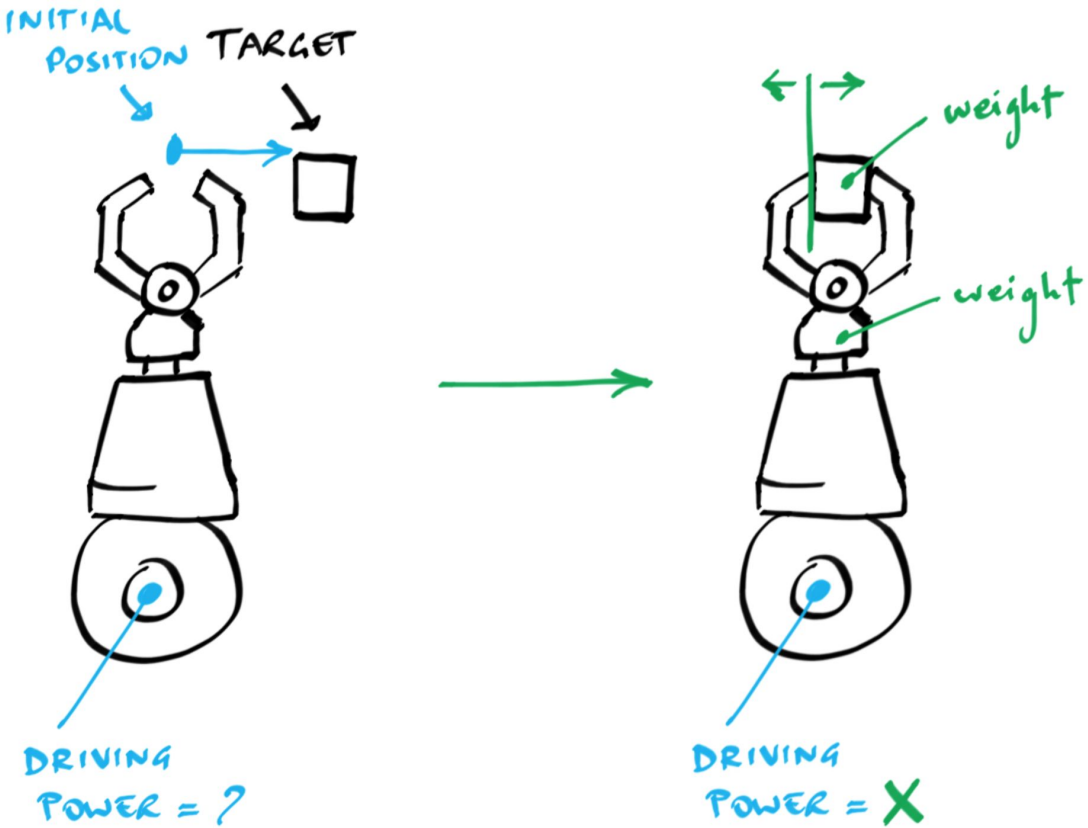

```
PROC main()
  TPErase;
  trapped := FALSE;
  done := FALSE;
  MoveAbsJ p0, v2000, fine, tool0;
  WaitRob \ZeroSpeed;
  CONNECT pers1int WITH stopping;
  IPers trapped, pers1int;
  CONNECT monit1int WITH monitor;
  ITimer 0.1, monit1int;
  WaitTime 1.0;
  MoveAbsJ p1, vmax, fine, tool0;
speed
ENDPROC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

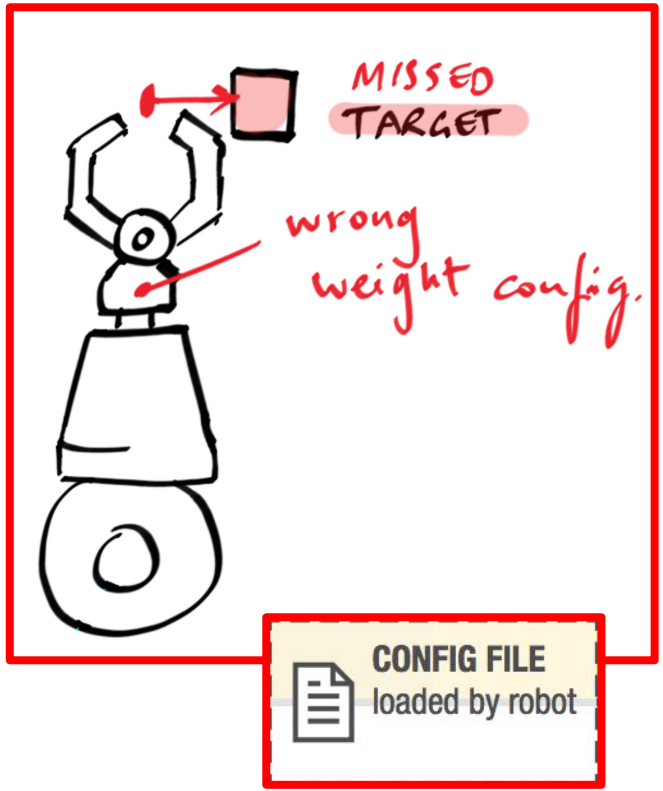
“Implicit” parameters



CONFIG FILE
loaded by robot

“Implicit” parameters





POLITECNICO MILANO 1863
NECST laboratory

Connected

(Part 1)

They are *already* meant to be connected

POLITECNICO MILANO 1863
NECST laboratory

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

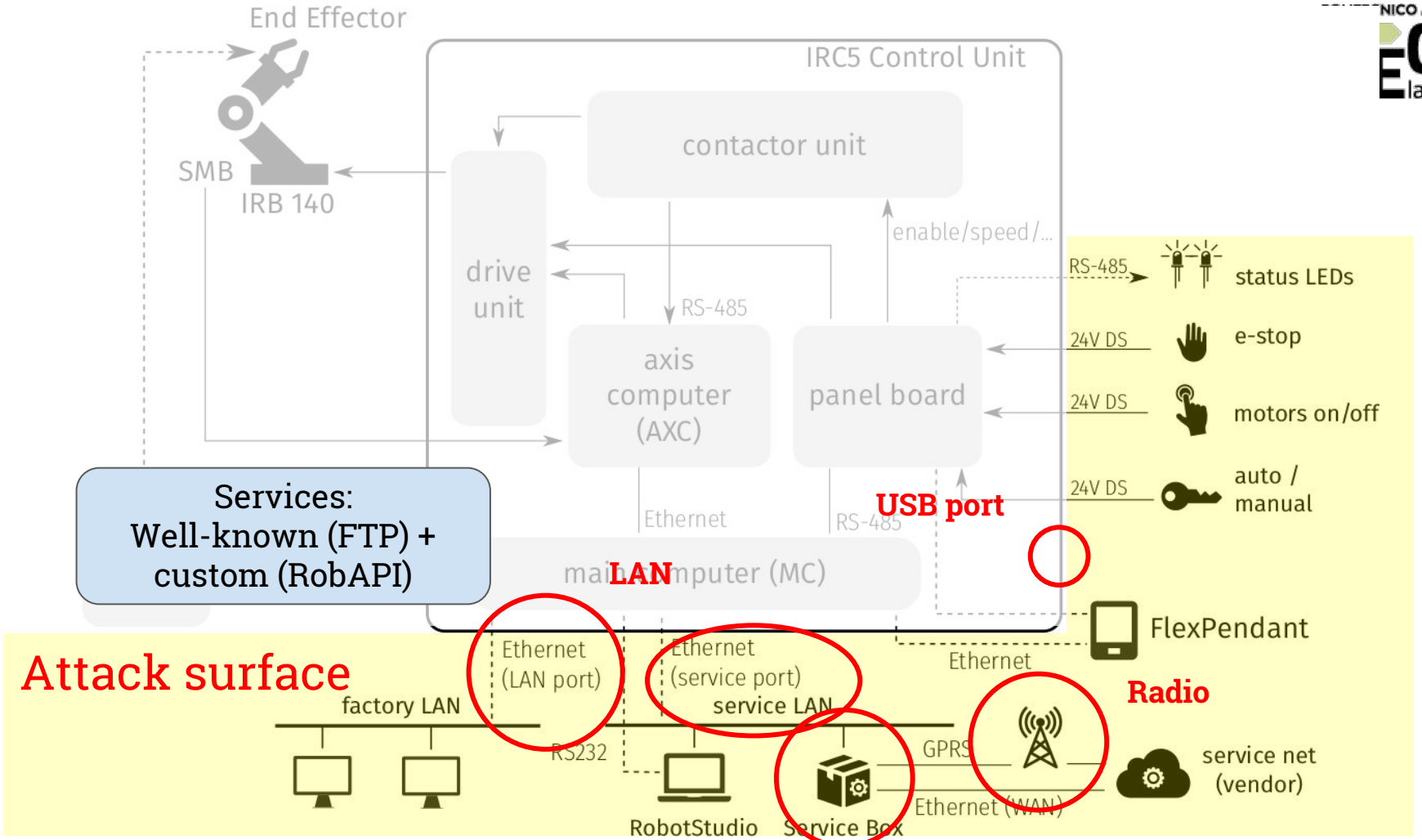
```
PROGRAM email NOHOLD, STACK = 10000
CONST ki_email_cnfg = 20
  ki_email_send = 21
```

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


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

Connected Robots: Why?

POLITECNICO MILANO 1863
NECST laboratory

- **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?


We assess
attack impact by
reasoning on
requirements

Requirements: "Laws of Robotics"

POLITECNICO MILANO 1863
NECST laboratory

Safety

Accuracy

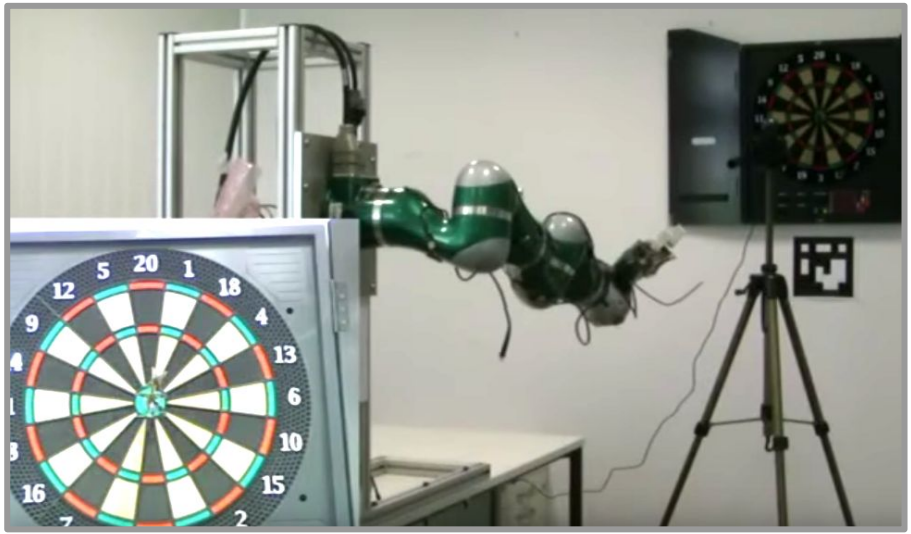
Integrity

Requirements: "Laws of Robotics"

Safety

Accuracy

Integrity



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

Requirements: "Laws of Robotics"

POLITECNICO MILANO 1863
NECST laboratory

Safety

Accuracy

Integrity

Robot-Specific Attack

POLITECNICO MILANO 1863
NECST laboratory

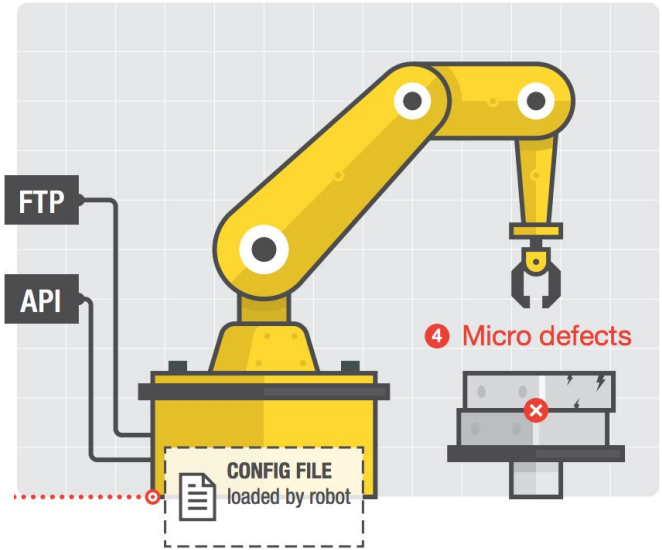
Safety

Accuracy

Integrity

violating any of these requirements via a *digital vector*

Control Loop Alteration



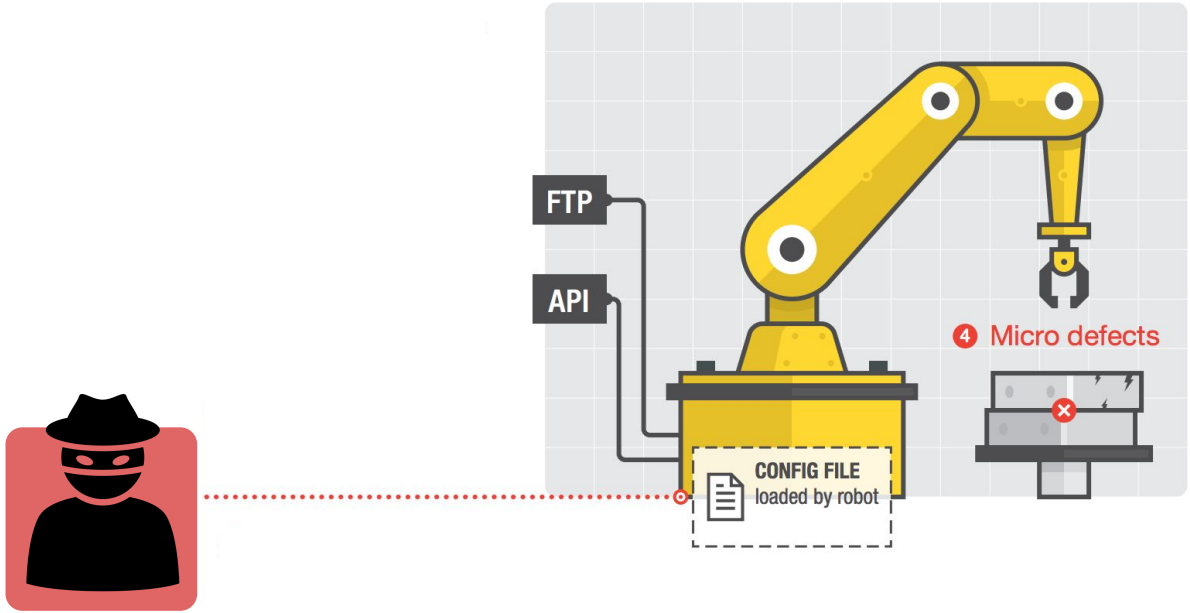
Attack 1

Safety

Accuracy

Integrity

Control Loop Alteration



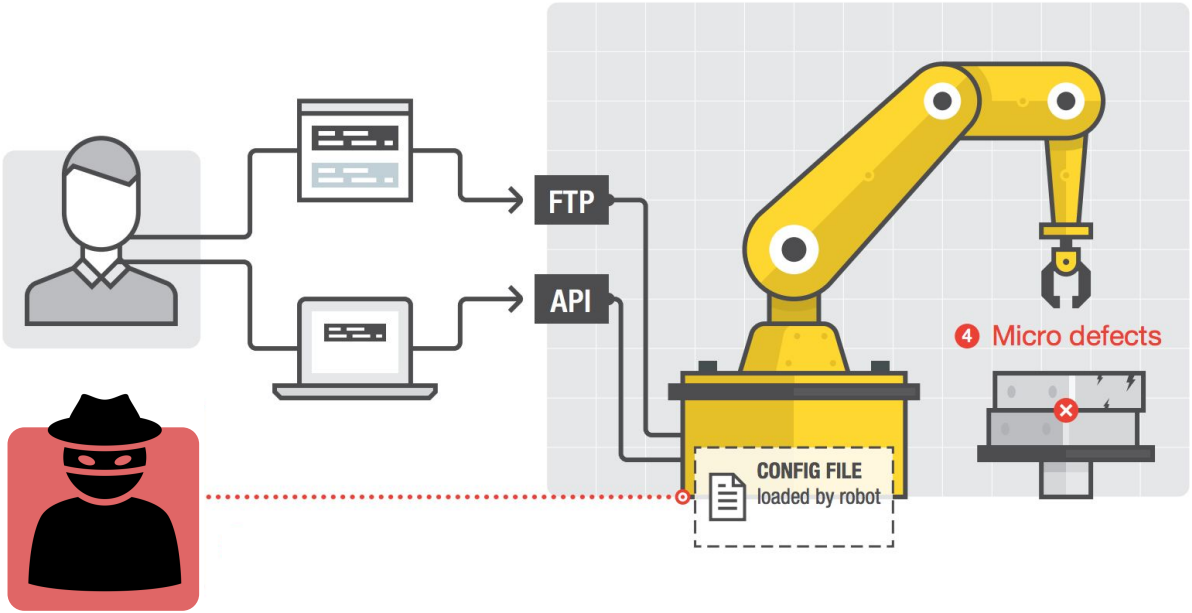
Attack 1

Safety

Accuracy

Integrity

Control Loop Alteration



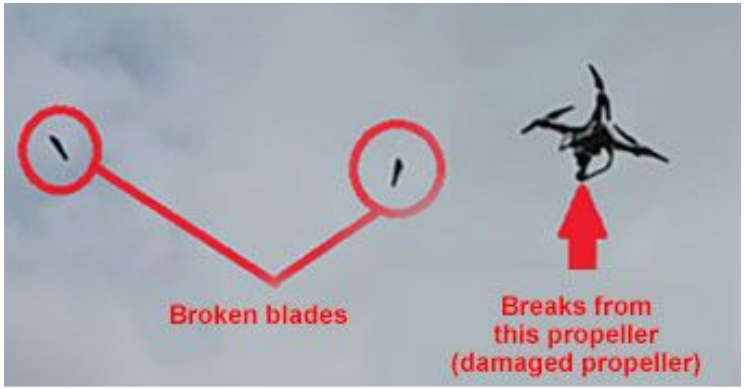
Attack 1

Safety

Accuracy

Integrity

Micro-defects in additive manufacturing



dr0wned - Cyber-Physical Attack with Additive Manufacturing
Sofia Belikovetsky, Mark Yampolskiy, Jinghui Toh, Yuval Elovici

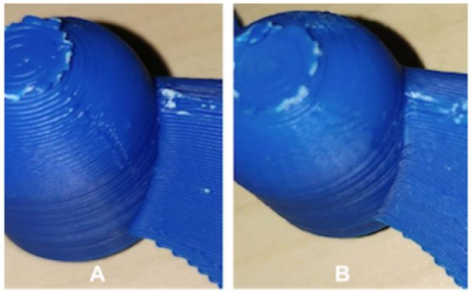
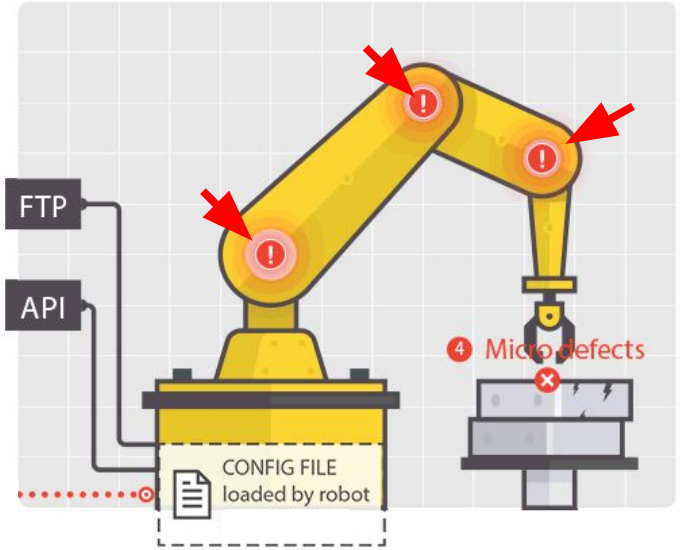


Figure 12. Two printed caps site-by-site. Cap A is *sabotaged* and Cap B is *benign*

Figure 13. Two printed propellers site-by-site. The Upper is *benign* and the lower is *sabotaged*

Calibration Tampering



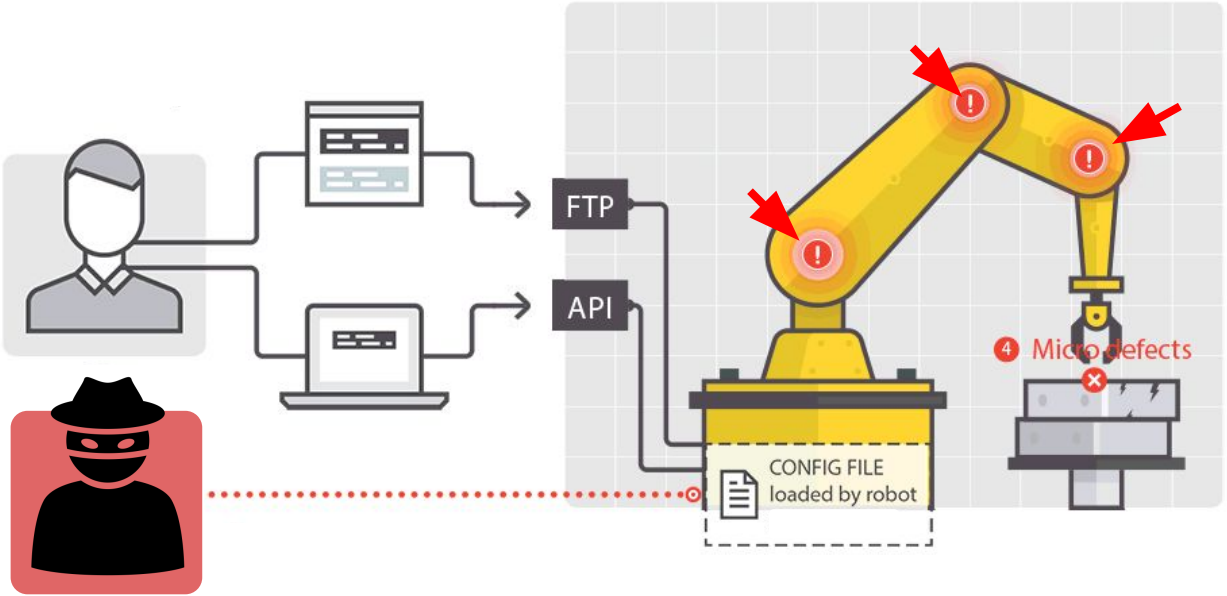
Attack 2

Safety

Accuracy

Integrity

Calibration Tampering



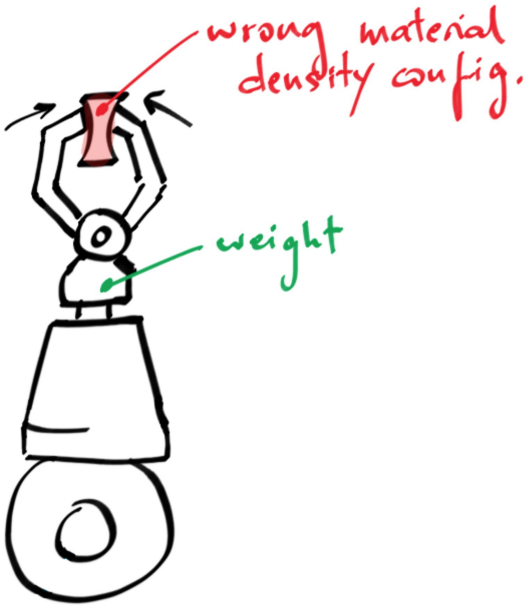
Attack 2

Safety

Accuracy

Integrity

Production Logic Tampering



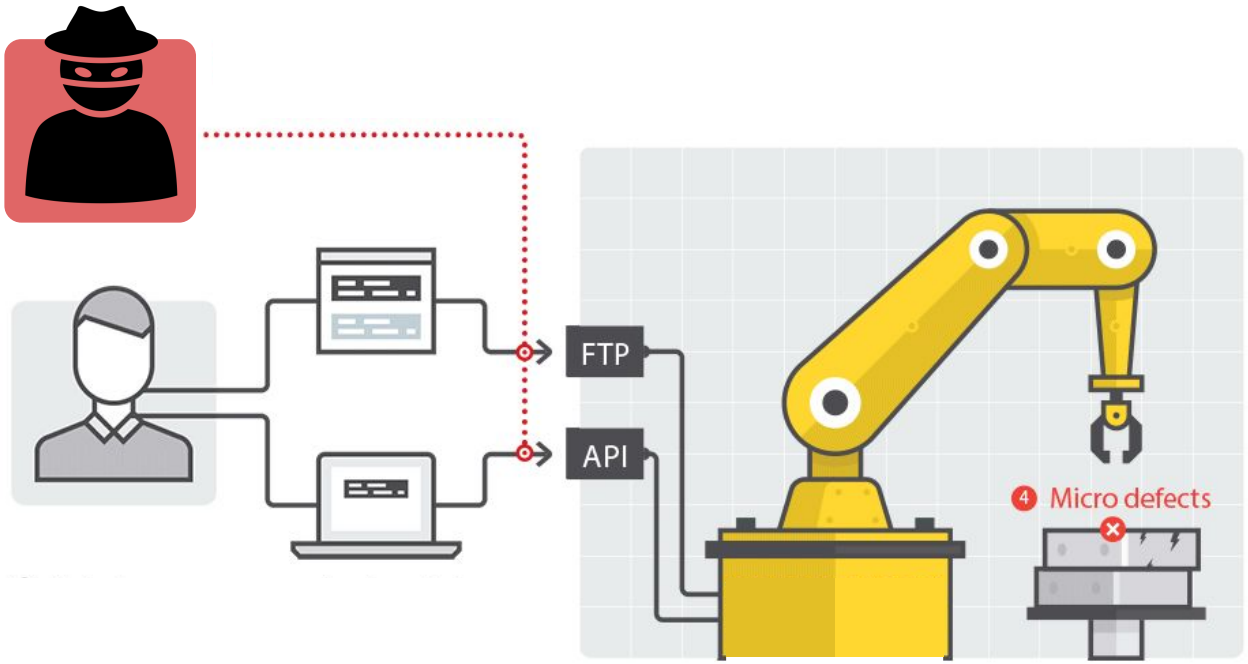
Attack 3

Safety

Accuracy

Integrity

Production Logic Tampering



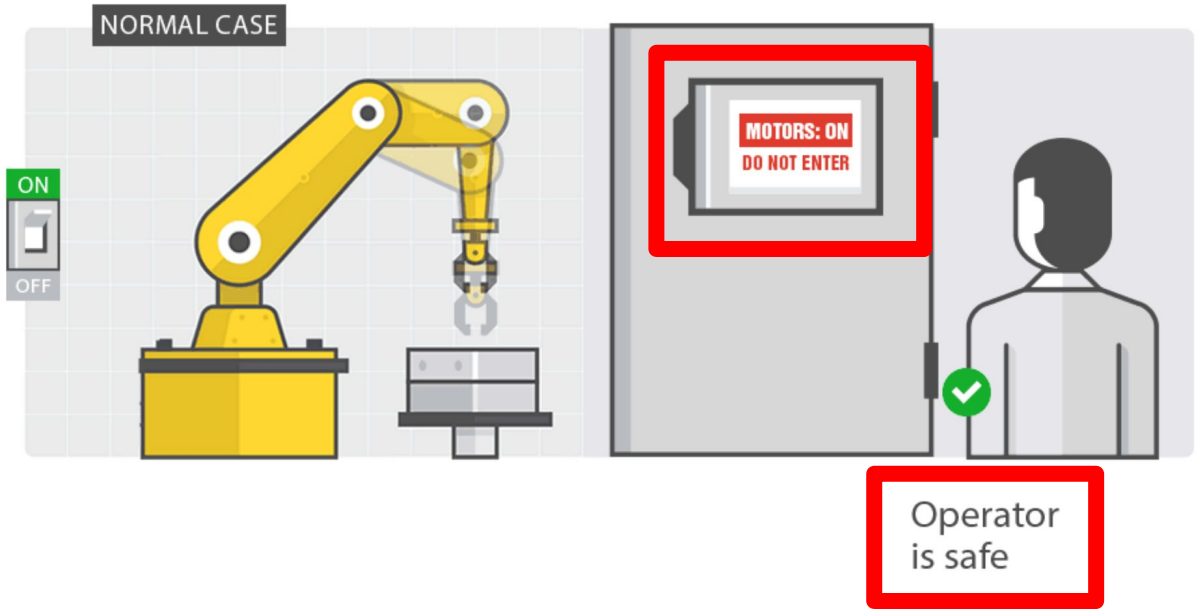
Attack 3

Safety

Accuracy

Integrity

Displayed or Actual State Alteration

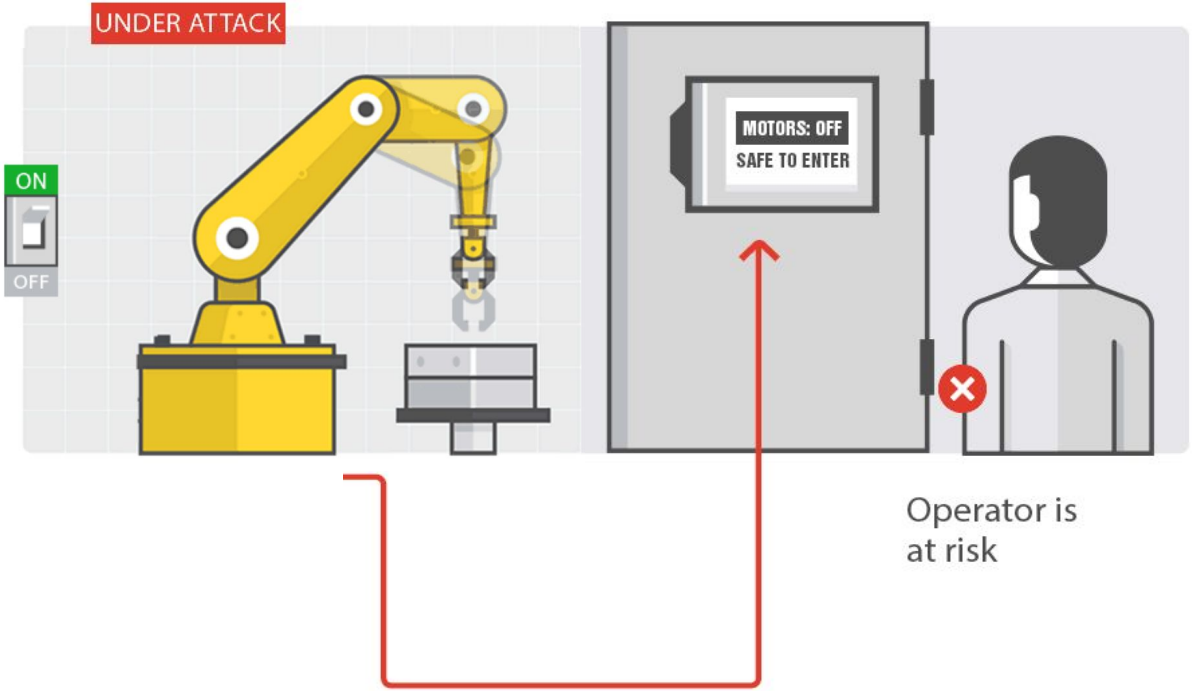


Attacks 4+5

Safety

Accuracy

Integrity



Attacks 4+5

Safety

Accuracy

Integrity

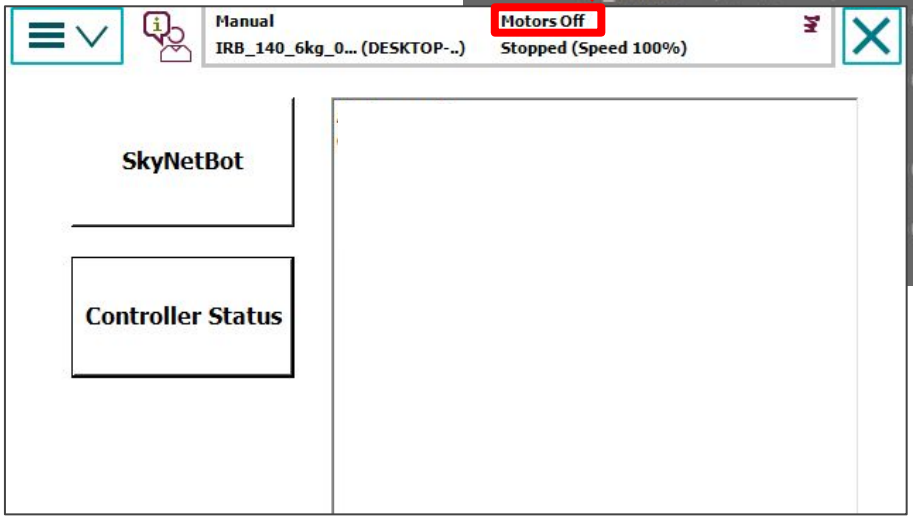
Displayed State Alteration PoC

POLITECNICO MILANO 1863
NECST laboratory

Malicious DLL

Teach Pendant

```
        IL_025c:  /* 03   |                    */ ldarg.1
        IL_025d:  /* 6F   | (0A)               */ call       instance string [System.Drawing/*23000
() /* 0A000028 */
        //IL_0262:  /* 02  |
        ldstr "Motors Off"                                    obotics.Tps.Controls.St
        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
```



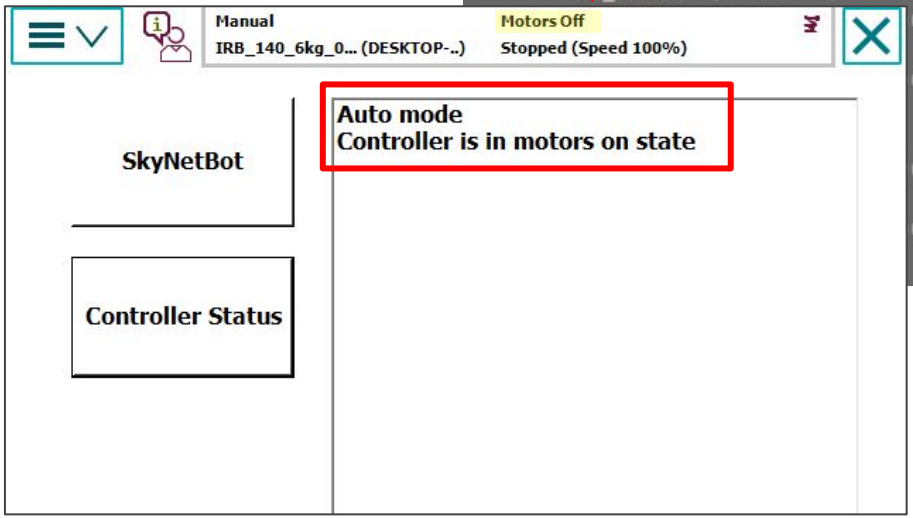
POLITECNICO MILANO 1863
NECST laboratory

Malicious DLL

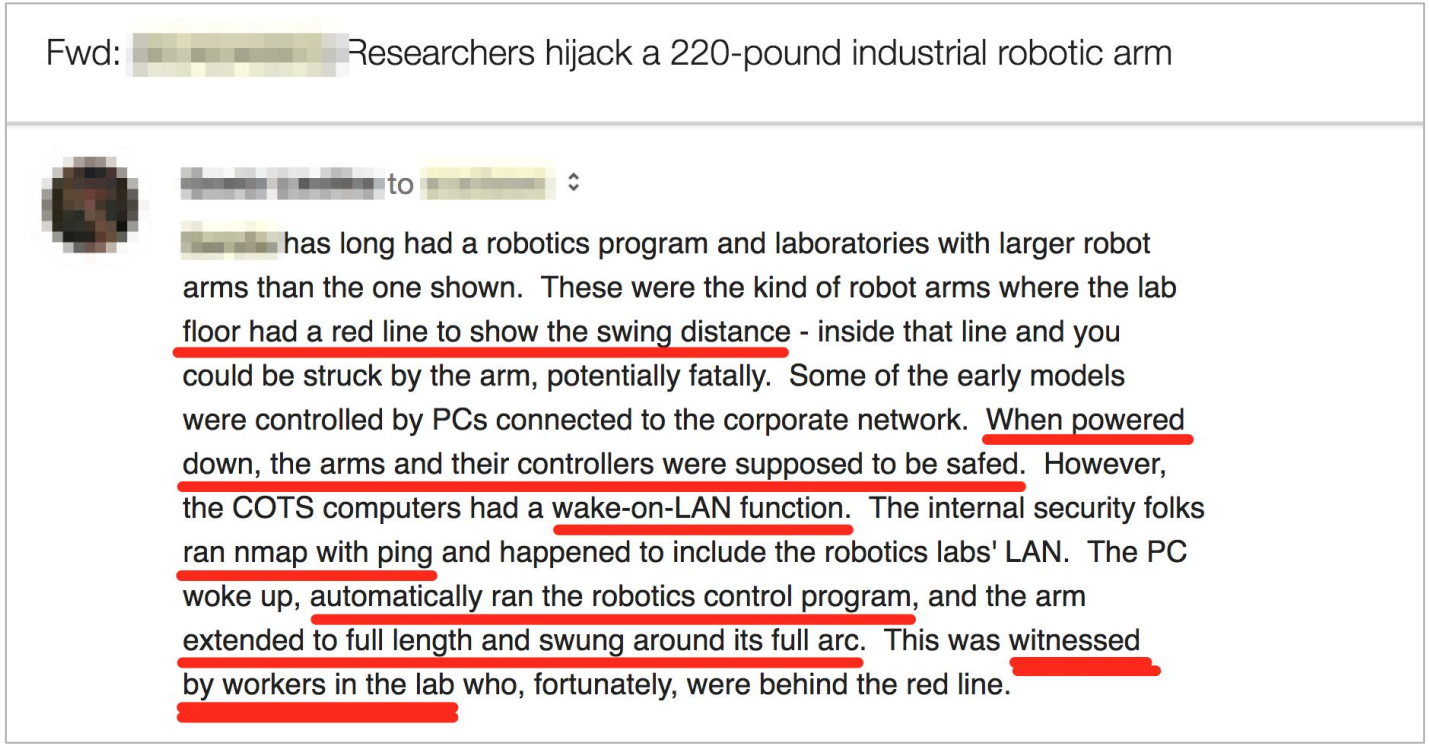
Teach Pendant

```
        IL_025c:  /* 03   |                    */ ldarg.1
        IL_025d:  /* 6F   | (0A)               */ call       instance int32 [System.Drawing/*23000
-() /* 0A000028 */
        //IL_0262:  /* 02  |
        ldstr "Motors Off"                                                  obotics.Tps.Controls.St
        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
```



Standards & Regulations vs. Real World



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

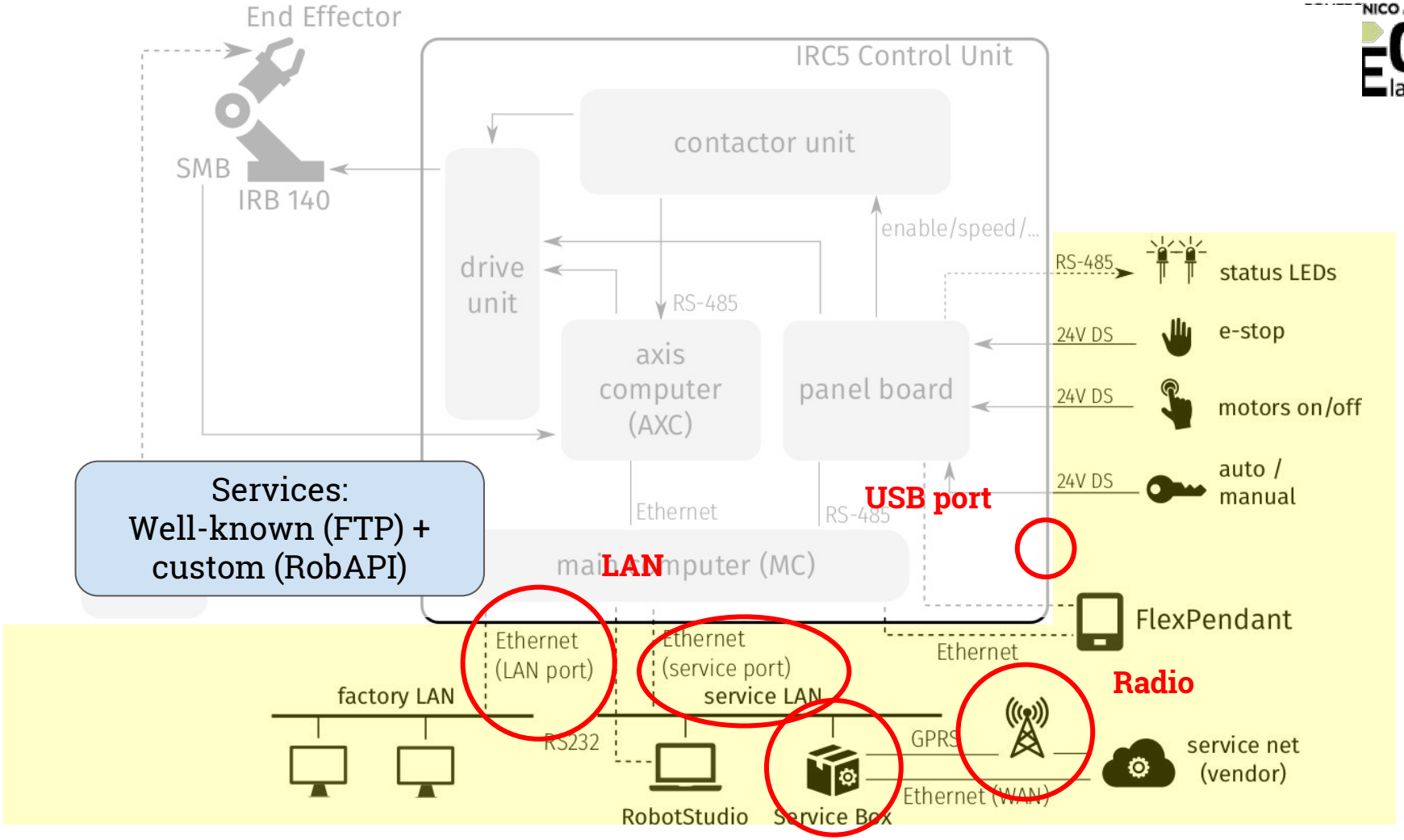
[redacted] to [redacted]

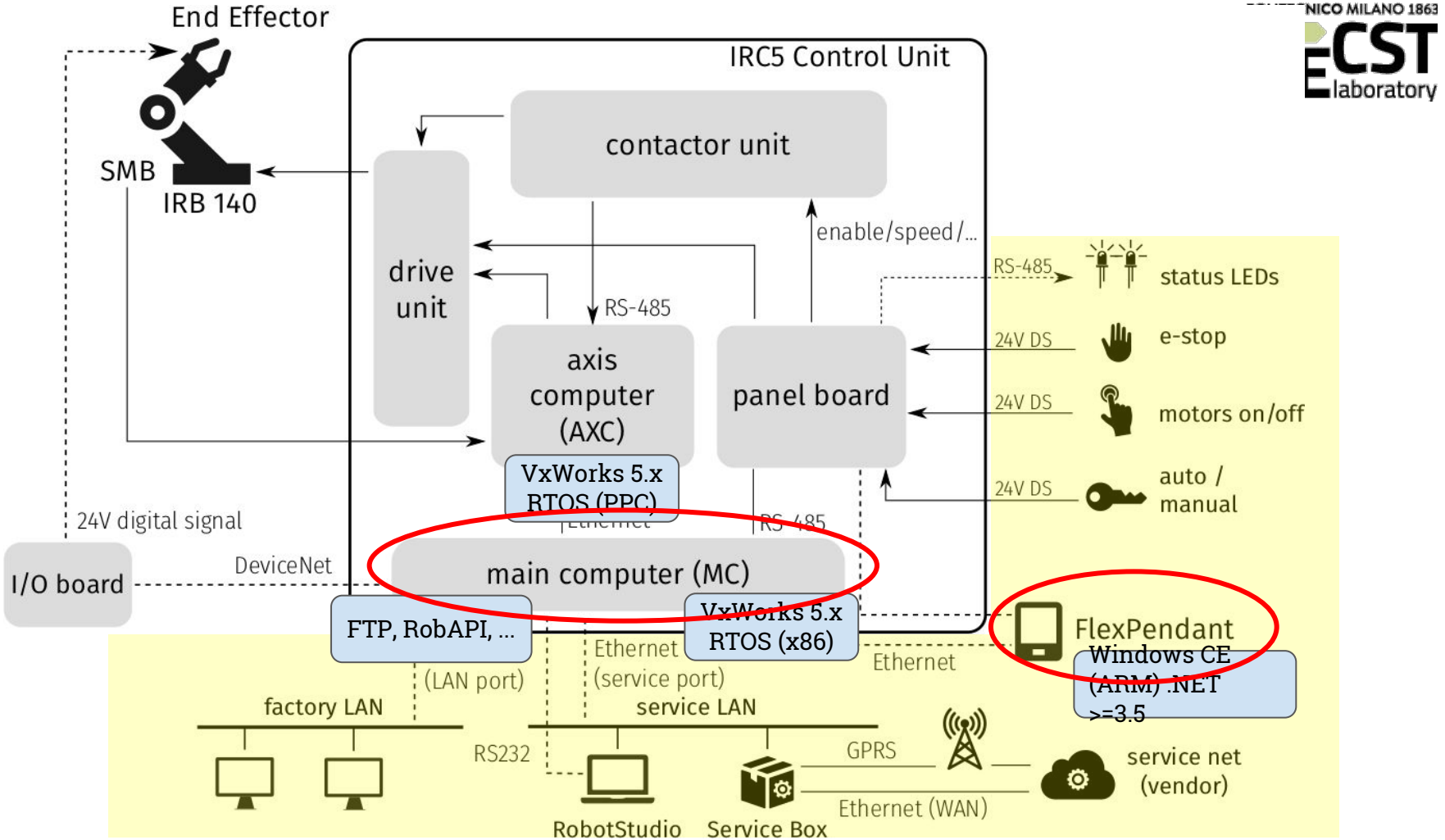
[redacted] has long had a robotics program and laboratories with larger robot arms than the one shown. These were the kind of robot arms where the lab floor had a red line to show the swing distance - inside that line and you could be struck by the arm, potentially fatally. Some of the early models were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

Collaborative Robotics

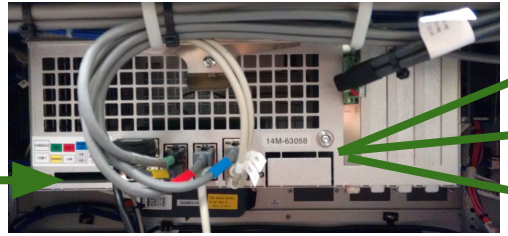
POLITECNICO MILANO 1863
NECST laboratory


let's compromise
the controller
KUKA
Container Systems


End Effector
SMB
IRB 140
IRC5 Control Unit
contactor unit
drive unit
enable/speed/...
RS-485
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
USB port
LAN
Services:
Well-known (FTP) +
custom (RobAPI)
Ethernet (LAN port)
Ethernet (service port)
Ethernet
FlexPendant
Radio
factory LAN
service LAN
RS232
GPRS
service net (vendor)
RobotStudio
Service Box
Ethernet (WAN)


End Effector
SMB
IRB 140
IRC5 Control Unit
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)
Ethernet
(LAN port)
factory LAN
service LAN
RS232
GPRS
service net (vendor)
Ethernet (WAN)
RobotStudio
Service Box

Update problems

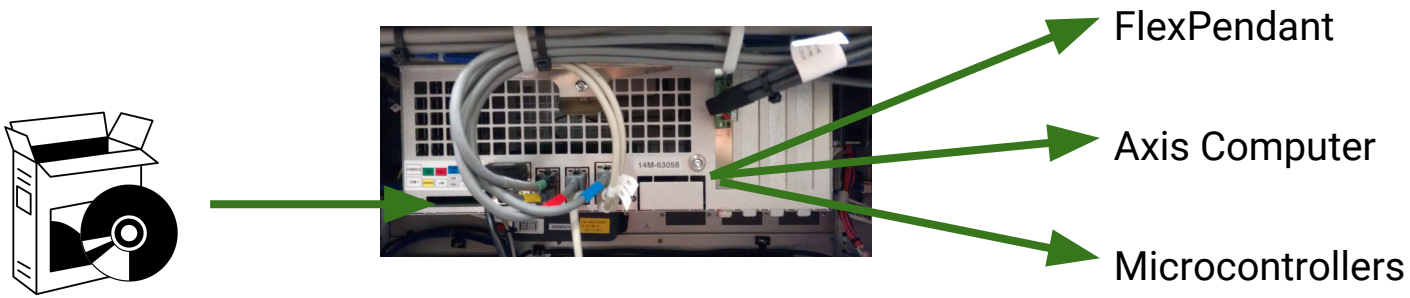


FlexPendant

Axis Computer

Microcontrollers

Update problems

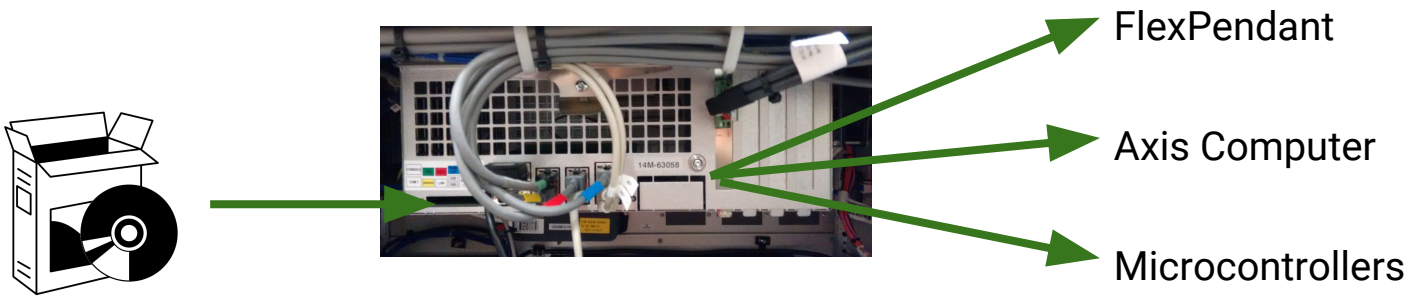


How? FTP at **boot**

```
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!

POLITECNICO MILANO 1863
NECST laboratory

```
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”

ABBVU-DMRO-124642

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
```

ABBVU-DMRO-124642

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**

ABBVU-DMRO-124642

Enter `/command`

POLITECNICO MILANO 1863
NECST laboratory

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

POLITECNICO MILANO 1863
NECST laboratory

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

Some **memory corruption**

Mostly **logical vulnerabilities**

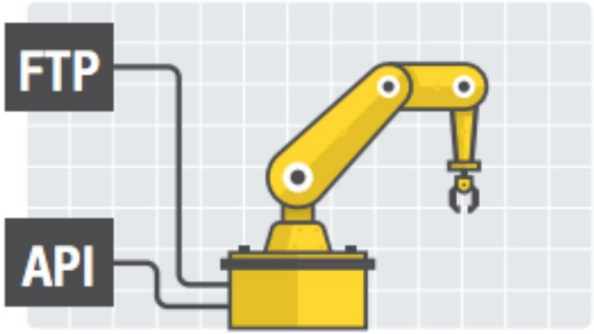
All the components blindly **trust** the **main computer (lack of isolation)**

Complete attack chain (1)

POLITECNICO MILANO 1863
NECST laboratory

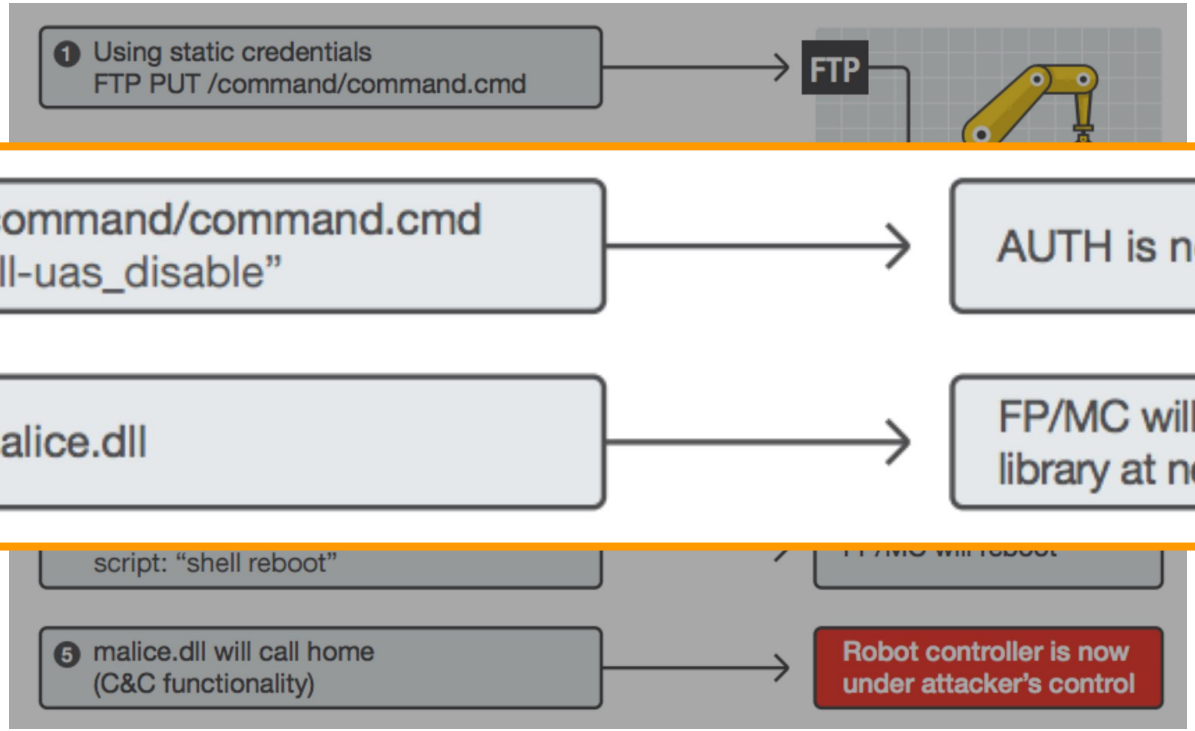
1. Using static credentials
   FTP PUT /command/command.cmd

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

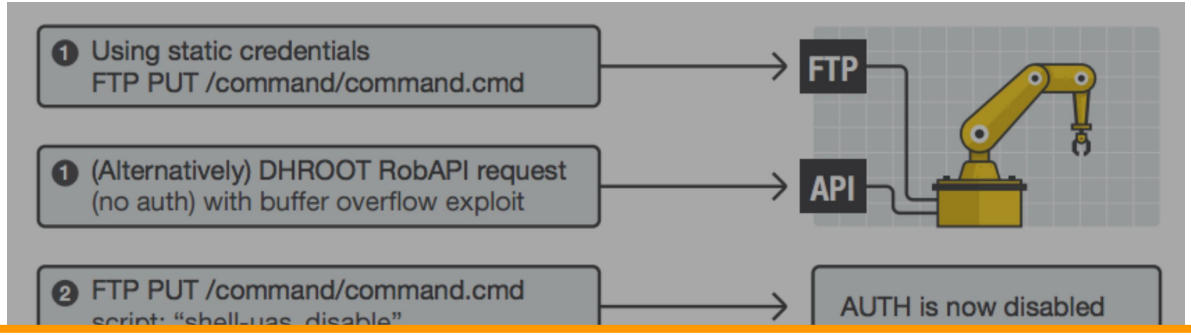


3. FTP PUT malice.dll → FP/MC will load malicious library at next boot
4. FTP PUT /command/command.cmd
   script: “shell reboot” → FP/MC will reboot
5. malice.dll will call home
   (C&C functionality) → **Robot controller is now under attacker’s control**

Complete attack chain (2)



Complete attack chain (3)



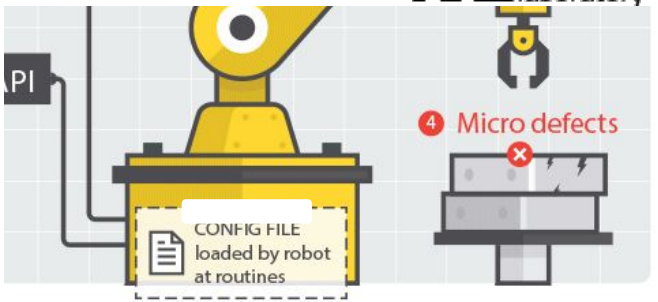
4 FTP PUT /command/command.cmd
script: “shell reboot”

→ 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:

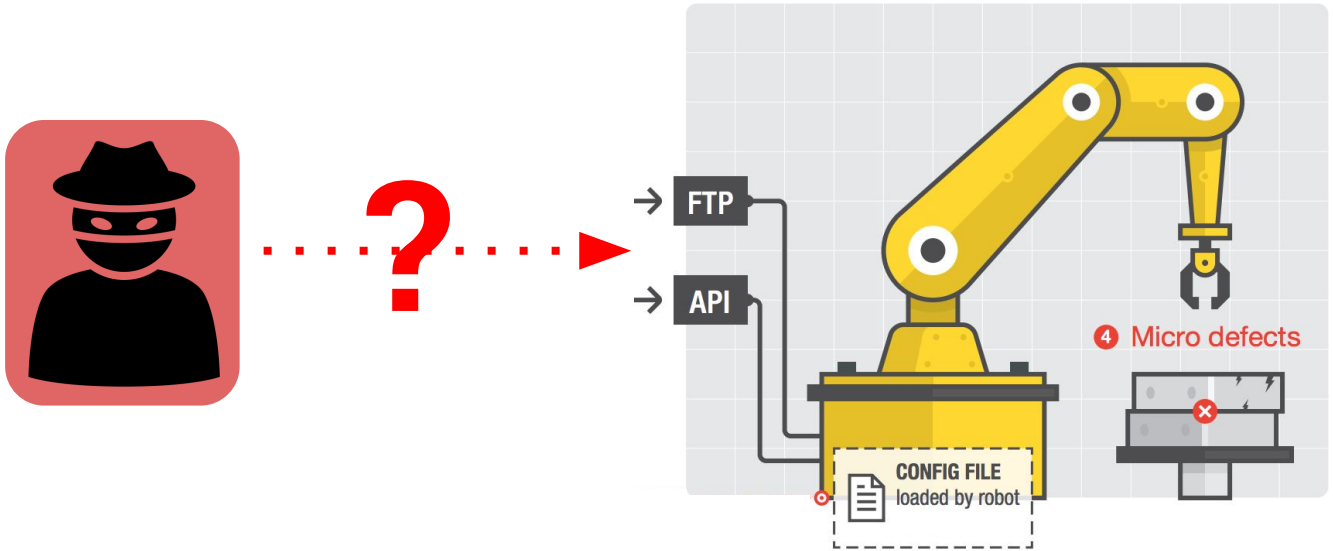
- Users’ credentials and permissions
- Sensitive configuration parameters (e.g., PID)
- Industry secrets (e.g., workpiece parameters)

Obfuscation: bitwise XOR with a “random” key.

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

That’s how we implemented the attacks

Attack Surface



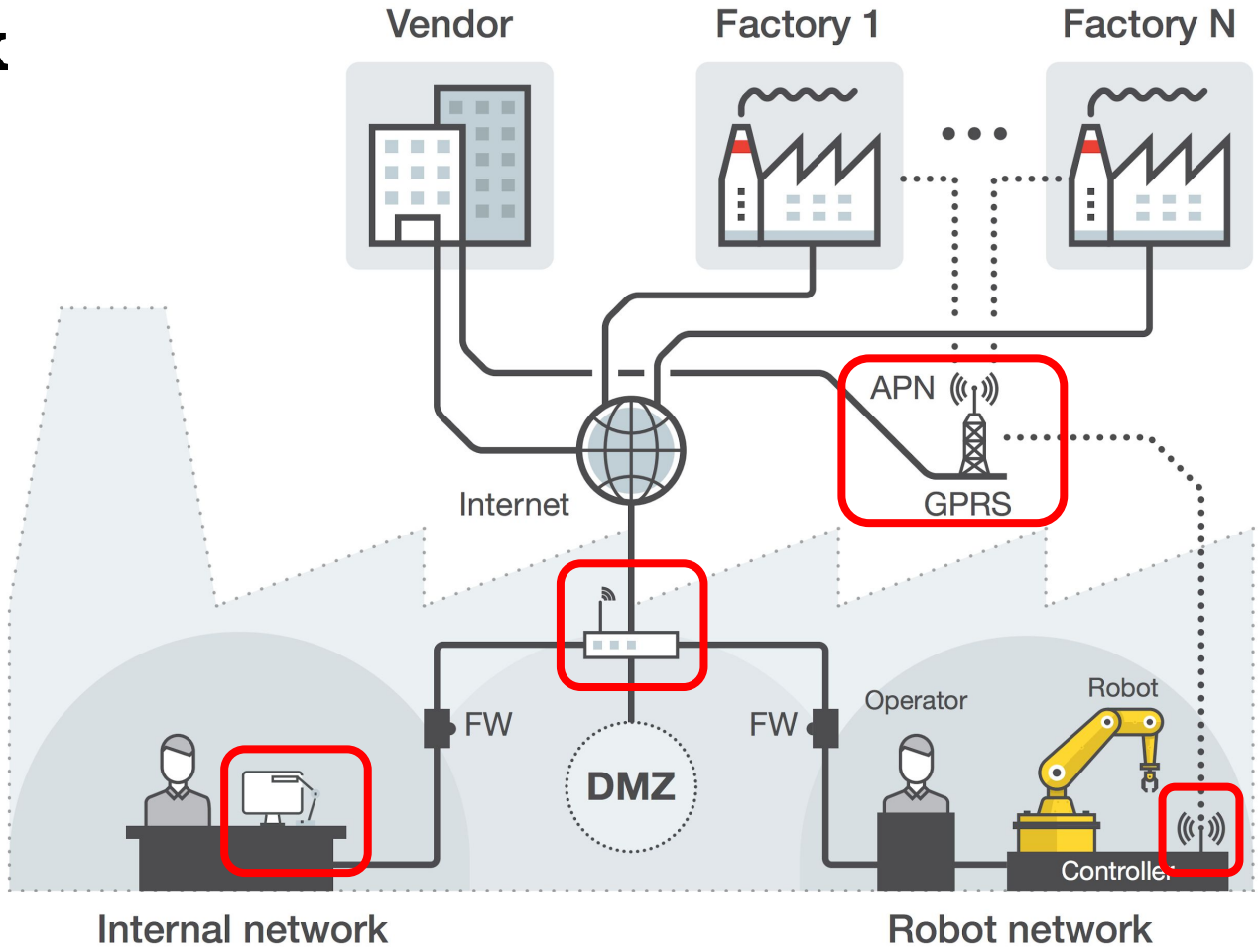
Attack Surface

Network

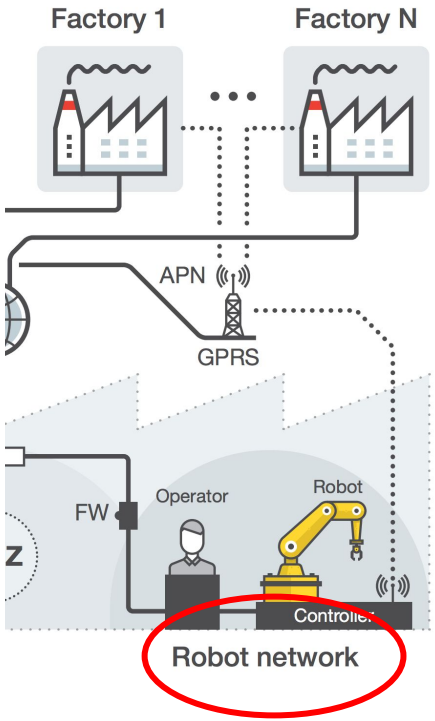
Physical (but digital)

Programming Languages

Network


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

Remote Exposure of Industrial *Robots*



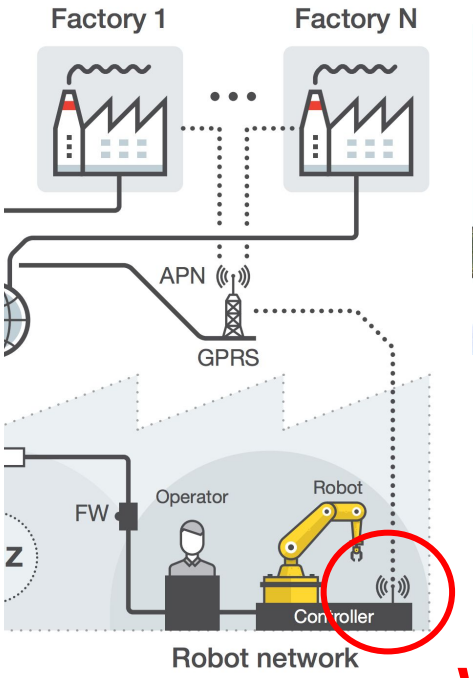
Search	Entries	Country
ABB Robotics	5	DK, SE
FANUC FTP	9	US, KR, FR, TW
Yaskawa	9	CA, JP
Kawasaki E Controller	4	DE
Mitsubishi FTP	1	ID
Overall	**28**	**10**

Not so many...

(yesterday I've just found 10 more)

Remote Exposure of Industrial *Routers*

POLITECNICO MILANO 1863
NECST laboratory



...way many more!

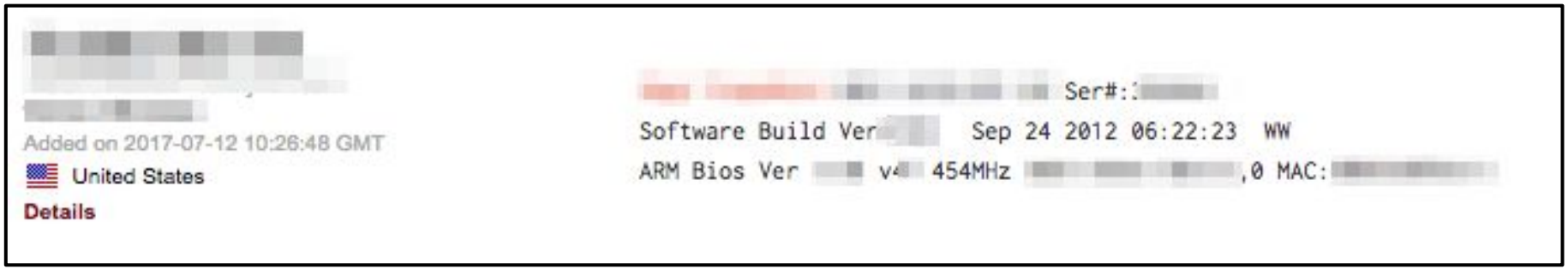
Brand	Exposed Devices	No Authentication
Belden	956	
Eurotech	160	
eWON	6,219	1,160
Digi	1,200	
InHand	883	
Moxa	12,222	2,300
NetModule	886	135
Robustel	4,491	
Sierra Wireless	50,341	220
Virtual Access	209	
Welotec	25	
Westermo	6,081	1,200
TOTAL	83,673	5,105

Unknown which routers are actually robot-connected

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



Typical Issues (1)

POLITECNICO MILANO 1863
NECST laboratory

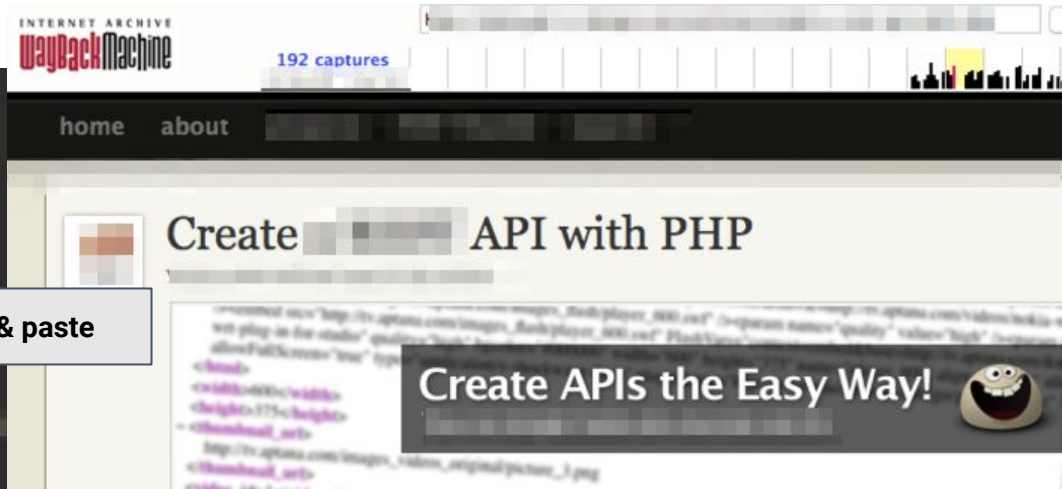
Outdated Software Components

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

Typical Issues (2)

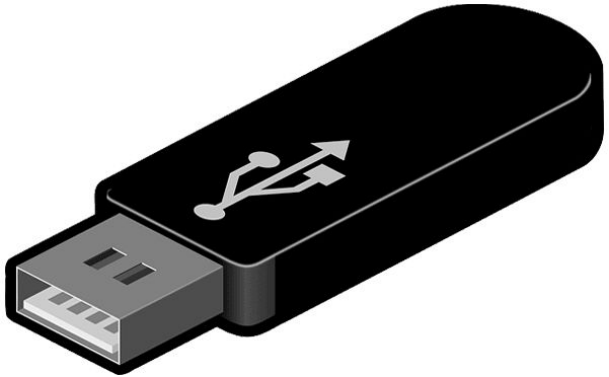
Insecure Web Interface

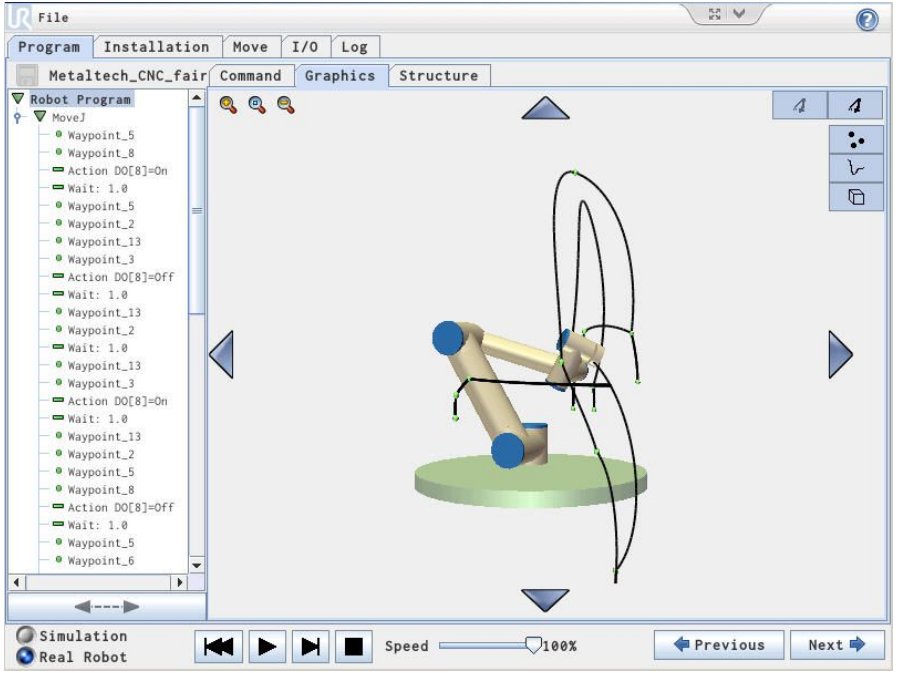
- Poor input sanitization
- E.g., code coming straight from a "beginners" blog



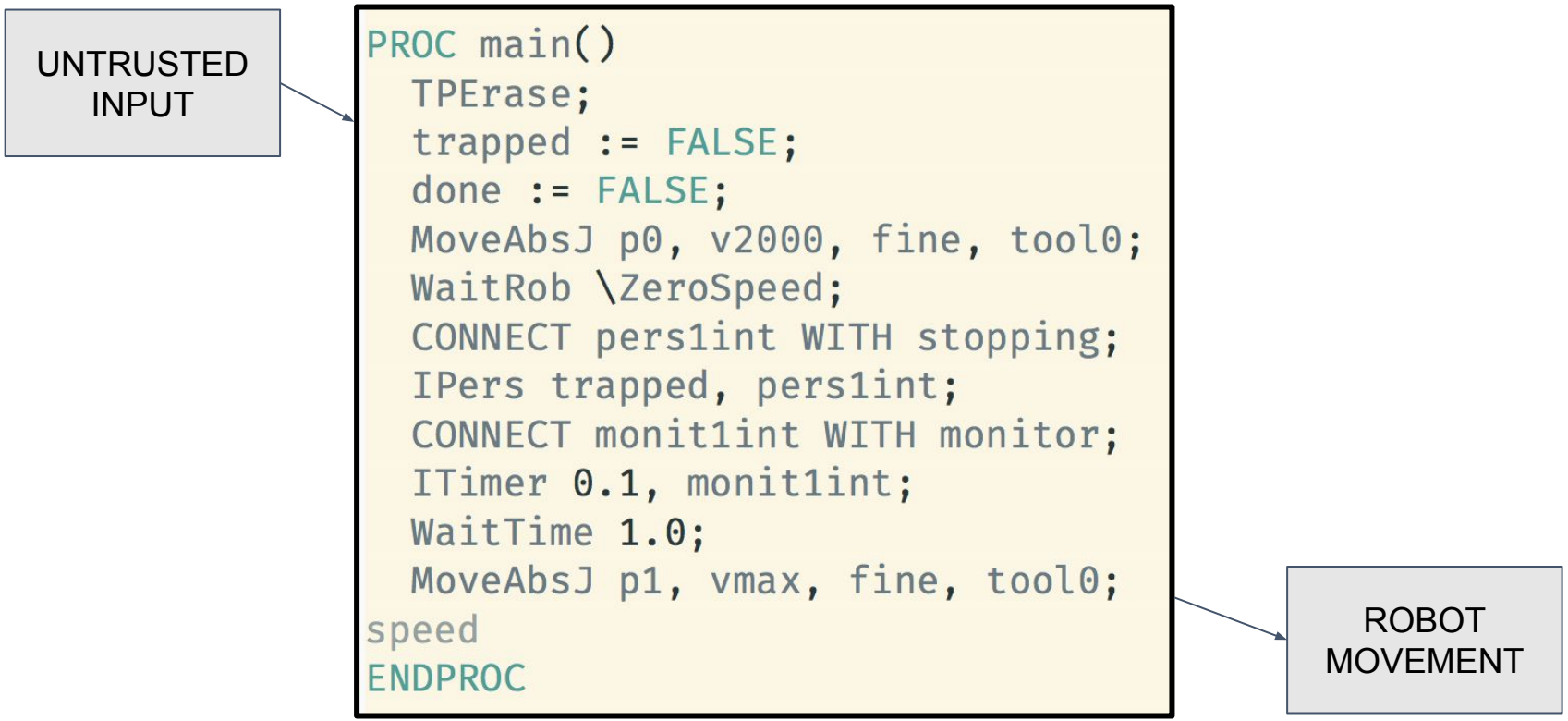
Cut & paste

Physical Attack Surface





Programming Languages Attack Surface



Conclusions

Conclusions

Robots are increasingly being **connected**

Industrial robot-specific class of attacks

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

What should we do now?

POLITECNICO MILANO 1863
NECST laboratory

Some **vendors** are very **responsive**

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

Hints on Countermeasures

POLITECNICO MILANO 1863
NECST laboratory

Short term

Attack detection and deployment hardening

Medium term

System hardening

Long term

New standards, beyond safety issues

Questions?

Please reach out!

stefano.zanero@polimi.it
@raistolo

Papers, slides, and FAQ
http://robosec.org