POLITECNICO
MILANO 1863
DIPARTIMENTO DI ELETTRONICA
INFORMAZIONE E BIOINGEGNERIA

Robotica industriale e sicurezza dei dati nella fabbrica connessa

Mario Polino

NECSTLab,
Dipartimento di Elettronica Informazione e Bioingegneria,
Politecnico di Milano

Who am I ?

Mario Polino, PhD
SecRec @ Polimi
http://jinblack.it
🐦 @JinBlackx

InfoSec:
Malware Analysis, Binary Analysis,
Cyber Physical System Analysis

CTF Player @ Tower of Hanoi
(🐦 @towerofhanoi)

T0fH

Computers are Everywhere!

- SmartPhone
- Autonomous Car
- SmartGrid
- SmartBuilding
- Internet of Things
- Industry 4.0

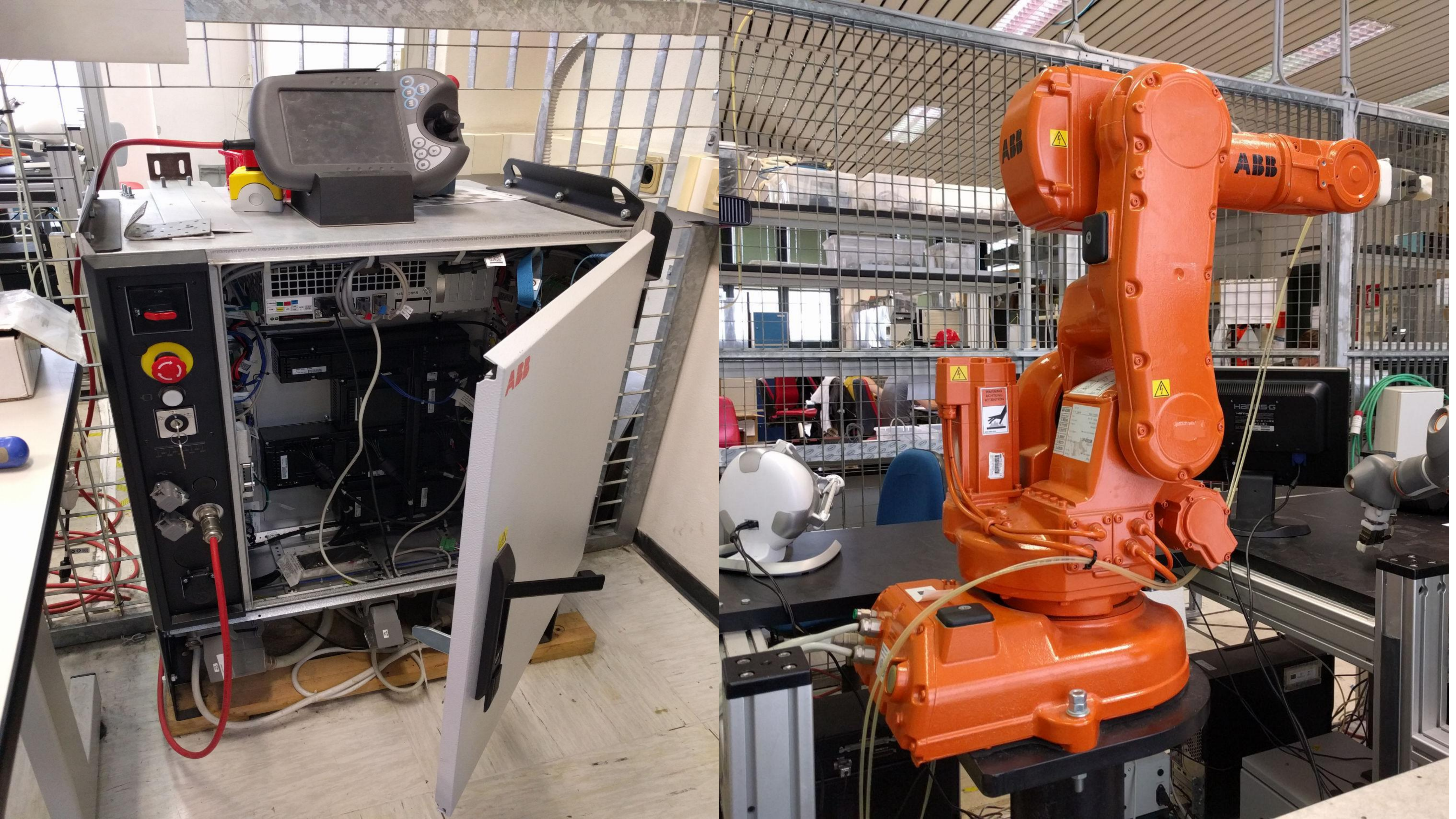
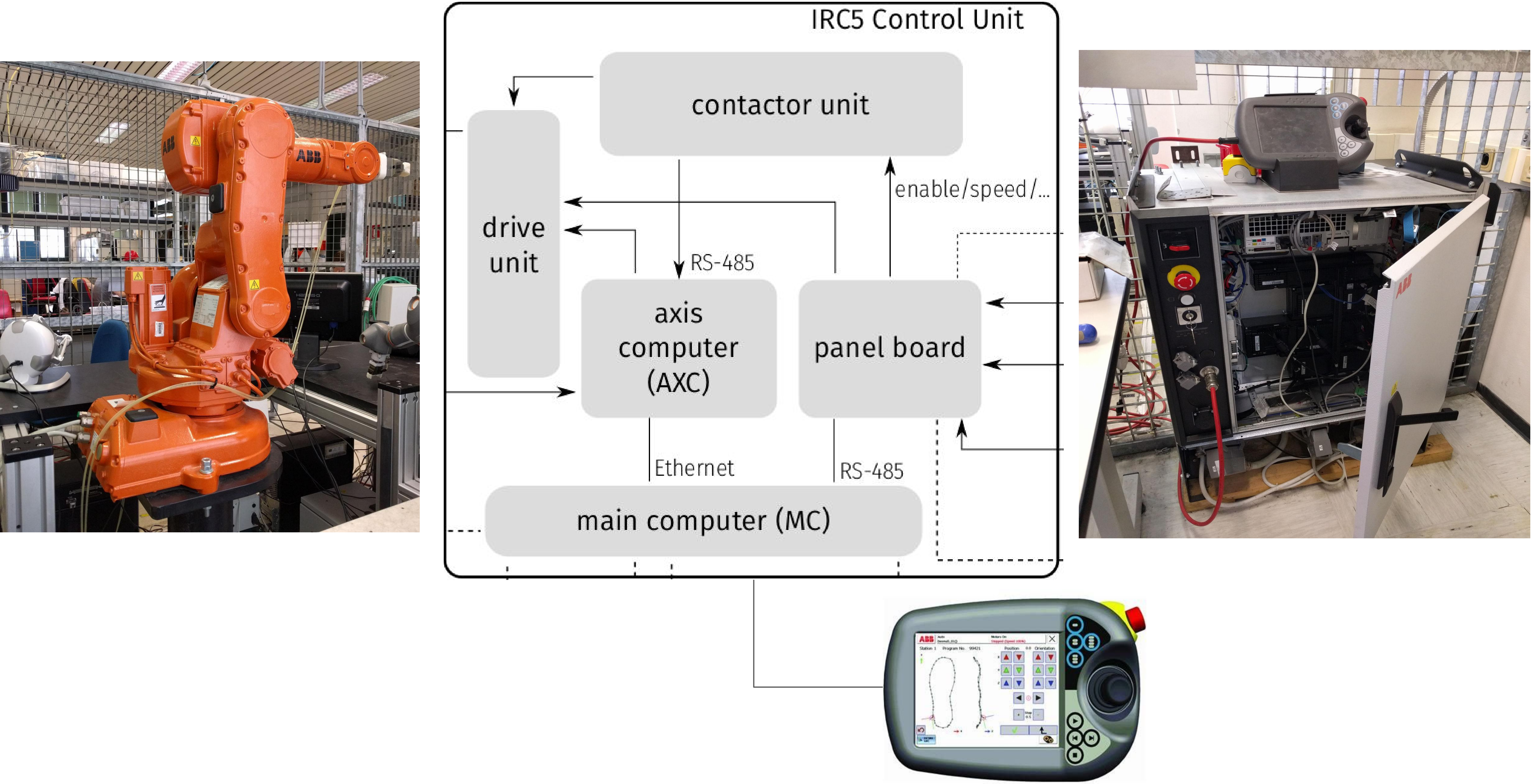
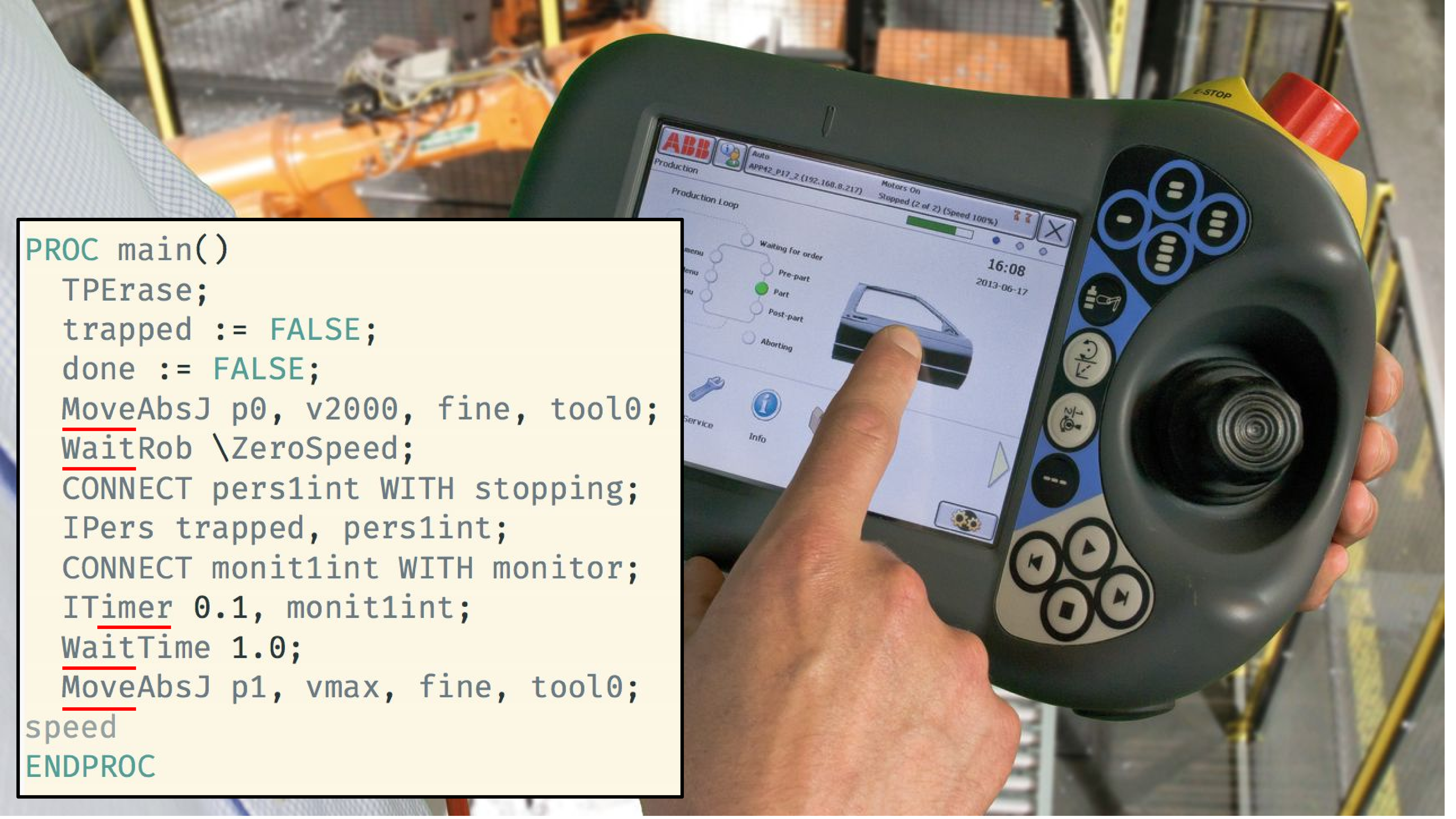
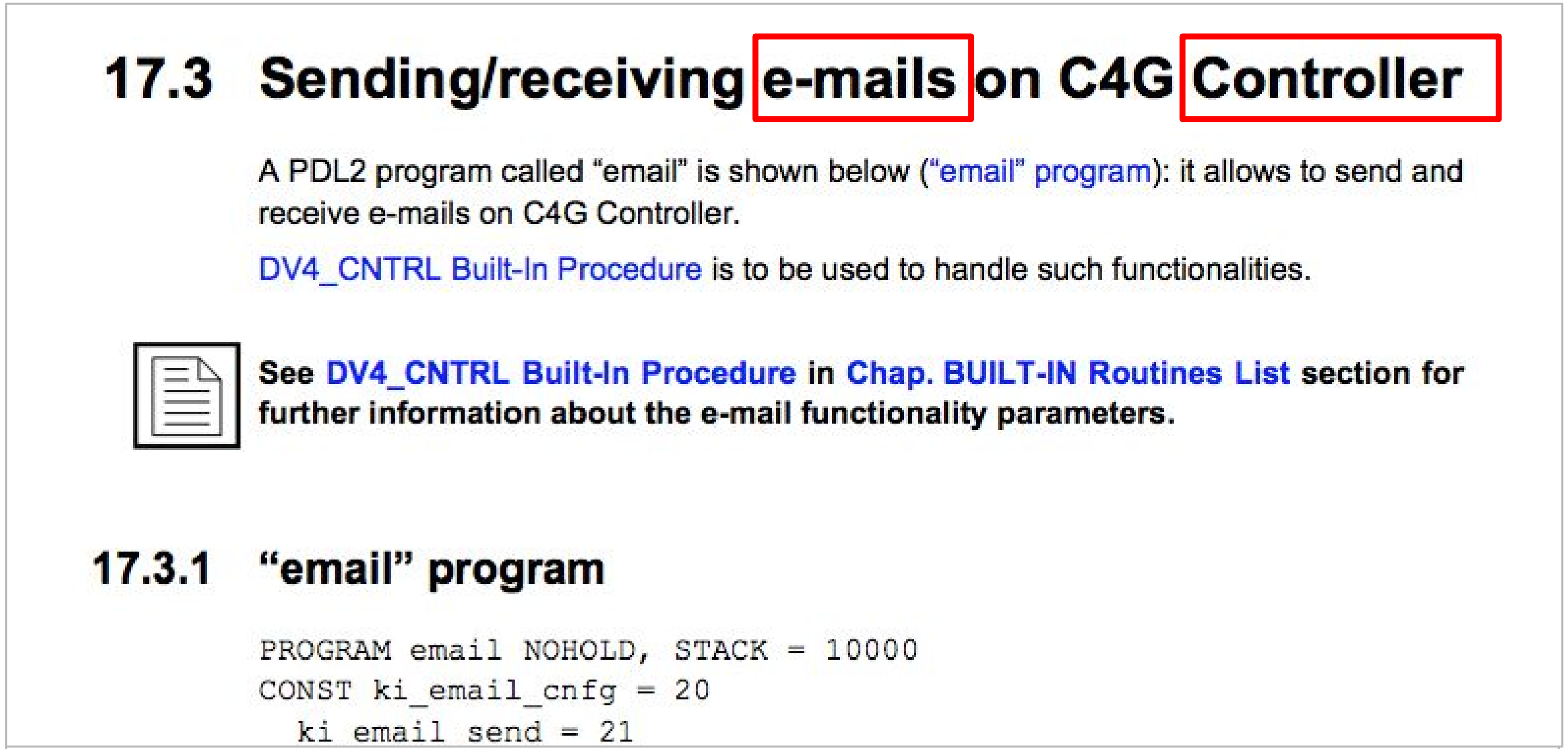


ABB
ABB
ABB
ABB


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



```
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
```



17.3 Sending/receiving e-mails on C4G Controller

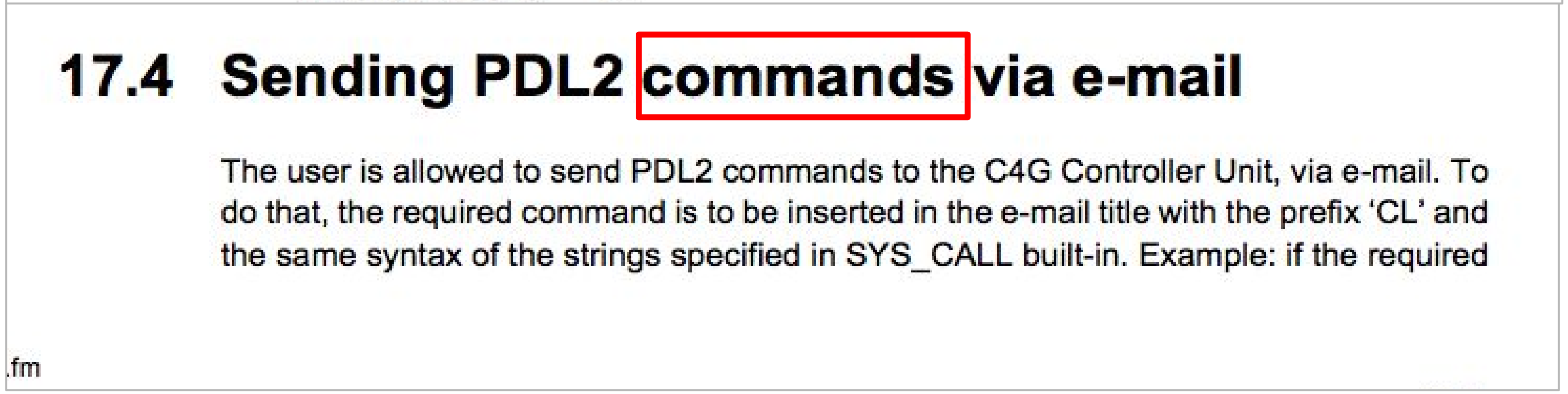
A PDL2 program called “email” is shown below (“email” program): it allows to send and receive e-mails on C4G Controller.

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.

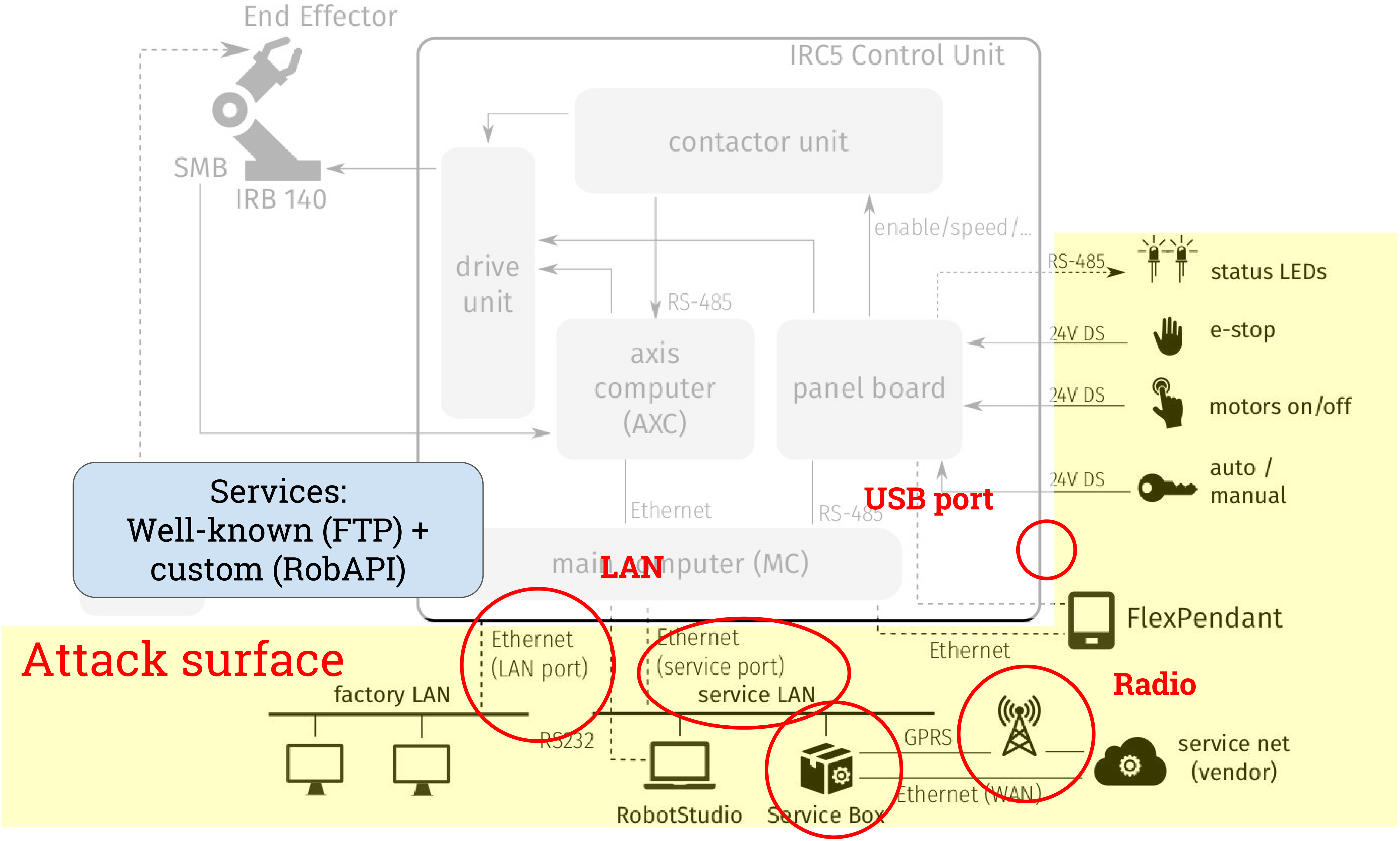
17.3.1 “email” program

```
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



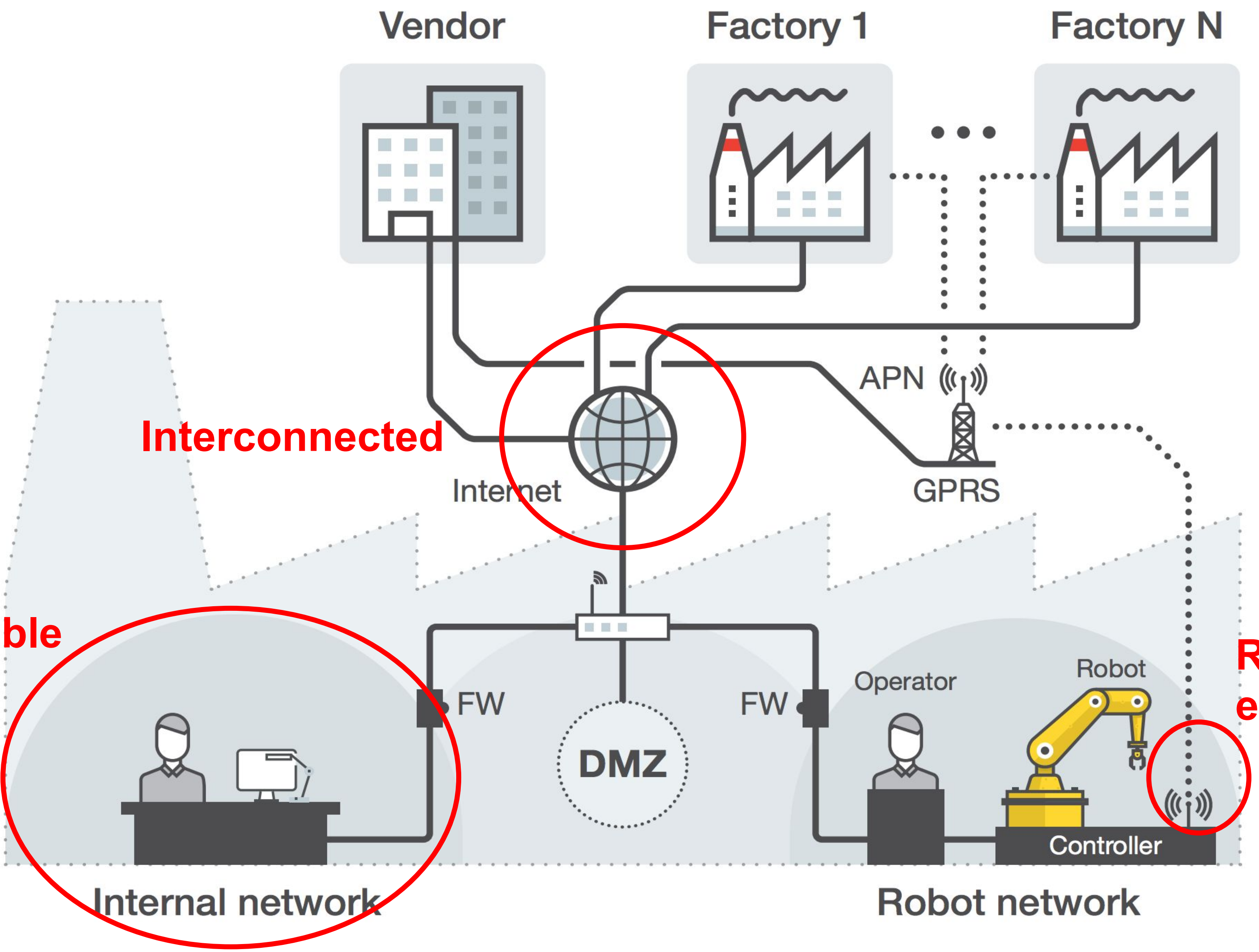
Services:
Well-known (FTP) +
custom (RobAPI)

Attack surface

USB port

LAN

Radio



Interconnected

Flexibly programmable

Remotely exposed

Connected?

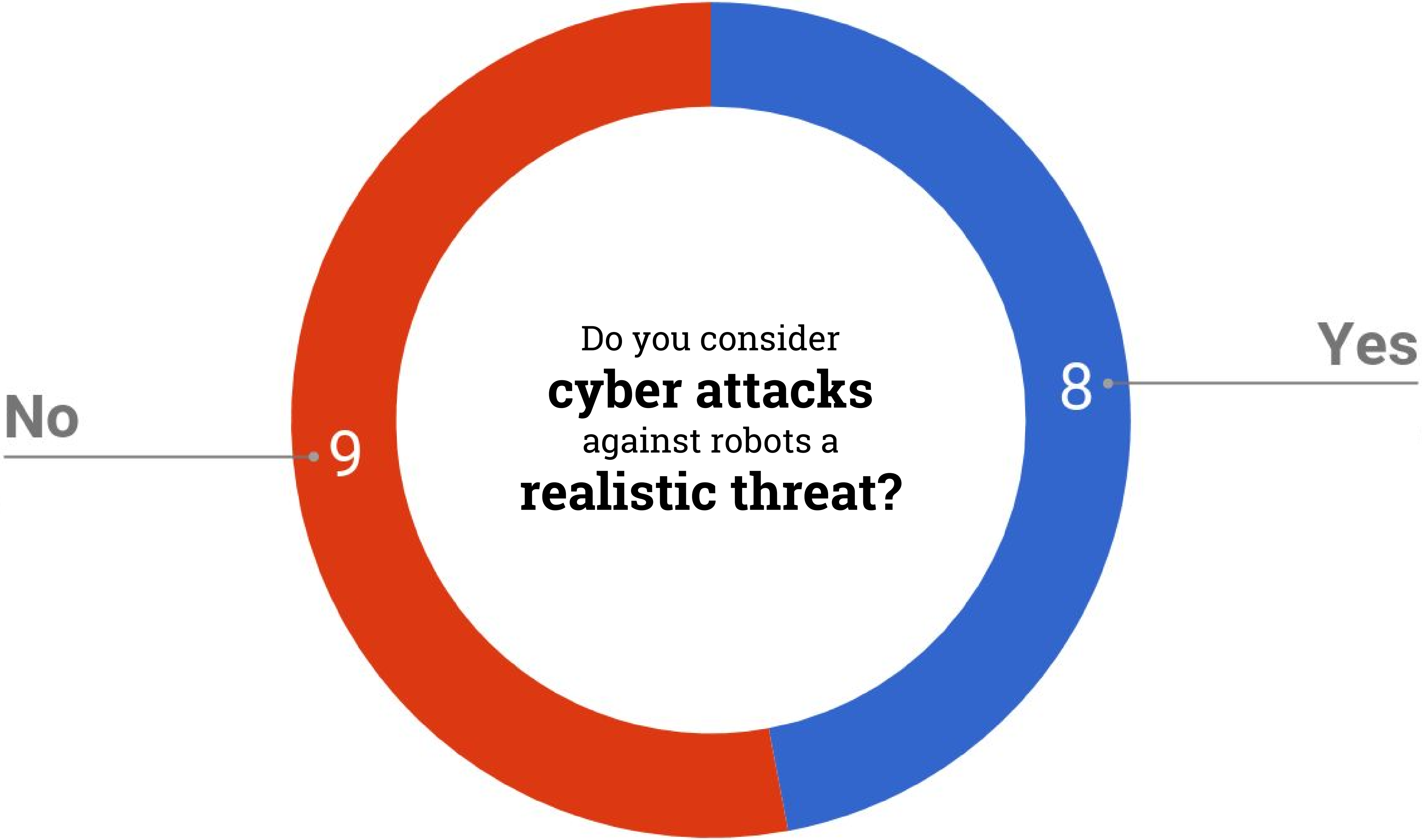
↓

Do you consider

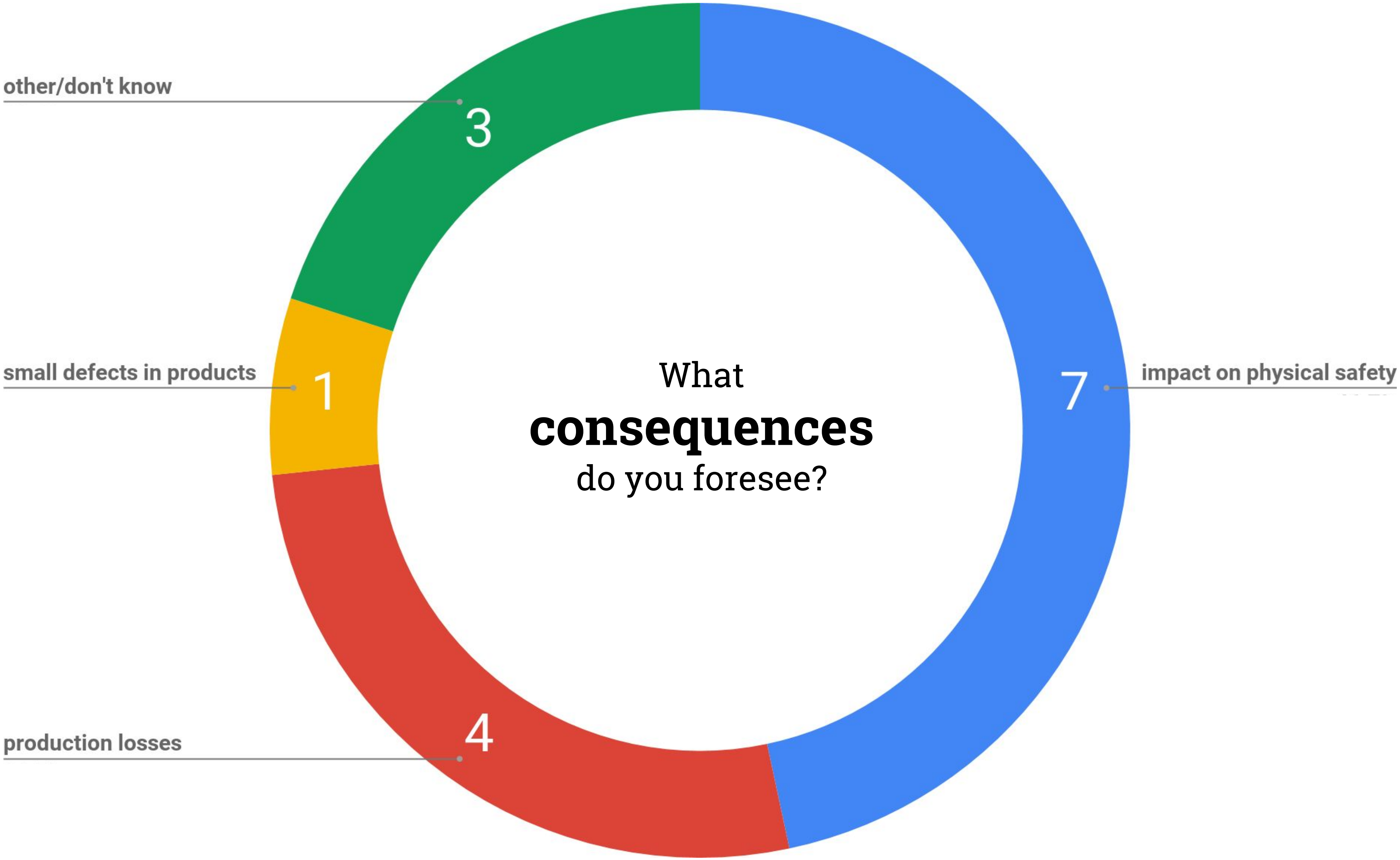
cyber attacks

against robots a

realistic threat?

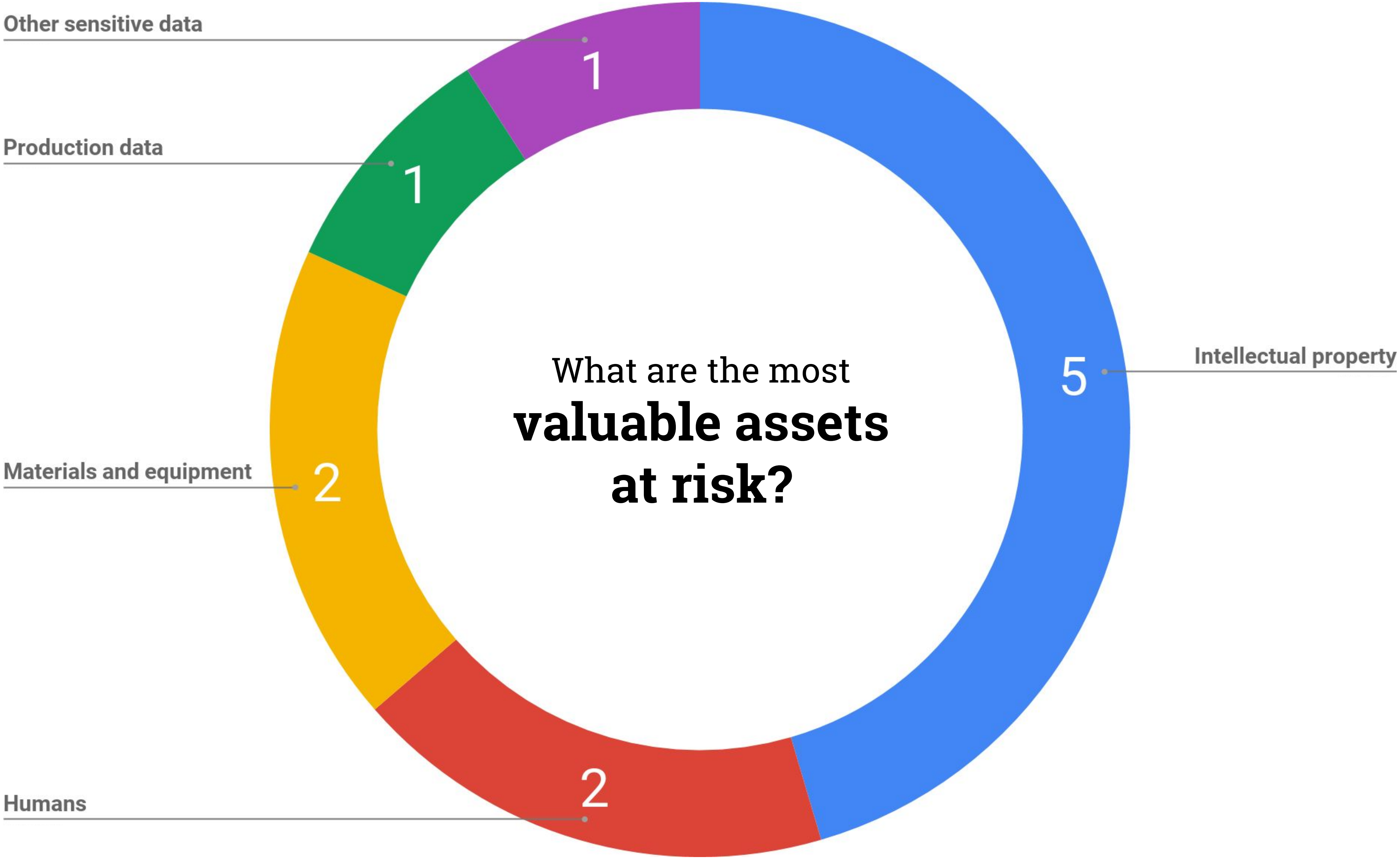


Do you consider **cyber attacks** against robots a **realistic threat?**



What **consequences** do you foresee?

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



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

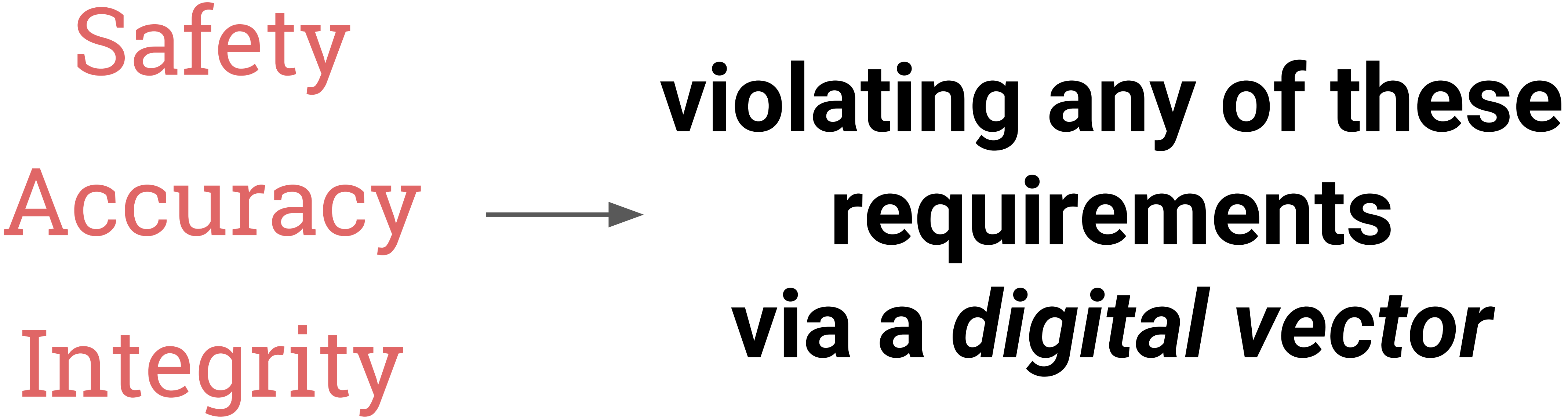
Requirements: "Laws of Robotics"

Safety

Accuracy

Integrity

Robot-Specific Attack



Safety

Accuracy

Integrity

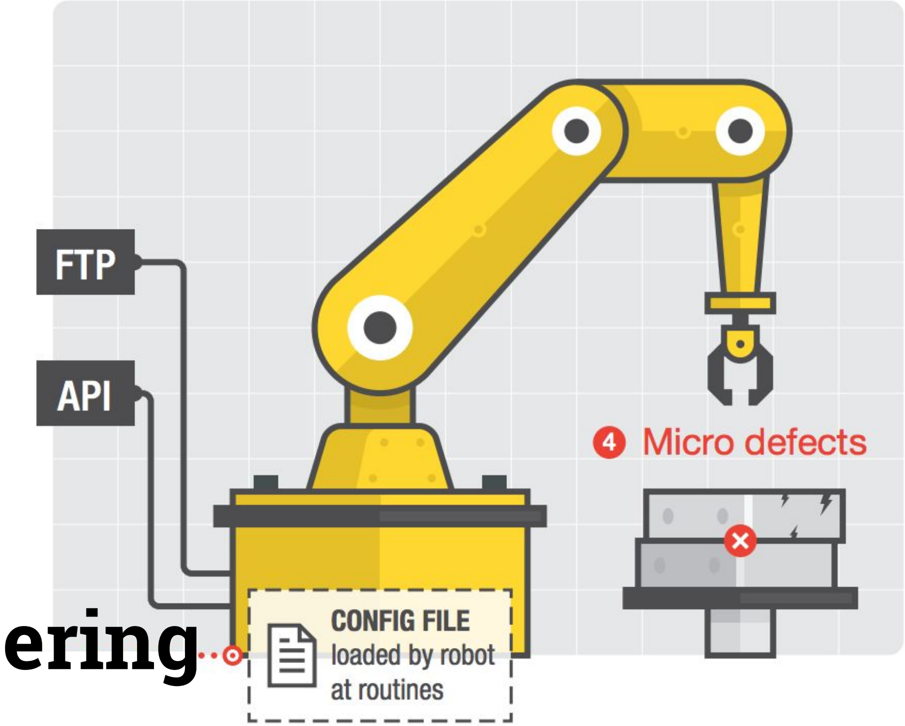
violating any of these requirements via a *digital vector*

Robot Specific Attacks

Control Loop Alteration

Calibration Tampering

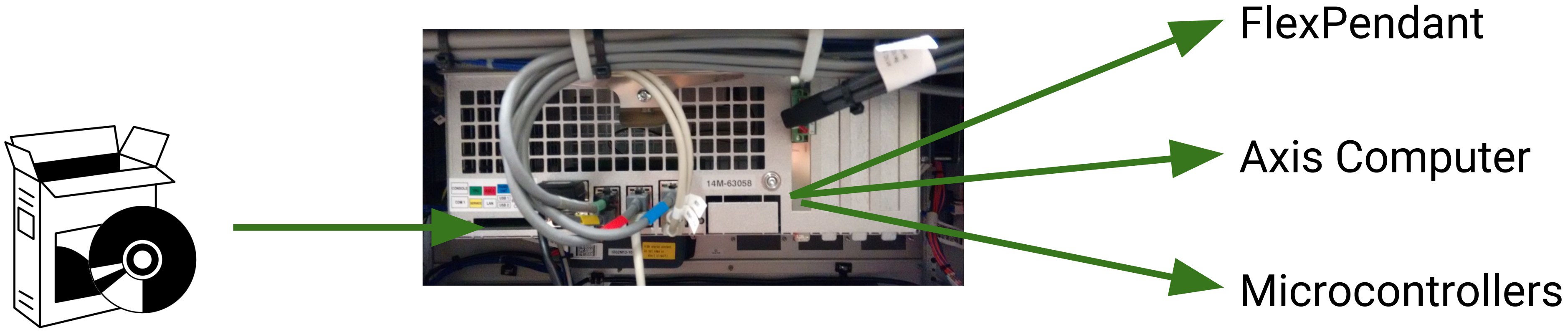
Production Logic Tampering



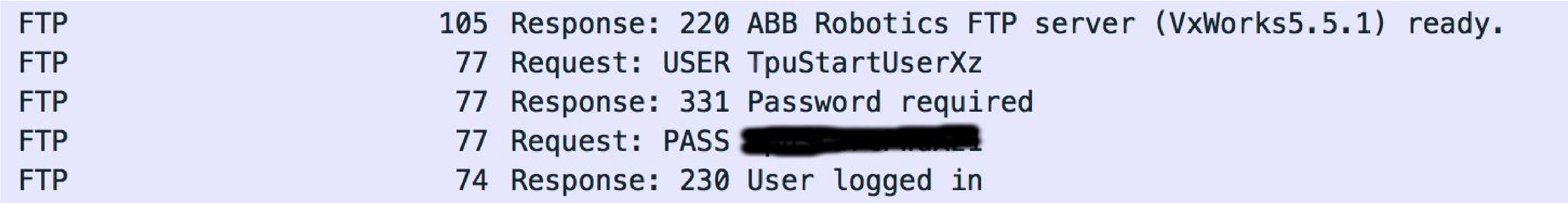
Attacks
Safety
Accuracy
Integrity

is there any vulnerability?

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

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

Buffer overflows

Ex. 1: RobAPI

- Unauthenticated API endpoint
- Unsanitized `strcpy()`

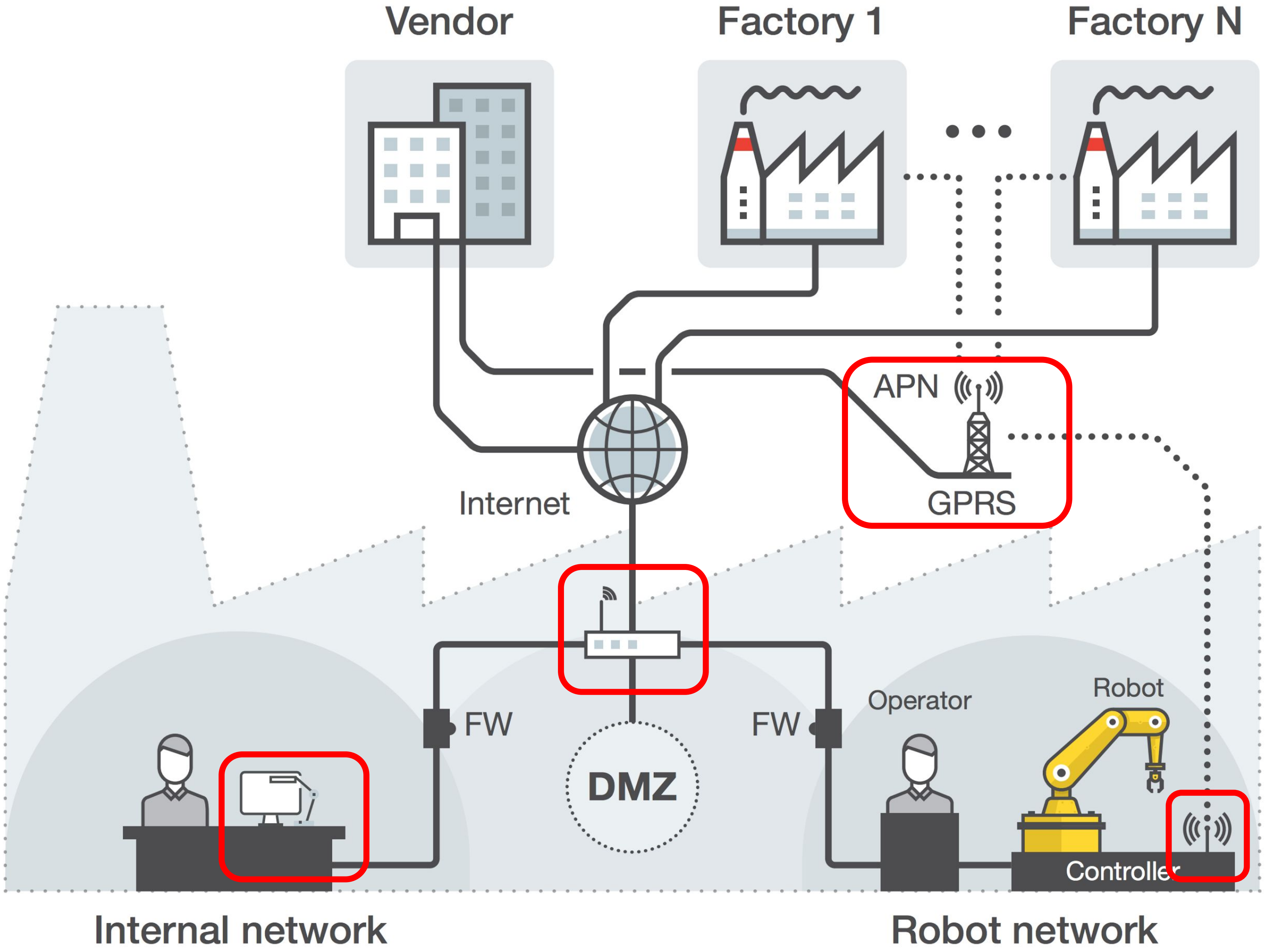
→ **remote code execution**

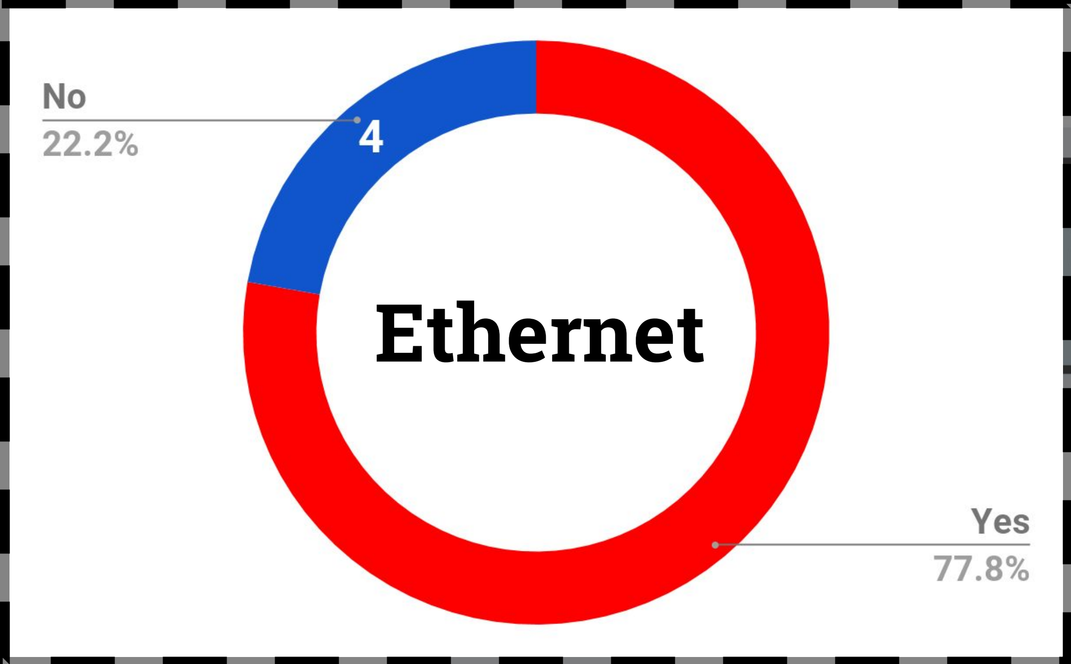
Ex. 2: Flex Pendant (`TpsStart.exe`)

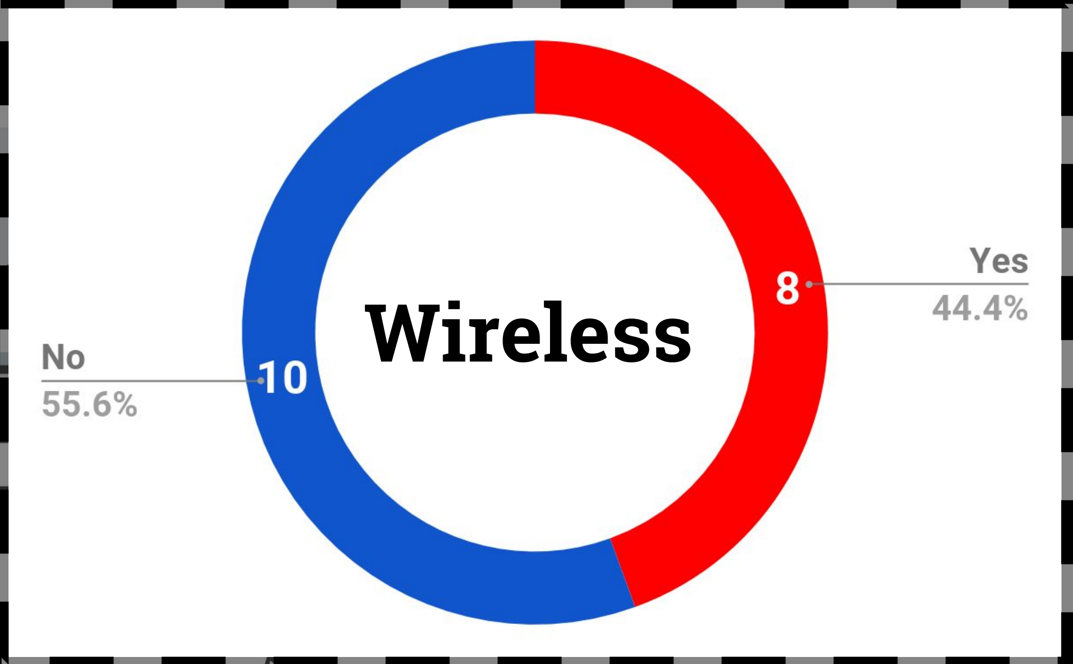
- FTP write `/command/timestampAAAAAAA.....AAAAAAA`
- file name > 512 bytes ~> Flex Pendant DoS

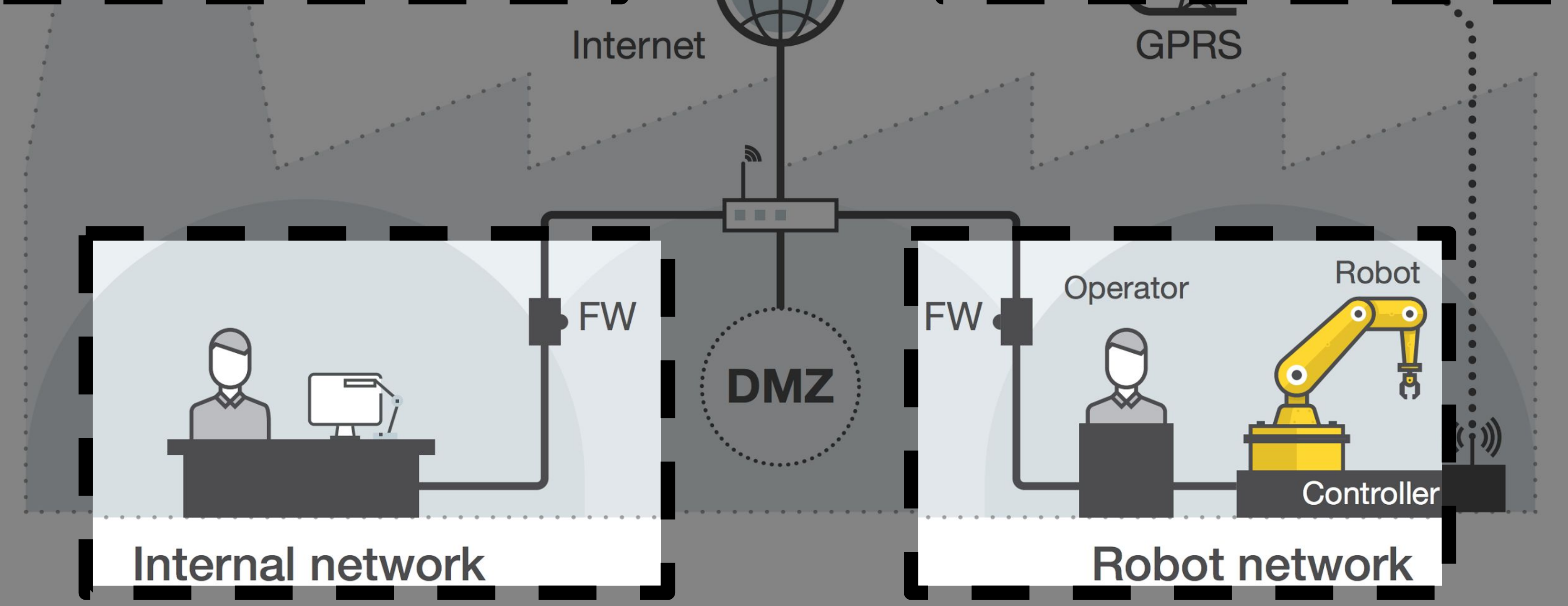
ABBVU-DMRO-124641, ABBVU-DMRO-124645

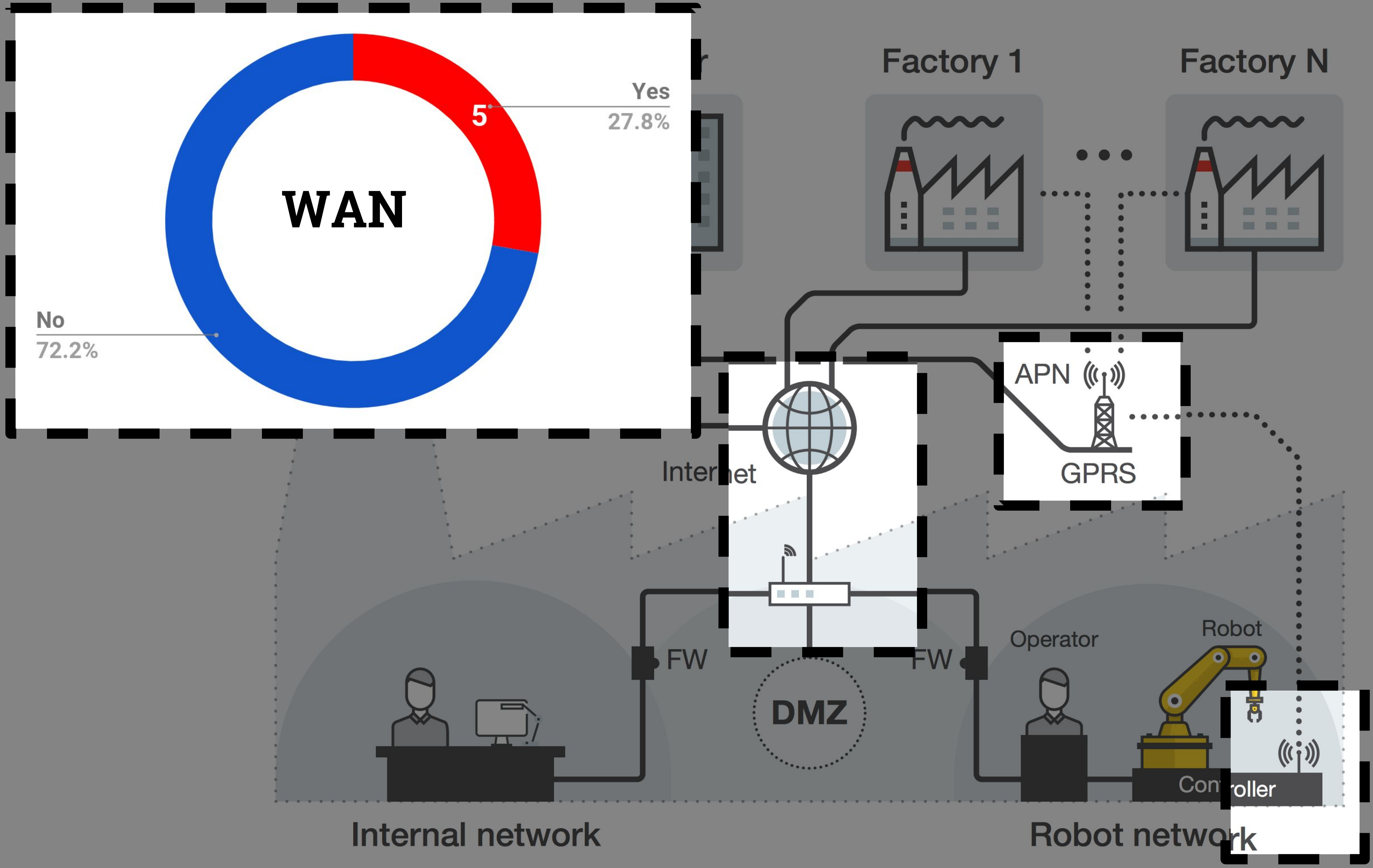
Connected

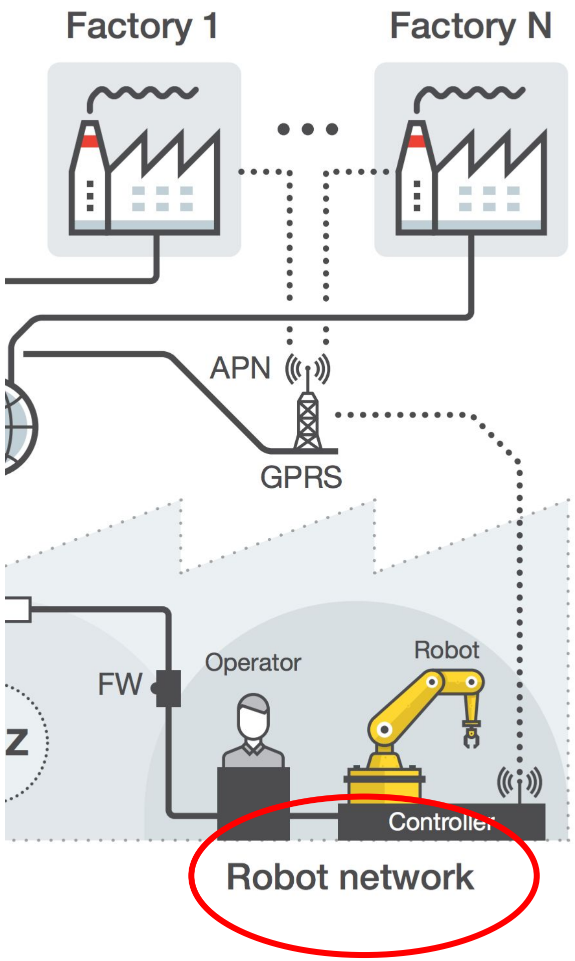

Vendor
Factory 1
Factory N
APN
GPRS
Internet
FW
FW
DMZ
Operator
Robot
Controller
Internal network
Robot network


Ethernet
No
22.2%
4
Yes
77.8%


Wireless
No
55.6%
10
Yes
44.4%
8


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

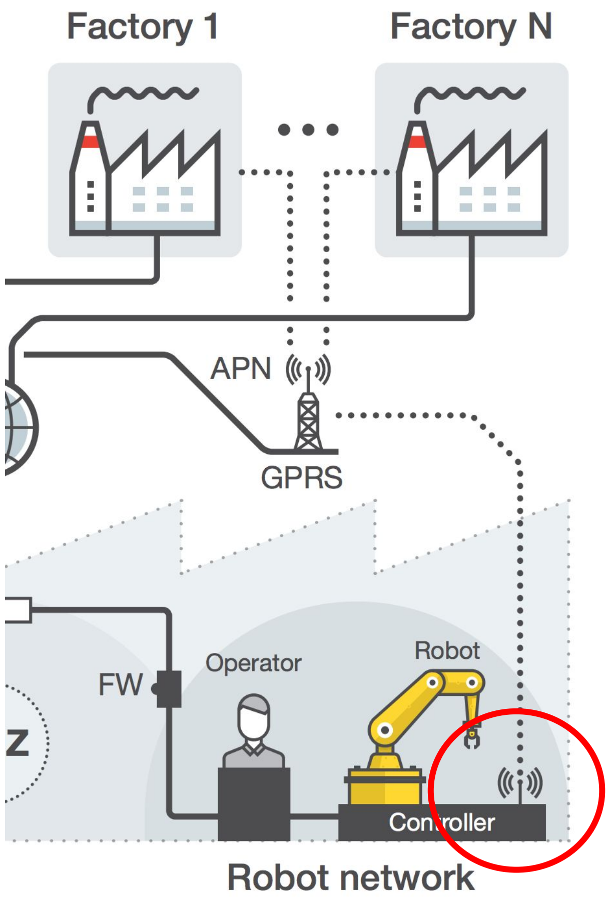

WAN
Yes
5
27.8%
No
72.2%
Factory 1
Factory N
APN
GPRS
Internet
DMZ
FW
FW
Operator
Robot
Controller
Internal network
Robot network



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...

(Shodan+ZoomEye+Censys)



...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

Outdated Software Components

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

Bottom line

Connect your robots with care

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

Conclusions

Takeaways

Things are Vulnerable

Connect with Care

⚠ Do not blindly **trust** all the components

Short term

Attack detection and deployment hardening

Medium term

System hardening

Long term

New standards, beyond safety issues

Mario Polino

mario.polino@polimi.it

Papers, slides, and FAQ

http://robosec.org