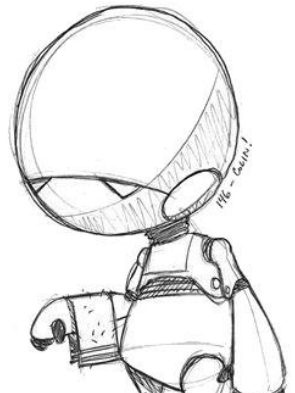
An experimental security analysis of an Industrial Robot Controller

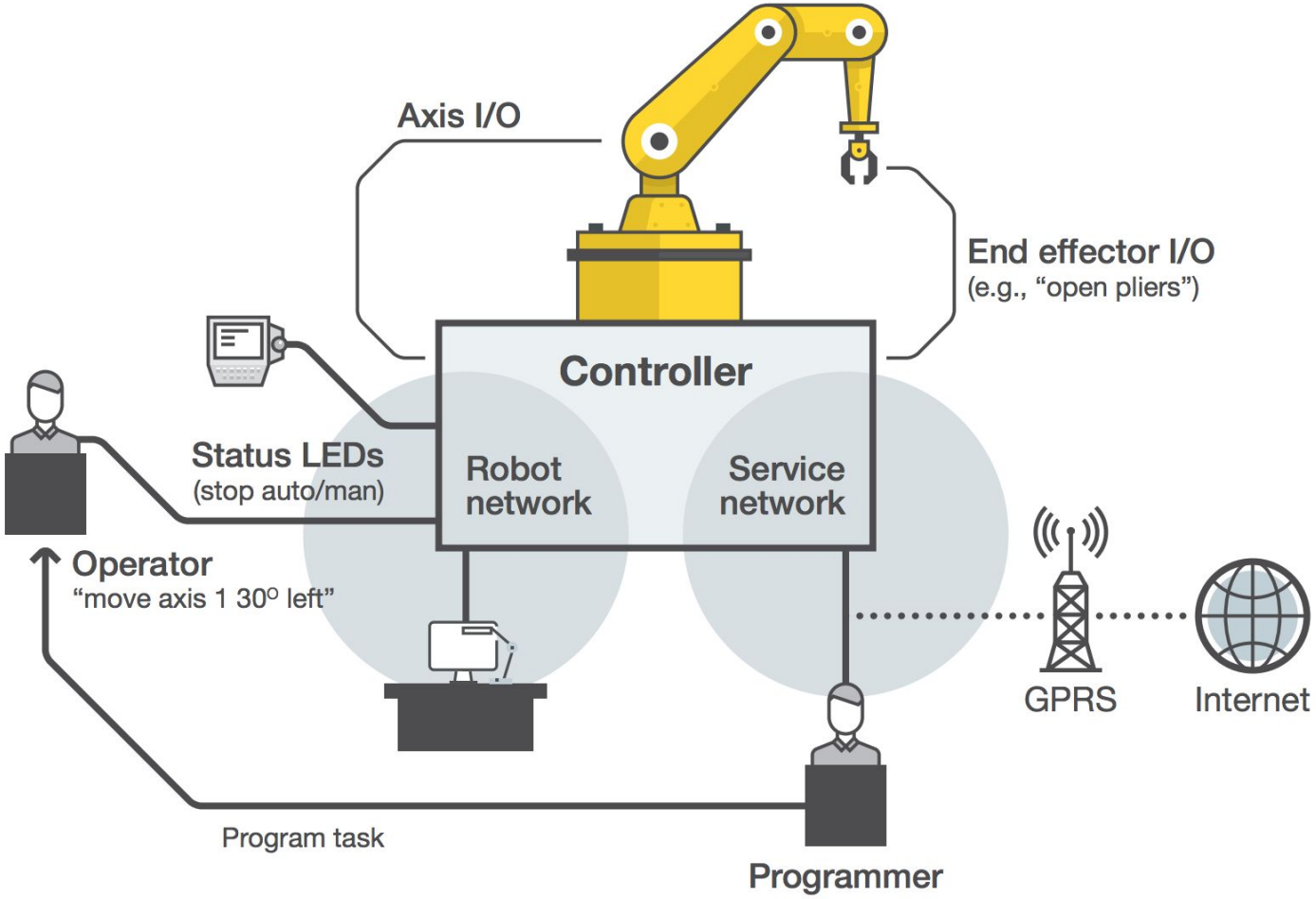
Davide Quarta, Marcello Pogliani, Mario Polino,
Federico Maggi, Andrea Maria Zanchettin, Stefano Zanero

San José (CA), May 22nd, 2017
38th IEEE Symposium on Security and Privacy

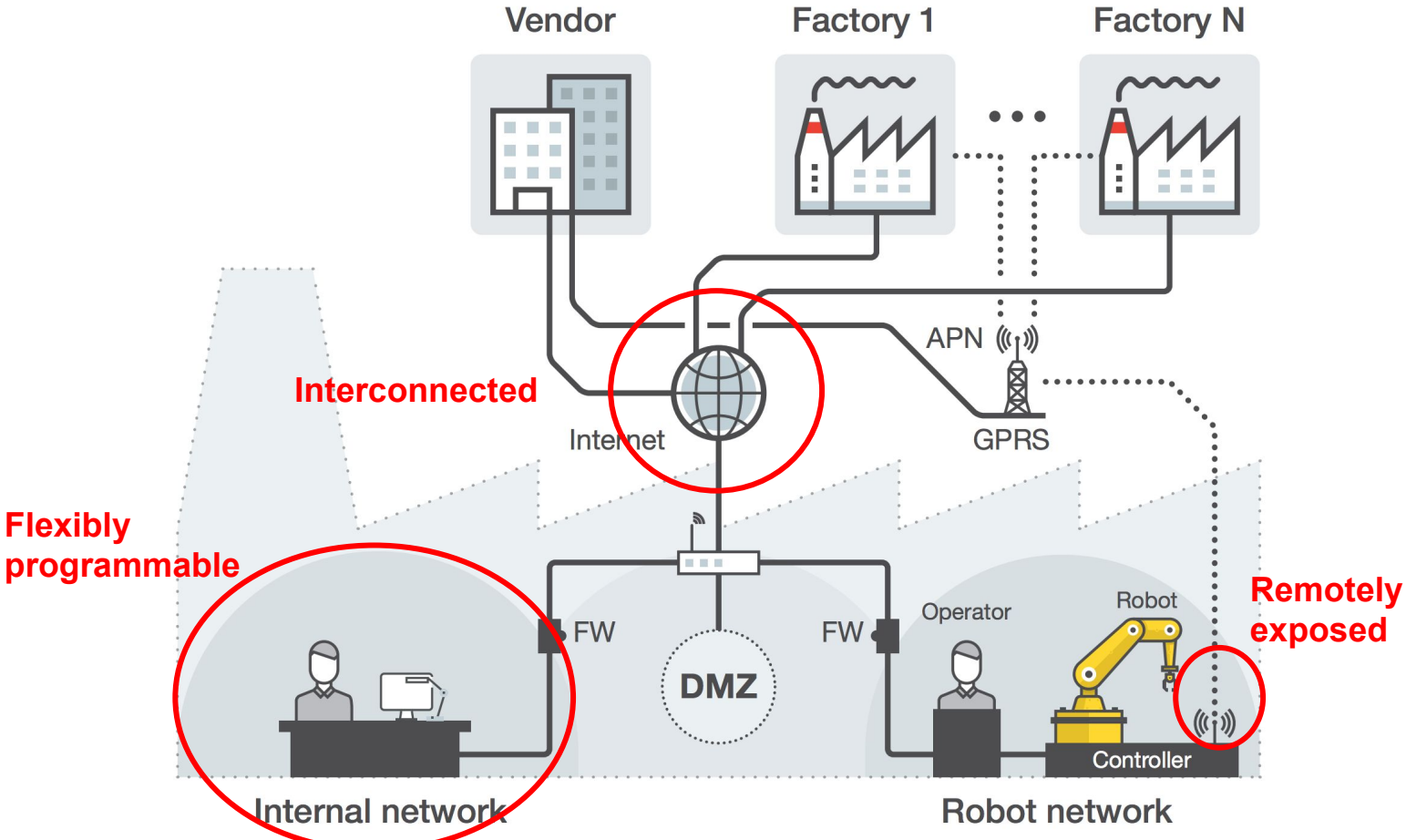
POLITECNICO
MILANO 1863
DIPARTIMENTO DI ELETTRONICA
INFORMAZIONE E BIOINGEGNERIA

TREND
MICRO™




Axis I/O
End effector I/O
(e.g., “open pliers”)
Controller
Status LEDs
(stop auto/man)
Robot network
Service network
Operator
“move axis 1 30º left”
GPRS
Internet
Program task
Programmer

Motivation: Industry 4.0 Trends



Motivation: Lack of Awareness

Survey: Robot users vs. system security

50 domain experts—users interviewed: 20 answers

- **28%*** access control policies *not enforced*
- **30%** robots accessible *over Internet*
- **76%** *never* performed a pentest
- **> 50%** not a *realistic* threat

* some users did not answer all the questions

How do we define a robot-specific attack?

Requirements: Laws of Robotics

- **I/O Accuracy**
  - **Read** precise values
  - **Issue** correct/accurate commands
- **Safety**
  - Never harm **humans**
  - Correctly **inform** operator
- **Integrity**
  - No **damage** to the robot

Requirements: Laws of Robotics

- I/O Accuracy
  - **Read** precise values
  - **Issue** correct/accurate commands
- **Safety**
  - Never harm **humans**
  - Correctly **inform** operator
- Integrity
  - No **damage** to the robot

Requirements: Laws of Robotics

- **I/O Accuracy**
  - **Read** precise values
  - **Issue** correct/accurate commands
- **Safety**
  - Never harm **humans**
  - Correctly **inform** operator
- **Integrity**
  - No **damage** to the robot

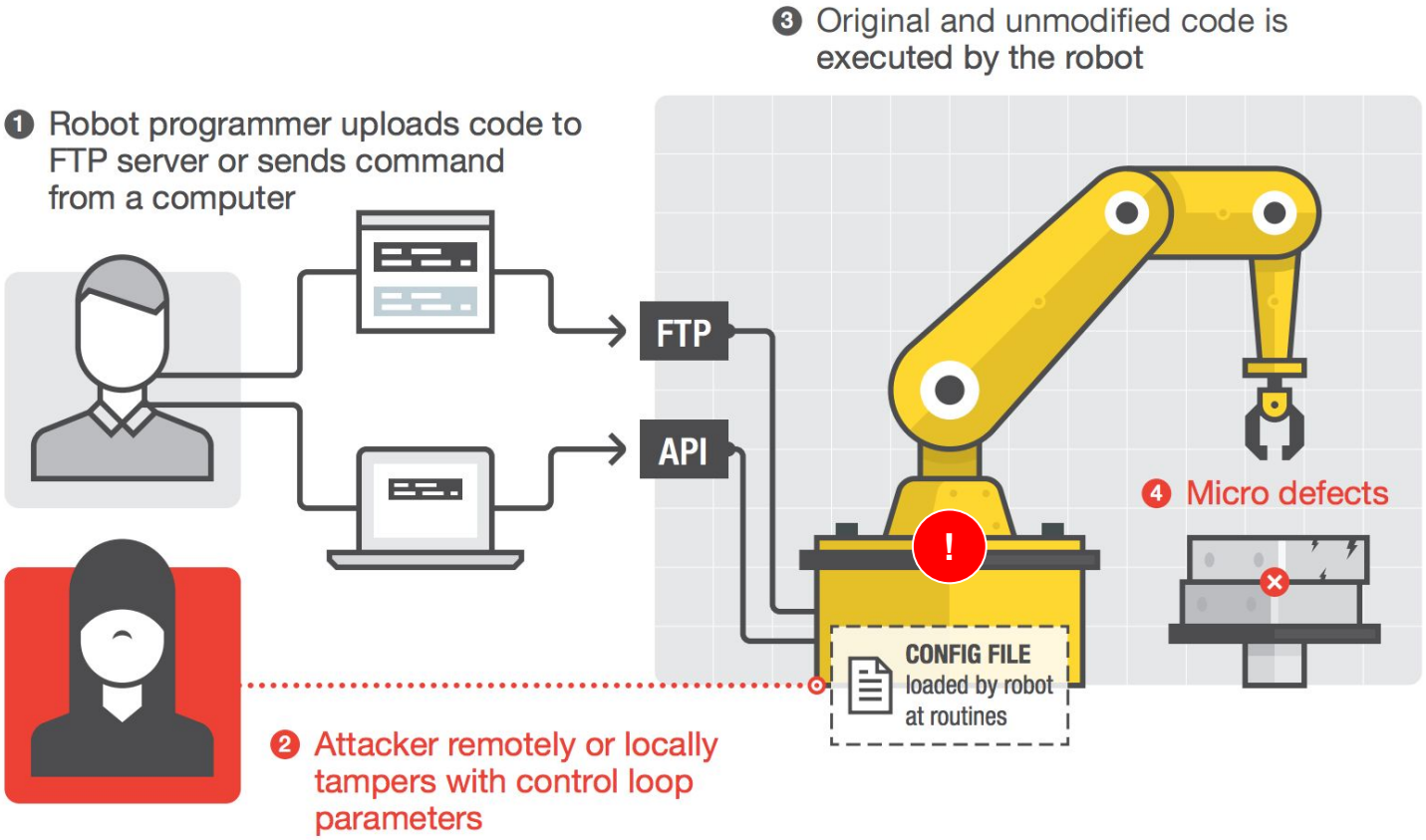
Requirements: Laws of Robotics

- **I/O Accuracy**
  - Read precise values
  - Issue correct/accurate commands
- **Safety**
  - Never harm humans
  - Correctly inform operator
- **Integrity**
  - No damage to the robot

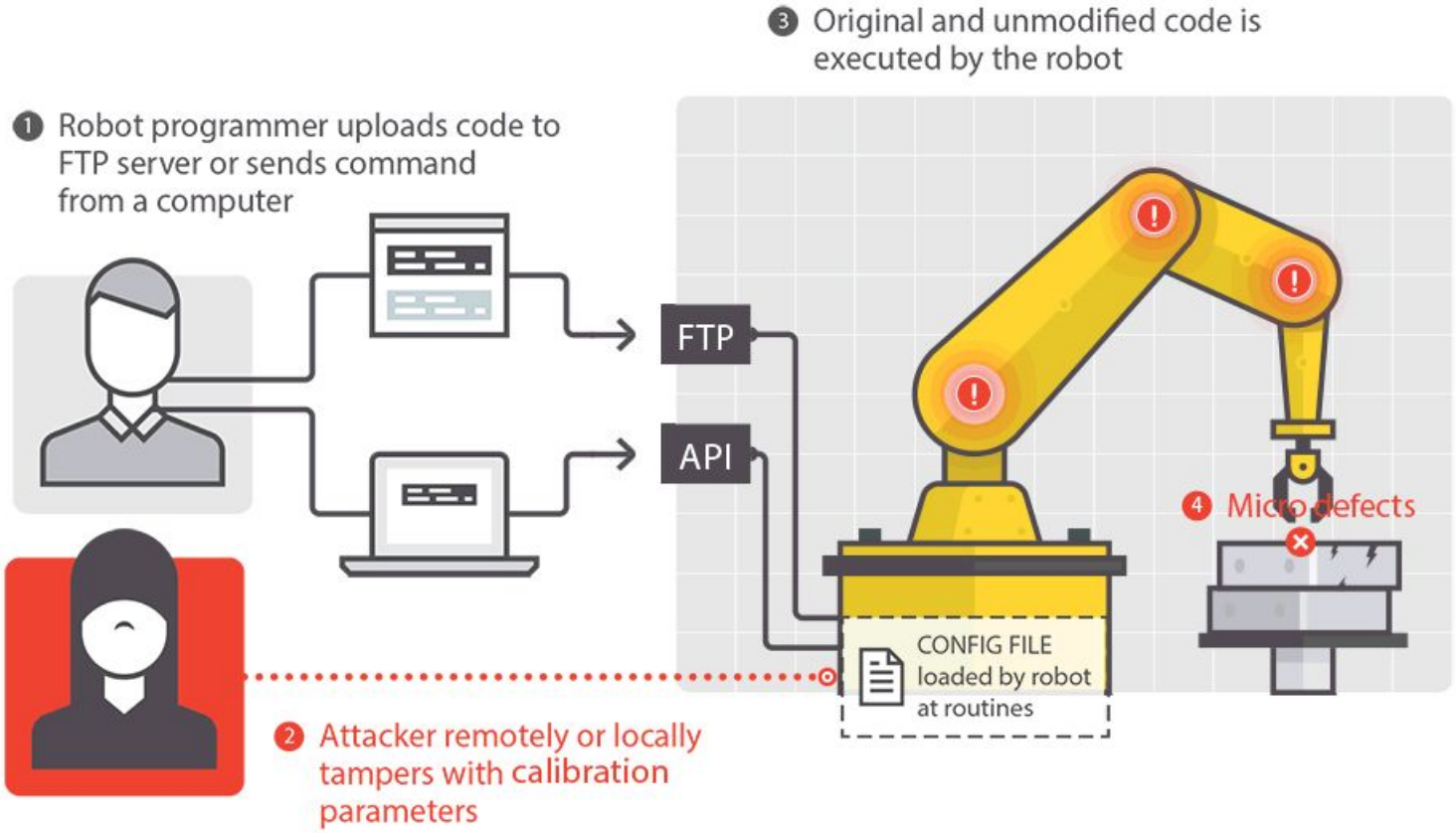
Robot-specific Attack:
Digital-borne violation of any of these requirements

5 Robot-specific Attacks

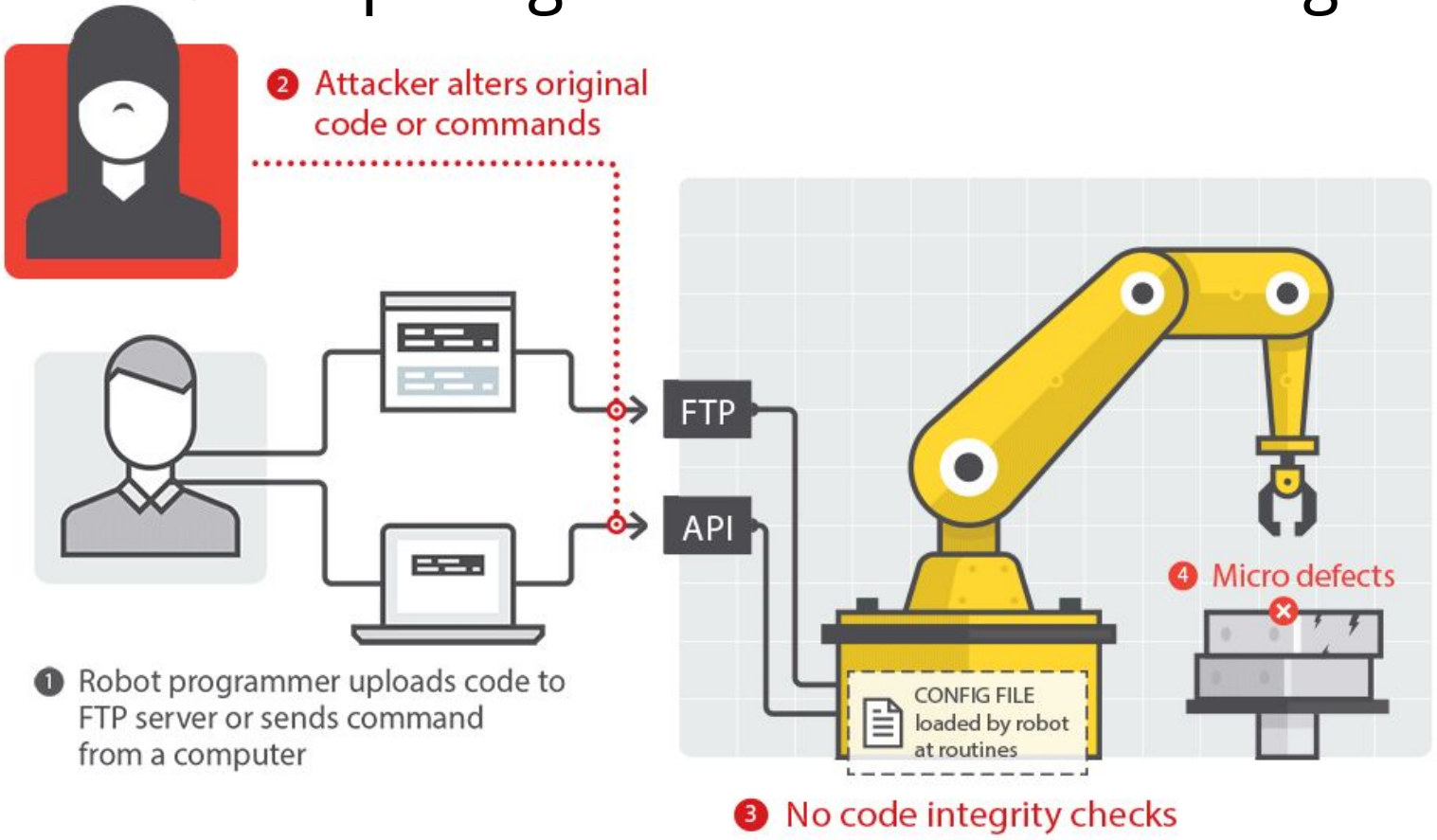
Attack 1: Control Loop Alteration



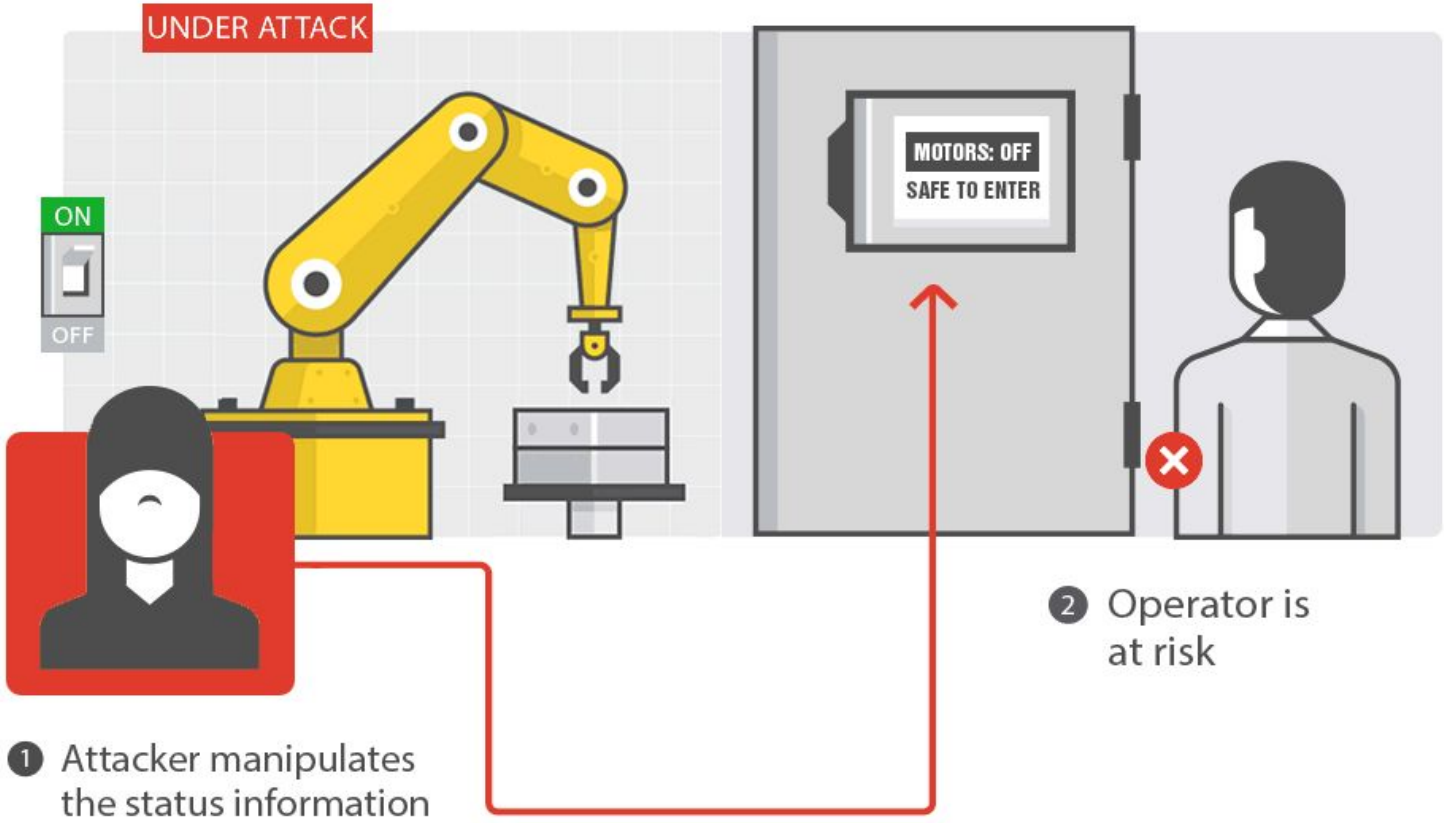
Attack 2: Tampering with Calibration Parameters



Attack 3: Tampering with the Production Logic



Attack 4 & 5: (Perceived) Robot State Alteration



Custom Physical Protections, if any (despite regulations)

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

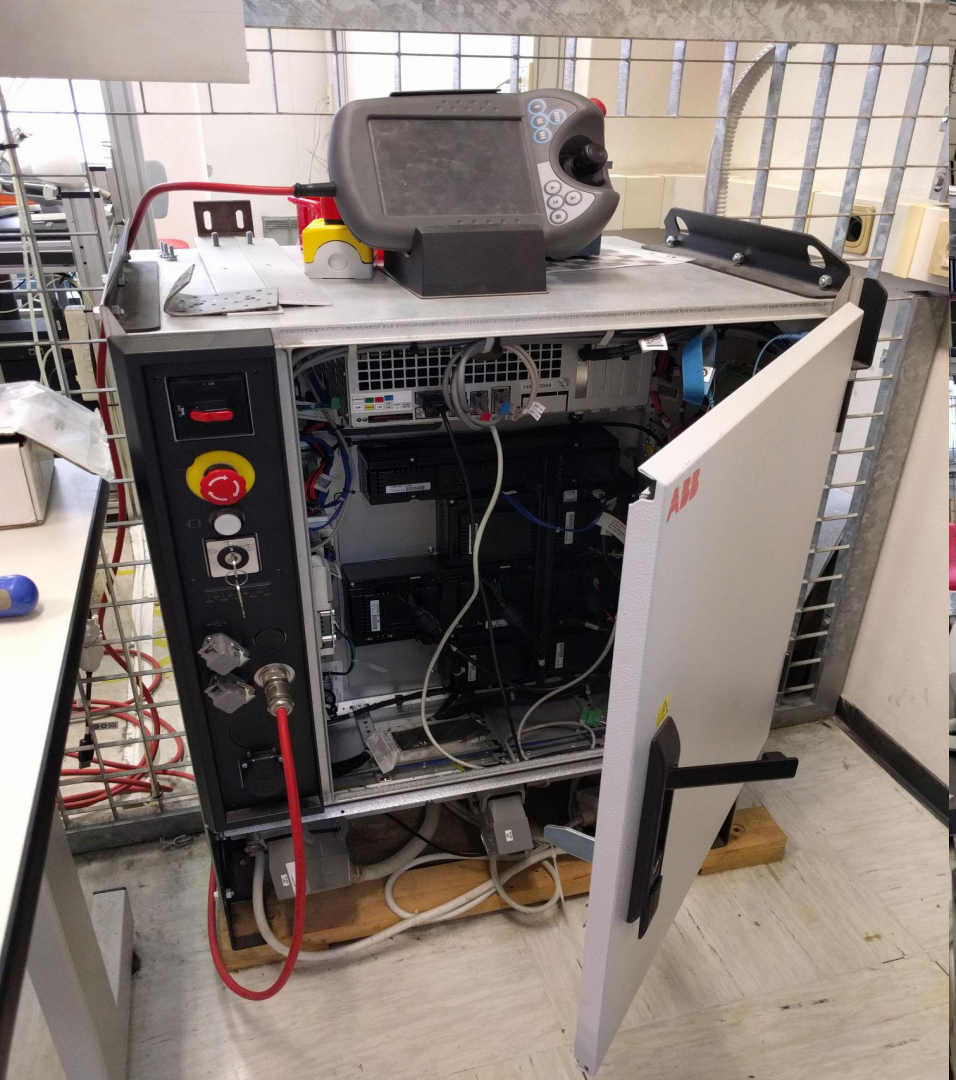
[redacted] to [redacted]

[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.

From Attacks to Threat Scenarios

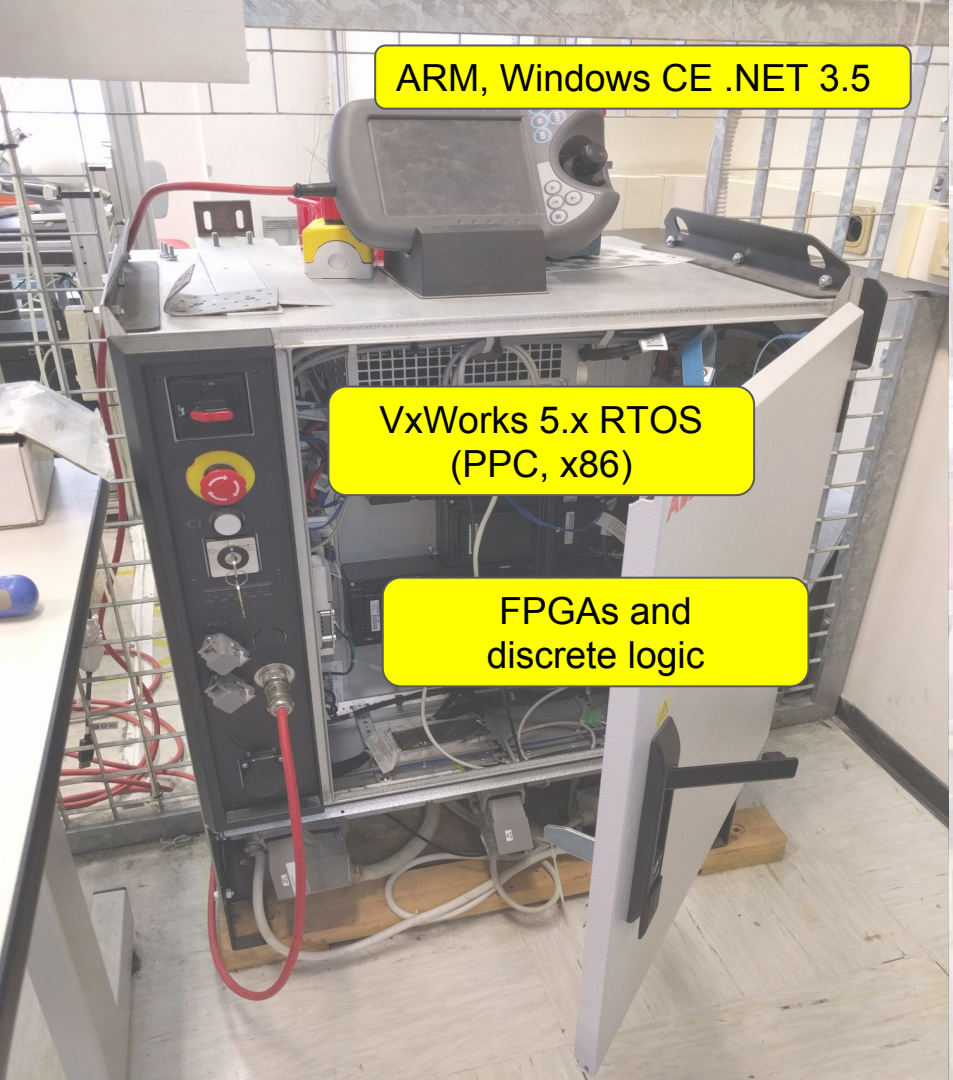
1) Production Plant Halting
2) Production Outcome Alteration
3) Physical Damage
4) Unauthorized Access
5) Ransom requests to disclose micro defects

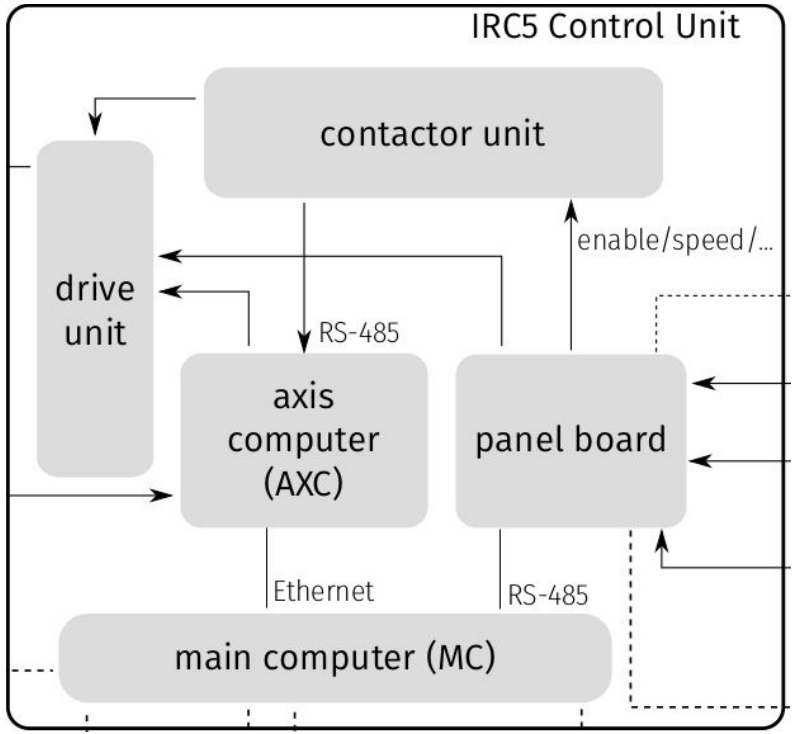
Case Study

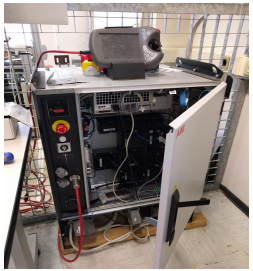


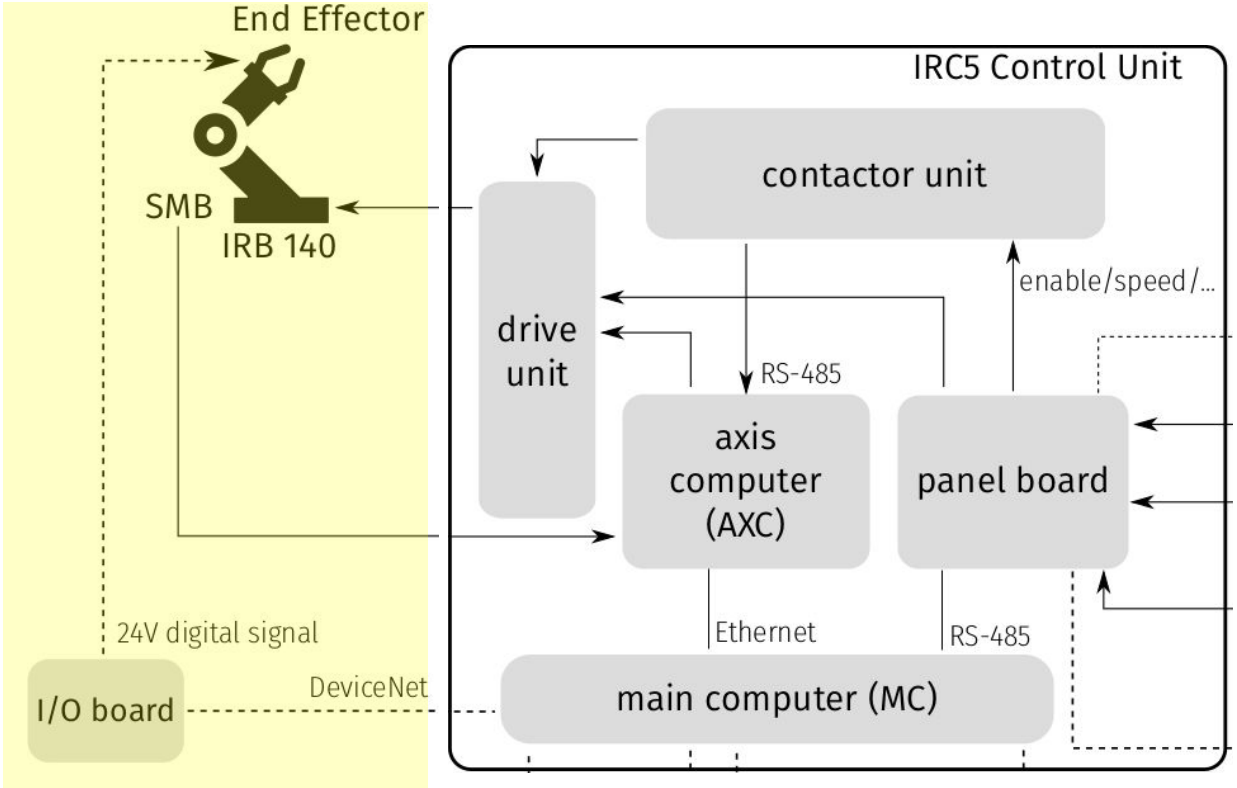
ABB

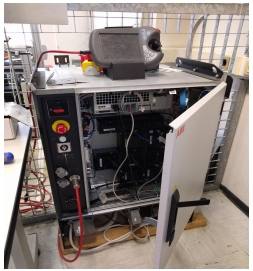

ABB
ABB

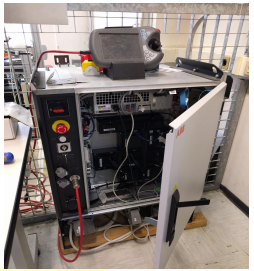

ARM, Windows CE .NET 3.5
VxWorks 5.x RTOS
(PPC, x86)
FPGAs and
discrete logic

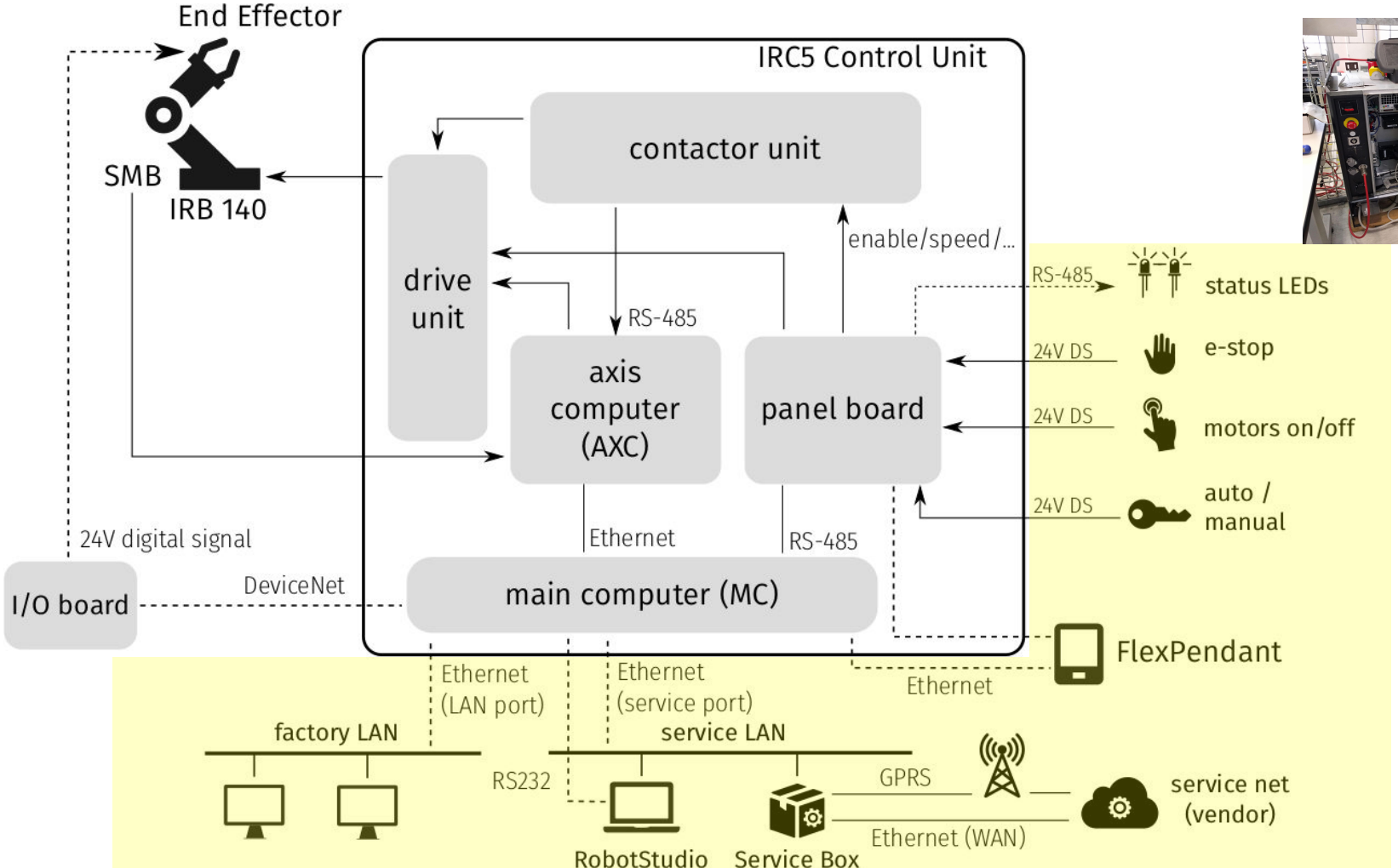

IRC5 Control Unit
contactor unit
drive unit
enable/speed/...
RS-485
axis computer (AXC)
panel board
Ethernet
RS-485
main computer (MC)

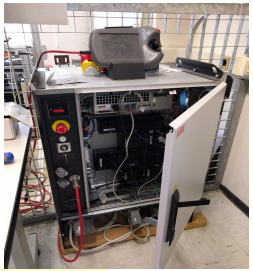



End Effector
SMB
IRB 140
IRC5 Control Unit
contactor unit
drive unit
enable/speed/...
RS-485
axis computer (AXC)
panel board
Ethernet
RS-485
24V digital signal
I/O board
DeviceNet
main computer (MC)






End Effector
IRC5 Control Unit
SMB
IRB 140
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
24V digital signal
Ethernet
RS-485
I/O board
DeviceNet
main computer (MC)
FlexPendant
Ethernet
Ethernet (LAN port)
Ethernet (service port)
factory LAN
service LAN
RS232
GPRS
service net (vendor)
Ethernet (WAN)
RobotStudio
Service Box



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

24V digital signal

Ethernet

RS-485

I/O board

DeviceNet

LAN

main computer (MC)

WAN

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)

Industrial Routers

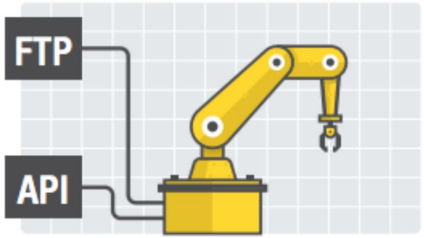
Brand	Exposed Devices	No Authentication	Known Vulnerabilities	New Vulnerabilities
Belden	956		4	1
Eurotech	160			
eWON	6,219	1,160	10	
Digi	1,200		2	1
InHand	883			
Moxa	12,222	2,300	30	1
NetModule	886	135		1
Robustel	4,491		1	
Sierra Wireless	50,341	220	4	
Virtual Access	209		1	
Welotec	25			
Westermo	6,081	1,200	7	2
TOTAL	83,673	5,105	59	6

Vulnerabilities

a. **BOF leading to RCE** (ABBVU-DMRO-124641)
b. **BOF in FlexPendant** (ABBVU-DMRO-124645)
c. **BOF in /command endpoint** (ABBVU-DMRO-128238)
d. **Command Injection** (ABBVU-DMRO-124642)
e. **Authentication bypass** (ABBVU-DMRO-124644)

Full Controller Exploitation

1. Using static credentials
   FTP PUT /command/command.cmd
1. (Alternatively) DHROOT RobAPI request
   (no auth) with buffer overflow exploit



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

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

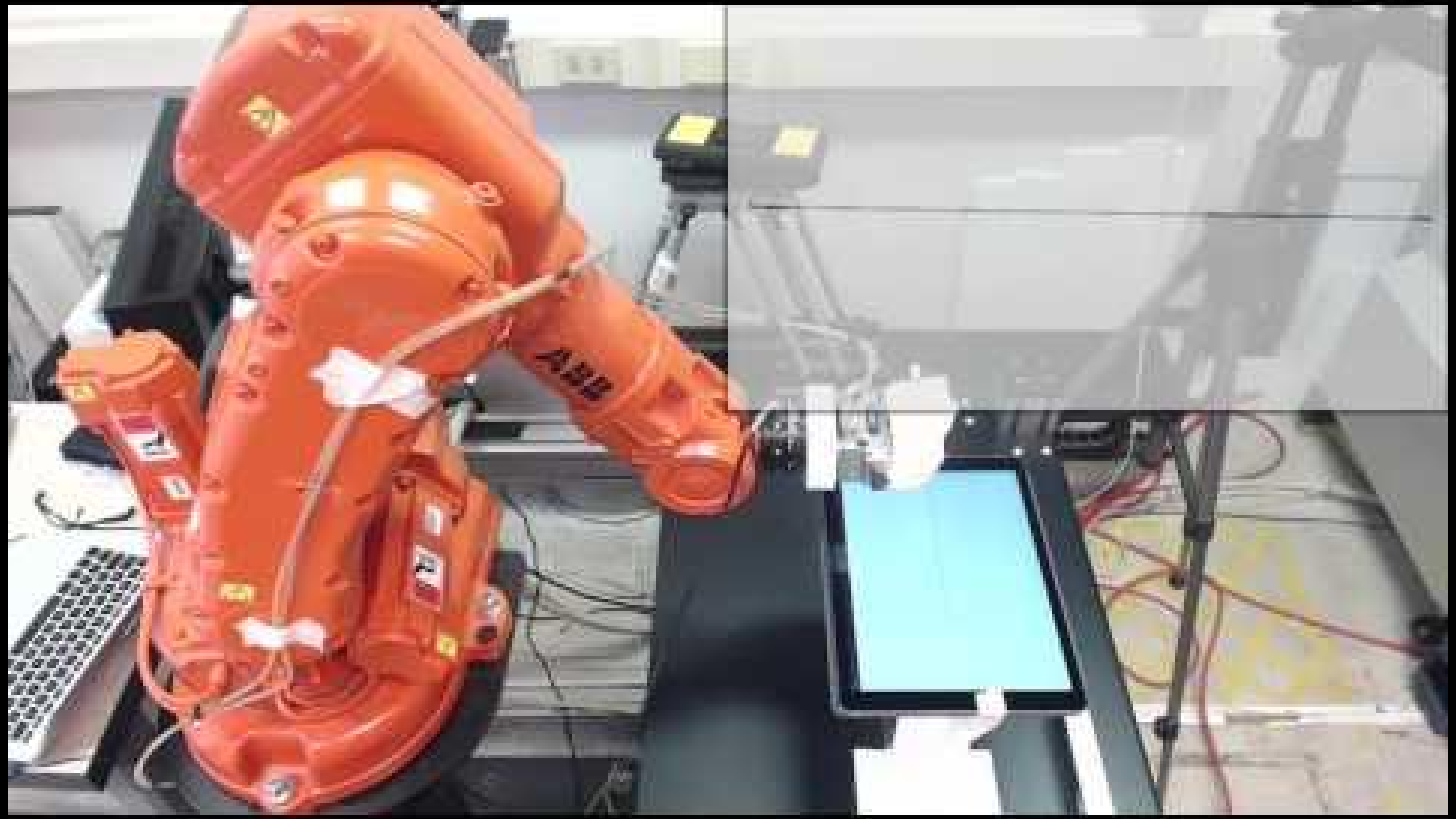
→ FP/MC will reboot

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

→ **Robot controller is now under attacker’s control**

Attack POCs

1) **Accuracy** Violation: PID parameters detuning (Attack 1) **DEMO**
2) **Safety** Violation: User-Perceived Robot State Alteration (Attack 4)
3) **Integrity** Violation: Control-loop alteration (Attack 1)



ABB

Attack POCs

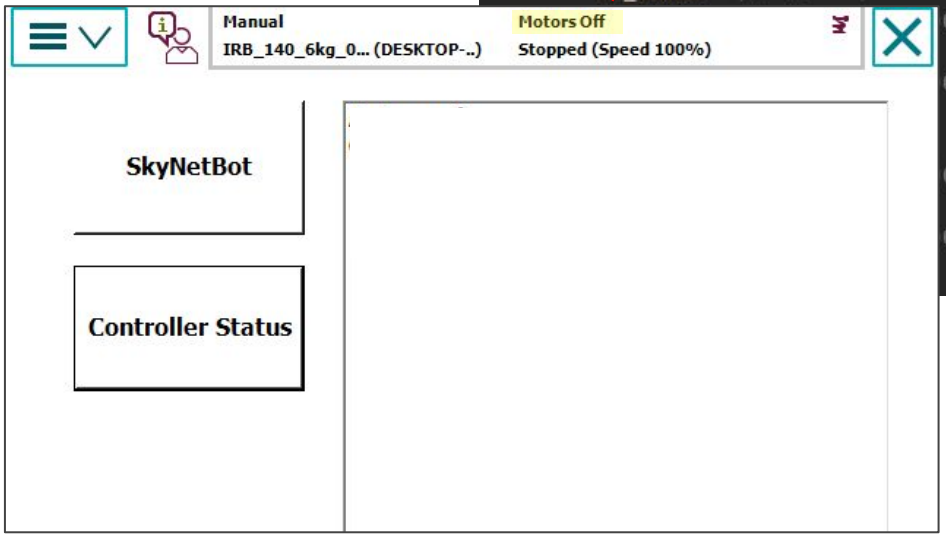
1) **Accuracy** Violation: PID parameters detuning (Attack 1)
2) **Safety** Violation: User-Perceived Robot State Alteration (Attack 4)
3) **Integrity** Violation: Control-loop alteration (Attack 1)

POC 2: **Safety** Violation

Malicious DLL

```
        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
```

Teach Pendant

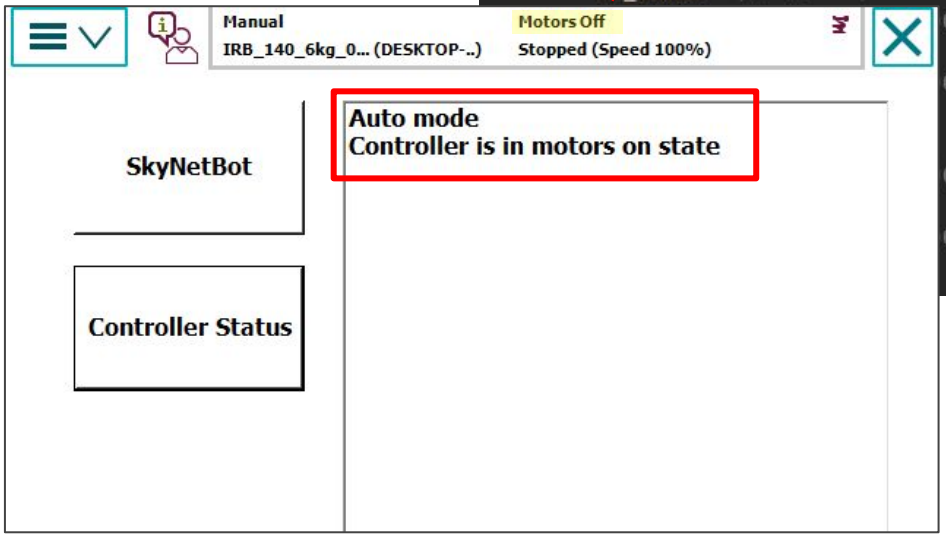


POC 2: **Safety** Violation

Malicious DLL

```
        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
```

Teach Pendant



Attack POCs

1) **Accuracy** Violation: PID parameters detuning (Attack 1)
2) **Safety** Violation: User-Perceived Robot State Alteration (Attack 4)
3) **Integrity** Violation: Control-loop alteration (Attack 1)

POC 3: **Integrity** Violation

- Robot's arm **collapse** on itself
- Motors substantially damaged

Quite a risky POC!
Verified with a robotics' expert

Conclusions: Future Challenges

- New standards, beyond safety issues
- Attack detection and hardening
- Secure collaborative robots
- (Detailed countermeasures in the paper)

http://robosec.org

Questions?

Davide Quarta, Marcello Pogliani, Mario Polino,
Federico Maggi, Andrea Maria Zanchettin, Stefano Zanero

San José (CA), May 22nd, 2017
38th IEEE Symposium on Security and Privacy

POLITECNICO
MILANO 1863
DIPARTIMENTO DI ELETTRONICA
INFORMAZIONE E BIOINGEGNERIA

TREND
MICRO™