



## Small Wonder:

Uncovering Planned Obsolescence Practices in Robotics and What This Means for Cybersecurity



**Víctor Mayoral-Vilches**  
Alias Robotics




**ALIAS ROBOTICS**  
Robot Cybersecurity



**Federico Maggi**  
Trend Micro Research



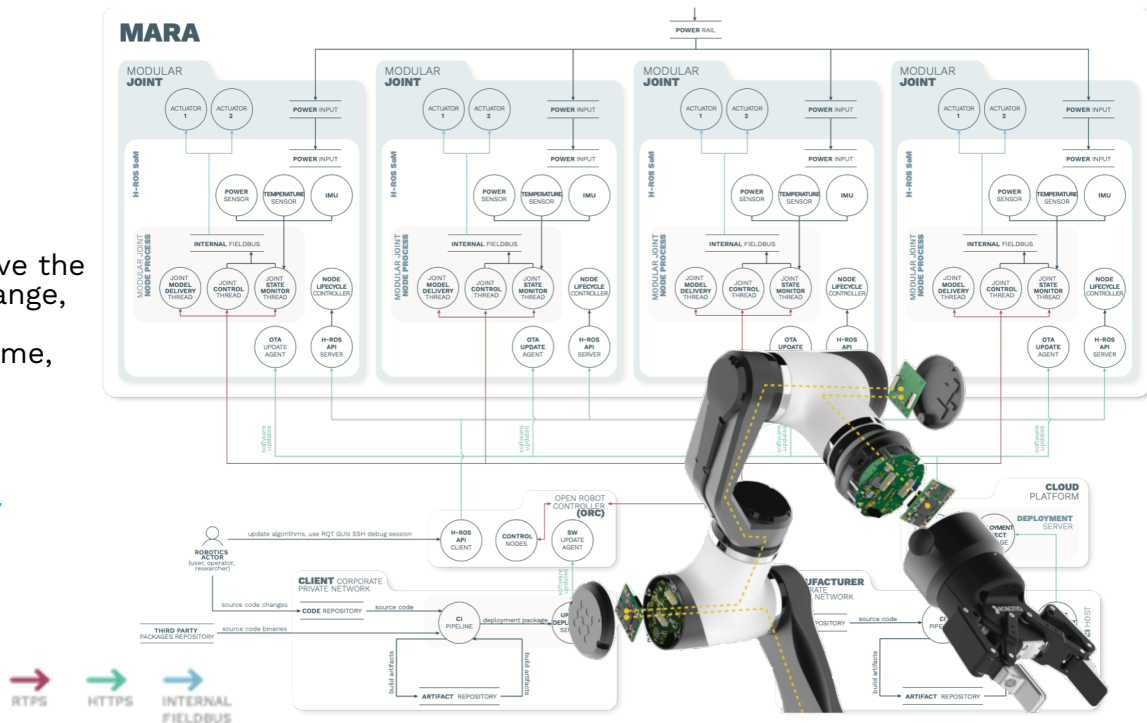
**TREND**  
MICRO™

| research 

# ROBOTS ARE NETWORKS OF NETWORKS

Networks that comprise sensors to perceive the world, actuators to produce a physical change, and dedicated computational resources to process it all and respond coherently, in time, and according to its application<sup>[1]</sup>.

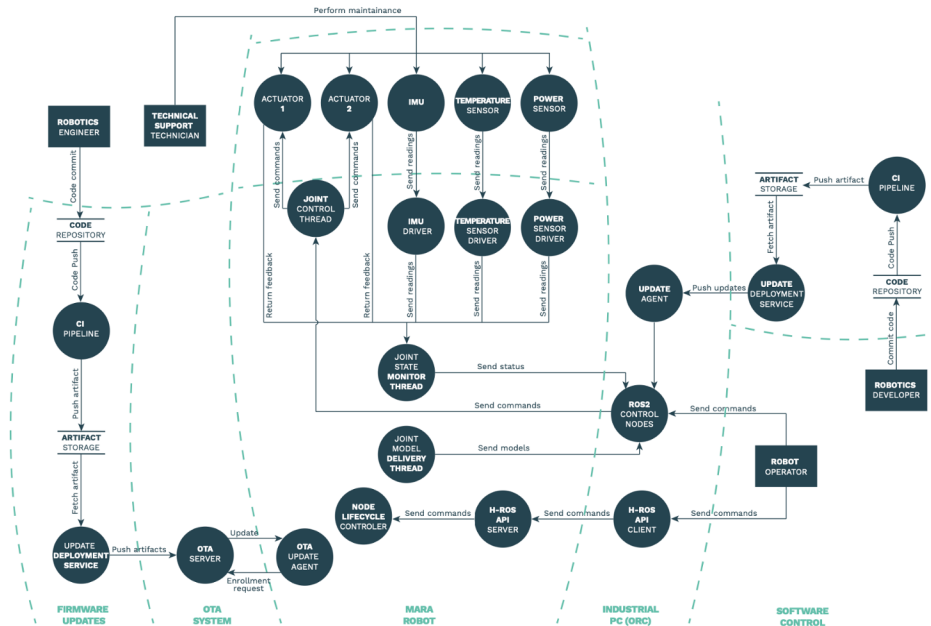
[1] Mayoral-Vilches, V., Hernández, A., Kojcev, R., Muguruza, I., Zamalloa, I., Bilbao, A., & Usategi, L. (2017). The shift in the robotics paradigm—the hardware robot operating system (h-ros); an infrastructure to create interoperable robot components. In *Adaptive hardware and systems (ahs), 2017 nasa/esa conference on* (pp. 229–236).





# THERE IS NO SAFETY WITHOUT SECURITY IN ROBOTICS

Safety cares about the robot not harming the environment (or humans) whereas security deals with the opposite, aims to ensure the environment does not conflict with the robot's programmed behavior. There's an intrinsic connection between safety and security. Functional safety standards reflect this aspect.



# ONLY SAFE IF SECURE

**IEC 61508 indicates the following in section 7.4.2.3:**

"If the hazard analysis identifies that malevolent or unauthorized action, constituting a security threat, as being reasonably foreseeable, then a security threats analysis should be carried out."

**Moreover, section 7.5.2.2 from IEC 61508 also states:**

"If security threats have been identified, then a vulnerability analysis should be undertaken in order to specify security requirements."

IEC 61508  
FUNCTIONAL SAFETY

2021/\* /EC  
EUROPEAN MACHINERY DIRECTIVE

IEC 62443  
SECURITY FOR INDUSTRY

#ONLYSAFEIFSECURE

safety requirements  
spawn from security  
research

## TERADYNE-DERIVED COLLABORATIVE ROBOTS

claimed designed to augment human capabilities by closely (physically) cooperating without causing any harm. Past research however hints that the lack of security measures in these robots leads to safety hazards



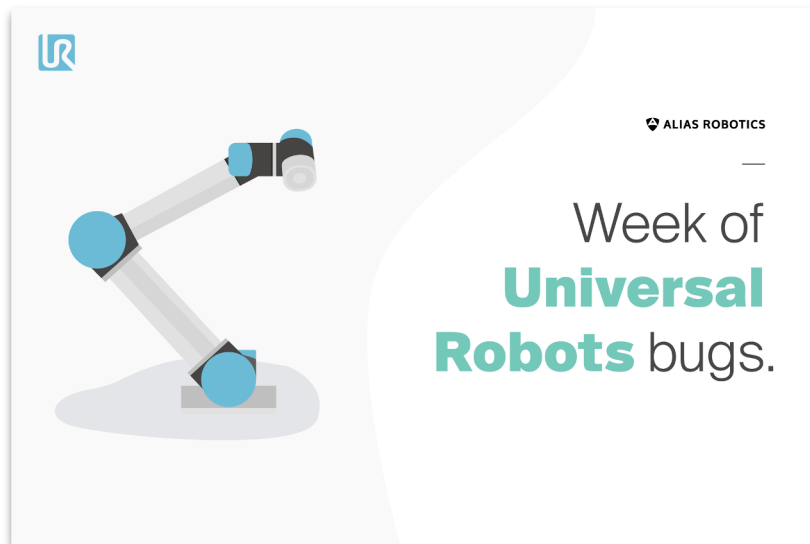
## MATERIAL OBSOLESCENCE COMMON PRACTICES<sup>[2]</sup>

1. **Making items difficult to repair** (by raising the cost of repair, requiring special tools, private networks, etc.)
2. **Failing to provide information** (for instance, manuals are not provided)
3. **Systematic obsolescence** (making parts among models incompatible or making it impossible to fix newer models with parts from the older models)
4. **Numbering** (frequently changing the model numbers to make it psychologically less attractive to use old models)
5. **Legal approaches** (prohibiting access and modification to the internal structure of products by means of copyrights and patents)

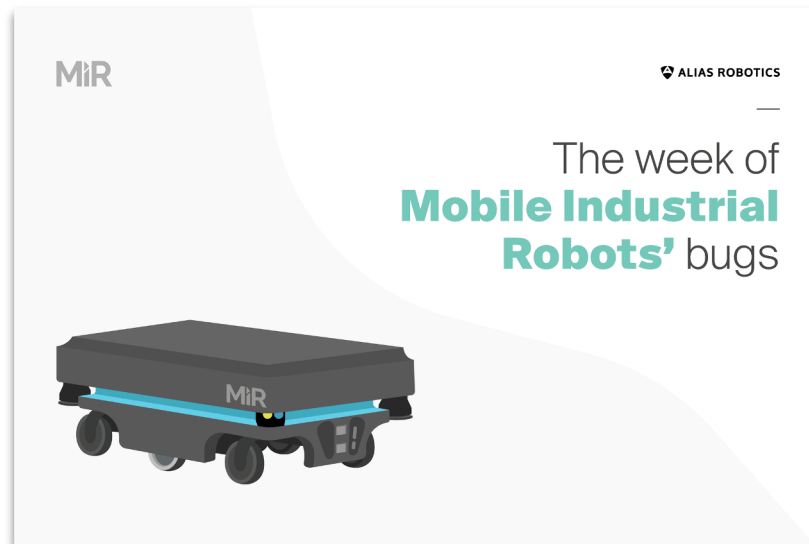
[2] Hatta, M. (2020). The right to repair, the right to tinker, and the right to innovate. *Annals of Business Administrative Science*, 0200604a.



# OPPOSING MANUFACTURERS THAT ENDANGER END-USERS

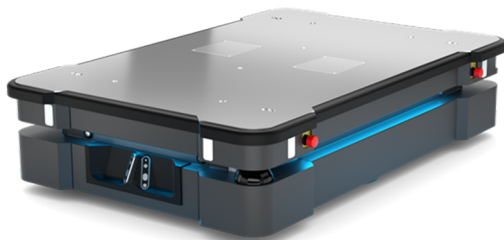


<https://news.aliasrobotics.com/week-of-universal-robots-bugs-exposing-insecurity/>



<https://news.aliasrobotics.com/the-week-of-mobile-industrial-robots-bugs/>

**65K USD**



“MiR’s business model is based on MiR selling its robots through a distributor network, and the distributors or integrators are fully responsible for the distribution/commissioning of MiR products in collaboration with the end user”.

**Ole Storm,**  
Mobile Industrial Robots R&D Manager (May 2020)

- “- The customers are not entitled to any upgrade unless the product requires it, to solve a specific issue.
- The software upgrades are provided by your distributor.
- We do not provide access to the release note of the software to end user”

**Fernando Fandiño Oliver,**  
Mobile Industrial Robots Sales Director,  
Southern Europe & MEA (May 2020)



**30K USD**

**70K USD**



“... it is my understanding that a device must be connected in some form to the internet, via Wifi or mobile data to be at risk from a cyber attack. As our robot operates completely independently from the internet, I don't see how it can be externally hacked.”

**Simon Ellison,**  
Vice President Sales & Marketing at UVD Robots  
(May 11 2020)

“We are aware about the potential challenges of using the products on a network with access to the internet or on insecure local networks.”

**Lars-Peter Ellekilde,**  
Founder and CEO at Enabled Robotics (Apr 27 2020)

**? USD (~ 50K)**



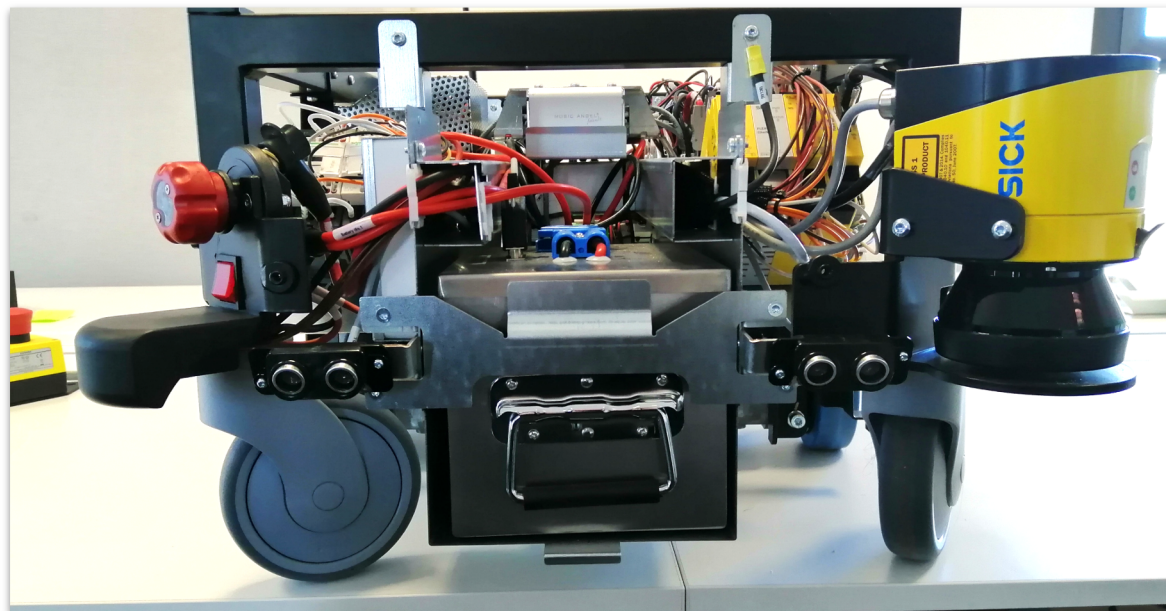


## ROBOT TEARDOWN

A teardown in robotics is the process of taking apart a robot to understand how it is made and works.

More formally, it is the approach to modeling the functional behavior and physical components of a robot.

*All of the work was performed by researchers and provided to the public free of charge as a public service and not for any competitive purposes.*



1- Scope

2- Tooling

3- Supply chain

4- Dissassembly

5- Info. gathering

# Robot Teardown

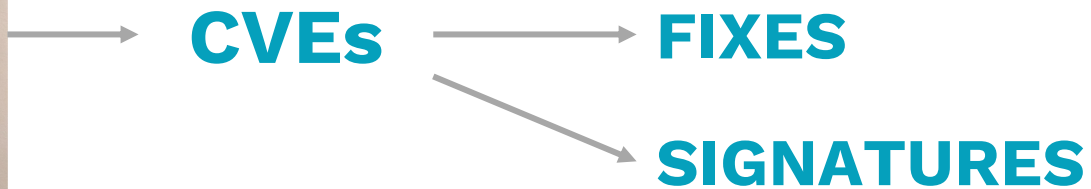
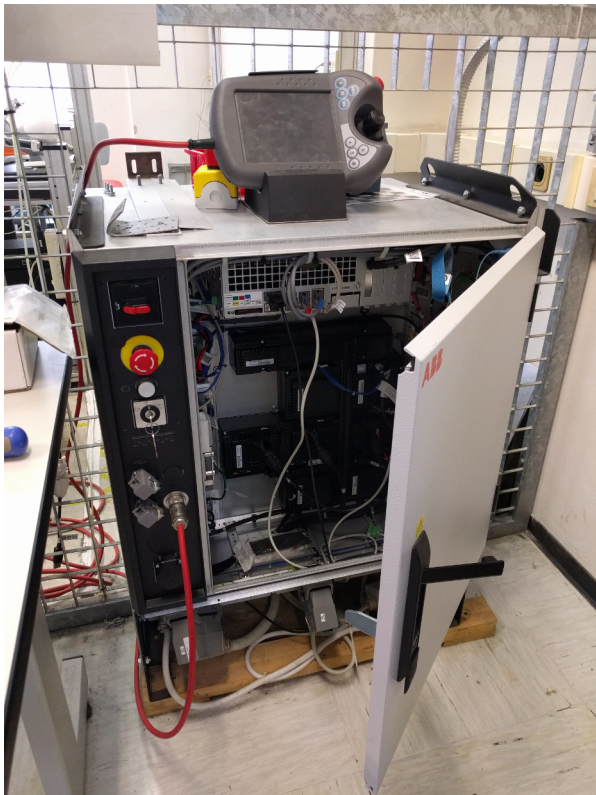
## Why and how



**Federico Maggi**  
Trend Micro Research









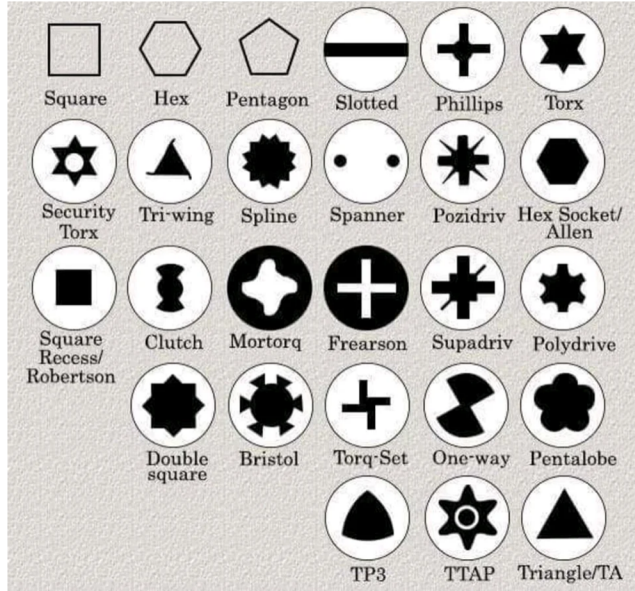
1- Scope

2- Tooling

3- Supply chain

4- Dissassembly

5- Info. gathering



1- Scope

2- Tooling

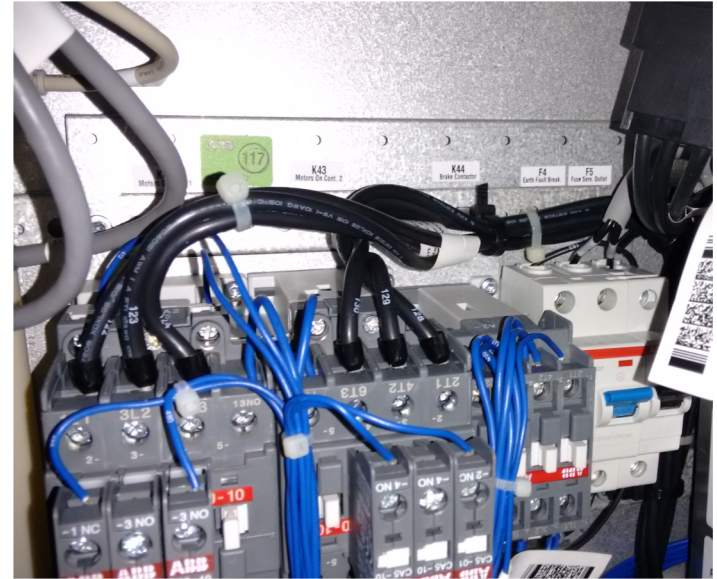
3- Supply chain

4- Dissassembly

5- Info. gathering

T-shirt design from <https://www.etsy.com/listing/1012449494/i-void-warranties-men-t-shirt-husband>





1- Scope

2- Tooling

3- Supply chain

4- Dissassembly

5- Info. gathering



1- Scope

2- Tooling

3- Supply chain

4- Dissassembly

5- Info. gathering



# MANUALS

1- Scope

2- Tooling

3- Supply chain

4- Dissassembly

5- Info. gathering



abb programming manual ext:pdf site:edu

All Images Videos News Shopping

About 28,700 results (0.61 seconds)

<http://pergatory.mit.edu> > ABB\_Robotics > general ▾ PDF Block  
**Product On-line Manual IRB 6400R**

Manual, or contact your nearest **ABB** Flexible Automation Centre involves choosing **Instructions** and arguments from lists of.  
481 pages

<http://futurecnc.code.arc.cmu.edu> > 2011/12 > RA... ▾ PDF Block  
**RAPID Reference Manual - Future CNC**

**ABB** assumes no responsibility for any errors that may appear in  
RAPID reference part 1, **Instructions A-Z. Program** execution.  
464 pages

[forum.adamcommunity.com](http://forum.adamcommunity.com)

[dof.robotiq.com](http://dof.robotiq.com)

[automationforum.in](http://automationforum.in)

[robot-forum.com/robotforum](http://robot-forum.com/robotforum)

[control.com](http://control.com)

[solisplc.com/forum](http://solisplc.com/forum)

[forums.mrplc.com](http://forums.mrplc.com)

[reddit.com/r/robotics](http://reddit.com/r/robotics)

[plc.myforum.ro](http://plc.myforum.ro)

[forum.universal-robots.com](http://forum.universal-robots.com)

[forums.robotstudio.com](http://forums.robotstudio.com)

1- Scope

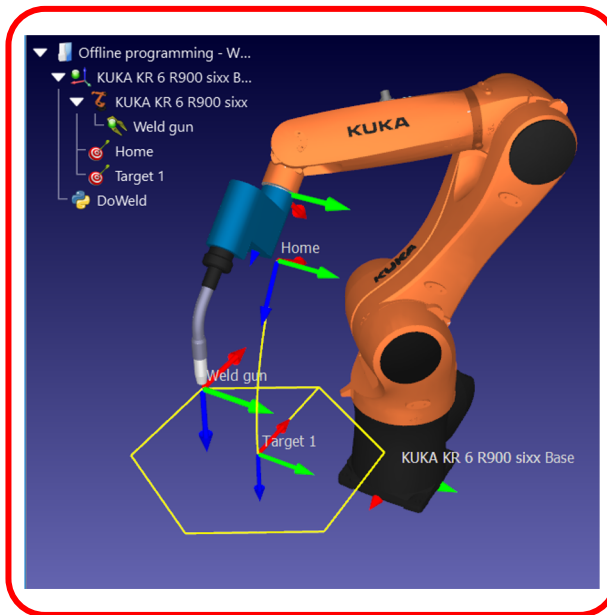
2- Tooling

3- Supply chain

4- Dissassembly

5- Info. gathering





# SIMULATION SOFTWARE (CTRL-Z)

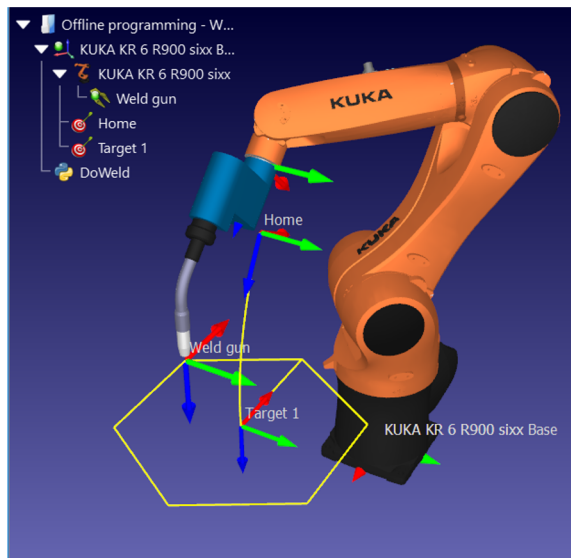
1- Scope

2- Tooling

3- Supply chain

4- Dissassembly

5- Info. gathering



```

axc
axc.bat
axc.cmd
axc.idb
axc.sym
dsp.out
mc_extctrl_2010-12-21
mc_extctrl_2011_03_11
mc_extctrl_2011_03_11.idb
mc_ORIGINAL
mc_ORIGINAL.idb
mc.bat
mc.cfg
mc.sym_extc...2010-12-21
mc.sym_extc...2011_03_11
mc.sym_ORIGINAL
servo
    
```

OS

1- Scope

2- Tooling

3- Supply chain

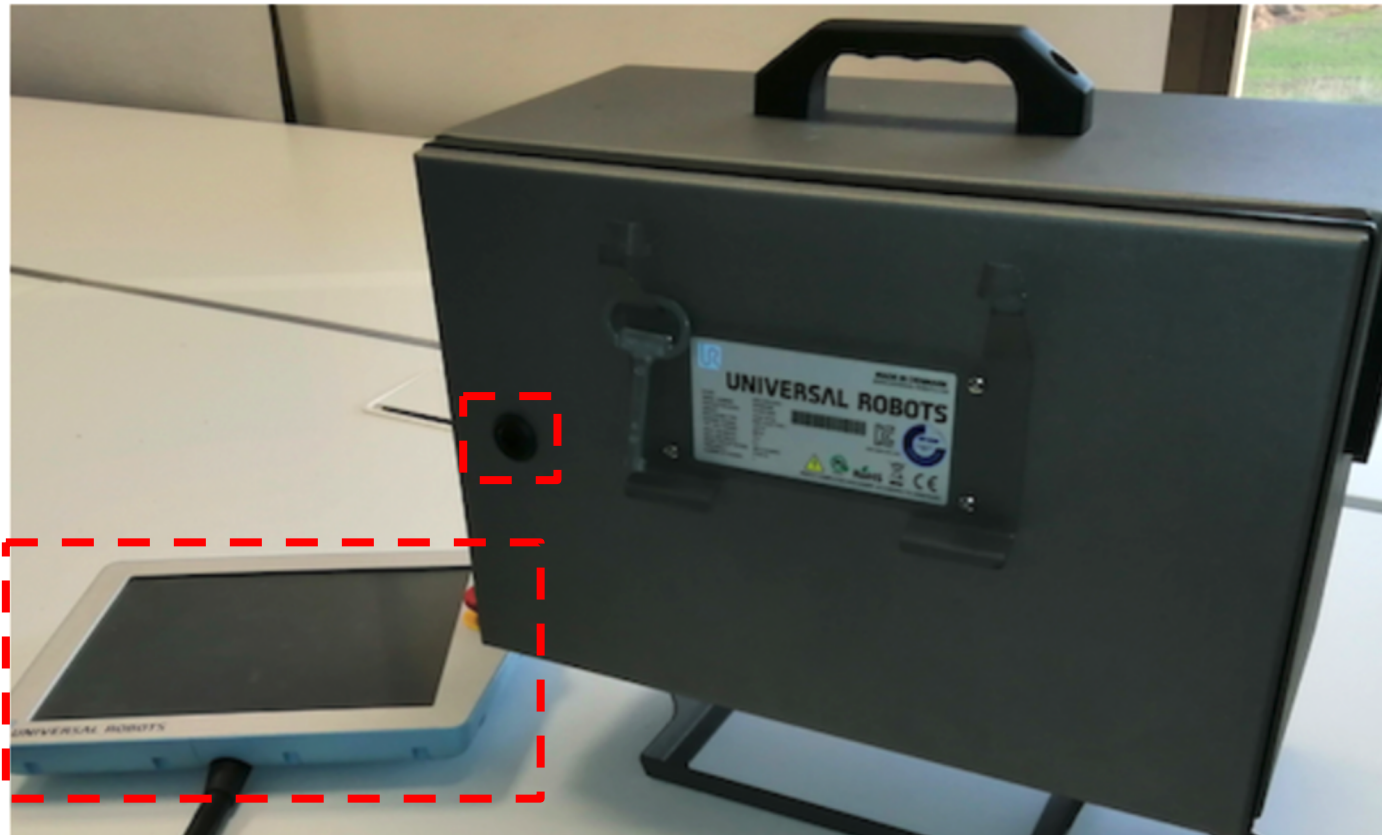
4- Dissassembly

5- Info. gathering

# **CASE STUDY 1**

## **TEARDOWN OF AN INDUSTRIAL COLLABORATIVE ROBOT**





UR3 CB3.1









## LPC435x/3x/2x/1x

32-bit ARM Cortex-M4/M0 MCU; up to 1 MB flash and 130 KB SRAM; Ethernet, two High-speed USB, LCD, EMC

Rev. 5.4 — 10 January 2020

Product data sheet



### 3. Applications

- Motor control
- Power management
- White goods
- RFID readers
- Embedded audio applications
- Industrial automation
- e-metering



I/O (SPI, I2C) interface, and multiple digital and analog peripherals. The



**Suitability for use** — NXP Semiconductors products are **not designed, authorized or warranted to be suitable for use in life support, life-critical or safety-critical systems or equipment, nor in applications where failure or malfunction of an NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage.** NXP Semiconductors and its suppliers accept no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.



# **CASE STUDY 2**

## **TEARDOWN OF A NEXT-GEN INDUSTRIAL COLLABORATIVE ROBOT**







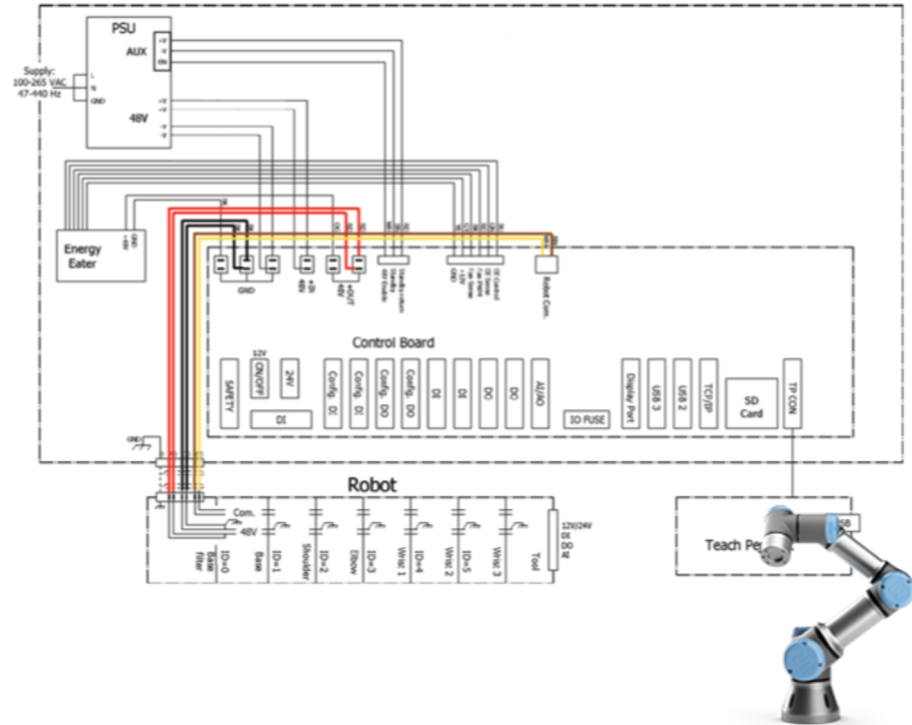
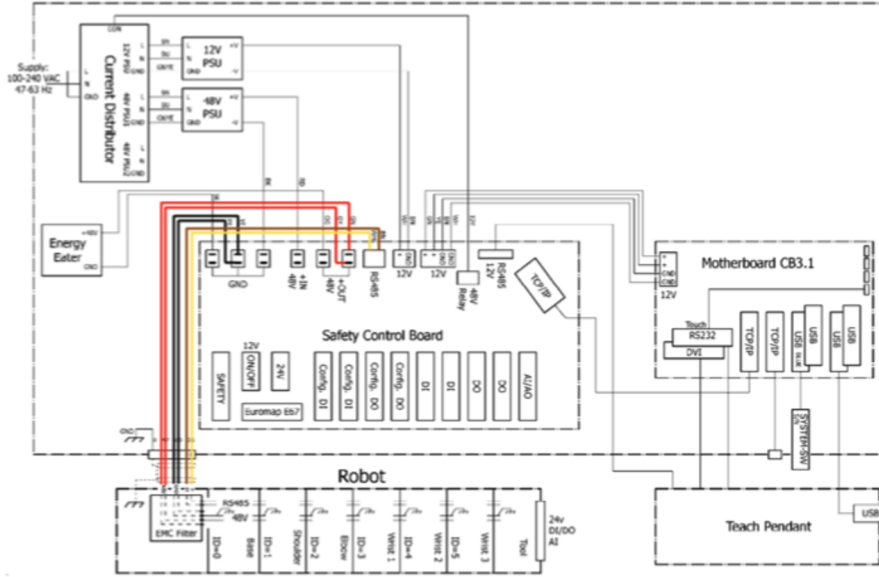
DS181 (v1.26) March 23, 2021

Product Specification

## Introduction

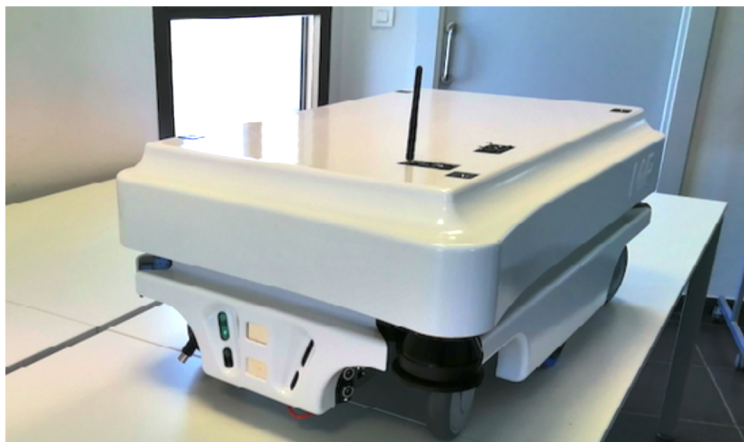
Artix®-7 FPGAs are available in -3, -2, -1, -1LI, and -2L speed grades, with -3 having the highest performance. The Artix-7 FPGAs predominantly operate at a 1.0V core voltage. The -1LI and -2L devices are screened for lower maximum static power and can operate at lower core voltages for lower dynamic power than the -1 and -2 devices,

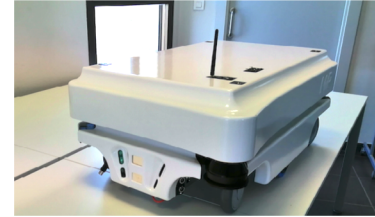
speed grade military device are the same as for a -1C speed grade commercial device). However, only selected speed grades and/or devices are available in each temperature range. For example, -1M is only available in the defense-grade Artix-7Q family and -1Q is only available in XA Artix-7 FPGAs.



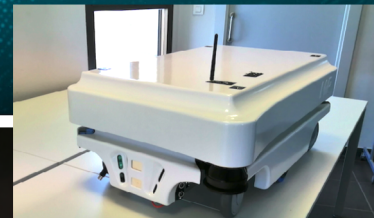
## **CASE STUDY 3**

# **TEARDOWN OF A MOBILE INDUSTRIAL ROBOT**









## Power Wires Identifications and Connection

### Important Safety Disclaimer

Dangerous uncontrolled motor runaway conditions can occur for a number of reasons, including, but not limited to: command or feedback wiring failure, configuration error, **faulty firmware**, errors in user script or user program, or controller hardware failure.

The user must assume that such failures can occur and must make their system safe in all conditions. Roboteq will not be liable in case of damage or injury as a result of product misuse or failure.



# Teardown-enabled Security Research



**Víctor Mayoral-Vilches**  
Alias Robotics

# TEARDOWN-ENABLED SECURITY RESEARCH

CVE ID	RVD ID	DESCRIPTION	REPORT
CVE-2019-19626	RVD#1408	Bash scripts (magic UR files) get launched automatically with root privileges and without validation or sanitizing	<a href="https://github.com/aliasrobotics/RVD/issues/1408">https://github.com/aliasrobotics/RVD/issues/1408</a>
CVE-2020-10280	RVD#1495	Universal Robots URCaps execute with unbounded privileges	<a href="https://github.com/aliasrobotics/RVD/issues/1495">https://github.com/aliasrobotics/RVD/issues/1495</a>
CVE-2020-10267	RVD#1489	Unprotected intellectual property in Universal Robots controller OS 3.1 across firmware versions	<a href="https://github.com/aliasrobotics/RVD/issues/1489">https://github.com/aliasrobotics/RVD/issues/1489</a>
CVE-2020-10266	RVD#1487	No integrity checks on UR* platform artifacts when installed in the robot	<a href="https://github.com/aliasrobotics/RVD/issues/1487">https://github.com/aliasrobotics/RVD/issues/1487</a>
CVE-2020-10265	RVD#1443	UR dashboard server enables unauthenticated remote control of core robot functions	<a href="https://github.com/aliasrobotics/RVD/issues/1443">https://github.com/aliasrobotics/RVD/issues/1443</a>
CVE-2020-10264	RVD#1444	RTDE Interface allows unauthenticated reading of robot data and unauthenticated writing of registers and outputs	<a href="https://github.com/aliasrobotics/RVD/issues/1444">https://github.com/aliasrobotics/RVD/issues/1444</a>
CVE-2020-10278	RVD#2561	Unprotected BIOS allows user to boot from live OS image	<a href="https://github.com/aliasrobotics/RVD/issues/2561">https://github.com/aliasrobotics/RVD/issues/2561</a>
CVE-2020-10270	RVD#2557	Hardcoded Credentials on MIRX00 Control Dashboard	<a href="https://github.com/aliasrobotics/RVD/issues/2557">https://github.com/aliasrobotics/RVD/issues/2557</a>
CVE-2020-10279	RVD#2569	Insecure operating system defaults in MIR robots	<a href="https://github.com/aliasrobotics/RVD/issues/2569">https://github.com/aliasrobotics/RVD/issues/2569</a>
CVE-2020-10276	RVD#2558	Default credentials on SICK PLC allows disabling safety features	<a href="https://github.com/aliasrobotics/RVD/issues/2558">https://github.com/aliasrobotics/RVD/issues/2558</a>
CVE-2020-10273	RVD#2560	Unprotected intellectual property in Mobile Industrial Robots (MIR) controllers	<a href="https://github.com/aliasrobotics/RVD/issues/2560">https://github.com/aliasrobotics/RVD/issues/2560</a>
CVE-2020-10277	RVD#2562	Booting from a live image leads to exfiltration of sensible information and privilege escalation	<a href="https://github.com/aliasrobotics/RVD/issues/2566">https://github.com/aliasrobotics/RVD/issues/2566</a>
CVE-2020-10269	RVD#2566	Hardcoded Credentials on MIRX00 Wireless Access Point	<a href="https://github.com/aliasrobotics/RVD/issues/2566">https://github.com/aliasrobotics/RVD/issues/2566</a>
CVE-2020-10275	RVD#2565	Weak token generation for the REST API	<a href="https://github.com/aliasrobotics/RVD/issues/2565">https://github.com/aliasrobotics/RVD/issues/2565</a>
CVE-2020-10274	RVD#2556	MIR REST API allows for data exfiltration by unauthorized attackers (e.g. indoor maps)	<a href="https://github.com/aliasrobotics/RVD/issues/2555">https://github.com/aliasrobotics/RVD/issues/2555</a>
CVE-2020-10271	RVD#2555	MIR ROS computational graph is exposed to all network interfaces, including poorly secured wireless networks and open wired ones	<a href="https://github.com/aliasrobotics/RVD/issues/2555">https://github.com/aliasrobotics/RVD/issues/2555</a>
CVE-2020-10272	RVD#2554	MIR ROS computational graph presents no authentication mechanisms	<a href="https://github.com/aliasrobotics/RVD/issues/2554">https://github.com/aliasrobotics/RVD/issues/2554</a>

+100 security  
flaws detected

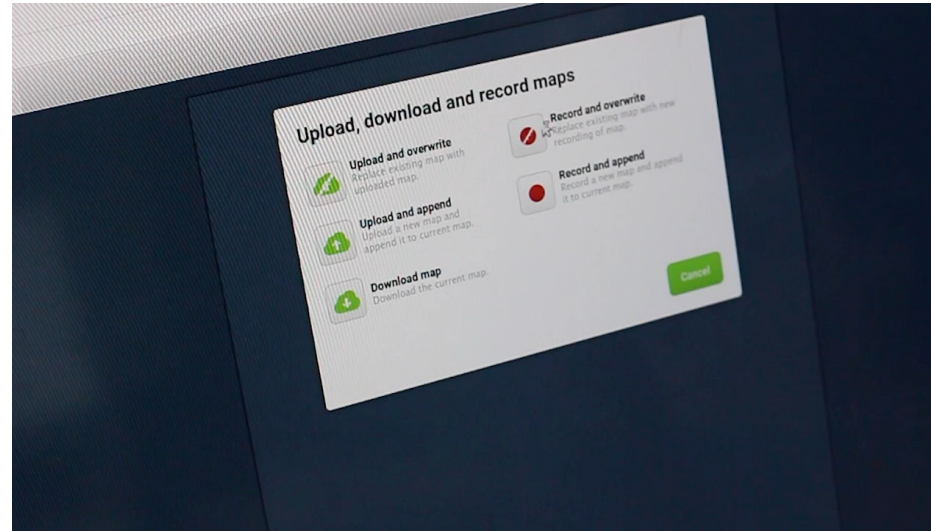
17 new CVE IDs,  
still zero days today

ROBOT VULNERABILITY DATABASE (RVD)

All disclosed and  
catalogued in the open

<https://github.com/aliasrobotics/RVD>



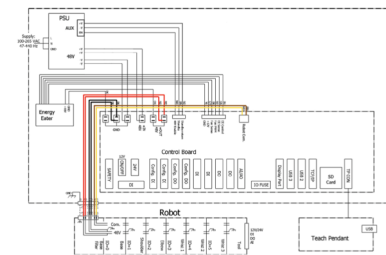




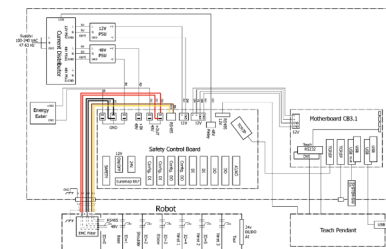


**Don't trust**  
(vulnerable) robots

# FINDING PLANNED OBSOLESCENCE INDICATORS



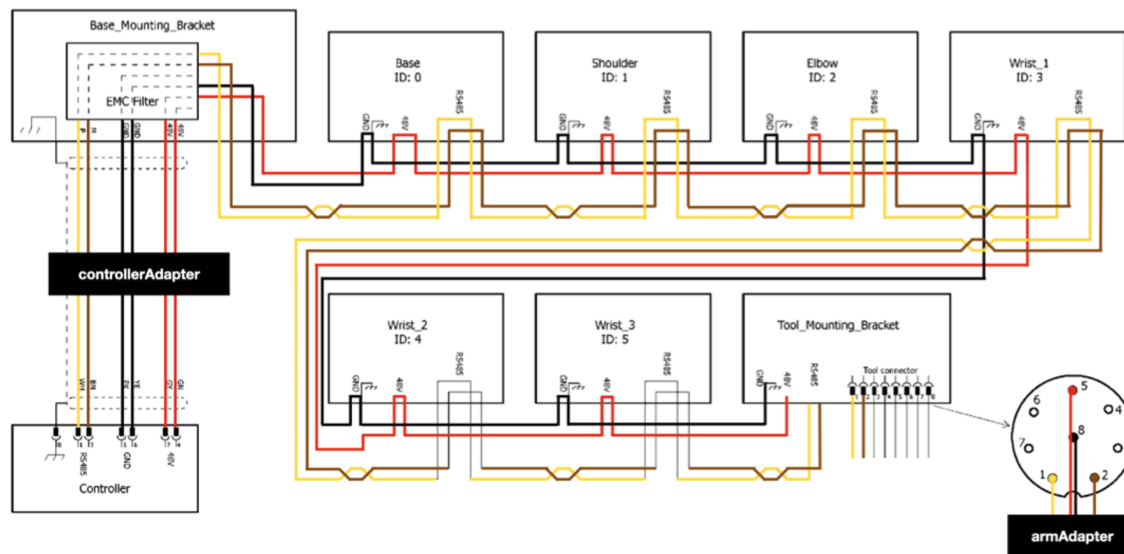
B) Simplified electrical diagram of Universal Robots UR3 CB-Series collaborative robot.



A) Simplified electrical diagram of Universal Robots UR3 CB-Series collaborative robot.

*All of the work was performed by researchers and provided to the public free of charge as a public service and not for any competitive purposes.*

# BYPASSING PLANNED OBSOLESCENCE



*All of the work was performed by researchers and provided to the public free of charge as a public service and not for any competitive purposes.*

**Figure 5:**

Simplified electrical diagram of the robotic arms from Universal Robots including our two hardware contributions: a) the **controllerAdapter**, which helps connecting the robotic arm to either the CB-series or the e-Series and b) the **armAdapter**, which allows to control the arm without the controller.

## **(DISTINGUISHED) ROBOT MANUFACTURER QUOTES**

“Security... yes. We have PL-D level.”

Leading manufacturer of industrial robot manipulators

“We make open systems. The security flaws indicated greatly facilitate system integration.”

Leading collaborative robots manufacturer

“We know our robots have a set of reported vulnerabilities but our end-users don’t care.”

Leading automation manufacturer and system integrator.

“We leave solving those (security flaws) to the end user.”

Leading manufacturer of industrial robot manipulators.

“Everything will be fixed in the next release” ... (3 months later) ... “It can’t be fixed”.

Leading manufacturer of industrial robot manipulators.

~~“(Robot) cybersecurity is up to the robot user”~~

Leading manufacturer of collaborative robots.

**(Robot) cybersecurity is up to the robot hacker.**



## SOUND BYTES

1. Security in robots is nothing new but the **consequences of insecurity are critical**. Flaws (including security ones) in robots lead to **safety hazards**, and can kill.  
**#onlysafeifsecure**
2. Robot **teardowns are needed for security research**, for quality assurance of hardware and for putting **pressure on manufacturers** to ensure security (and thereby human safety) first in their designs.
3. We need a **“Right for Repair” in robotics**. Robot waste is of no concern to manufacturers, who **employ planned obsolescence practices avoiding repairs**. The US (and not China) leading the way in bad practices.



# QUESTIONS?

## Small Wonder:

Uncovering Planned Obsolescence Practices in Robotics and What This Means for Cybersecurity



**Víctor Mayoral-Vilches**  
Alias Robotics



**Federico Maggi**  
Trend Micro  
Research

Thanks also to University of Klagenfurt and our co-authors:  
Unai Ayucar-Carbajo, Alfonso Glera-Picón,  
Stefan Rass, Martin Pinzger and Endika Gil-Uriarte.

#BHUSA @BlackHatEvents

