Extended abstract: Robot teardown, stripping industrial robots for good

***Abstract*—Similar to Ford in the 1920s with cars, most robot manufacturers nowadays employ planned obsolescence practices and organize dealers and system integrators into "private networks", providing repair parts only to "certified" companies to difficult repairs and evade competition. We introduce robot teardown as an approach to improve robot hardware, research its security and pressure manufacturers to act ethically and invest in security. We show how by applying common reverse engineering principles, we're able to discover security vulnerabilities and fight systematic obsolescence repurposing an older controller with newer robots, saving tenths of thousands of dollars.**

***Index Terms*—teardown, robotics, security, repair, safety**

Robotics is the art of system integration [1]. Building a robot requires one to carefully select components that exchange information across networks while meeting timing deadlines. In a way, a robot is a network of networks. One that comprises sensors to perceive the world, actuators to produce a physical change and dedicated compute resources to process it all and respond coherently, in time, and according to its application. Roboticists often conceive the robot not as one of its parts, but as the complete system including all its components, whether they're assembled under the same structure or physically distributed. In the case of a robot manipulator, these robots are often presented physically distributed and include the robot arm mechanics (which generally include actuators and sensors), the HMI or teach pendant, the controller (the main compute substrate for reasoning) and any additional safety mechanism related to the robot operation. The robotic system is thereby the composition of all these sub-systems and networks.

Under such system integration complexity, it isn't uncommon for one of the robot sub-components to fail over time, often leading to the complete system malfunction. Given the expensive prices of robots, it's only reasonable to consider the need for repairing these machines, often replacing individual faulty components for continued operation, or simply for re-purposing them. The European Commision (EC) showed early interest on this topic by producing in 2019 a report evaluating different scoring systems for repairing and upgrading different consumer-oriented products [2], including robots. More recently and as part of the Circular Economy Action Plan [3], EC has shown commitment towards establishing a new '*Right to Repair*' in the context of reviewing directive 2019/771. Hatta [4] summarizes major events in the U.S. with regard the *Right to Repair* and highlight that it wasn't until 2012 that the Automotive *Right to Repair* passed in Massachussets, empowering customers with tools to fight planned obsolescence. Hatta summarizes how material obsolescence works:

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

Similar to Ford in the 1920s, most robot manufacturers follow several of these practices nowadays and organize dealers (often called distributors) or approved system integrators into private networks, providing repair parts only to *certified* companies in an attempt to difficult repairs and evade competition. Amongst the most recent examples we observe an interesting development from Teradyne where two of its owned robotics companies (Universal Robots and Mobile Industrial Robots), follow this practice. The case of Teradyne is of special interest because its robots are advertised as collaborative, that is: 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 [5]–[7].

Cybersecurity in robotics is still on its early stages [8]–[11] and as in many other fields, remains addressed mostly in disconnected silos. With most efforts concentrated in IT, hardware security has received very limited attention. Building secure robots however demands consideration throughout domains (hardware, firmware, OS, application, network, cloud, etc.) [12] and across the robot lifecycle [13].

The present article introduces robot teardown as an approach to improve robot hardware and research its security. We advocate against the business priorities set in industry to avoid repairs and planned obsolescence. Instead, we advocate for a *Right to Repair* in robotics as a means to reduce robot e-waste and recycle components both across robots and throghout use-cases. Ultimately, we argue that robot teardowns will heavily impact the quality assurance of hardware in robotics, putting pressure on manufacturers and helping produce robots with better hardware security measures, thereby safer. Our contributions are three-fold: first, we show the empirical results of various robot teardowns performed on popular industrial collaborative robots and uncover various security flaws, some of which can be exploited externally (see Figure 1 for some preliminary illustration of our empirical work). Second, we demonstrate how as a result of the teardown and by applying minor fixes, we are able to repurpose a controller with a newer (unsupported) version of the same brand's manipulator mechanics (the robot arm), saving thousands of dollars in costs. Third, we demonstrate how through teardown and hardware security research, we are able to detect security threats early and mitigate them by simply extending the robotic system with off-the-shelf additional hardware elements that increase the overall cybersecurity posture with a minimal cost impact.

REFERENCES

[1] V. Mayoral-Vilches, A. Hernández, R. Kojcev, I. Muguruza, I. Zamalloa, A. Bilbao, and L. Usategi, "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*. IEEE, 2017, pp. 229–236.

[2] M. Cordella, F. Alfieri, and J. Sanfelix, "Analysis and development of a scoring system for repair and upgrade of products-final report," 2019.

[3] D.-G. for Communication (European Commission), "Circular economy action plan, for a cleaner and more competitive europe," 2020.

[4] M. Hatta, "The right to repair, the right to tinker, and the right to innovate," *Annals of Business Administrative Science*, p. 0200604a, 2020.

[5] L. Alzola Kirschgens, I. Zamalloa Ugarte, E. Gil Uriarte, A. Muñiz Rosas, and V. Mayoral-Vilches, "Robot hazards: from safety to security," *ArXiv e-prints*, Jun. 2018.

[6] V. Mayoral-Vilches, L. U. S. Juan, U. A. Carbajo, R. Campo, X. S. de Cámara, O. Urzelai, N. García, and E. Gil-Uriarte, "Industrial robot ransomware: Akerbeltz," *arXiv preprint arXiv:1912.07714*, 2019.

[7] S. Taurer, B. Breiling, S. Svrta, and B. Dieber, "Case study: remote attack to disable mir100 safety."

[8] F. Maggi, D. Quarta, M. Pogliani, M. Polino, A. M. Zanchettin, S. Zanero, and P. Di Milano, "Rogue Robots: Testing the Limits of an Industrial Robot's Security," Tech. Rep.

[9] F. Maggi and M. Pogliani, "Rogue automation: Vulnerabile and malicious code in industrial programming," *Trend Micro, Politecnico di Milano, Tech. Rep*, 2020.

[10] V. Mayoral-Vilches, L. U. S. Juan, B. Dieber, U. A. Carbajo, and E. Gil-Uriarte, "Introducing the robot vulnerability database (rvd)," *arXiv preprint arXiv:1912.11299*, 2019.

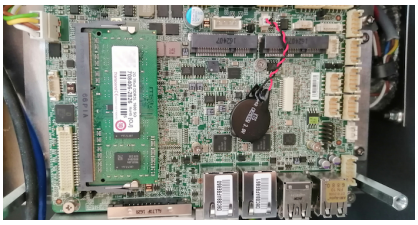
[11] V. Mayoral-Vilches, M. Pinzger, S. Rass, B. Dieber, and E. Gil-Uriarte, "Can ros be used securely in industry? red teaming ros-industrial," *arXiv preprint arXiv:2009.08211*, 2020.

[12] V. Mayoral-Vilches, L. Alzola Kirschgens, A. Bilbao Calvo, A. Hernández Cordero, R. Izquierdo Pisón, D. Mayoral Vilches, A. Muñiz Rosas, G. Olalde Mendia, L. Usategi San Juan, I. Zamalloa Ugarte, E. Gil-Uriarte, E. Tews, and A. Peter, "Introducing the robot security framework (rsf), a standardized methodology to perform security assessments in robotics," *ArXiv e-prints*, Jun. 2018.

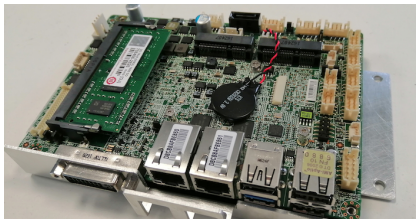
[13] V. Mayoral-Vilches, N. García-Maestro, M. Towers, and E. Gil-Uriarte, "Devsecops in robotics," *arXiv preprint arXiv:2003.10402*, 2020.

(a) Universal Robots UR3 robot CB3.1 controller and associated teach pendant (HMI). The controller has a generic mechanical lock aimed to secure physically access.

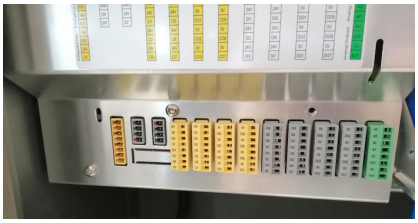
(b) Inside the controller we can see various connectors and cables exposed. The left side includes I/O and safety, whereas the right one leads to the main computer.



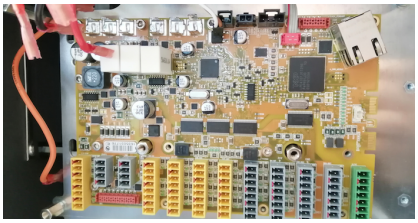
(c) The main computer of the controller with a 2G DDR3L RAM module from Transcend. Ethernet PHYs are connected to automotive-grade controllers from Intel.



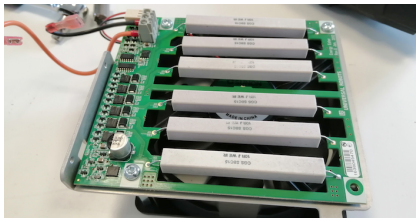
(d) Besides the USB stick found connected outside, and beyond minor non-volatile memories, no additional secondary memory is located in the PCB.



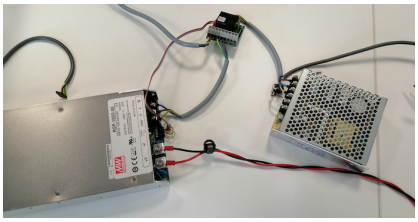
(e) The safety side of the controller (documented in the user manuals) includes quick connectors which can be removed by carefully wiggling them out.



(f) After removing the metal shields, the safety board electronics are fully displayed. The main logic is driving by an NXP LPC4437JET256 microcontroller.



(g) The energy-eater board. This component tends to head a fair bit and should generally be checked in case of failure for signs of degradation.



(h) A safety relay and two Power Supply Units (PSUs) identified, one for the compute logic (12 V) and another one to power the actuators (48 V).

(i) Final figure depicting all the components contained inside of the Universal Robots UR3 CB3.1 controller, leaving aside the teach pendant.

Fig. 1: UR3 collaborative robot from the danish Universal Robots (owned by the US Teradyne).